Osterman Research

SOLUTION ANALYSIS

Solution Analysis by Osterman Research
Published **September 2019**

Office 365 Advisory Report, Q3/2019

OFFICE 365 ADVISORY REPORT

Welcome to the **Osterman Research Office 365 Advisory Report**:

- Osterman Research maintains a continually updated knowledge base on Office 365 designed for vendors and corporate decision makers who need to understand the intricacies of the platform and how it's changing over time. Our goal in producing this report is to help decision makers understand more than just the "check boxes" of Office 365's many capabilities, and to get into the details of how these work and the implications they will have on the existing processes, workflows and other platforms in use within their organizations.

- The information in this report is based on published and non-NDA material available from Microsoft and a variety of other sources.

- This report provides information on Office 365 in the areas of:

    - Archiving
    - Authentication
    - Data Loss Protection
    - eDiscovery
    - Encryption
    - File Sharing
    - Security

AN IMPORTANT CAVEAT

This report discusses what we consider to be some limitations within the Office 365 platform, and how third-party solutions might be better suited for use in many situations. However, please note:

- We consider Office 365 to be a robust and capable platform that should be considered for use by virtually any organization. We think it's a good platform and we recommend its use.

- That said, every platform has certain limitations and/or things it doesn't do quite as well as various alternatives. We think that these alternatives should be considered in light of specific corporate requirements. Moreover, what may be a "limitation" for one organization may not necessarily be a limitation for another, and so the information presented in this report should be considered in that light.

CONTACT AND ENQUIRIES

If you have any questions on this report, please contact Michael Osterman at +1 206 683 5683 or michael@ostermanresearch.com.

Table of Contents

Office 365 Analysis Service

Welcome to the **Osterman Research Office 365 Analysis Service**:

- This service provides a continually updated knowledge base on Office 365 for vendors and IT departments.
- It is based on published and non-NDA material available from Microsoft and other sources.
- Access is by subscription - for the complete service, or just a subset of content.

The complete service provides an ongoing and detailed analysis of Office 365 in the areas of:

- Archiving
- Authentication
- Data Loss Protection
- eDiscovery
- Encryption
- File Sharing
- Security

Date last updated - 2019-09-10 at 10:19:35 NZST

Contact and Enquiries

- To increase your subscription level, please contact Michael Osterman.
- To send content to be analyzed for inclusion in the service, please send links to articles, blog posts and other sources to office365@oranalysisservice.com.

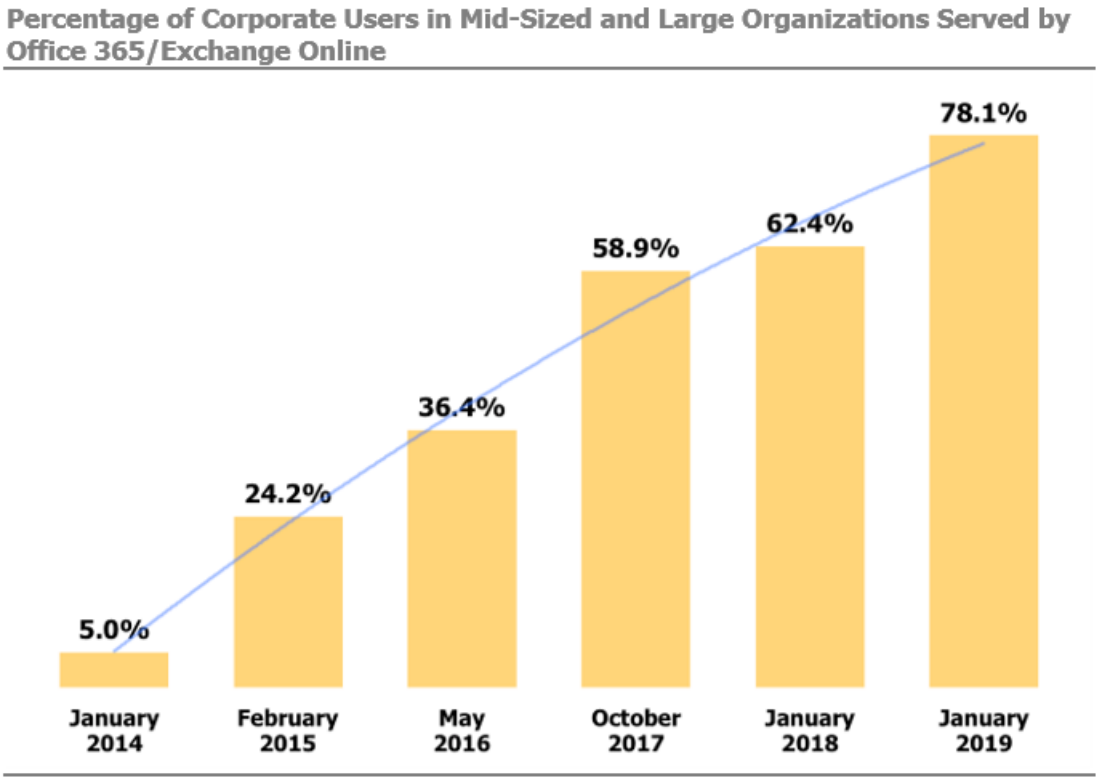
Office 365 - Overview

Microsoft Office 365 has taken the world by storm, including the corporate and enterprise sectors that were expected to reject cloud services only half a decade ago.

Microsoft has posted strong year-on-year growth in subscriber numbers for Office 365 in commercial organizations, such as:

- November 2015 - **60 million** active users
- March 2016 - **70 million** active users
- September 2016 - **85 million** active users
- March 2017 - **100 million** active users
- October 2017 - **120 million** active users
- March 2018 - **135 million** active users
- September 2018 - **155 million** active users. See Office 365 Market Snapshot - Microsoft's 1Q2019.
- January 2019 - (estimated) **162 million** active users. See Office 365 Market Snapshot - Microsoft's 2Q2019.
- March 2019 - **180 million** active users. See Office 365 Market Snapshot - Microsoft's Q3 2019.

By early 2019, Microsoft expects 70 percent of its customers to be using Exchange Online in Office 365, rather than Exchange on-premises. Osterman Research's surveys clearly demonstrate the validity of Microsoft's claims for the growth in Office 365 and Exchange Online:



Source: Osterman Research, Inc.
Note: Yellow bars are actual survey results; blue line is a trend line

However, despite high usage numbers for Exchange Online and Microsoft's traditional Office productivity suite licensed and delivered as a cloud service (Office ProPlus), customers embracing Office 365 must make some important decisions about many of its features and functions compared to those offered by third parties. That's not to say that organizations should not consider and deploy Office 365 (we believe that in most cases they should). But decision makers must be fully aware of the limitations inherent in the native capabilities offered with Office 365 and how third-party solutions can often better satisfy their requirements.

In this knowledge base, we evaluate what's available in Office 365 in 2018 in the areas of security, archiving, compliance, encryption, backup/recovery and eDiscovery, highlighting areas of concern for customers adopting Exchange Online, SharePoint Online, OneDrive for Business, Skype for Business and Azure Activity Directory.

Key Takeaways

- Office 365 is not a single offering from Microsoft. Instead, it's a starting point for licensing a range of higher-priced and additional services from Microsoft's cloud portfolio, such as Azure Information Protection, Azure Active Directory, and higher priced plans that offer more advanced capabilities (such as the improved capabilities in Enterprise E5 compared to the much more commonly deployed Enterprise E3). In reality, organizations may better satisfy their needs by using a less expensive Office 365 plan and supplementing its capabilities with best-in-class, third-party offerings instead.
- Microsoft is rapidly evolving the capabilities of Office 365, and it is challenging to know when Office 365 – and the wider complementary portfolio of Microsoft cloud services – are adequate to satisfy a particular set of requirements. Microsoft produces useful capabilities, but they are often replaced in short order. Corporate decision makers face the challenge of understanding which Office 365 capabilities are still current, which have been improved, which will be deprecated, and how third party solutions can better satisfy their needs.
- The ground has shifted – collaboration and next-generation productivity tools are now widely available, offering modern tools and approaches for business challenges. But the new challenge is keeping employees from falling for increasingly advanced social engineering scams and malicious attacks, while ensuring data protection for personal and corporate data. Office 365 is a broad-based service that offers collaboration and productivity; are its security capabilities good enough to offer the protection that is necessary? And will "good enough" today be good enough tomorrow?
- Cybersecurity is among the top priorities for organizations in the current environment, and yet cybersecurity talent is hard to find, and so there is a significant skills gap worldwide. As a result, organizations are increasingly reliant on their cybersecurity vendors and partners.
- While Office 365 is a robust service offering – particularly the basic Exchange Online and Office ProPlus offerings – like all cloud services it is not perfect, as evidenced by Microsoft's own breakneck pace of upgrading the service. Highlighting current issues of concern assists organizations in making effective plans with clear insight about the best path forward for Office 365.
- The high number of active users for Office 365 - 155 million at September 2018 - does not mean equal usage and adoption across the workloads in Office 365. Exchange Online and SharePoint Online are highly utilized workloads; others are much smaller. See Office 365 Numbers by Workload.
- Office 365 is designed at scale for a set of general use cases, and Microsoft's design parameters for Office 365 may not align with the needs of a particular organization. As with any cloud service, the profile of a particular customer may differ from what is offered by Microsoft. Therefore, the role of this knowledge base is to explore what does and doesn't work, highlighting potential red flags for an organization's deployment.

Archiving - Overview

Few organizations are all-in on Office 365 to the exclusion of everything else. The vast majority have many other content repositories, on-premises data stores, and other Microsoft and non-Microsoft cloud services. The addition of Office 365 to an organization's information management architecture means the addition of new content sources and content types that need to be secured, controlled, and governed. While potentially unlimited storage is available in Office 365, keeping all data and content in perpetuity is a bad approach from business, legal, and information management perspectives.

Free data storage doesn't negate the other expenses of information, including:

- **Confusion caused by out-of-date information**. The wrong information in the hands of the right people will spread misinformation and lead to decision-making on out-of-date, irrelevant and poor intelligence.
- **Time wasted wading through wrong information**. Information and knowledge workers already spend too much time searching for the right information; keeping unnecessary content around longer than necessary only gets in the way and slows the ability to find, retrieve, and make use of the right information.
- **Legal exposure and risk**. When information that is responsive or potentially responsive to a legal case has been retained beyond what was necessary, risk increases. Having too much information available increases the legal and discovery costs for searching, identifying, culling, reviewing, and producing responsive content.
- **Supervision**. The ability to supervise content is also an issue for highly regulated sectors, such as financial services. Office 365 tools will not adequately address this requirement in many cases.

[**March 2018**] Respondents to an Osterman Research survey on the importance of content management capabilities provided the following ratings:

Importance of Various Content Management Capabilities
Percentage Responding "Important" or "Extremely Important"

Capability	%
The ability to have in-place search and review eDiscovery capabilities within the Office 365 stack	66%
The ability to have in-place eDiscovery capabilities within the Office 365 stack	63%
The ability to have in-place search and review eDiscovery capabilities across multiple vendors' solutions	53%
The ability to have in-place eDiscovery capabilities across multiple vendors' solutions	48%

Source: Osterman Research, Inc.

Audit Logs - Office 365

About

- **Unified Audit Logging**. Office 365 offers a unified audit logging service across key workloads, and is accessed through the Security & Compliance Center. Auditing for most workloads is turned off by default (and thus must be turned on to start the process of collecting audit entries); one prominent exception is audit logging of administrator actions in Exchange Online which is turned on by default. Audit entries in the Security & Compliance Center are retained for 90 days (or one year for Office 365 E5 and Microsoft 365 users), after which they are purged. A recent change to audit logging of Exchange items means that an administrator can set a higher (or lower) default period.
    - [**July 2018**] Audit reports for user actions within Exchange mailboxes will be enabled by default; previously an Exchange administrator had to turn this on for each mailbox after it was provisioned. This will be enabled via a tenant-wide setting. An organization can opt-out entirely (no mailbox auditing) or opt-out for specific mailboxes only. Setting either requires the use of PowerShell.
    - [**March 2019**] Microsoft announced that the work to enable Exchange Mailbox Auditing in Exchange Online by default has been completed. However, the roll-out of default logging to the Unified Audit Log is still in progress. Pushing audit entries to the Unified Audit Log still requires the use of manual settings.
- **Default Audited Events**. From July 2018, the default list of events that are captured for auditing were expanded:
    - New audit events are added automatically to the default configuration.
    - However, Exchange admins can create custom configurations which will be unaffected by the default configuration.
- **90 Days or One Year**. Microsoft offers two retention durations for audit log entries: 90 days and one year. Which duration applies depends on the Office 365 plan the organisation has: those with Office 365 E5 or a Microsoft 365 plan get the longer timeframe. Organisations with lesser plans get the shorter duration. See Audit Log Retention Increased to One Year - for Some Users (October 2018).
- **Office 365 Cloud App Security**. Office 365 Cloud App Security – an integrated component of the Enterprise E5 license and an optional add-on for other plans – captures audit log data from Office 365 and moves it to Azure, but even then, such audit log entries are stored only for 180 days. Organizations that need long-term access to audit report items – such as seven years' worth of data under some compliance regulations – should be aware of the limitations of the Office 365 Audit Log service. See Office 365 Cloud App Security.
- **Parallel Moves with Azure AD Activity Logs**. [July 2018] Microsoft released into public preview the ability to route Azure AD Activity Log entries (audit logs and sign-in logs) to an Azure storage account, Event Hub, or other SIEM or custom solution. Microsoft acknowledged that customers have been asking for longer-term storage options for Azure AD Activity Logs. When routing to a storage account or Event Hub, retention can be set from 1-180 days, or if the value is left at 0, indefinitely (something like 2 billion days).
    - Microsoft says that an organization with 1000 users will pay less than US$2 per year for the Azure storage account for holding all associated records.
    - While this does not apply to Office 365 Audit Logs, Microsoft's moves with Azure AD Activity Logs may foreshadow new options for Office 365 Audit Logs in the near future.

Issues for Customers to Consider

- Mail flow events in Exchange Online do not create audit log entries. That is, when a mail flow rule triggers against an email message, no record of this triggering is logged.
- Many of the settings require the use of PowerShell. There is no UI-equivalent.
- The Office 365 Audit Log only retains audit events for 90 days - for Office 365 subscribers with Enterprise E3 or below. There is no way to increase this time frame. This means the Audit Log can do nothing for an organization trying to track down an issue or problem that occurred outside of the last three months.
    - **Exception** - Exchange Online, where an administrator can change the default from 90 days for Exchange audit log entries only.
    - **Office 365 E5 and Microsoft 365** - offer a maximum of one year of data retention for audit logs, a change that was introduced to public preview in October 2018. But it only applies to audit log records generated after the longer duration comes into effect.

- Entries in the Audit Log cannot be put on a legal or litigation hold, in order to show specific actions taken by users over time that are subject to a discovery request or part of early case assessment.
- While Microsoft has taken steps to integrate the presentation of audit logs across Office 365 in the Security & Compliance Center, important administration tasks are still centered in the Exchange Admin Center. This nuance causes confusion for admin users. For example:
    - Gaining the right to search the Office 365 Audit Log in the Security & Compliance Center requires setting role permissions in the Exchange Admin Center, e.g., having the View-Only Audit Logs or Audit Logs role in the Exchange Admin Center. Setting these in the Security & Compliance Center has no effect.
    - Capturing of audit logs across Office 365 can be turned on or off completely in the Exchange Admin Center.
- Exporting audit log items from Office 365 is limited to 5,000 entries unless all results are exported, for which the limit is 50,000 items. An organization with auditing turned on will generate at least 10-20 audit items per individual per day for a light user, and potentially a couple of hundred items per day for an active information worker. Some medium-sized organizations, let alone their larger counterparts, will hit the 50,000 item limit every day. In such a scenario, an administrator will need to specify and generate at least one export every day, and hope that the time delay in capturing audit report entries doesn't mean that items that should be collected are missed from the report.
    - **Note** - Microsoft has increased the display of entries from 1,000 to 5,000 over the past two years.
- The limit of 50,000 items per export can obfuscate what is really happening. For example, if a user's account is brute force attacked, only a few of these login failures may show in a search. But if you search specifically for the user's account, you may find many thousands of additional login failures. However, the lack of signals in the first would blind you to the need to do the second.
- Exports are delivered as CSV files to be saved locally (outside of Office 365), the collection of which must be managed. Paradoxically, as an exported file of audit items, there is nothing to prevent an errant administrator from removing evidence of his or her own wrongdoing; the exported file does not guarantee authenticity of the historical information contained inside.
- Searches in the Audit Log are not logged. This makes it impossible to know who has been searching for what information.
- The Audit Log captures many types of events, but it does not cover all events. For example:
    - Whether messages were encrypted or not is not logged.
    - **Exchange Online** - Soft deletion of a Folder in a mailbox is not logged (unlike soft delete of a message).
    - **SharePoint Online** - Sending a secure sharing link to multiple external people only captures the name of the first external user, not all of them.
    - **SharePoint Online** - Additions, changes and deletions within the Term Store are not logged.
    - **Microsoft Teams** - Messages in personal chats are not logged, and neither are messages posted by guest users.
- Logging in the Admin Center is insufficient. For example:
    - **Skype for Business Admin Center** - Audit logging is not supported. There is no audit logging of changes.
    - **Office 365 Admin Center** - Many of the changes made by admins in the Admin Center are not logged. e.g., changes to Office 365 licensing and subscriptions are not logged. This lack of auditing makes it impossible to see who made a specific change.
- Events are not logged in real-time nor available for real-time analysis. Microsoft says it can take from 30 minutes to 24 hours depending on the specific event that is being logged; customers have noted that it can take even longer and that audit events may never appear at all.
- The Office 365 Audit Log service does not capture events from on-premises Microsoft servers for organizations with a hybrid setup, such as Exchange Server and SharePoint Server in addition to Office 365. It cannot, therefore, provide a consolidated view of auditable activities for organizations with hybrid infrastructure
- It is not possible to scope access to only specific workloads the Office 365 Audit Log, such as only to audit log events from Exchange Online, or only Power BI, or only Microsoft Teams. Access to the Audit Log is all or nothing.
- **Truncated Records**. Some Audit Log entries were truncated of essential information starting in June or July 2018. Specifically, operations related to group membership, as initially recorded in the Azure AD Activity Logs, were stripped from the log entry when copied across to the Office 365 Audit Log. See Audit Log Truncates Azure AD Records (September 2018).
    - [**May 2019**] Microsoft fixed the record truncation problem in early May 2019, eight months after being alerted to the problem. For compliance related records, this is unacceptable. See Weekly News Drop (May 17).
- The Audit Log suffers from WYQIWYD - or what you query isn't what you download. The downloaded data does not reliably match the data returned from a search query.
- The reason for specific actions taken by an admin user on an Office 365 service is not captured and displayed in the Audit Log.

It is impossible to piece together the reasoning behind a change based on the general information presented in the Audit Log.

Lack of Archiving for Some Content Types

About

- Archiving – moving business data out of one business system into a separate, secured location for optimized storage, immutability, and better data governance – is not offered for some important content types in Office 365. These include SharePoint, Skype for Business, additional message types, and third-party content.

Issues for Customers to Consider

- SharePoint content, such as documents and list items, can be retained in place through retention policies, or moved to another location in SharePoint when it has expired or become irrelevant. These retention or move actions can be triggered based on specific date-based and event triggers only, and for organizations staying within their assigned storage limits for SharePoint, SharePoint's In-Place Records Management in SharePoint may be sufficient. What is not possible, however, is to archive SharePoint content that is no longer current to alternative and cheaper storage systems. Although it is possible to purchase unlimited SharePoint storage capacity, it attracts premium pricing. Organizations with large quantities of SharePoint data are not well served if they want to keep their SharePoint content trimmed and current without incurring additional long-term SharePoint storage fees, or that want to archive content away from SharePoint Online based on event triggers beyond date-based metadata. Moreover, SharePoint is not write once, read many (WORM) compliant; a serious issue for organizations in regulated industries.
- Skype for Business Online relies on Exchange Online for archiving if specific conditions are met. No native archiving service for Skype for Business Online is available. By default, Skype instant messaging transcripts are retained in the Conversation History folder in each user's Exchange Online mailbox, but unless the mailbox is on legal or litigation hold, a user can delete their instant messaging transcripts at will, which doesn't provide an immutable or reliable archive of past messages. The need for legal hold to force the retention of Skype messages means that all Exchange Online mailboxes must be on hold at all times for this to work, which we consider to be an odd design. If a mailbox is on hold, peer-to-peer and multiparty instant messages are retained, as well as content upload activities during meetings. Other actions within Skype for Business are not retained, such as peer-to-peer file transfers, audio/video for peer-to-peer instant messages and conferences, application sharing, and conferencing annotations.
- Text messages on BlackBerry devices will be archived into Office 365 if a third-party agreement is in place to capture these messages. Text messages on other devices, including iOS and Android, are not captured. With BlackBerry now having a low and dwindling market share in comparison to iOS and Android, capturing only BlackBerry messages is not as useful as it might otherwise be.
- Content from specific third-party messaging, collaboration, social media and other content sources can be archived into Exchange Online in Office 365 as converted email messages if agreements are in place with a third-party data partner. Messages are stored in the Exchange Online mailbox belonging to the specific user, and for content that cannot be tracked to a named individual, a catch-all mailbox is used. Most of the context of content from Twitter, Facebook, Yahoo! Messenger, DropBox and Salesforce Chatter is lost when these rich media sources are converted to email messages, making it difficult to re-create a historically valid chain of events.
    - [**April 2019**] Microsoft announced that it is adding native connectors for third-party data by the end of Q3 2019. These native connectors will be built into the Microsoft 365 Compliance Center, and will negate the need for working with a third-party to capture and archive such data. No mention was made about moving away from storing all items as email messages, however. See Archiving with Native Connectors.
    - [**May 2019**] Microsoft released native third-party data ingestion to general availability. Ingested data is still being converted to email messages and stored in an Exchange Online mailbox. See Records Management.

Practical Storage Limitations in SharePoint Online

About

- SharePoint lists and libraries can hold up to 30 million items

Issues for Customers to Consider

- There is a limit of 5,000 list items or documents that can be displayed in any one view. This was enforced in SharePoint Online to ensure that all tenants get good performance on SharePoint queries, but it has the practical implication of forcing unnatural content segregation design decisions by SharePoint developers within organizations to try to get around the 5,000-item threshold. It frequently means that end users are stopped from doing their work because the 5,000-item limit has been reached, or a lookup against a list with more than 5,000 list items has failed. This is a long-term issue for customers, and while Microsoft has been working recently to address this issue, it has suffered several false starts. Some customers are so frustrated by the 5,000-item list threshold that they are considering moving away from SharePoint Online entirely.

Activity Logs - Azure AD

About

- [July 2018] Microsoft released into public preview the ability to route Activity Log entries (audit logs and sign-in logs) to an Azure storage account, Event Hub, or other SIEM or custom solution. Microsoft acknowledged that customers have been asking for longer-term storage options for Azure AD Activity Logs. When routing to a storage account or Event Hub, retention can be set from 1-180 days, or if the value is left at 0, indefinitely (something like 2 billion days).
    - Splunk is currently the only SIEM tool that supports Azure AD Activity Log entries.
    - Microsoft says that an organization with 1000 users will pay less than US$2 per year for the Azure storage account for holding all associated records.

Issues for Customers to Consider

- The free and basic editions of Azure AD will only retain activity and security audit items for a maximum of 7 days. With a subscription to Azure AD Premium P2, this can be increased to a maximum of 30 days for activity items and 90 days for security items.

Update Log - Archiving

June 2019

June 25 - Preservation Hold Library Update - in SharePoint Online

May 2019

May 23 - Records Management

May 13 - Audit Log Truncation Resolved

April 2019

April 23 - Archiving with Native Connectors

January 2019

January 29 - Records Management Updates

September 2018

September 25 - Audit Log Retention Increased to One Year - for Some Users. Only applies to Office 365 E5 and Microsoft 365 plans.

September 12 - Audit logs in Office 365 are truncating some of the data copied across from the Azure AD Activity Logs. See Audit Log Truncating Azure AD Records.

August 2018

August 2 **-** New Guided Workflow for Deleting Microsoft 365 Users

July 2018

July 26 - Public preview - Activity logs from Azure AD can be routed to an Azure storage account or Event Hub for long term storage. Has implications for Activity Logs - Azure AD and potential implications for Audit Logs - Office 365. Announced via Enterprise Mobility + Security Blog.

July 12 - Mailbox auditing on Exchange mailboxes will be enabled by default, and the default audit configuration will change to include more audit events. Announced on July 12, for progressive roll-out by end calendar year 2018. Has implications for Audit Logs - Office 365. Announced via Security, Privacy & Compliance Blog.

Authentication - Overview

About

- Microsoft offers several approaches for authenticating users against Office 365:
  - Cloud-only identities created, stored and managed in Azure Active Directory. If organizations also have on-premises infrastructure and identity services (such as Active Directory in Windows Server), users must either use two identities (one for on-premises and one for Office 365) or identities must be linked somehow.
  - On-premises identities in Windows Server Active Directory are extended for use in Office 365 as well. This means the core identity is managed on-premises in Active Directory, but is able to be used for authenticating against Office 365 too. There are several options for federating with Azure AD. Another option is to synchronize password hashes from Windows Server AD to Azure AD.
- The Microsoft Authenticator app for Windows Phone, Apple iPhone, and Android devices enables the use of two-factor authentication through a trusted app, as an alternative to using a code sent by text message.
  - For Apple iPhone users, Microsoft released a companion app for the Apple Watch in August 2018, with general availability scheduled for September 2018. This allows an Apple Watch user to set up their Watch for approving push notifications that require a PIN or biometric signal as the second factor. See Apple Watch App for Microsoft Authenticator.
- Microsoft is committed to eliminating vulnerabilities in its identity systems, including vulnerabilities in standards-based identity capabilities it embraces.
  - [July 2018] Microsoft added two new bounty types and increased the bounty value on vulnerabilities in its identity systems.
- The user provisioning service in Azure AD can be used to automatically provision and deprovision access to third-party cloud apps.
  - [August 2018] Eight new cloud apps were added to the list that can be automatically provisioned and deprovisioned, including Asana, BlueJeans, and Zendesk.
  - Microsoft says Azure AD manages over 30 million user identities in other cloud apps, and that in the 12 months to August 2018, the number of Azure AD tenants using user provisioning for at least one cloud app has doubled.
- Multi-factor authentication is available for Office 365 users. This is powered through Azure Active Directory. See Multi-Factor Authentication.
- Disabling basic authentication in Exchange Online reduces account compromise rates by 67%. See Weekly News Drop - March 22, 2019.
- [**April 2019**] Password Protection in Azure AD allows an organization to define a custom list of banned words which cannot be used as passwords; these are evaluated when a user changes or resets their password. The custom list is banned in addition to several other lists and methods built globally into the Azure AD service. Using the custom list requires Azure AD P1 or P2 licensing, although the functionality is exposed and usable without such licensing in place. See Azure AD Password Protection Released to GA.

Issues for Customers to Consider

- **Cascading Disruptions**. As a non-regional service, disruptions in one region to Azure AD can have flow-on or cascading effects to other data centers and regions. While the intent is that Azure AD is globally resilient, Microsoft's architecture for Azure has not yet delivered a fail safe cloud-based authentication service.
  - [**Example**] A lightning strike in Texas on September 4, 2018 disrupted the cooling systems at the US South Central data center in San Antonio. This had a major impact on both Office 365 and Azure services, with customers outside of the US South Central region experiencing Azure AD authentication problems. See Data Center Outage in US South Central.
  - [**May 2019**] At Build 2019, Microsoft announced several investment areas to improve the durability of Azure. Whether these investments will prevent a repeat of recent service disruptions remains to be seen. See Azure Durability.
- **Azure AD Security Groups and Office 365 Groups**. Authentication is handled by Azure AD, but access permissions to resources are increasingly managed by Office 365 Groups. Without using PowerShell, it is not possible to synchronize the members of an Azure AD Security Group with an Office 365 Group.
- **Managing Guest Access**. Office 365 is increasingly supporting access from guest users - those outside a given tenant - but offers no tools for managing the lifecycle of guest accounts once created. A guest can remove their own account from a tenant, but if they don't do this, the account stays in place until an administrator disables it. This results in a proliferation of outdated

guest accounts. See Lifecycle Management of Guest Accounts in Office 365.

- [**May 2019**] Microsoft announced Azure AD Entitlement Management, which enables policy-based provisioning and deprovisioning of access to resources, for both internal users and guest accounts. If a guest is given access to resources through Entitlement Management, when all current entitlements expire, the guest account will be disabled and then deleted 30 days later. These capabilities require Azure AD Premium P2 licensing. See Azure AD Entitlement Management.

- **B2B Collaboration Policy**. An administrator can use the Azure AD B2B Collaboration policy to block guest user access to Office 365 Groups (via the External Collaboration Settings option in Azure AD). This can hold either a blacklist (deny) or whitelist (allow), but not both at the same time. However, if a guest user from a newly blocked domain already exists in Azure AD before a block policy is put in place, that guest user account will continue to function, and will continue to be available for addition to other Office 365 Groups. Setting a new block (deny) policy does not apply retrospectively, and no warning is given that current guest user accounts from the blocked domain already exist in Azure AD.
- **Support for Passphrases**. Office 365 does not support the use of passphrases, which are generally longer phrases containing multiple natural language words that are easier to remember than a password with a difficult pattern. For example, a passphrase could be "I am Clarke Kent and I am Superman." This is a 34-character "password" that is simultaneously easy-to-remember for the end user but, due to its length, harder for an attacker to guess or crack. Office 365 does not support passphrases because Azure AD accounts do not support the use of spaces, and are limited to a maximum of 16 characters.
  - [**May 2019**] Microsoft introduced support for passwords with 256-characters, including spaces, which means that passphrases and much longer passwords are now supported by Office 365. See Support for Longer Passwords.

Federation with Azure AD

About

- Organizations with Microsoft Active Directory on-premises can federate with the cloud-based Azure Active Directory. This enables users to gain single sign-on to Office 365 (and if configured, other cloud applications as well) using their on-premises identity.
- Federation requires additional server infrastructure on-premises for publishing identities to Azure AD, and any outages of this on-premises infrastructure compromises the ability for users to log into Office 365, unless Password Hash Synchronization is also used in parallel.
- The ability to use Azure AD Connect is included in the edition of Azure AD used with Office 365, although each user can only use single sign-on for gaining access to a total of 10 cloud apps, with Office 365 counting as one of these.
- Microsoft offers the Active Directory Federation Services (ADFS) capability for enabling a federated integration between Windows Server AD on-premises and Azure AD in the cloud.
- Microsoft also supports federation using third-party identity services for customers that do not want to use ADFS, including:
    - **PingFederate**. The ability to automatically create the integration details required for using PingFederate to federate Active Directory with Azure AD was released to General Availability (August 2018).

Issues for Customers to Consider

- If users require access to more than 10 cloud applications using single sign-on, one of the higher priced Azure AD plans - Premium P1 or Premium P2 - will be required per user. The right to access a greater number is also included in the Enterprise Mobility + Security plans, or a Microsoft 365 plan.

Multi-Factor Authentication (MFA)

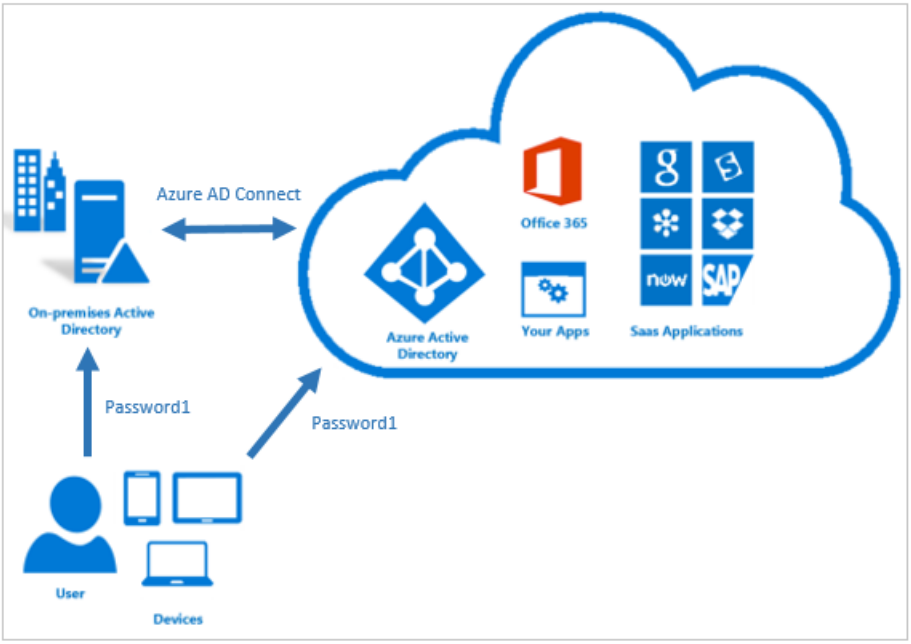
About

- Commonly abbreviated as MFA. Can also be called 2FA (two-factor authentication).
- Microsoft offers MFA via the Azure Active Directory MFA service, commonly called Azure MFA. There are three editions of Azure MFA:
  - An edition that comes with an Office 365 license, for users and administrators. This is a bundled service, not an additional cost one.
  - A free edition for any user with the Azure AD Global Administrator role in Azure AD tenants.
  - The full edition that requires an Azure AD Premium P1 or P2 license. Supports MFA for cloud-based and on-premises applications.
- Microsoft recommends that MFA is required for everyone with an administrative, privileged, or high impact user account.
  - Example - Office 365 administrators
  - Example - Chief Financial Officer
- MFA is widely recommended for privileged accounts (e.g., administrator accounts)
  - [June 2018] Microsoft previewed a new security setting, whereby MFA is enabled by default for privileged accounts.
  - During preview, the default is off, so organizations can choose to opt-in
  - After general availability, the default will be on, so organizations can opt-out to disable.
- [July 2018] Microsoft previewed a combined way in which the phone number entered for MFA can also be used for self-service password reset.
- The second factor can be supplied through one of several ways:
  - Microsoft Authenticator app
  - Phone call
  - SMS text message
  - App passwords for applications that do not support MFA
  - Hardware OATH token - introduced to public preview in October 2018, for users with the full Azure MFA. Not available for the Office 365-only edition of Azure MFA. See Support for Hardware OATH Tokens in Azure MFA (October 2018).
- Each user can have up to five MFA devices registered at once. See Support for Multiple MFA Devices Per User (October 2018).
- Microsoft added support for biometric sign-in to a Microsoft account without requiring a password on Windows 10 1809 and Microsoft Edge in November 2018. It will extend this capability to Azure AD accounts in early 2019. See Password-Less Sign-On Coming for Azure AD (November 2018).
- Using MFA has been shown to reduce the likelihood of account compromise or credential breach by 99.9%.

Issues for Customers to Consider

- It is early days for baseline protection in Azure AD. For example, the first baseline policy was only released in preview in June 2018.
- Microsoft's introduction of new capabilities for MFA often breaks current authentication rights, such as preventing affected users from using various Office 365 services. Customers find this annoying and disruptive.
- Microsoft's implementation of MFA in Azure and Office 365 delivers a single point of failure. If MFA is down, affected users can't log in. This happened several times during September and November 2018:
  - September 4, 2018 - Data Center Outage in US South Central
  - November 19, 2018 - Global MFA Outage (14 hours)
  - November 27, 2018 - Multi-Hour MFA Outage in the United States (at least 3 hours)

Password Hash Synchronization



About

- Password Hash Synchronization is one of the methods offered by Microsoft to share identities between Windows Server Active Directory and Azure AD. Using password hash synchronization enables a user to sign into Azure AD (and Office 365 by implication) using the same user name and password used to sign into on-premises applications through Windows Server AD.
- Password hashes are synchronized to Azure AD using AD Connect.
- The user's password in Windows Server AD is stored as an MD4 hash of the password. Before being sent to Azure AD, the MD4 hash is further processed in AD Connect through multiple steps to create an SHA256 password hash. In essence, this is a much more secure hash of the MD4 hash.
    - Microsoft says that all passwords undergo a per-user salt and 1,000 iterations of the SHA256 key hashing algorithm. The per-user salt creates a different hash even if the same password is used by more than one person.
- Active Directory Federation Services can be configured to also support password hash synchronization, which has the benefit of still enabling access to Azure AD / Office 365 by users if the on-premises identity services are not available due to an outage or other problem.
- If Azure AD is compromised and the SHA256 hash obtained by an attacker, this hash cannot be used for authenticating against Windows Server AD in a pass-the-hash attack.
- The AD Connect process synchronizes between Windows Server AD and Azure AD every two minutes. After a new MD4 hash has been further processed, any new SHA256 password hashes are sent to Azure AD.
- If a user is subject to password hash synchronization, their Azure AD account password is set to Never Expire.
- Password Hash Sync works in combination with Azure AD Smart Lockout, IP Lockout, and the leaked credentials service in Azure AD Risk Events.

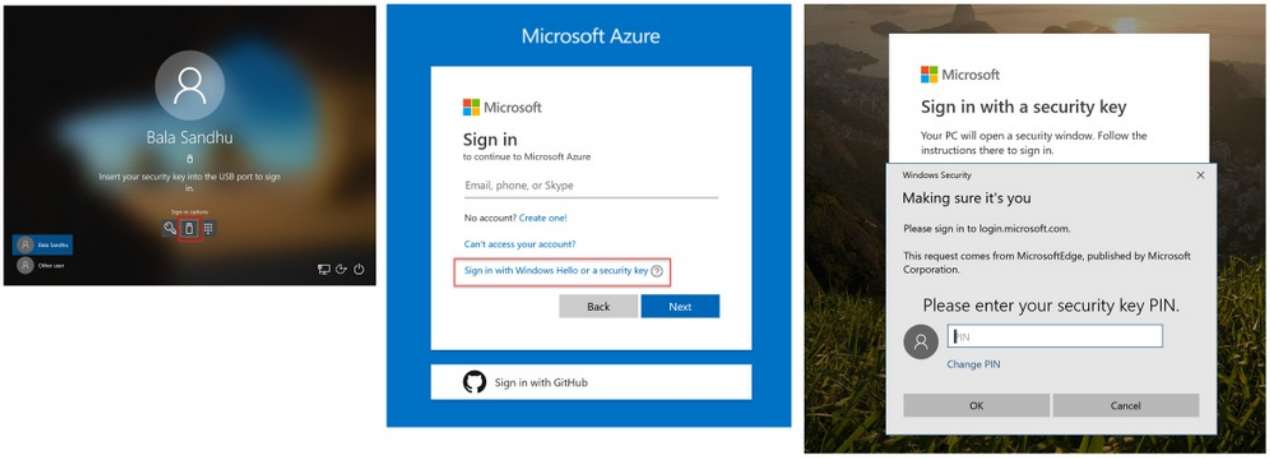
Issues for Customers to Consider

- The use of password hash synchronization does not, by itself, provide single sign-on for users. Users have two separate identities - one in Windows Server AD and a separate identity in Azure AD - that have the same attributes (user name, password), but they are not one-and-the-same identity. Single sign-on must be separately enabled so the on-premises identity is passed to Azure AD for users on the corporate network using corporate devices.
- Changing a password on-premises and having the new password hash synchronized to Azure AD does not immediately affect a user with a current Azure AD session. The user's new password will only be required when Azure AD requires a re-authentication, which could be as long as 180 days later, if the user has selected "Keep Me Signed In."

- As a consequence of an Azure AD account password being set to Never Expire when password hash synchronization is enabled, a user unable to log into their expired on-premises account will still be able to log into their Azure AD account using the now expired password.
- If the Windows Server AD attribute of accountExpires is used, it will expire a given user account at a certain point. However, this attribute is not synchronized to Azure AD, so that an expired on-premises account will still be operational in Azure AD. Disabling or expiring the Azure AD account requires additional steps.

Passwordless Authentication with Azure AD

About



Microsoft offers passwordless authentication with Azure AD using FIDO2-based security keys, including the Microsoft Authenticator app. Microsoft argues that passwords are no longer an effective security mechanism, and something very different is necessary.

Details of passwordless authentication include:

- Once set up, users will be able to sign-in to Azure AD-connected apps and services without using a password. Each user will require a FIDO2-based security key, the Microsoft Authenticator app, or Windows Hello. Or multiples thereof.
- Microsoft updated the admin portal for Azure AD, adding a new Authentication Method Policy blade in public preview. This enables an Azure AD administrator to configure users for passwordless authentication.
- Once enabled for passwordless authentication by an admin, users can add authentication methods including security keys.
- While Microsoft Authenticator is a valid FIDO2-based authenticator, Microsoft has also partnered with security key hardware providers to support other form factors. At the time of the public preview, the initial three partners are Feitian Technologies, Yubico, and HID Global.

Timeline:

- Public preview - released July 10, 2019.

Issues for Customers to Consider

- This announcement covers accounts in Azure AD, such as Office 365 work and school accounts. Microsoft released passwordless authentication for Microsoft accounts in June. See Weekly News Drop - June 14.
- Many of the security tools in Microsoft's toolkit aim to mitigate the effects of a compromised password or identify when a compromised password is being used by an attacker. By going back to the root of the problem and offering ways to eliminate passwords entirely, a complete set of follow-on problems should eliminated or greatly reduced.
- Loss of a phone or security key is going to be annoying. Administrators will have the ability to reissue keys, but the cost of "resetting my password" is going to leap from only a call to the help desk to a call to the help desk plus the cost of a new physical security key. This cost will, however, be less than the cost of a security breach.

Self-Service Password Reset

About

- Self-Service Password Reset (SSPR) is a capability of Azure Active Directory.
- [July 2018] Microsoft previewed a combined way in which the phone number entered for self-service password reset can also be used for multi-factor authentication.
- [August 2018] Microsoft released two new options for a user to prove who they are in order to reset their password: mobile authenticator app and mobile app code.

Azure Key Vault

About

- An Azure service for storing cryptographic keys and other secrets.
- The default key is an RSA 2048-bit key, with some options for RSA 3072-bit and RSA 4096-bit keys.
- Keys can be protected by software only or by a hardware security (HSM) module.
- Microsoft does not have access to your keys, and applications only have indirect access. Applications use shared access signatures, which provide indirect access.
- Keys can be automatically rotated.
- Keys can be segregated for dev / test. Keys required for production can be made more widely available.
- Key Vault is available in two service tiers: Standard and Premium.
- **Standard Keys** - only offers software-protected keys, with RSA 2048-bit the default key. RSA 3072-bit and 4096-bit keys are in preview; these will be 5x as expensive to use as the 2048-bit option.
- **Premium Keys** - offers both software-protected and HSM-protected keys.
- Key Vault is used for:
    - Customer Key in Office 365

Issues for Customers to Consider

- The worldwide outage of Microsoft Teams in mid-February 2019 was traced to Key Vault as the single point of failure. See Worldwide Microsoft Teams Outage.

Update Log - Authentication

July 2019

July 11 - Authentication Methods Reporting

July 10 - Passwordless with Azure AD

June 2019

June 10 - Passwordless Sign In to Windows and Microsoft Accounts

May 2019

May 28 - Azure AD Provisioning Updates

May 23 - Identity Data in Europe

May 20 - Azure AD Entitlement Management

May 14 - Azure Durability

May 14 - Support for Longer Passwords

May 6 - Third-Party App Usage of Microsoft Identities

April 2019

April 19 - Weekly News Drop - Changing Authentication Flow

April 10 - New page - Password Hash Synchronization

April 3 - Azure AD Password Protection Released to GA

March 2019

March 13 - Microsoft 365 Roadmap Updates - Staged User Rollout to Azure AD Cloud Authentication

February 2019

February 26 - Worldwide Microsoft Teams Outage

January 2019

January 29 - Support for Email OTP in Azure AD

November 2018

November 30 - Real-Time Microsoft Cloud App Security Controls for On-Premises Web Apps

November 27 - Multi-Hour MFA Outage in the United States

November 20 - Password-Less Sign-On Coming for Azure AD

November 19 - Global MFA Outage on November 19, 2018

October 2018

October 23 - Support for Multiple MFA Devices Per User

October 23 - Support for Hardware OATH Tokens in Azure MFA

October 18 - Lifecycle Management of Guest Accounts in Office 365

September 2018

September 4 - Data Center Outage in US South Central

August 2018

August 27 - Apple Watch App for Microsoft Authenticator

August 7 - Released - support for automatic user provisioning through Azure AD's user provisioning service added for eight additional cloud services. These were Asana, BlueJeans, Bonusly, Cornerstone OnDemand, LucidChart, ThousandEyes, and Zendesk. Joins currently supported services ("dozens available"), such as - Salesforce, Workday, Slack, GoToMeeting, Jive, ServiceNow, Dropbox, Box and others. See Authentication - Overview. Announced via Enterprise Mobility + Security Blog.

August 6 - Microsoft re-iterated that a new combined experience for multi-factor authentication and self-service password reset is available in preview. See Multi-Factor Authentication and Self-Service Password Reset. Announced via Enterprise Mobility + Security Blog.

August 2 - The ability to use the Azure AD Connect wizard to generate the configuration details required for federating with PingFederate was released to General Availability. This capability was previously released in public preview in May 2018. The integration means that organizations with an on-premises Active Directory can federate user account details with Azure AD using PingFederate (instead of Microsoft's ADFS federation tool). See Federation with Azure AD. Announced via Enterprise Mobility + Security Blog.

July 2018

July 30 - Previewed - a new roles and administrators experience for reviewing and managing role assignments in Azure AD. The intent is to streamline access to understand who has what role within Office 365 and other applications connected to Azure AD. Users can be added to a new role, or removed from a current one. There are 23 roles in the preview available for user assignment, across Azure AD, Office 365, and Dynamics 365. Roles can also be managed using Privileged Identity Management (requires a Premium P2 license in Azure AD), so that users only gain elevated privileges as required, rather than having elevated rights all the time (called standing rights). Note that the experience shows granular roles for Azure AD, but only high-level or top-level roles for services such as SharePoint, Exchange, Power BI, and others. Sub-roles or more granular role access within these services must still be managed within the admin interface for the respective services. Announced via Enterprise Mobility + Security Blog.

July 23 - Released - two new identity-related bounty types and an increased bounty for vulnerabilities in Microsoft's identity systems. New bounty types: [1] for vulnerabilities in the Open ID Connect family of specifications, and [2] collections of inappropriately shared sensitive user data. Increased bounty: Microsoft will pay up to $100,000 in some cases for vulnerabilities in its identity systems. See Authentication - Overview. Announced via Enterprise Mobility + Security Blog.

July 6 - Previewed - new combined registration experience for multi-factor authentication and self-service password reset. Allows the entry of a phone number for MFA (for receiving verification codes) to also be used for self-service password reset. Allows the deletion of a phone number for MFA to also be deleted for self-service password reset. Released in Preview. Organizations have to opt in. Related to Roadmap ID 31548 on Office 365 Roadmap. See Multi-Factor Authentication and Self-Service Password Reset.

June 2018

June 29 - Preview - new default option that all privileged accounts have multi-factor authentication enforced. While in Preview organizations can opt in. After General Availability, this will be turned on by default, and organizations can opt out. See Multi-Factor Authentication. Announced via June 2018 updates for Microsoft 365.

June 28 - General Availability - Conditional Access App Control, part of Microsoft Cloud App Security in Enterprise Mobility + Security. Allows the setting of policies to determine whether an authentication request can be approved based on context factors about the authentication request, such as device type, user location, and user type, among others. Integrates with the policies in Azure AD Conditional Access. Announced via Security, Privacy and Compliance Blog.

June 26 - Using multi-factor authentication with the administrative processes for Exchange Online. See eDiscovery Workflow. Announced via Security, Privacy and Compliance Blog.

June 19 - Public Preview - Azure AD Password Protection. Provides the ability for organizations to [1] create a specific list of banned passwords (called the "Custom Banned Password List"), and [2] extend password protection to Windows Server AD for on-premises protection. In addition to any customer-supplied list of passwords, Microsoft curates its own list, the contents of which is not publicly disclosed. This is called the "Global Banned Password List." Custom banned password list is included in Azure AD Basic. Extending password protection to Windows Server AD requires at least Azure AD Premium 1. Announced via Enterprise Mobility + Security Blog.

June 19 - Public Preview - Azure AD Smart Lockout. Provides lockout settings on repeated password failures to stop bad actors from signing into a user's account. Does not stop a valid user from logging in. Available in all versions of Azure AD, including Office 365. Announced via Enterprise Mobility + Security Blog.

Data Loss Protection

Overview

- With the increasing complexity of infrastructure and rapid proliferation of data types, it is vital for organizations to adopt a DLP solution with coverage for all file types. Moreover, basic keywords are not sufficient for DLP policy creation. Many organizations need to create policies for custom fields such as medical ID numbers, etc.
- Exchange Online admins have the ability to create Exchange-only policies through the Exchange Admin Center. See DLP in Exchange Online.
- Microsoft is investing in a Unified DLP engine, accessible through the Security & Compliance Center. See DLP in Security & Compliance Center.
- DLP in Office 365 is only one part of Microsoft's wider investments in information protection. See Azure Information Protection for the wider (and still developing story), and Microsoft Information Protection for the overall framework of services and capabilities for protecting sensitive information.

DLP in Exchange Online

About

- Exchange admins can configure DLP rules through the Exchange Admin Center. DLP in Exchange Online is the older approach for DLP in Office 365. Microsoft is encouraging administrators to move to DLP in the Security & Compliance Center.

Issues for Customers to Consider

- DLP rules only support basic actions when sensitive information is identified, lacking the finesse and nuance of competitive offerings. For example, while DLP rules can stop a message and some types of documents from flowing through Exchange Online when sensitive information is identified, it is not possible to redact or sanitize the sensitive information in the message or document, or automatically encrypt when required, and still flow the message through to the recipient. Human intervention by the original sender or an administrator is required to fix the identified problem, which can create a backlog of messages requiring manual assessment and intervention to resolve.
- Basic document fingerprinting is available, where a template of a sensitive document can be saved and used for identifying future documents that have the same structure. Only full matches to the specific document fingerprint will be identified, however, while partial matches will evade detection.
- A message that violates a DLP rule can be routed only for review or approval to an explicitly named individual or the sender's manager. There are no more nuanced options, such as performing a directory lookup based on the sender's name or department name to find the local compliance officer, or routing messages to a quarantine for analysis by a group of administrators.
- DLP rules will detect sensitive information only in a specific set of 58 file types, which are weighted in favor of the different variants of Word, Excel, PowerPoint, and other Office file formats. Non-supported file types containing sensitive information will not be captured if they are sent through Exchange Online. Likewise, sensitive information hidden in images will not be identified because Office 365 cannot perform OCR on scanned documents and screenshots.

DLP in Security & Compliance Center

About

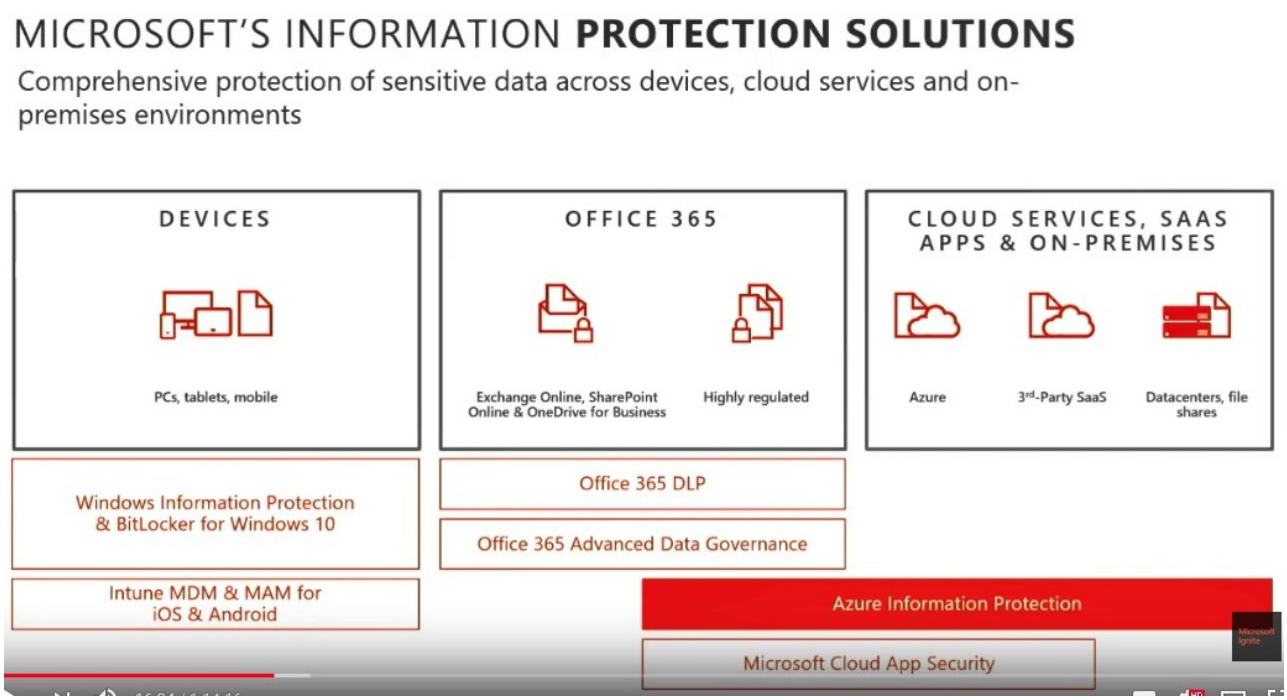
- Office 365 offers a unified data loss prevention (DLP) policy creation and reporting engine in the Security & Compliance Center, covering four Office 365 workloads (Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams). DLP policies are about identifying sensitive information in email messages and documents, based on Microsoft's set of more than 80 structured, sensitive information types, using basic keyword and regex (regular expressions) matching.
- [**June 2018**] Microsoft introduced five new sensitive information types for data types pertaining to GDPR. There is also a template (or grouping of the current and new GDPR data types) into a common GDPR template for use as a unitary item in DLP and data governance policies. See Update Log - DLP.
- For organizations uncertain of the sensitive information being sent or shared through Office 365, DLP policies can be created in test mode that are invisible to the end user and that impose no affect on messages and files. An administrator can review the DLP logs to ascertain the scope and scale of sensitive information in the Office 365 tenant, and plan to take appropriate action based on real-life experience.
- Microsoft will add the ability to create a custom sensitive information type using the user interface of the Security & Compliance Center. Previously this could only be accomplished using an XML file. See Office 365 DLP Updates (October 2018).
- [**March 2019**] DLP policies in the Security & Compliance Center can be applied to chat and channel conversations in Microsoft Teams. DLP rules will block chat and channel messages if they contain sensitive information, as defined by a match to a sensitive information type that has been enabled. DLP policies for Teams requires Enterprise E5 or the Advanced Compliance add-on; it is not available with the Enterprise E3 plan. The addition of Microsoft Teams to the scope of DLP policies was announced in October 2018. See Office 365 DLP Updates.
- [**June 2019**] DLP policies are evaluated in priority or execution order, and the first rule that matches identified content in an email message or document is applied. Microsoft now offers the ability to set the priority or execution order of DLP policies in the Security & Compliance Center, by re-arranging the set of rules that have been created.
- [**August 2019**]

Issues for Customers to Consider

- DLP policies are evaluated in priority or execution order, and the first rule that matches identified content in an email message or document is applied. This means there is no balanced analysis of which DLP policy would be best to apply to a specific message or document, or no attempt at identifying the "best match" on a message-by-message or document-by-document basis. In other words, a general policy that has a higher priority or execution order will be applied ahead of a specific policy that has a lower priority or execution order.
- There are no workflow options for messages and files that violate a DLP policy. For example, if an email message triggers a policy, it is either blocked or encrypted. There is no policy action option for routing the violating message to an administrator or administration queue for review. As with DLP in Exchange Online, DLP in the Security & Compliance Center doesn't offer any nuanced options to request a review by someone other than the original end user.
- While Office 365 offers DLP capabilities, these are limited to Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. Other Office 365 workloads - such as Yammer - are excluded, as are other document storage and conversational systems outside of Office 365. This partial coverage of Office 365 workloads means that Office 365 does not offer a unified DLP rules and remediation engine that can be used for all document storage and conversational systems in use across the enterprise, nor does it handle everything in Office 365.
- Analyzing content for sensitive data relies on the Sensitive Information Types provided by Microsoft, or a custom-definition created by the customer. Sensitive data matching is simple to circumvent to exfiltrate data; the matching algorithms look for exact matches and are easy to trick. For example:
    - Matching a credit card number can be circumvented by changing any one of the 16 digits into the equivalent word. For example, writing the last four digits as "997four" will not match against the credit card regex.
    - Matching a SWIFT code can likewise be circumvented by changing a digit to a word, or a letter to the Air Force alphabet equivalent. For example, instead of writing the SWIFT code of WPACNZ2W (which will be matched against the sensitive information type), writing it as WPACNovemberZ2W will not trigger a match, and therefore not be caught by the DLP rule. This is even when the email subject line and the email body specify that a SWIFT code is included in the message.

    - In summary, matching sensitive data requires too much perfection in how sensitive data is formed in a message, and does not use a balanced evaluation for the presence of sensitive data.
- Even without attempting to deliberately obfuscate the presence of Sensitive Information, messages containing sensitive information are missed by DLP policies if explanatory metadata is missing from the email. For example, an email that contains a Social Security Number but not the explanatory phrase "Social Security Number" does not trigger a DLP policy looking for Social Security Numbers.
- While a DLP policy can be triggered based on content in the subject line of an email, if the policy action is to encrypt the message then the policy will be without effect because Office 365 Message Encryption passes the subject line through in clear text. It is not encrypted.
- DLP policies cannot proactively flag email sending mistakes, such as addressing an email to the wrong recipient due to auto-complete mistakes. Office 365 does not analyze a user's normal sending patterns to warn of misaddressed messages (including the wrong recipients in the To or Cc fields). It cannot, likewise, use anomaly detection capabilities to detect when a user is sending an email with malicious intent.
- No organizationally-tailored DLP policies are automatically enabled in Office 365; each must be manually configured and fine-tuned. Too few organizations have the cybersecurity skill set available to effectively configure DLP policies. Microsoft has recently introduced new intelligence capabilities that will detect sensitive information that is flowing that should be protected by a DLP policy, and will alert an administrator that some type of remediation action is taken. Whether this soft recommendation approach is enough remains to be seen. There is also a default DLP policy that looks for the presence of one or more credit card numbers sent to someone outside the organization; this is in Policy Tips mode with an alert to the end user.
- DLP policies cannot be targeted to specific groups or regions to help global firms facing different regulatory requirements around the world. The exception to this appears to be for organizations using the new Multi-Geo service, which enables tailoring based on geo (but not necessarily country).
- Documents in SharePoint Online and OneDrive for Business that are identified by a DLP policy as containing sensitive information are blocked in place, to prevent access from anyone beyond the document owner, the person making the most recent change, and the site owner from having access. There is no ability to automatically sanitize the document of sensitive information, or to encrypt the sensitive information within the document while keeping the rest of the document available. Even more significantly, there is no sense that people beyond the three individuals may have a valid justification for accessing the document with the sensitive information intact. Office 365's block-and-prevent stance may cause problems for valid business processes, possibly decreasing productivity and throughput.
- Actions by an administrator in creating or modifying a DLP policy are not logged to the Office 365 Audit Log. This makes it impossible to know who created a DLP policy and how it has been modified (and by whom) over time.
- DLP policies and sensitive information types cannot identify offending text in scanned images or scanned text. OCR is not supported.

Azure Information Protection



About

- DLP in Office 365 is only one portion of Microsoft's wider Information Protection strategy and direction. DLP is an important part of the Office 365 story, but Microsoft's wider investments in various information protection solutions signal that it is only one piece of a wider solution set.
- Azure Information Protection is a broader play from Microsoft for protecting data from loss, as well as inadvertent or inappropriate usage. Azure Information Protection is not included in Office 365 licensing plans, and must be purchased directly, as part of Enterprise Mobility + Security, or with one of the Microsoft 365 enterprise plans.
- Azure IP Labels - a short descriptive phrase that can be added to a document - is Microsoft's key means of identifying the protection to be applied to that single document (or email or other item). In Microsoft's current design, a document or email can have one-and-only-one label. A label can convey two signals (singularly or combined): the sensitivity of the document (and thus what information security is needed for it), and the retention timeframe for the document (how long the document must be retained for, or not deleted for). For example, a document labeled with "Confidential - 7 Years" has an information security rating of "Confidential" and a retention timeframe of "7 Years."
- Defining an Azure IP Label offers settings for encryption and visual markings, such as watermarks, headers, and footers.
- For customers with the correct plans, Microsoft is moving toward a consistent labeling experience across Azure Information Protection and the Office 365 Security & Compliance Center. Labels defined in one service will automatically appear for use in the other, although this remains a work-in-progress.
    - [**September 2018**] The Security & Compliance Center as the central play in labeling was released to general availability. See Updates to Information Protection.
    - [**4Q2018**] The existing Classification Labels in Office 365 were renamed Retention Labels. The consistent labeling experience between Azure IP and Office 365 introduced a new type of label into Office 365 called Sensitivity Labels.
- Azure Information Protection can be used to classify and protect PDF documents on Windows, with support for using the standard Adobe Acrobat Reader software plus an Azure Information Protection plug-in to allow access to classified and protected PDF documents in Acrobat Reader. The file extension remains .pdf - unlike earlier treatment - and currently only supports Adobe Acrobat Reader. The full Acrobat client is not supported, nor are other PDF readers from other vendors.
    - Public Preview - October 12, 2018. See Adobe Acrobat Reader and Azure Information Protection.
    - General Availability - December 11, 2018. See Adobe Acrobat Reader and Azure Information Protection.
- During 2019, Microsoft will add the ability for an end user to manually apply a sensitivity label without using the Azure Information Protection client. This will support Mac, Android, Windows, and Office Online. See Manual Sensitivity Labels.

- An integration is available between Azure Information Protection and Windows Defender ATP. If activated, whenever a file with a sensitivity label is created or modified on a Windows 10 device, this fact will be reported to Azure Information Protection Analytics. The dashboard in Azure Information Protection Analytics provides a summarized dashboard of where sensitive data has been discovered.
    - Public Preview - December 7, 2018. See Azure Information Protection and Windows Defender ATP.
- Includes various components:
    - Azure Rights Management Service
- [**January 2019**] Microsoft Cloud App Security can be set to inspect files protected with Azure Information Protection, thereby looking inside encrypted files to ensure sensitivity data is being appropriately protected and to ensure that sensitive data isn't being exfiltrated through obfuscation. See Inspecting Encrypted Files in Microsoft Cloud App Security.
- [**March 2019**] Microsoft released to public preview new capabilities for detecting credentials stored in documents, systems and applications without appropriate controls. The initial short list of credentials that can be detected focus exclusively on Azure (with one exception), but wider support on multiple levels is planned. See Credential Detection Using Azure Information Protection.
- [**April 2019**] Microsoft released its new unified labeling client for Azure Information Protection to general availability. Unlike the previous client - which is still available and offers more features than the unified client so far - the new Unified Labeling Client downloads labels and policy settings from the Office 365 Security & Compliance Center (or the split Microsoft 365 ones) rather than the Azure Portal. See Weekly News Drop - April 19.
    - Sensitivity labels in the Office 365 Security & Compliance Center can be configured to automatically apply a sensitivity label in Office apps if [1] the Unified Labeling Client is installed, and [2] a match of content is made against one or more sensitive information types configured in the label.
- [**April 2019**] Existing labels on documents previously labeled using a different vendor's labeling solution can be migrated to Azure Information Protection labels. Doing so requires the Azure Information Protection admin to create a mapping between the current label and the most relevant new Azure Information Protection label. Label migration is currently only supported using the Azure Information Protection client, and is not supported in the new Unified Labeling Client nor in the native labeling experience in Office apps.

Issues for Customers to Consider

- Only one Azure Information Protection label can be applied to a document or email, and the label mixes two mutually exclusive items: the sensitivity of the document (and thus the level of information security required) and the retention requirement for the document (how long it must be retained for, or how long it must not be deleted for). Neither item affects the other, and neither is driven by the requirements of the other; one is driven by sensitivity, and the other by regulation. Once all the permutations of sensitivity and retention are developed, users will face an overwhelming list of labels to select the definitively correct one from - which will be cognitively overwhelming and annoying, and thus generally left undone.
- Microsoft's assertion is that the author of a document is the best judge of its sensitivity, and thus which information security label should be applied to it. Manual labeling of documents with metadata has never been a very successful strategy, and this fundamental assertion seems out-of-place to us. The author may have some sense of the sensitivity of the document, but being [1] able to correctly select the right sensitivity label and [2] actually selecting the right one every time is a major risk. If the entire Azure Information Protection dream relies on people correctly selecting the right label for every document and email, the dream is ill-founded.
- Microsoft offers automatic application of labels, based on the content within a document or email. This capability is only available in the highest priced Azure Information Protection plan or bundle.

Microsoft Information Protection

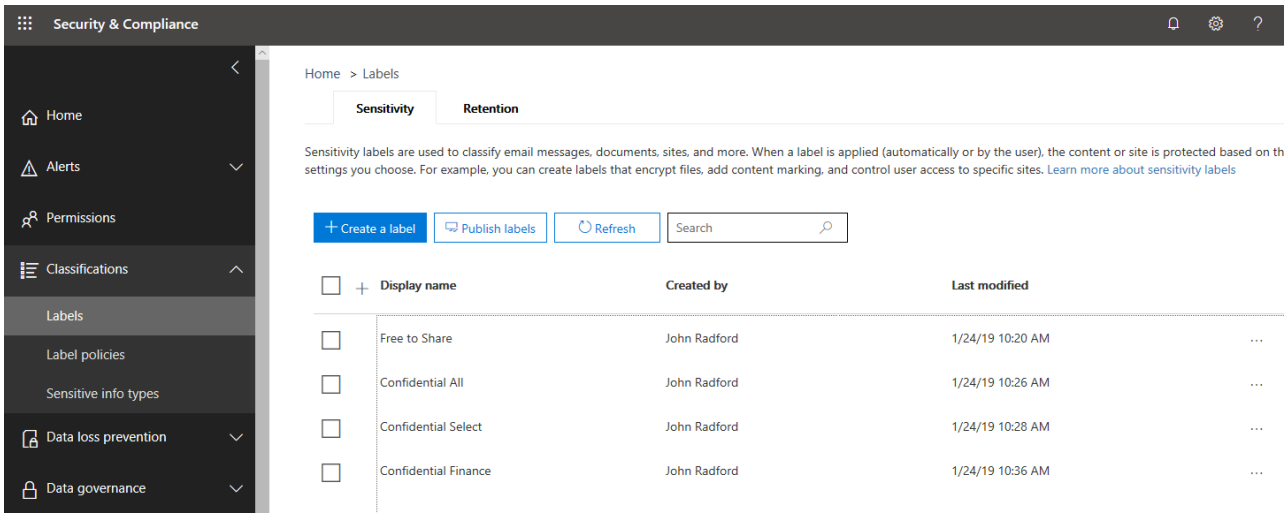
Microsoft Information Protection is a framework for products and integrated capabilities for protection sensitive information.

Microsoft Information Protection encompasses:

- Azure Information Protection
- Office 365 Information Protection, such as Office 365 DLP and Office 365 Cloud App Security
- Windows Information Protection
- Microsoft Cloud App Security

Microsoft Information Protection is not a subscription or product offering.

Sensitivity Labels



About

- Sensitivity labels were introduced in Office 365 in 4Q 2018.
- Sensitivity labels deal with the confidentiality status of a document or message. Some documents or messages contain no special content that demands confidentiality. Other documents and messages contain content that is confidential, a scale that can have several levels such as confidential but accessible by any employee, confidential but only accessible by certain employees, or completely confidential and top secret to a very small and select group of individuals.
- Sensitivity labels are one of the two types of labels available in Office 365 (the second is a Retention label). A label applies controls to the content it is attached to; a sensitivity label applies controls such as encryption, headers and footers, watermarks, and more to email messages and documents.
- Labeling content - manually by a user, or automatically by content analysis - provides an easy way to quickly segregate the commercial, information, client or knowledge sensitivity of a given email or document. For example, an email containing the business strategy for the next 3 years is highly sensitive, and if it is labeled as Confidential or Top Secret, controls can be put in place to limit who can access the email message. Likewise, a document containing personal data about a client (or employee) should be protected from unauthorized access. On the other hand, an email message about food left in the staff cafe has low sensitivity.
    - [**May 2019**] Microsoft announced that sensitivity labels will be able to be defined for a SharePoint site at the site level, which will automatically apply the sensitivity label to content in the site. See SharePoint Security and Compliance Updates.
- The configuration of a sensitivity label offers three controls:
    - **Encryption** - for automatically applying encryption to both email messages and files or just email messages. Settings are also available for content expiration and offline access. If encryption is turned on, permissions must be configured for specific users or groups, one option of which is everyone in the tenant.
    - **Content Marking** - for automatically applying a watermark, header, and/or footer to the labeled content.
    - **Endpoint Data Loss Prevention** - for enforcing data loss prevention settings on Windows devices running Windows Information Protection. When content (files only, not email messages) carrying a sensitivity label is identified by Windows Defender ATP, endpoint DLP through Windows Information Protection will protect against data leaks. There are various policy settings required in Windows Defender ATP and Windows Information Protection to make this chain of protection work.
- Once a sensitivity label has been created, it must be published for use within client applications. A label can be published to the entire organization, or to subset using users and/or groups. For example, in the screenshot above, the "Confidential Finance" sensitivity label is only available for use by members of the Finance Team group, because of how it was published. People not in the Finance Team group will not see the label.
- General-purpose scales of confidentiality (and the labels that correspond with those) can be complemented by labels that are specific to a particular project, such as due diligence for a merger and acquisition. Publishing such a label only to the defined

group of people working on the M&A assessment hides the presence of the label from everyone else, and therefore doesn't run the risk of disclosing the presence of a pending change beyond the people who have to know.
    - [**Exception**] Any person with access to the classifications section in the Security & Compliance Center could observe the presence of a project-specific label, and also to whom the label was published. Ideally, a non-descript code word should be used to obfuscate the real intent of the label to reduce the risk of improper disclosure.
- Each individual piece of content - an email message or a file - can have a maximum of one sensitivity label applied to it. Each piece can also have a maximum of one retention label applied as well.
- [**February 2019**] Microsoft added the ability to use S/MIME encryption with a Sensitivity Label rather than Office 365 Message Encryption. This option is intended for customers who already have a working S/MIME infrastructure. See Sensitivity Labels with S/MIME.
- [**March 2019**] Sensitivity Labels can be configured for automatic application to some content in Office 365, or to offer a recommendation on a sensitivity label that a user can accept or dismiss. Auto-labeling requires an Azure Information Protection P2 subscription, and the use of the Azure Information Protection unified labeling client. See Information Protection Updates, and Auto-Labeling of Sensitivity Labels.
- [**April 2019**] Native labeling within Office 365 ProPlus is scheduled for release in the second half of 2019. The Microsoft 365 Roadmap says 3Q. See Weekly News Drop April 5.

Issues for Customers to Consider

- A sensitivity label works with DLP protections on Windows devices through Windows Information Protection. Sensitivity labels can not currently work with or trigger DLP rules in Office 365, although this capability is supposedly coming.
- [**April 2019**] Retention Labels in Office 365 disappeared for several weeks in March 2019, and users were unable to add new Retention Labels to documents. Microsoft finally restored labeling functionality in late March and was able to restore labels to documents in early April 2019. See Retention Labels Meltdown.

Update Log - Data Loss Protection

August 2019

August 8 - Exact Data Match in DLP

May 2019

May 22 - SharePoint Security and Compliance Updates

April 2019

April 8 - Retention Labels Meltdown

April 3 - Native Labeling Coming to Office 365 ProPlus in 2H 2019

March 2019

March 7 - Information Protection Updates, and Auto-Labeling of Sensitivity Labels

March 5 - Credential Detection Using Azure Information Protection

February 2019

February 12 - Sensitivity Labels with S/MIME Option

January 2019

January 29 - Inspecting Encrypted Files with Microsoft Cloud App Security

January 24 - DLP and Windows Defender ATP

January 24 - New page added: Sensitivity Labels

January 2 - Standalone Upgrades for Microsoft 365 E3

December 2018

December 19 - Manual Sensitivity Labels on Mac, Android, Windows and Office Online scheduled for 2019.

December 11 - Adobe Acrobat Reader and Azure Information Protection - released to General Availability.

December 7 - Azure Information Protection and Windows Defender ATP.

October 2018

October 12 - Microsoft and Adobe released the Public Preview of support for classifying and protecting PDF documents using Azure Information Protection. See Adobe Acrobat Reader and Azure Information Protection.

October 8 - three upcoming changes in Office 365 DLP: the ability to create custom sensitive information types in the UI of the Security & Compliance Center, integration with Microsoft Teams Chat for blocking chat messages that contain sensitive information,

and different default file handling in SharePoint Online and OneDrive for Business. See Office 365 DLP Updates.

September 2018

September 8 - the new Encrypt-Only template for Office 365 Message Encryption will be triggerable by a DLP rule in the Office 365 Security & Compliance Center. See Apply Encrypt Only with a DLP Rule in the Office 365 Security & Compliance Center.

June 2018

June 19 - General Availability - Five New Sensitive Information Types for GDPR. Microsoft released 5 new sensitive information types for identifying personal data relevant to GDPR. These are available for individual use in DLP or data governance policies. Microsoft also released a new GDPR template, which groups all EU-relevant sensitive information types together, for use as a single entity in policies. The new data types are: EU passport number, EU national identification number, EU driver's license number, EU tax identification number (TIN), and EU social security number (SSN) or equivalent ID. See Data Loss Protection. Announced via Security, Privacy and Compliance Blog.

eDiscovery - Overview

Overview

eDiscovery is about finding electronic communications that match certain conditions (or search constructs). eDiscovery is generally used to locate communications that may be relevant to a legal case, to meet specific regulatory requirements, or more broadly for internal governance.

In this section, we look at Office 365's capabilities in the areas of:

- Searching for content
- Support for searching and indexing specific file types
- Workflow for eDiscovery cases
- Working with legal holds
- Creating supervision policies, such as what is required for FINRA.

Please note the following, as these have implications for eDiscovery in Office 365:

- Microsoft may change its licensing approach for inactive mailboxes in Microsoft Exchange.

Research by Osterman

Earlier in 2018, Osterman asked respondents to a survey about the importance of various eDiscovery capabilities.

Importance of Various Content Management Capabilities
Percentage Responding "Important" or "Extremely Important"

Capability	%
The ability to have in-place search and review eDiscovery capabilities within the Office 365 stack	66%
The ability to have in-place eDiscovery capabilities within the Office 365 stack	63%
The ability to have in-place search and review eDiscovery capabilities across multiple vendors' solutions	53%
The ability to have in-place eDiscovery capabilities across multiple vendors' solutions	48%

Source: Osterman Research, Inc.

Content Search

About

- Microsoft offers a search capability within its eDiscovery toolkit in the Security & Compliance Center. The use of these search capabilities requires that an eDiscovery case is created first. Once a case is created, one or more content searches can be created and saved within the case.
- Microsoft separately offers a Content Search option in the Security & Compliance Center. This is located under the Search & Investigation title. While Content Search is described as an eDiscovery tool as well, there is no ability to create an eDiscovery case. It also does not offer the ability to move a search into an eDiscovery case after a case is created.
- Microsoft offers a range of eDiscovery capabilities for searching for responsive material across Office 365, plus a more advanced eDiscovery service called Advanced eDiscovery that adds text analytics, machine learning, and relevance and predictive coding for early case assessment.
- With its latest approach to eDiscovery through the Security & Compliance Center, Microsoft has removed some of the limitations from its earlier attempts to provide enterprise-class content search for eDiscovery and other requirements, such as limited search scopes (where a maximum of 10,000 Exchange mailboxes could be searched at once in an eDiscovery search), as well as separate eDiscovery tools for Exchange Online and SharePoint Online.
- Content available for searching in the Security & Compliance Center is:
    - **Exchange Online** - email and attachments, whether encrypted or not.
    - SharePoint -
    - OneDrive -
    - **Microsoft Teams** - messages (including chats in Skype for Business), files in Microsoft Teams, and summary data on calls and meetings (the latter was added July 2018). Non-channel chat transcripts can also be made available for content search for those users with an Exchange on-premises mailbox (with certain provisions, from June 2018).

Issues for Customers to Consider

- Summary details for calls and meetings in Microsoft Teams only include names and times; there is nothing available on what the meeting was actually about. For example, the subject line for the meeting is not included. If there was an agenda for the meeting, this is not tied to the summary details record. Therefore, a content search can show that a call or meeting happened, but cannot show what it was about. By implication, keyword searches on summary details for calls and meetings will not work.

- Due to batch processing, searches using the native Office 365 functionality are fairly slow. It can take several minutes to run a single search and search time increases based on the number of mailboxes in question.

- The eDiscovery capabilities in the Security & Compliance Center take a unified approach to responsive content in three key Office 365 workloads only: Exchange Online, SharePoint Online, and OneDrive. Other workloads – such as Yammer, Microsoft Stream, and Microsoft Teams – are excluded. Further, an eDiscovery case created in the Security & Compliance Center cannot search for responsive content in non-Office 365 content repositories, such as those maintained on-premises or in other cloud services. This limited approach means that any organization with content outside of Office 365 – including SharePoint 2013 and 2016 on-premises – will need multiple eDiscovery tools, in addition to having to instantiate, perform, and coordinate multiple eDiscovery cases in each separate tool. This is an expensive, complex and error-prone situation.

- Customers have recently been given the ability to import non-Office 365 data for analysis into Advanced eDiscovery. This has to be organized in a particular structure, uploaded into Azure, connected through a series of manual steps, and then processed by Advanced eDiscovery. Once processed, additional new content cannot be added to the Azure container. Another separate non-Office 365 data import has to be organized instead.

- Searching Exchange Public folders is an all or nothing proposition. There is no ability to scope the search to a targeted list. This means far too much information will be exposed to eDiscovery managers.

- It is not possible to configure a more limited search scope for eDiscovery managers searching OneDrive and SharePoint Online repositories, and Exchange mailboxes. Any eDiscovery manager can search any OneDrive folder, SharePoint Online site, or Exchange mailbox anywhere in the world; these should be able to be restricted by geographical region or country to safeguard and protect data.

- It is not possible to set the search scope on email messages to exclude the signature block, so if a keyword appears in email signatures, it will generate a high rate of false positives. This is an annoying time waster for eDiscovery personnel, and expensive for the organization.

- Messages encrypted with rights management protections can be automatically decrypted at the time of export, but a separate export must be run to handle these messages as individual entities. The export of encrypted messages cannot take place in line with any other export activities.
- Search results for Exchange Online, SharePoint Online and OneDrive must be exported from Office 365 to facilitate the review process; the Exchange content as one or more PST files, and the SharePoint and OneDrive content as individual files (with an option for all versions). There are multiple problems with the Office 365 approach: it creates a duplicate set of content outside of Office 365 which must be protected, there is no reporting on actions taken on the exported content in the eDiscovery case in Office 365 because Office 365 is blind to post-export actions, if the search is run again in Office 365 then a subsequent export is required along with integration of multiple sets of data, and there is no connection between what was collected and the coding decisions made to that content in order to inform future cases and reduce the volume of potentially responsive content in Office 365. The need to export content to Azure – with the time delays that are introduced from Office 365 to Azure and then Azure to a local computer – creates unhelpful delays in an urgent process for compliance officers. With GDPR coming on stream in late May 2018, the potential existence of personal data in additional locations will raise significant data governance concerns.
- It is not possible to do an eDiscovery search for sensitive data in Exchange Online. These capabilities are available for SharePoint Online and OneDrive for Business, but not for Exchange Online.
- Encrypted documents in SharePoint Online and OneDrive for Business are invisible to Content Search, because the search indexing process is unable to look inside encrypted documents. This is different to the experience in Exchange Online, where the search indexing process can decrypt encrypted email messages to assess content inside. See Searching Encrypted Documents and Emails (January 2019).

eDiscovery Workflow

About

- Microsoft offers a range of eDiscovery capabilities for searching for responsive material across Office 365, plus a more advanced eDiscovery service called Advanced eDiscovery that adds text analytics, machine learning, and relevance and predictive coding for early case assessment.
    - [July 2018] Microsoft announced new beta capabilities for creating named subsets of data in Advanced eDiscovery. Content can now be tagged with user-created tags, and either exported as a collection or used for further search and investigation purposes.
- Advanced eDiscovery is available in the premium Enterprise E5 plan, and as an additional cost add-on to the Enterprise E3 plan.
    - [**January 2019**] Microsoft released a significant update to Advanced eDiscovery. See Updates to Advanced eDiscovery.
    - [**April 2019**] The updates to Advanced eDiscovery were released to General Availability on April 30, 2019.
- With its latest approach to eDiscovery through the Security & Compliance Center, Microsoft has removed some of the limitations from its earlier attempts to provide enterprise-class eDiscovery, such as limited search scopes (where a maximum of 10,000 Exchange mailboxes could be searched at once in an eDiscovery search), as well as separate eDiscovery tools for Exchange Online and SharePoint Online.
- [**January 2019**] Microsoft offers the ability to specify the PST file export size when using the eDiscovery Export tool. The default export size is set to 10 GB. Using a registry key on the computer running the eDiscovery Export tool, a user can specify a lower value if required. While specifying a larger number is supported, Microsoft recommends against doing so due to the risk of data corruption in very large PST files. Note that the change is computer-by-computer, not as a policy setting in the Security & Compliance Center. See Control Over PST Output Size in eDiscovery.

Issues for Customers to Consider

- There is no workflow or project tracking of an eDiscovery case, such as the status of the case, who is involved, and which tasks are being worked on and by whom.
    - [**January 2019**] Microsoft's update to Advanced eDiscovery adds these capabilities for Advanced eDiscovery customers. See Updates to Advanced eDiscovery.
- An eDiscovery case administrator has no ability within the Security & Compliance Center to send legal hold notification alerts, nor reminders or escalations. These have to be handled out-of-band. As above, the lack of workflow and project tracking capabilities is not ideal.
    - [**January 2019**] Microsoft's update to Advanced eDiscovery adds these capabilities for Advanced eDiscovery customers. See Updates to Advanced eDiscovery.
- Searches for keywords that are started in the Content Search tool cannot be imported into an eDiscovery case. The two services are different and offer no integration. The only way for a search to work in an eDiscovery case is for it to be created within the case.
- eDiscovery cases are made up of holds and searches. No two searches within any eDiscovery case in the organization can have exactly the same name. Office 365 will only permit a given name to be used once in eDiscovery cases across the entire tenant.
- All cases are created and managed in an ad-hoc way, with a compliance officer entering ad-hoc search terms. It is not possible to create a case template for repeatability and auditing, with standard search queries and locations, key actions and requirements to complete, and an audit trail of what was and wasn't done. This is of particular concern to organizations that are not doing eDiscovery all the time; the ad-hoc approach means that prior learnings and approaches are likely to be forgotten and overlooked in a current eDiscovery case, possibly exposing an organization to sanction for insufficient production of evidence.
- Exports from Office 365 are not protected and so are at risk of alteration and spoliation. The output is a raw native export and not in a preservation format, such as forensic image format, which many eDiscovery collection tools offer. Moreover, there are no additional encryption options provided by Microsoft to encrypt the export.
    - [**May 2019**] In Q4 2019, Microsoft is planning on enabling secure access by external users to a case in Advanced eDiscovery, negating the need for exports under some circumstances. See Advanced eDiscovery Updates for Q3 and Q4.

- Due to batch processing, searches using the native Office 365 functionality are fairly slow. It can take several minutes to run a single search and search time increases based on the number of mailboxes in question.
- The eDiscovery capabilities in the Security & Compliance Center take a unified approach to responsive content in three storage containers in Office 365 - user and group mailboxes in Exchange Online, sites in SharePoint and OneDrive, and Exchange public folders. Workloads that store content in these containers can be searched; but other workloads that do not are excluded (such as Yammer, Microsoft Stream, and Microsoft Planner). Further, an eDiscovery case created in the Security & Compliance Center cannot search for responsive content in non-Office 365 content repositories, such as those maintained on-premises or in other cloud services. This limited approach means that any organization with content outside of Office 365 – including SharePoint 2013 and 2016 on-premises – will need multiple eDiscovery tools, in addition to having to instantiate, perform, and coordinate multiple eDiscovery cases in each separate tool. This is an expensive, complex and error-prone situation.
    - [**April 2019**] Microsoft announced that eDiscovery for Yammer will be available by the end of calendar year 2019. See Yammer in Europe and eDiscovery.
    - [**May 2019**] Microsoft said that Office 365 E5 customers will be able to get full conversations as they appear in Yammer in eDiscovery when released. Office 365 E3 customers will only get a per message view.
- Customers have recently been given the ability to import non-Office 365 data for analysis into Advanced eDiscovery. This has to be organized in a particular structure, uploaded into Azure, connected through a series of manual steps, and then processed by Advanced eDiscovery. Once processed, additional new content cannot be added to the Azure container. Another separate non-Office 365 data import has to be organized instead.
- Searching Exchange Public folders is an all or nothing proposition. There is no ability to scope the search to a targeted list. This means far too much information will be exposed to eDiscovery managers.
- It is not possible to configure a more limited search scope for eDiscovery managers searching OneDrive and SharePoint Online repositories, and Exchange mailboxes. Any eDiscovery manager can search any OneDrive folder, SharePoint Online site, or Exchange mailbox anywhere in the world; these should be able to be restricted by geographical region or country to safeguard and protect data.
- It is not possible to set the search scope on email messages to exclude the signature block, so if a keyword appears in email signatures, it will generate a high rate of false positives. This is an annoying time waster for eDiscovery personnel, and expensive for the organization.
- Messages encrypted with rights management protections can be automatically decrypted at the time of export, but a separate export must be run to handle these messages as individual entities. The export of encrypted messages cannot take place in line with any other export activities.
- Search results for Exchange Online, SharePoint Online and OneDrive must be exported from Office 365 to facilitate the review process; the Exchange content as one or more PST files, and the SharePoint and OneDrive content as individual files (with an option for all versions). There are multiple problems with the Office 365 approach: it creates a duplicate set of content outside of Office 365 which must be protected, there is no reporting on actions taken on the exported content in the eDiscovery case in Office 365 because Office 365 is blind to post-export actions, if the search is run again in Office 365 then a subsequent export is required along with integration of multiple sets of data, and there is no connection between what was collected and the coding decisions made to that content in order to inform future cases and reduce the volume of potentially responsive content in Office 365. The need to export content to Azure – with the time delays that are introduced from Office 365 to Azure and then Azure to a local computer – creates unhelpful delays in an urgent process for compliance officers. With GDPR shifting into enforcement mode from late May 2018, the potential existence of personal data in additional locations raises significant data governance concerns.
- Administrators with multi-factor authentication enabled are not able to export results to PST from eDiscovery. The attempted export fails.
    - [**June 2018**] Microsoft explained how MFA requirements can co-exist with certain Exchange Online administrative processes, including those carried out through the Security & Compliance Center. It is possible that these changes [1] address the above limitation, or [2] indicate that a resolution is coming for the above limitation.

Indexing File Types

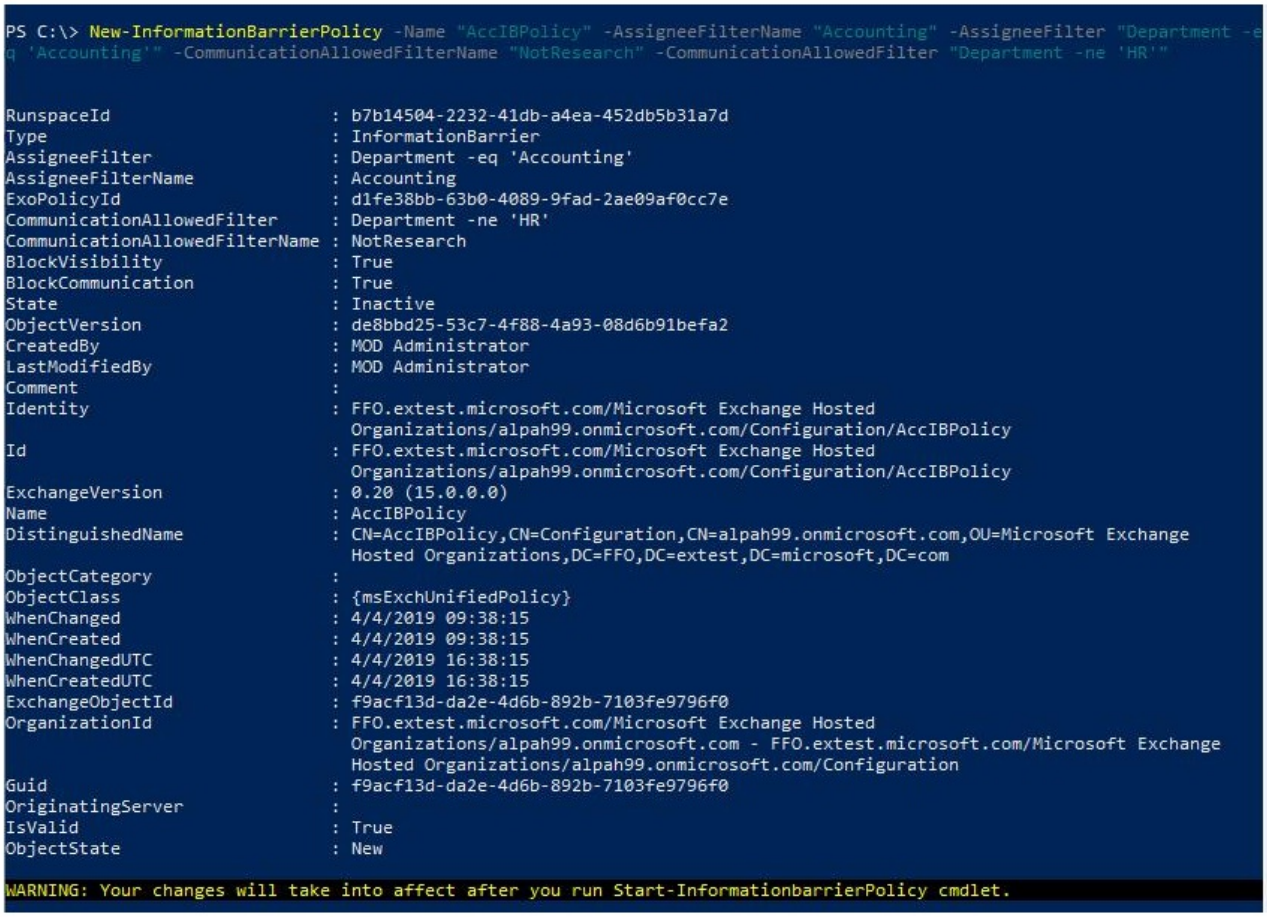
About

- Office 365 can index a specific list of 58 file types, which is weighted in favor of the various file formats in Microsoft Office products.
- [**May 2019**] Microsoft announced that eDiscovery will support full text searches of documents protected with sensitivity labels. See SharePoint Security and Compliance Updates.

Issues for Customers to Consider

- When undertaking an eDiscovery search and performing an Early Case Assessment, any file that is not included in the 58 will be flagged as unprocessed. When applying DLP rules, file types not included in the 58 will not trigger the capture rules. The implication is the need for a manual review of these non-supported file types by a compliance or security officer, adding cost and decreasing timeliness of information exchange.
- Keyword searches may also miss relevant content due to the use of a “best-effort” index. If an organization makes regular use of non-supported file types, it should look at third-party tools that will index additional file types.

Information Barriers in Teams



Information Barriers for Microsoft Teams enforces ethical walls between users of Microsoft Teams in the same tenant. Ethical walls provide policy-enforced methods of preventing specific people from interacting through the tool. Information Barriers was released to preview on April 30.

Capabilities include:

- A new Information Barrier Policy is created using PowerShell cmdlets (above). The policy defines the rules on people who can't interact or share a chat thread, voice call or the same workspace in Microsoft Teams. In the above policy, it seems as through people who work in the Accounting department are being prevented from interacting with anyone who works in the HR department.
- Attempts to cross the Information Barrier - on purpose or accidentally - will be blocked in the user interface. For example, attempting to add a new member to a team who is prohibited by an Information Barrier from joining, will fail because the user will not show in the search results. Likewise, attempting to start a new private chat with a prohibited colleague will fail, and an error message will be displayed.
- Existing communications are checked when a new Information Barrier is created. If violations are identified, corrective action is taken to ensure nothing further is shared, for example, by changed one-to-one chats to read-only, or removing a user from a group chat.
- When released to general availability, Information Barriers will require E5 licensing (Office 365 or Microsoft 365), or an E3 plan with the Advanced Compliance add-on.

Issues for Customers to Consider

- Ethical wall requirements are mandatory in certain industries, such as particular financial services areas. The absence of ethical wall capabilities in Microsoft Teams will have prevented some firms from embracing the toolset, and thus these new capabilities will remove this obstacle.
- Defining via PowerShell is okay for the initial release, but hopefully a GUI approach won't be too far off.

- Ethical walls go much further than just access control. Any Microsoft Team can be configured with limited access rights, therefore preventing people excluded from the access rights list from being able to participate in the content and conversation in the workspace. But access rights can be changed by an administrator at any time. Ethical walls enforce the separation until removed.
- There is no mention of error logging of attempts to cross the Information Barrier. The action is blocked for the user in the user interface, but it is unclear whether the failed attempt is also logged for administrator review.
- Exchange Online also includes ethical wall options, but policies defined for Exchange Online are separate from Information Barriers for Microsoft Teams.

License Required for Ex-Employees' Mailboxes

About

- When an employee leaves an organization, but their mailbox must be retained, it was historically true that a full user license was still required to keep the mailbox. Microsoft has removed this licensing requirement, and so-called “inactive mailboxes” in Exchange Online can be retained free of charge. This means that an administrator can put a mailbox on legal hold and remove the associated user account, thereby freeing up the user account for use by another current employee.
- The mailbox is retained for the duration of the legal hold as an inactive mailbox without incurring any charge to the organization.

Issues for Customers to Consider

- Microsoft has signalled its intent to introduce a new license requirement for inactive mailboxes, originally scheduled to come into force from October 1, 2017. This was going to be priced at US$3 per mailbox per month, or US$36 per mailbox per year.
- After receiving push-back from customers and MVPs, Microsoft revoked the introduction of this cost until further notice. It is likely that inactive mailboxes will attract new licensing terms during 2019 or 2020.

Litigation Hold Capabilities

About

- Legal and litigation hold in Office 365 offers only basic capabilities compared to some third-party offerings.
- Historically, Microsoft offered workload-specific legal hold capabilities for Exchange Online and SharePoint Online, but has recently created a new unified approach in the Security & Compliance Center. It is no longer possible to create new legal holds on SharePoint content from the previous SharePoint eDiscovery Center, and while Microsoft intends to similarly deprecate the ability to create new legal holds on Exchange content within the Exchange Admin Center, customer push-back has delayed its removal.
- The current In-Place Hold in Exchange Online enables the creation of multiple separate legal holds that are transparent to the user, and that can be based on different parameters such as time-based, search query-based, and indefinite (until further notice).

Issues for Customers to Consider

- Current legal holds created in Exchange or SharePoint cannot be migrated into the new experience in the Security & Compliance Center. They are separate objects that must run their course and then expire, rather than being something that can be pulled across for a unified view of current and outstanding legal holds.
- The litigation hold capabilities deal only with content in Office 365, but not content stored elsewhere. Organizations with significant data repositories outside of Office 365 – on-premises and in other cloud services – will require multiple, disparate systems for setting and apply legal holds, creating a complex legal compliance minefield.
- No workflow support for coordinating with data custodians across the organization who may have content that is responsive to the legal hold parameters. While these could be manually created and sent, no audit trail reporting would be created for subsequent review.
- Searches for responsive material are point-in-time, and do not automatically keep the result set up-to-date. Human intervention is required to re-run all current legal hold searches, and then apply a hold to new material.
- Office 365 can search and index only a specific list of file types. If non-supported file types are identified during a content search, they will be flagged for human review. Organizations with file types not on the supported list will face high manual analysis costs for document-by-document review to meet legal requirements.
- After searching for content in Exchange Online, the search preview pane will display a maximum of 200 items for an In-Place eDiscovery Search, listing the mailboxes and items found. However, these items cannot be displayed in the search preview pane; they must be exported to a discovery mailbox for review. Better in-line support for previewing messages directly from the search pane is not available.
- The advanced eDiscovery capability in Office 365 is not “in-place”. The advanced tools provide eDiscovery capabilities within the suite of Office 365 applications and are not integrated directly into the data sources. Therefore, the effort is a two-step process, requiring a search and export for data using the limited Security & Compliance Center capabilities, selecting the advanced eDiscovery center as a destination before one can actually run the advanced tools. Therefore, there is no way to iterate and search on the source data without multiple manual repetitive blind operations.
- For content searches based on multiple keywords, the search results do not show which keyword triggered the inclusion of a specific item. The only way for an analyst to know which keyword was responsible in Office 365 is to set up multiple single keyword searches.

Supervisory Review for FINRA

About

- Certain industry regulations, such as those enforced by the Financial Industry Regulatory Authority (FINRA), require the capture and review of communications between particular people, or people in a specific group, to ensure no nefarious or unauthorized topics are being disclosed or discussed. Office 365 previously offered a Supervisory Review capability that could work with Exchange Online messages, which had a range of issues.
- In May 2017, Microsoft replaced the legacy Supervisory Review capability with a new Supervision tool that requires the Enterprise E5 plan or the Advanced Compliance add-on. Administrators with the correct access permissions can set up one or more supervision policies.
- Microsoft made no changes to Supervision between May 2017 and the end of January 2019, indicating that it is a low priority capability for Microsoft.
- [**January 2019**] Microsoft announced a new version of Supervision that addresses some of the weaknesses and concerns below. See New Supervision.

Issues for Customers to Consider

- Every person who is to be covered by a Supervision policy requires an Enterprise E5 license, or the Advanced Compliance add-on. This is a per-user licensing requirement, not an organizational-level option.
- Supervision works only with Exchange Online in Office 365, but does not address Microsoft's other communication tools, such as Microsoft Teams, Yammer and Skype for Business. This scope of coverage is too narrow in our opinion.
- Once a supervision policy has been set up, a private shared mailbox is provisioned for receiving captured messages. Supervisory reviewers must connect to the shared mailbox to review and assess each message.
- There is no built in workflow to alert reviewers of a new supervision policy that gives them the ability to review messages. Advising reviewers must be handled out-of-band by the person who set up the supervision policy.
- A person can be set as both the person to put under supervisory review and the reviewer of a given policy. There is no checking to enforce segregation of these roles.
- It is not possible to use Microsoft's sensitive information types in Supervision policies.
- When adding conditions to the supervision policy, the words or phrases must match exactly. A mis-spelt variant will not trigger the supervisory rule. It would be useful if Office 365 offered the ability to use fuzzy matching to give a broader impression of what else what happening through Exchange Online.
- The use of Outlook as the supervision interface means that standard Outlook capabilities - such as creating a new email, replying to a message, and deleting a message - are visible in the interface. Note that the delete option for an individual message is greyed out on the tool bar, and clicking the delete button on a single message surfaces a prompt to say you can't delete the message. Clicking the delete all option on the tool bar deletes all messages in the mailbox, but a background process then puts all messages back into the mailbox. These interface elements are confusing and unnecessary.
- The filter options provided within Outlook don't make sense for supervision. There is no ability to sort and filter messages based on content or metadata relevant to the supervision policy.
- Attempting to delete all messages in a supervision mailbox is not audit logged against the messages.
- A supervisor can reply to or forward a message from within the supervision mailbox. There is no ability, however, to audit or review what messages have been sent from the supervision mailbox.
- Microsoft offers no workflow or case management capabilities for messages in the supervision mailbox. An out-of-band process must be used.
- A reviewer with access to multiple Supervision mailboxes must go through each supervision mailbox one-at-a-time. There is no ability to gain a unified view across multiple supervision policies.
- Aside from the name of the supervision mailbox, there is no indication of what the supervision policy settings are or why messages are being collected into the mailbox.
- Supervisory review works only in Outlook on the web. Although an Outlook client add-in has been promised (and one is available that can be installed, albeit with PowerShell commands), it is non-functional and doesn't work.
- There is no migration support between the old Supervisory Review feature and the new Supervision feature. Policies from the previous approach have to be deleted; they cannot be migrated and updated, and they are not automatically updated by

Microsoft.

- While messages are captured for post-delivery or after-the-fact review, there is no ability to quarantine an offending message and have it routed for approval before release. The damage could already be done, since the message has actually been sent and delivered.
    - Note that while Supervision does not support quarantining offending messages, Office 365's Data Loss Protection service offers some capabilities in this area.
- The Office 365 audit log is blind to supervision policies. Creating, editing, and deleting supervision policies are not audit logged.
- While Supervision is positioned as a significant upgrade to the previous Supervisory Review capability in Office 365, the above analysis suggests its capabilities will not be adequate for many organizations.

Supervision 2019

About

- Microsoft introduced a new version of Supervision in late January 2019, which will roll out to eligible customers during February 2019 (our code name is Supervision 2019). See New Supervision. The new version addresses several of the concerns and weaknesses from the previous version - see Supervision 2017.
- Supervision 2019 is positioned to address three use cases: compliance with communications monitoring regulations, internal communications policy monitoring, and identifying risks in communications. For internal communications policy monitoring, the service is being positioned to help with monitoring acceptable use, ethical standards, and the presence of offensive language. For identifying risks, Microsoft suggests that the service can look for unauthorized communications about confidential projects.
- Supervision 2019 enables supervision of Exchange emails, chats and channels in Microsoft Teams, and any third-party data that is imported into Office 365. These three types are supported because all are stored in an Exchange mailbox.
- Supervision policies enable the tracking of users and groups. Tracking a user enables their Exchange email and chats in Teams to be captured for supervision. Tracking a group captures messages in the group's Exchange email and channels in the associated Microsoft Team.
- Adds a browser-based interface within the Security & Compliance Center for reviewing, tagging, commenting and resolving communications items flagged for review. The add-in for Microsoft Outlook is still available, and Outlook on the web can also be used.
- Works with Microsoft's standard sensitive information types and any custom information types defined by the client.
- [**May 2019**] Several new capabilities are due for delivery in May 2019, such as the ability to scope policies to include chat messages from Skype for Business Online, and the ability to set policies to exclude email messages from specified email domains from being captured in the Supervision set. See Supervision 2019 Updates.
- [**Q4 2019**] Microsoft announced that several new capabilities will be added to the review experience in Supervision 2019 by the end of Q4 2019, as well as updates to policy creation (with a new wizard and a new set of pre-configured templates for common policies). See Supervision 2019 Updates.

Issues for Customers to Consider

- Supervision 2017 and the earlier edition only worked with Exchange email messages. Supervision 2019 adds support for chats and channels in Microsoft Teams, and any third-party data that is imported into Office 365 (and thus by design, stored in Exchange). Supervision 2019 does not support other communications modalities that do not use Exchange as the message store - such as Yammer.
- Messages that violate a policy in Supervision cannot be escalated within the Supervision service to the person's line manager, a compliance officer, or the HR department (depending on the type of violation - regulatory or internal policy only). The reviewer must extract the offending message from Supervision and notify or work with other parties outside of its confines.
    - [**Q4 2019**] Microsoft announced that message escalation will be available in Supervision 2019 by the end of Q4 2019. See Supervision 2019 Updates.
- The addition of Microsoft Teams is a good step for Microsoft, but the delay of 24-hours for displaying chat and channel messages in Supervision is unacceptable. As a first-class Office 365 service, messages should be avaliable within minutes, as is the case with Exchange email.

Update Log - eDiscovery

August 2019

August 12 - Compliance Boundaries

May 2019

May 22 - SharePoint Security and Compliance Updates

May 8 - Advanced eDiscovery Updates for Q4 2019

April 2019

April 30 - Advanced eDiscovery Updates at GA - see Weekly News Drop

April 30 - Information Barriers in Microsoft Teams

April 19 - Supervision 2019 Updates

April 19 - Yammer in Europe and eDiscovery

January 2019

January 29 - Updates to Advanced Discovery (managing cases, managing custodians, working sets, review and redact, etc.)

January 14 - Control Over PST Output Size in eDiscovery

January 4 - Searching Encrypted Documents and Emails

July 2018

July 26 - Microsoft announced the beta of new search and tagging capabilities in Advanced eDiscovery, for creating subsets of search results. Most customers will get access to the new beta capabilities in August 2018. After content has been identified through keywords, metadata or the other analysis techniques in Advanced eDiscovery (such as themes), the user can create tags (labels) for specific documents in the result set. The user can choose to only export documents with a certain tag. There is a new search property for creating a result set with only documents having a certain tag. Note that the capability is still in beta and has numerous practical shortcomings at this time. Microsoft acknowledges issues such as only being able to preview 10,000 documents from a given search, being unable to select documents from multiple preview pages, and bulk untagging not working under some conditions.

- See eDiscovery Workflow.
- Announced via Security, Privacy & Compliance Blog.

July 2 - Microsoft released additional eDiscovery capabilities for Microsoft Teams. Summary records for every meeting and call will now be available for an eDiscovery search. This is in addition to the current capability of searching instant messaging transcripts. These summary records are stored in the Exchange mailbox of each person involved in the call or meeting. Note that the summary record shows who joined and when they joined and left, but does not include any details about the meeting. For example, the subject line of the meeting (from an invite) is not included in the summary record. This means a keyword search will not return any summary records on calls and meetings. Note also that it can take up to 8 hours for the call detail record to be available for searching in the Security and Compliance Center.

- See Content Search.
- Announced via Microsoft Teams Blog.

June 2018

June 26 - Using multi-factor authentication with the administrative processes for Exchange Online. When multi-factor authentication is enabled, certain administrative processes in Exchange Online don't work. Microsoft explained how to make various administrative scenarios in Exchange Online work with MFA enabled.

- See eDiscovery Workflow.
- Announced via Security, Privacy and Compliance Blog.

June 1 - Microsoft introduced new eDiscovery capabilities for hybrid organizations, that have Exchange on-premises and some usage of Office 365. The new capabilities address eDiscovery (but not legal hold) for Microsoft Teams. Group chats in a Microsoft Teams channel are unaffected by this change. Those chat transcripts are saved to the group's mailbox in Office 365, and are already available for eDiscovery. The announcement affects person-to-person and person-to-ad hoc group chats through the Chat tab (which Microsoft calls 1xN chats). These chat transcripts will be saved in a new cloud-storage mailbox for each participant in the chat; Microsoft essentially splits the individual's mailbox - with Exchange content remaining on-premises, and Teams content going to a cloud mailbox. The intent is to simplify the transition to the cloud, but decoupling the Exchange migration from the use of newer Office 365 capabilities, such as Microsoft Teams.Microsoft Support must carry out the engineering required to implement the above change. It takes 2-3 weeks to deploy. It is available by application only. Chat transcripts are available for eDiscovery cases, and Compliance Content Search, Preview and Export. Note that chat transcripts are not available for legal hold nor retention policies yet, although Microsoft acknowledges these requirements and is planning its strategy.

- See Content Search.
- Announced via Microsoft Teams Blog.

Encryption - Overview

About

Encryption is used in Office 365 for:

- Encrypting email messages and attachments.
- Encrypting data at-rest.

Encryption of Email Messages and Attachments

Microsoft offers two message encryption services in Office 365. Both were called Office 365 Message Encryption.

- Microsoft does not provide a different version number for the two services called Office 365 Message Encryption.
- One way of distinguishing them is to call the first "Legacy OME" and the second "New OME." In September 2018, Microsoft called the first OME Previous (OMEv1).
- Another way that people outside Microsoft differentiate the two is OMEv1 and OMEv2.
- See Office 365 Message Encryption - Version 1
- See Office 365 Message Encryption - Version 2

Encryption of Data at-Rest

Microsoft encrypts data at-rest in Office 365.

- Hard drives in all Office 365 data centers are encrypted using BitLocker.
    - But - an administrator with physical access to the machine could still access customer data.
- Service Encryption offers additional defense in depth for customer data, thereby preventing administrator access.
- Customers have the option of generating an encryption key to be used in the encryption chain for Service Encryption.
    - See Customer Key

Office 365 Message Encryption - "Version 1"

About

- Office 365 Message Encryption Version 1 was offered until September 2017.
- Replaced by Office 365 Message Encryption ("New OME" or "OMEv2"), which has the same name but is based on a different design. See Office 365 Message Encryption - Version 2.

Capabilities

- Part of the higher-cost Enterprise plans (e.g., Enterprise E3 and E5), and as an optional fee-additional add-on to other plans.
- Message was sent as an encrypted HTML attachment, with support for messages and attachments up to 25 MB in total.
- Intent - that an Office 365 user could sent encrypted email to any recipient without having to know what email service, email client, or encryption capabilities they supported.
- Used the recipient's email address as the public key.
- Messages could only be viewed by the recipient in the Office 365 viewing portal.
- A mobile app was available for iOS and Android, but some people found this difficult to use.
- Powered by Azure Rights Management (Azure RMS).

Critique

- Applying encryption was only a server-side action, via Exchange Transport Rules
  - For manual encryption, the user had to include the right trigger word (such as "encrypt" in the subject line)
  - For automatic encryption, an administrator had to set up rules
- The decision to encrypt a message was triggered largely by manual action on the behalf of the sender. He or she needed to include the word “encrypt” in the subject line (or something similar), which would then be captured by an Exchange transport rule configured to look for that key word. More automated options were also possible through Exchange transport rules, including the recipient being outside the organization and the presence of certain words or phrases in the message.
- On receiving a legacy OME message, the recipient had to save the HTML attachment, open it in a supported browser, and login to the Office 365 viewing portal using an Office 365 or Microsoft account, or request a one-time passcode. Access was also possible on iOS and Android mobile devices, using a special viewer app for OME messages; users on other mobile devices needed to use a supported browser. These additional steps were required even for other Office 365 users using Outlook 2016 for Windows, the premier and most advanced email client offered by Microsoft. There was no support for fully transparent and seamless delivery of encrypted messages between Office 365 subscribers in different organizations.
- Legacy OME was not able to track or alter what happened to a message after it was sent, meaning that a message could not be revoked, and the sender had no insight into what happened to the message. Even though special actions involving the Office 365 service were required by the recipient to access the message, no post-delivery status information was available to senders or administrators.
- Did not offer a transparent, end-to-end encryption service that would automatically encrypt and decrypt messages for both senders and recipients without additional per-message steps and authentication requirements.
- Was offered until September 2017, when it was replaced by “New OME.” Both services have the same name, but are quite different in design.
- Will be deprecated at some point in the future. It is unclear what will happen to the messages sent using legacy OME technology, and for how long the ability to decrypt the message on the legacy Office 365 viewing portal will remain on offer.

Office 365 Message Encryption - "Version 2"

About

- Announced at Microsoft Ignite 2017 in September 2017.
- Replacement for Office 365 Message Encryption "Version 1". The new version has been designed to address some of the shortcomings in Version 1.
  - Note that "Version 1" and "Version 2" are not Microsoft terms for the two services. In September 2018, Microsoft called the earlier version "OME Previous."
  - "Version 2" is positioned as an upgrade to "Version 1", but Version 2 involves a significant re-factoring and change.
- New OME is enabled by default for eligible organizations (beginning February 2018). That means organizations with an Office 365 E3 or E5 plan.

Capabilities

- Leverages Azure Rights Management (Azure RMS) - part of Azure Information Protection - to provide a single method for sending encrypted messages inside and outside the organization.
- Adds support for other sign-in options for recipients, such as a Google account or Yahoo ID.
- Works seamlessly for sending encrypted messages from Outlook on the web to a recipient also using Outlook on the web.
- Increasingly works seamlessly for sending encrypted messages from newer versions of the Outlook for Windows desktop client (the Office 365 ProPlus variant) to a recipient using the newer versions of Outlook for Windows (the Office 365 ProPlus variant).
  - **But** - there are still version differences that render the experience uncertain
  - **But** - Outlook users of Office 2013, 2016 and probably 2019 may experience problems in decrypting OME messages.
- Provides encryption of attached Microsoft documents, such as Word, Excel, PowerPoint, InfoPath and XPS. Encryption while in transit is also offered for PDF documents, although encryption for PDF documents does not persist after the message has been received by the recipient.
- Encryption can be applied manually by the sender or automatically via pre-configured Exchange Transport Rules or Unified DLP in the Security & Compliance Center.
  - Manually by the sender - selecting a toolbar button to apply encryption. This is only possible on a message-by-message basis.
  - Automatically by Exchange Transport Rules - must be configured by an administrator in the Exchange Admin Center.
  - [**September 2018**] Microsoft added the ability to use a DLP rule in the Security & Compliance Center to apply the Encrypt-Only policy to email messages if they meet one or more sensitive information types. See Apply Encrypt Only with a DLP Rule in the Office 365 Security & Compliance Center.
- Is not compatible with Active Directory Rights Management Service. Customers must migrate to Azure RMS before enabling New OME.
- Protected messages sent to an Office 365 Group can be read by all group members, unless the encrypted message template has been scoped to a smaller set of users. Protected messages sent to a Shared Mailbox can be read by everyone with access to the Shared Mailbox, but this only works through Outlook on the web not the Outlook client. Protected messages sent to a channel in Microsoft Teams or a group in Yammer are rejected and not delivered.
- New OME offers two encryption policies:
  - Do Not Forward - both encrypts the message (and attachments) AND limits post-delivery actions by the recipient
  - Encrypt - only encrypts the message (and attachments), BUT does not limit post-delivery actions by the recipient
- Messages protected by either policy can be opened currently in:
  - Outlook on the web
  - Some versions of Outlook for Windows
- [**December 2018**] Microsoft previewed a report on the usage of Office 365 Message Encryption within a tenant. The report shows date sent, sender address, encryption template, whether a user or automated mechanism was used to encrypt the message, recipient address, and subject line. The report states what happened, but does not provide control options (such as revoking access to a given message, or checking on delivery status).
- [**May 2019**] Microsoft released Office 365 Advanced Message Encryption, for Office 365 E5 subscribers only (or those with E3

and the Advanced Compliance add-on). Advanced Message Encryption offers branded email templates, message expiration options (under certain conditions), and message revocation by an administrator (under certain conditions). See Advanced Message Encryption.

Issues for Customers to Consider

- New OME does not encrypt the subject line of the message. This is always passed through in plain text. This was not offered in Legacy OME either, but if it contains sensitive information, that will not be protected by encryption.
    - Generally speaking, OMEv2 offers encryption for Microsoft Office file types only, not for other file types such as PDF. It is focused on organizations using Word, Excel, PowerPoint, InfoPath, and XPS documents. Organizations with non-Microsoft file types in common use will not find OMEv2 of much value.
- In September 2018, Microsoft announced that PDF documents will be supported by the end of 2018. However, the fine print is that while PDF documents will be encrypted in transit, they will not be encrypted once the message is received. This means that PDF documents are handled differently to Office documents, an inconsistency that is sure to lead to data breaches by end users who assume enduring encryption for any email attachment. See Updates to Office 365 Message Encryption.
- New OME has very specific version requirements when working with Outlook for Windows.
    - Numerous users complain that it does not work for their setup.
- Clicking the Protect button in Outlook on the web applies the Do Not Forward policy by default. The end user must click Change Permissions and select Encrypt to use the Encrypt-Only policy.
    - [**January 2019**] In the new version of Outlook on the web (due early 2019), the default has been changed to **Encrypt** (only). This is a good direction for the offering; and the button is now directly called "Encrypt."

- Automatic encryption of messages requires the use of Mail Flow rules in the Exchange Admin Center or the Unified DLP part of the Security & Compliance Center. Rules cannot be set up in the unified Security & Compliance Center, although support for doing so is apparently coming (although there is no Office 365 Roadmap item for this change).
    - This means that Security and Compliance personnel must rely on an Exchange Administrator to set up the rules.
    - It also means there is no unified visibility into the actions that impact mail flow.

- There is no option for an end user to automatically encrypt all messages they send through Outlook. This must be done on a message-by-message basis.
    - Possible option - the user could request that a Exchange Transport Rule be created to automatically encrypt all of their outbound message traffic.

- Encrypted messages sent to recipients using Google Gmail and Yahoo Mail can use their Google or Yahoo identity to decrypt the message in the viewing portal. This is a transparent process for the recipient, but means that:
    - If the sender sends the encrypted email to the wrong recipient, the wrong recipient will be able to access the encrypted message using just their Google or Yahoo credentials. The sender and sender organization cannot demand additional identity verification to assure the message has been received by the correct recipient. This results in a data breach situation that will be difficult for the sending organization to identify.
    - If a user's Google or Yahoo account is compromised, the hacker will be able to use the transparent decryption process to access encrypted messages. This results in a data breach situation that will be difficult for the sending organization to identify.
    - If the recipient's account is compromised, the hacker will be able to send encrypted replies to the original sender and other recipients. This could be used for distributing encrypted phishing messages that are more difficult to detect.

- As with Legacy OME, there is no post-delivery insights or reporting capabilities for OMEv2, nor the ability for the sender to revoke access to the message.
    - **Therefore** - the sender cannot see if the message has been opened by the recipient. Separate messages or calls are required to confirm receipt.
    - **Therefore** - the sender cannot change the encryption status or rights after the message has been sent.
    - **Therefore** - if a sender realizes they have sent a message to the wrong recipient, they cannot know if a data breach situation has occurred or not.
    - **Therefore** - if an encrypted message is marked as spam or filtered as junk mail, the sender has no way of knowing in-band that his or her message was not delivered as expected. Separate messages or calls will be required.

- OMEv2 does not offer the ability to force multi-factor authentication when a recipient accesses an encrypted message. Other encryption products support this capability to improve identity verification and reduce the likelihood of being caught in a data breach situation caused by a compromised account of a recipient.

- The sender of an encrypted message cannot revoke access to an encrypted message from Outlook or Outlook on the Web.

Microsoft introduced a revocation process in 4Q2018 - in preview only - that enables an IT administrator to revoke messages on the behalf of a sender. This requires the administrator to locate the message ID for the offending message (such as through a Message Trace in Exchange Online), and the use of PowerShell cmdlets to complete the revocation process. This is cumbersome, burdensome, and error-prone.

- Revocation by an IT administrator is an all-in process - the message is revoked for all recipients. It is not possible to remove access for a specific recipient only, nor to add a new recipient to the previously sent message. This lack of nuance complicates any existing encrypted email discussions flowing from the original, causing a break in workflow for all recipients.

- The Audit Log in the Security & Compliance Center does not capture the encryption status of messages. If messages are supposed to be sent encrypted, there is no way to verify that this policy was actually applied to a specific message.
  - [August 2018] Reports on messages encrypted with Office 365 Message Encryption will be added to the Security & Compliance Center sometime during late August 2018 and early October 2018. This report will be called the OME Report.
  - **See also** - Audit Logs - Office 365

- Delegates to a mailbox can read the owner's encrypted messages, unless they are encrypted using the Do Not Forward policy. However, the implication of using Do Not Forward for the actual recipient is that the document is read-only, and not available for collaboration.

- OMEv2 is only partially supported on Outlook for Mac. Specifically:
  - [**Receiving**] An OMEv2 message protected with the Do Not Forward policy can be received and replied to as in-line behavior. e.g., it works just like any other message, with the added rights enforced.
  - [**Receiving**] An OMEv2 message protected with the Encrypt Only policy can NOT be received and replied to as in-line behavior; it must be opened using a Web browser.
  - [**Sending**] An email message cannot be protected using the Do Not Forward or Encrypt Only policy template. These are not available in Outlook for Mac.
  - [**September 2018**] Outlook for Mac will fully support OMEv2 in Q1 2019. See Outlook for Mac to Support Office 365 Message Encryption in 2019.
  - [**October 2018**] The timeframe for Outlook for Mac support was brought forward to November 2018, from Q1 2019.
  - [**February 2019**] Outlook on Mac includes the Encrypt button on the Options tab menu when composing a new message. By default it applies the Encrypt template, and the drop-down options include Do Not Forward and several sensitivity labels. For customers who have access to the latest version of Outlook for Mac, this addresses the question of Mac support.

- Users are unable to use the Outlook for Mobile clients - on Android and iOS - for encrypting a message using OMEv2. There is no button or setting available for applying encryption. The only way currently for a message to be encrypted from a mobile device is if an Exchange Transport Rule has been configured that will catch the message.
  - [**August 2018**] Outlook Mobile will offer the ability for labelling messages with a classification and protection policy by the end of 2018.

- Third-party email autosignature products only support encrypted messages if client-side processing is offered by the vendor, because server-side processing is unable to decrypt the message. Client-side processing is not always supported by the third-party vendor, only works in some versions of Outlook when it is offered, and generally doesn't support mobile and native email apps.

Customer Key

About

- Enables customers to add a customer-supplied encryption key to Office 365 for encrypting Office 365 data at-rest.
- Applies to:
  - Customer data stored in mailboxes - for Exchange Online and Skype for Business.
  - Customer data stored in files - in SharePoint Online and OneDrive for Business.
  - Does not apply to data in-transit.
- Announced and released in September 2017, at Microsoft Ignite 2017.
  - Support for government customers (GCC, GCC High and DoD) in July 2018, for Exchange Online only.
  - Support for SharePoint Online and OneDrive for Business due before the end of 3Q 2018
- Requires one of the following plans:
  - Enterprise E5
  - Advanced Compliance SKU added to E3 or other
  - Also requires a subscription to Azure Key Vault

Capabilities

- Exchange Online supports granular encryption policies, with support for up to 50 data encryption policies
  - These are enacted against mailbox groups
- SharePoint Online and OneDrive for Business support only a single encryption policy:
  - For Multi-Geo customers - one encryption policy per multi-geo region
  - For all others - one encryption policy per Office 365 tenant.
- Keys must be stored in Azure Key Vault.
- Keys can be rolled - which means a new version is created.
- Microsoft offers an escrow model in case a customer loses their keys, or their keys are compromised. This is called the Availability Key.
- A customer can revoke their keys to crypto-delete content in Office 365. Microsoft has an approval and sign-off process to make this happen.

Issues for Customers to Consider

- Microsoft offers greater granularity for different encryption policies in Exchange Online than in SharePoint Online and OneDrive for Business.
  - Exchange Online supports up to 50 different encryption policies; these are enacted via mailbox groups.
  - SharePoint Online and OneDrive for Business, by comparison, support only a single encryption policy per Office 365 tenant (or per region in a Multi-Geo setup). Further granularity - such as by Hub Site or SharePoint Site Collection - is not available.
- Only applies to Exchange Online (and Skype for Business data stored in an Exchange mailbox), SharePoint Online and OneDrive for Business.
  - Does not support other services, such as Yammer, Power BI, Microsoft Teams, etc.
- Various setup steps can only be done by PowerShell. There is no UI alternative.

Office 365 Feature	Issues for Customers to Consider
	Various setup steps can only be done by PowerShell. There is no UI alternative.

Applies to some data in Office 365 at-rest: • Customer data stored in mailboxes - for Exchange Online and Skype for Business. • Customer data stored in files - in SharePoint Online and OneDrive for Business. • Does not apply to data in-transit.	Only applies to Exchange Online (and Skype for Business data stored in an Exchange mailbox), SharePoint Online and OneDrive for Business. Does not support other services, such as Yammer, Power BI, Microsoft Teams, etc.
Exchange Online supports granular encryption policies, with support for up to 50 data encryption policies. These are enacted against mailbox groups.	
SharePoint Online and OneDrive for Business support only a single encryption policy: • For Multi-Geo customers - one encryption policy per multi-geo region • For all others - one encryption policy per Office 365 tenant.	Microsoft offers greater granularity for different encryption policies in Exchange Online than in SharePoint Online and OneDrive for Business • Exchange Online supports up to 50 different encryption policies; these are enacted via mailbox groups. • SharePoint Online and OneDrive for Business, by comparison, support only a single encryption policy per Office 365 tenant (or per region in a Multi-Geo setup). Further granularity - such as by Hub Site or SharePoint Site Collection - is not available.
Keys must be stored in Azure Key Vault.	
Keys can be rolled - which means a new version is created.	
Microsoft offers an escrow model in case a customer loses their keys, or their keys are compromised. This is called the Availability Key.	
A customer can revoke their keys to crypto-delete content in Office 365. Microsoft has an approval and sign-off process to make this happen	

•

History

- September 2017 - announced at Microsoft Ignite 2017, and released to General Availability for commercial customers.
  - Excluded - government customers.
- July 2018 - added support for government customers, for Exchange Online only.

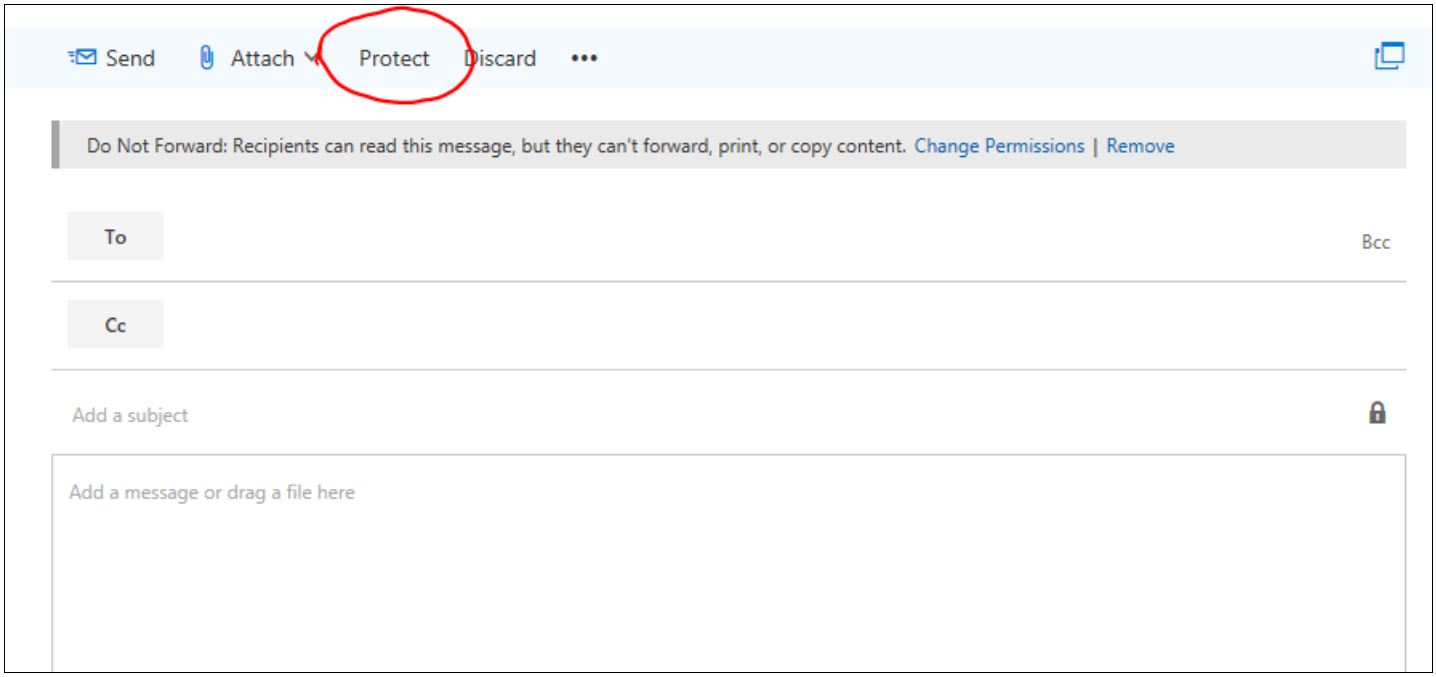
Do Not Forward

About

- Part of Office 365 Message Encryption v2
- Encrypts the message and significantly limits the range of possible actions that the recipient can undertake after receiving the message.
- Released in September 2017 with New OME.

Capabilities

- In Outlook on the web, the user clicks Protect on the toolbar to apply encryption. The default policy is "Do Not Forward," and this is applied to the current message.



Sender Uses	Recipient Uses	Result	Comment
Outlook on the web	Outlook on the web	Seamless	Message is sent and received within Outlook on the web. Message opens for the recipient without requiring any special intervention.
Outlook on the web	Outlook for Windows E3 Plan ProPlus Version 1805 Build 9330.2124 Monthly Channel	Doesn't work	Message cannot be opened in Outlook for Windows

Issues for Customers to Consider

Encrypt Only

About:

- Part of Office 365 Message Encryption v2. Released in February 2018.
- Microsoft says that it "only encrypts the message and attachments"
    - Comparison - the Do Not Forward policy uses encryption and limits access only to the original recipients.

Issues for Customers to Consider

- Encrypt Only was released to overcome shortcomings in the original Do Not Forward policy provided in OMEv2, which tied together encryption and post-delivery rights management.
-
    - **Reality** - Encrypt Only encrypts the message but still uses Azure Rights Management to enforce post-delivery rights management (although on a smaller scale than Do Not Forward)
    - **Implication** - attachments downloaded from the OME Portal by non-Office 365 users could not be opened by the authorised user, even in Microsoft Office applications like Word, Excel, and PowerPoint. There is no way to open these encrypted (and rights protected) attachment.
        - **Therefore** - in June 2018, Microsoft enabled Office 365 Administrators to turn off post-delivery rights management for attachments protected by the Encrypt Only policy.
        - Requires using PowerShell to set.
        - Can only be set as a tenant-level global setting.
        - Only applies to attachments downloaded via the OME Portal. Does not apply in other situations.
        - Unclear what the Office version requirements are for this to work
            - For example - does this work with Office 2010 and earlier?

History

- February 2018 - released as the second encryption policy option in OMEv2
- June 2018 - admin controls introduced for optionally removing post-delivery rights management on encrypted attachments

Azure Rights Management Service

About

- One component of Azure Information Protection. Also called Azure RMS
- Uses encryption, identity, and authorization policies for protection.
- Policies can be applied manually and automatically:
  - Manually by a user selecting a protection policy in Outlook on the web or an Outlook client
  - Automatically by an administrator creating a mail flow rule in Exchange

Issues for Customers to Consider

Update Log - Encryption

May 2019

May 8 - BitLocker Management Using Intune

April 2019

April 30 - Advanced Message Encryption

February 2019

February 12 - Sensitivity Labels with S/MIME Option

January 2019

January 29 - Inspecting Encrypted Files with Microsoft Cloud App Security (not Office 365 Cloud App Security)

October 2018

October 10 - Azure DC Virtual Machines at Public Preview

September 2018

September 25 - a bevy of updates and pending changes for Office 365 Message Encryption. See Updates to Office 365 Message Encryption.

September 8 - the new Encrypt-Only template for Office 365 Message Encryption will be triggerable by a DLP rule in the Office 365 Security & Compliance Center. See Apply Encrypt Only with a DLP Rule in the Office 365 Security & Compliance Center.

September 6 - Outlook for Mac will support Office 365 Message Encryption in the first quarter of calendar year 2019. See Outlook for Mac to Support Office 365 Message Encryption in 2019.

August 2018

August 20 - Microsoft released an end-to-end encryption option for conversations in the consumer version of Skype. Encryption is performed using the Signal Protocol from Open Whisper Systems.

August 2 - Microsoft disclosed that a reporting capability for Office 365 Message Encryption is due in late August to early October 2018. A new OME Reports area will be available in the Security & Compliance Center. See Office 365 Message Encryption - Version 2. Announced via Office 365 Message Encryption Ask Microsoft Anything (August 2018).

August 2 - Microsoft stated that its Outlook Mobile clients for Android and iOS will gain the ability before the end of 2018 to apply a classification and protection label to a given message, such as Do Not Forward or Encrypt Only. See Office 365 Message Encryption - Version 2. Announced via Office 365 Message Encryption Ask Microsoft Anything (August 2018).

July 2018

July 2 - Customer Key is now available for Exchange Online in Office 365 instances for government customers. See Customer Key. Announced via Microsoft TechCommunity.

June 2018

June 13 - Microsoft released new Admin Controls for the Encrypt Only Policy. Enables an administrator to specify whether Encrypt Only OMEv2 messages will have persistent encryption or not, after being downloaded by a non-Office 365 user. Announced and released on June 13, 2018. See Encrypt Only. Announced via Microsoft TechCommunity.

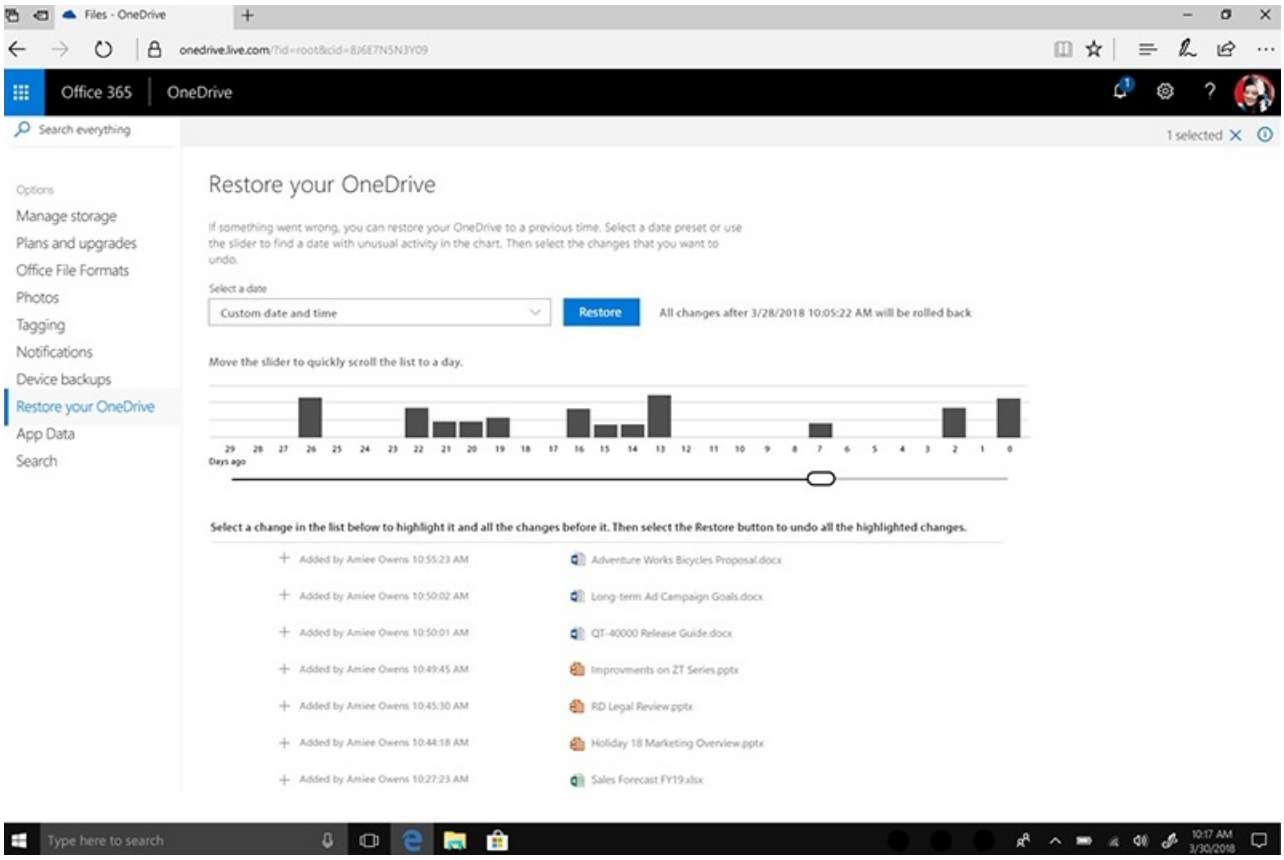
Early June - New support for Office Message Encryption v2. Recent versions of Outlook for Windows now supports OMEv2 via inline display.

File Sharing - Overview

About

- Microsoft is introducing approaches for actively managing the quantity of OneDrive data stored on a local device.
  - [**Example**] In Windows 10 Version 1809, the Storage Sense feature integrates with OneDrive. This allows the user to specify when to remove infrequently used files from their local device; the integration between Storage Sense and OneDrive is opt-in, meaning that is off by default. See Windows 10 and OneDrive Sync Settings.
- Microsoft is going beyond the mere sync of files stored in a folder hierarchy. For example:
  - Files attached to a OneNote page are synced using OneDrive, which means the attached files always stay up-to-date, and can be made accessible via OneDrive (rather than OneNote). See OneDrive Files in OneNote (October 2018)
- Azure Files and Azure File Sync provides an alternative way of enabling file sharing, without using SharePoint or OneDrive for Business.
  - Azure Files is essentially a file server in Azure, providing centralized access to file services.
  - Azure File Sync synchronizes an on-premises file server into Azure Files. The version in Azure Files is then treated as the authoritative and master edition. Azure Files can be synchronized back to on-premises file servers to provide local access to data.
  - See Azure Files and Azure File Sync.
- [**October 2018**] Microsoft offers a recovery service for both OneDrive and SharePoint. Files Restore - available now for OneDrive and from December 2018 for SharePoint document libraries - enables the OneDrive owner or a SharePoint site administrator to roll back to any time from the previous 30 days.
  - See OneDrive Files Restore
  - See Files Restore for SharePoint Document Libraries (October 2018)
- Links can be created for sharing content stored in OneDrive and SharePoint Online, without resorting to emailing a copy as an attachment. Links can be scoped to give only specific permissions to the recipient, such as:
  - [**January 2019**] View-Only No Download - a new type of sharing link that provides view-only access within Office Online, and does not provide the recipient with the option to download the file. See Sharing Links That Block Downloads.
- [**January 2019**] Microsoft announced that a new default file save experience is coming in February 2019, so that Office 365 documents will default to saving in OneDrive or SharePoint Online, rather than a user's device. The default behavior applies to Word, Excel and PowerPoint documents on Windows and Mac. See Streamlining Files to the Cloud.
- [**August 2019**] A near-term version of Windows 10 will use Windows Search for searching in File Explorer rather than the previous File Explorer search experience. By using Windows Search, search results will seamlessly reflect files and documents on the user's device along with files and documents in their connected OneDrive account. See File Explorer Search in Windows 10.

OneDrive Files Restore



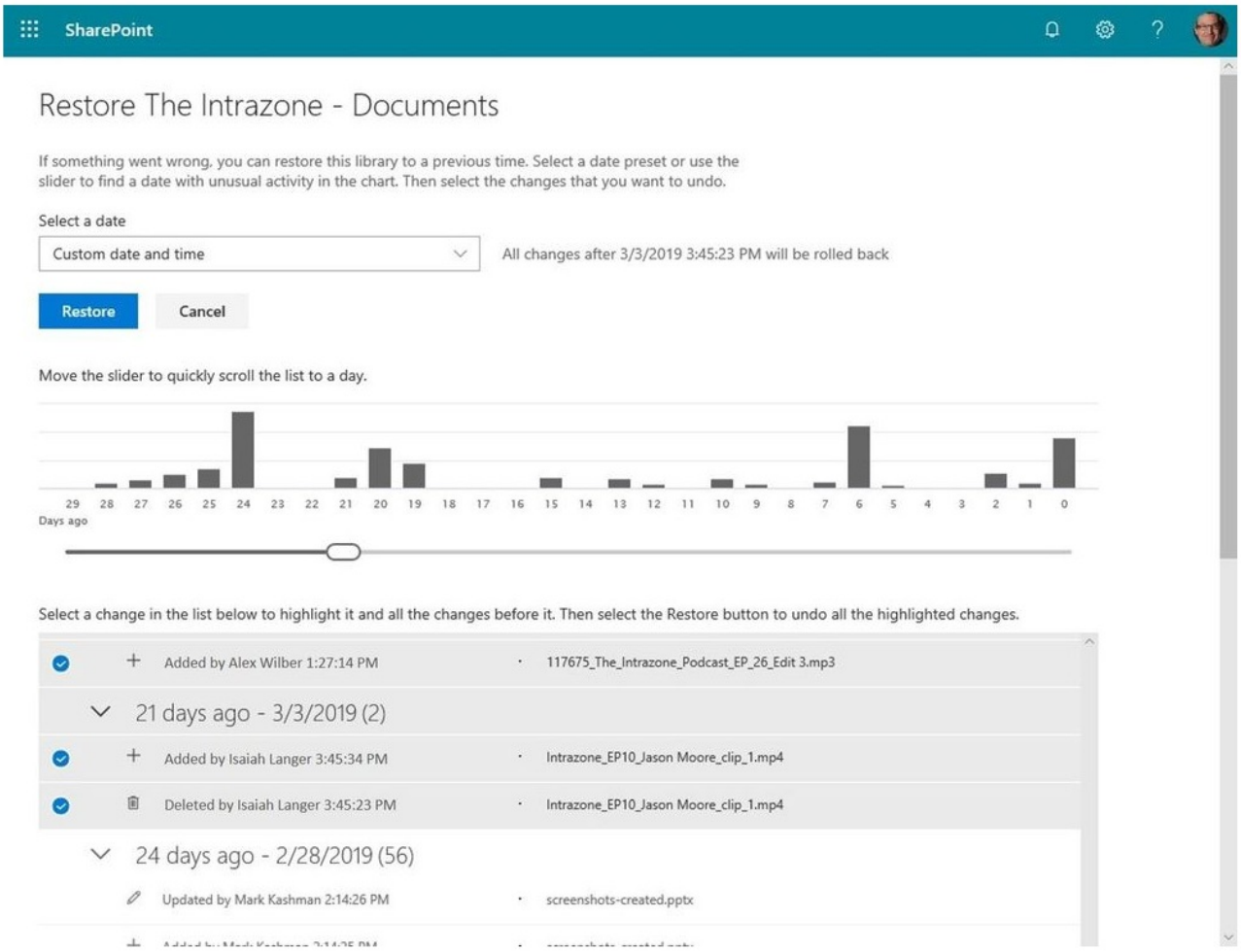
About

- Users with a OneDrive (personal) account and an Office 365 Home or Personal subscription have access to a Files Restore feature. This is designed to enable a user to recover from a ransomware attack, by restoring their entire OneDrive to any point in the past 30 days.
- Files Restore reverts OneDrive to a specific point in time from the past 30 days. It reverts all basic file and folder operations that transpired during the selected time period, but does not support a selective restoration.
- For selective restoration - for example, to recover a file or folder that was deleted accidentally rather than being subject to a ransomware attack - OneDrive offers access to the Recycle Bin for selective restoration, and/or Version History for each file to roll back to a previous version. However, selective restoration is offered on a best-efforts "maybe" basis, not a guaranteed one. See OneDrive and Granular Restore (March 2019).
- If Windows Defender on Windows 10 identifies an in-progress ransomware attack, it will notify OneDrive to cease synchronization operations. The specific date and time of the attack is used as the default roll-back time in the OneDrive file restoration page. A user can choose a timeframe that is earlier or later than this.
- Microsoft extended OneDrive Files Restore to SharePoint document libraries. This was announced in October 2018 and due in December 2018, but was not released until March 2019. See SharePoint Files Restore.

Issues for Customers to Consider

- Only basic file and folder activities are restored - e.g., create, delete, rename, update, move and copy. Sharing and permissions settings are not restored or reverted. These must be applied again.
- Files Restore relies on the Recycle Bin as its source of recoverable files and folders. Any files or folders that have been removed from the Recycle Bin - for example, by the user permanently deleting these items - are unrecoverable.
- Microsoft's examples assume that a ransomware infection leaves the computer operational for the user.

SharePoint Files Restore



About

- [**October 2018**] Microsoft announced that its Files Restore capability in OneDrive is coming to SharePoint document libraries. When announced in October 2018, this was originally due for December 2018. OneDrive Files Restore was the proof of concept. Office 365 subscribers were quick to request support for SharePoint document libraries as well.
  - SharePoint Files Restore was announced as released in March 2019. See Microsoft 365 Roadmap Updates - March 25, 2019.
  - SharePoint Files Restore was actually not released until April-May 2019. See Weekly News Drop - April 26, 2019.
- Files Restore for SharePoint works directly in SharePoint and across Office 365 where a SharePoint document library is surfaced, such as in Microsoft Teams, Outlook groups, and Yammer groups connected to an Office 365 Group.
- The restoration of a document library to a previous state - at any point during the previous 30 days - can be initiated by a site administrator or site owner. The capability is for the entire document library, not for recovering selected folders or files within a document library.
- Restoration is on a library-by-library basis. An administrator does not have the ability to use automation tools to recover multiple document libraries at once.
- Restoration relies on the use of version history. If version history is not turned on, previous versions of a document are not available.

Issues for Customers to Consider

- OneDrive Files Restore has two issues, and it is likely that these will also apply to the SharePoint experience. Specifically:
  - [**1**] Only basic file and folder activities are restored - e.g., create, delete, rename, update, move and copy. Sharing and permissions settings are not restored or reverted. These must be applied again.

    - [**2**] Files Restore relies on the Recycle Bin as its source of recoverable files and folders. Any files or folders that have been removed from the Recycle Bin - for example, by the user permanently deleting these items - are unrecoverable.
- Files Restore applies to document libraries only, not to list items. Since OneDrive doesn't support lists, this capability has not been tested there before bringing it across to SharePoint.

Azure Files and Azure File Sync

About

- Azure Files is a file service in Azure that is designed to offer a new option for centralized file services for organizations. Azure Files offers cloud based file services for single site and multisite organizations, with an option for local access via synchronization to all documents or just a subset of recent and relevant ones.
- Azure File Sync extends Azure Files to local servers that are kept in synchronization in near-real-time. Azure File Sync can be used to migrate documents from a local server into Azure Files, with the migrated version in Azure Files now considered the master version or copy.
- Azure File Sync offers a tiering option, whereby infrequently used documents can be automatically removed from local storage (with a pointer still displayed to the file). The master copy will remain accessible through Azure Files, and an end user can request the file at any time. Another option for tiering includes specifying a threshold for free space on the local server; once this is exceeded, older documents will be automatically removed from the local server (but remain accessible through Azure Files).

Issues for Customers to Consider

- Azure Files has a storage limit of 5 TiB (about 5.5 TB). This is insufficient for a centralized file service for most organizations.
- Azure Files and Azure File Sync does not offer a distributed file locking capability. This means that two people can open the same document from their local access server, and both copies of the document will be saved separately, with one noted as the conflict version.
- Azure Files and Azure File Sync does not offer real-time co-authoring and co-editing. These capabilities are offered for documents stored in Office 365 (SharePoint Online and OneDrive for Business), but not in Azure Files.

Update Log - File Sharing

September 2019

September 3 - Shared With Me in OneDrive

August 2019

August 22 - SharePoint Files Restore Failure

August 21 - File Explorer Search in Windows 10

July 2019

July 3 - Automatic Guest Account Creation in Azure AD

June 2019

June 25 - OneDrive Personal Vault

May 2019

May 21 - OneDrive Updates at SharePoint Conference 2019

March 2019

March 25 - Microsoft 365 Roadmap Updates - Time to Read and Inside Look to Files for OneDrive for Business.

March 25 - Microsoft 365 Roadmap Updates - Per Machine Install of Sync Client for OneDrive for Business.

March 25 - Microsoft 365 Roadmap Updates - Recommended View on Web for OneDrive for Business.

March 25 - Microsoft 365 Roadmap Updates - SharePoint Files Restore due in March 2019.

March 13 - Microsoft 365 Roadmap Updates - Updates to File Hover Card - OneDrive and SharePoint, Full-Fidelity Shared Libraries in OneDrive, and Customized Help Link for External Sharing in OneDrive for Business

March 12 - OneDrive and Granular Restore

January 2019

January 15 - No More Tenant-Level Opt-Out of Modern SharePoint

January 1 - New Files in Yammer Stored in SharePoint

January 1 - OneDrive Gains Fluent Update

January 1 - Sharing Links That Block Downloads

November 2018

November 15 - Access Requests from SharePoint Online

November 15 - OneDrive for Business Updates

October 2018

October 17 - Files Restore for SharePoint Document Libraries

October 17 - OneDrive Files in OneNote

August 2018

August 29 - New page added - OneDrive Files Restore

August 12 - Windows 10 and OneDrive Sync Settings

July 2018

July 19 - Azure File Sync released to General Availability. See Azure Files and Azure File Sync.

July 19 - The OneDrive client for Windows will automatically pause sync when the Windows device goes to battery saver mode, and resume when it goes out of battery saver mode. The user has an option to override this pausation. Announced in July, and will start rolling out during July 2018. See Microsoft TechCommunity.

July 19 - The OneDrive Activity Center has a new look for showing the status of the OneDrive desktop client. Announced in July, and will start rolling out from late July 2018. See Microsoft TechCommunity.

July 11 - Gartner placed OneDrive in the Leaders quadrant for its Content Collaboration Platforms Magic Quadrant. Microsoft is ranked as the vendor with the highest ability to execute. See Microsoft 365 Blog

Security

Overview

Safeguarding people from security threats and securing corporate data is critical in the current threat landscape. Verizon's Data Breach research found that more than nine out of 10 security breaches begin as a phishing or spear phishing attack, one in 14 people opened a malicious attachment, and one-quarter of users have been compromised more than once. The rise of ransomware has taken the threat level from critical to extreme. There were many examples in 2017 where the lack of effective cybersecurity measures became horrifically expensive:

- The international shipping company Maersk, for example, spent almost US$300 million to recover from the NotPetya ransomware attack in mid-2017, and had to re-install its complete IT infrastructure from scratch over 10 days: 4,000 servers, 45,000 PCs, and 2,500 applications. The firm had to revert to manual processes during these 10 days to track an average of one ship laden with 10,000 to 20,000 containers docking at a port somewhere in the world every 15 minutes.

- A more recent example is the SamSam ransomware attack that impacted the Colorado Department of Transportation in late February 2018, forcing the organization to shut down more than 2,000 computers so that the attack could be investigated.

Business email compromise, also known as whaling, CEO fraud, and imposter email, adds another vector of immediate financial threat to organizations. Figure 2 shows the security concerns and capabilities that are of greatest interest to organizations that have adopted Office 365 or plan to do so.

Importance of Various Security Concerns and Capabilities
Percentage Responding "Important" or "Extremely Important"

Capability	%
The ability to block zero-day threats	92%
The ability to detect and block all known threats	92%
The ability to block advanced threats	92%
The ability to block ransomware attacks	92%
The ability to detect and block email fraud and email spoofing	91%
The ability to block spear phishing attacks	90%
The ability to remove active content and other components in an email that might be malicious	83%
The ability to offer multi-factor authentication to manage user access	79%
The ability to block malicious files on OneDrive and SharePoint	76%
Maintaining control over third-party app access to Office 365 resources	76%
The ability to centrally manage policies across all communication channels, both within Office 365 and on other platforms	74%
The ability to block internal email threats	73%
The ability to plug in third party anti-malware, anti-spam and other security capabilities to Office 365	72%
Integration points into our security ecosystem (such as web, network access enforcement points)	67%
Support for an outbound email quarantine	64%
The ability to leverage a third-party two-factor authentication or multi-factor authentication solution	64%
The ability to audit and reverse retractions	59%
The ability to retract emails after they are sent	56%
The ability to retract documents once they are sent	56%
The ability to protect the personal email of employees, as well as enterprise email	51%

Source: Osterman Research, Inc.

Effective security must include measures to protect people and data on all channels. Organizations should seek solutions that provide integrated threat insights across both email and SaaS applications. By integrating threat insights, these solutions can limit access to sensitive data using compromised user credentials.

This section reviews the security capabilities on offer in Office 365, highlighting current capabilities and areas of concern.

Office 365 Advanced Threat Protection

About

- A security service in Office 365 that focuses on protection against advanced threats. Common acronym is **ATP**.
- Offers five services: Safe Links, Safe Attachments, Spoof Intelligence, Quarantine, and Advanced Anti-Phishing.
  - Safe Links - designed to identify certain threats in URL links.
  - Safe Attachments - designed to identify threats in Office documents.
  - Spoof Intelligence - insight into which senders are spoofing your domain or external domains sending to you, and the capability to allow or deny this spoofing.
  - Quarantine - suspect messages are moved to a quarantine area, rather than each user's Junk Mail folder. Also offered in Exchange Online Protection.
  - Advanced Anti-Phishing - control over what to do with phishing messages. From September, some anti-phishing capabilities will be added to Exchange Online Protection.

Feature	ATP standalone	Exchange Online Protection
Safe Links	Yes	No
Safe Attachments	Yes	No
Spoof intelligence	Yes	No
Quarantine	Yes	Yes
Advanced anti-phishing capabilities	Yes	No

- Available as part of the more expensive Enterprise E5 plan (US$35 per seat per month). It can also be licensed as a separate add-on.
- [**January 2019**] Microsoft is splitting the current Advanced Threat Protection add-on plan into two tiers, with the current capabilities now called ATP Plan 1. The new ATP Plan 2 will include Plan 1 plus Threat Intelligence (which was not previously included in ATP). After the introduction of the two new plans, the above table will require another column, as below. See ATP Splitting Into Two Plans.
  - [**July 2019**] Microsoft added the ability for customers on ATP Plan 1 to create a custom phishing alert for the activity type "Phishing email detected at time of delivery." This was previously only available in ATP Plan 2. Available July 2019. See Weekly News Drop - July 5.

Feature	Exchange Online Protection	ATP Plan 1	ATP Plan 2
Safe Links	No	Yes	Yes
Safe Attachments	No	Yes	Yes
Spoof Intelligence	No	Yes	Yes
Quarantine	Yes	Yes	Yes
Advanced Phishing Capabilities	No	Yes	Yes
Threat Intelligence	No	No	**Yes**

- ATP focused solely on Exchange Online until December 2017. From December, Microsoft expanded coverage for content at rest to SharePoint Online, OneDrive for Business, and Microsoft Teams. Files that are identified as malicious are blocked in place, so they cannot be opened, downloaded, or shared.
  - [**October 2018**] Microsoft announced that Safe Links protection will be added to Microsoft Teams in Quarter 2 of

CY2019. See Safe Links in Microsoft Teams.

- In September 2018, Microsoft introduced Microsoft Threat Protection. Office 365 Advanced Threat Protection is one of the services in the portfolio.
- In October 2018, Microsoft claimed that due to its investments over 2018 in phishing technology, it now has the lowest rate of missing phishing emails. See Microsoft's Phish Miss Rate - From Highest to Lowest?
- [**March 2019**] Microsoft is almost ready to release its initial Automated Incident Response playbooks to Office 365 Advanced Threat Protection. The two playbooks almost ready for release are User Reported Phish and Weaponized URL, and the intent of each playbook is to automatically collect additional insight, correlate threat signals, and neutralize the threat. See Update on Microsoft Threat Protection.
    - [**April 2019**] Microsoft released the two initial playbooks to public preview. See Weekly News Drop April 5.
- [**March 2019**] Microsoft is working on ways to strengthen the investigation capabilities available to administrators for examining phishing messages and potentially malicious URLs in messages. See Threat Explorer Updates.
- [**July 2019**] Microsoft is adding the option for full pre-delivery URL detonation for links in email messages. If enabled, the setting will scan URLs before an email is delivered to the end user. This may have some negative consequences, however. See Synchronous URL Detonation.

Issues for Customers to Consider

- **No Default Policies**. ATP offers the possibility of checking attachments and links for unknown and emerging threats, but before it can do so, an administrator must set up policies to apply Safe Attachments and Safe Links to individuals, groups and the organization. No threat protection is on by default, and even when it is on, users must be connected to Office 365 in order for Safe Links and Safe Attachments to work.
- **Content Not Actively Scanned**. While ATP newly supports content at rest in SharePoint Online, OneDrive for Business and Microsoft Teams, not all content is actively scanned in place for embedded threats. Files are scanned based only on various selection criteria, such as sharing activities, guest access, and other threat signals. ATP cannot provide a real-time dashboard of malicious files in Office 365. Additionally, many organizations store content in other SaaS applications, such as Box or G-Suite, which are not covered by ATP.
- **Scanning Latency**. Scanning email attachments for unknown threats using ATP can delay delivery and impact user productivity. When ATP was first released, some customers complained that emails were being delayed by 10-15 minutes on average, and up to three to five hours at peak times. In late 2017, Microsoft claimed that its average latency was around 60 seconds, but some customers continue to complain into 2018 that the average processing time they experience is unacceptable. Microsoft has introduced various countermeasures to reduce the perception of delay, including Dynamic Delivery and Document Preview, the latter of which enables the user to view and edit a safe version of the document while the full document is still being scanned. It remains to be seen how long these safe versions delivered via Document Preview remain safe, as threat actors work actively to circumvent the new controls.
- **No Whitelist**. ATP does not offer a whitelist or other integrated ability to mark particular domains as clear or safe, which is required by customers to bypass processing for internal domains, internal multifunction and copy machines, and trusted partners. This lack of granularity and fine-grained controls within the settings for ATP can make it difficult for organizations to tailor the service to their environments.
- Safe Links will check a URL at time-of-click against known blacklists of malicious sites. It does not actually evaluate for the presence of threats at the destination URL at time-of-click. Safe Links will pass a user through to a malicious web site if that site is not on a blacklist of known malicious sites. Some third party solutions offer dynamic URL scanning to check suspicious URLs before the time-of-click.
- Safe Links evaluates URLs at time-of-click, but once a link is evaluated as malicious when a user clicks it there is no ability for Advanced Threat Protection to remove instances of the same email from other user mailboxes.
- Microsoft is partially adding detonation to its URL checking repertoire through an integration with Safe Attachments. Documents linked via a URL in an email or document will now be detonated at time-of-click in Safe Attachments (for supported file types – such as Word, Excel and PowerPoint – and PDF documents as well). Sometime in the future Microsoft expects to use actual denotation for all URLs, although this is not yet available. Other, best-in-class solutions offer full URL detonation, which can detect malware-free attacks, such as credential phishing.
- Safe Links is designed primarily with users of Word, Excel and PowerPoint in mind, as long as they are using the Office 365 ProPlus versions on Windows or iOS and Android devices and are signed into the Office 365 service. It does not check links in

other file formats, when the user is on a Mac, and as above, the link is “checked” only against controlled blacklists rather than actually checking to see if the link is currently safe for the end user.

- Safe Attachments uses virtual sandboxing to assess the presence of malware and other threats in a document. This approach is not effective against certain types of threats like password-protected ransomware sent with the password in the body of the email. Competitive offerings go beyond sandboxing on virtual machines, and include the next-generation of advanced detection mechanisms, such as deep content inspection, recursive analysis of embedded documents, evaluation of threats below the application and operating system levels, identification of dormant code, sandboxing on controlled physical machines to analyze for malware that evades virtual sandboxing detonation, and more. Microsoft's ATP is not on par with some best-in-class, advanced, third party offerings on the market.
- The new capabilities in Safe Attachments have been available for a couple of months as of this writing. It is unclear yet whether Microsoft's latest engineering investments will be enough to identify new and emerging malware threats in documents, because previously unsafe attachments have been treated as safe by the service. Various ways of getting around the protections in Safe Attachments have been exploited, such as by using large files, zipping a file twice, obfuscating the injection of macros, delivering zero-kilobyte file attachments that trigger malware, and locally-produced files that conceal malicious coding, among others.
- Safe Links has previously been tricked into approving malicious links for end users. For example, the Punycode limitation has been exploited to deceive the malicious link checker with the safe ASCII version, while then using the Unicode version of the link to direct the browser to a malicious site. Malicious actors are constantly evaluating how to evade Microsoft's controls.
- Neither Safe Attachments or Safe Links are effective against whaling or CEO fraud messages that typically contain no dangerous link and no attachment. Some third party solutions offer dedicated whaling and spearphishing protection, including protection against homograph domain attacks.
- Customers cannot monitor the status of ATP within Office 365; its service health is bundled with other services. This means that customers paying the additional cost for the service cannot know if the service is currently impacted by an outage or other degradation, or is just being non-performant.
- ATP lacks hybrid capabilities, meaning that customers with Exchange or SharePoint on-premises, for example, must have a second and separate threat-protection offering. ATP handles only certain Office 365 workloads under specific conditions, and does not address data and systems beyond Office 365. This can cause problems with many customers operating a hybrid environment.
- Coverage by ATP requires each recipient to be licensed, along with an applicable policy to be configured for Safe Attachments and Safe Links scanning. If a covered recipient forwards an email with attachments to a non-covered recipient, ATP will not provide any security services.
- Microsoft is itself pushing threat protection beyond ATP in Office 365, with a new service in preview called Azure Advanced Threat Protection. This supplementary add-on service correlates multiple data sources, network traffic, event logs, VPN data and other signals from Windows Defender and Microsoft Edge to identify malicious activity.
- Microsoft says that ATP and EOP together only identify 600 million emails out of 400 billion emails each month as being malicious; this is a malicious catch rate of only 0.0015%. ATP and EOP together fail to see anything more, which is why so many malicious emails are still delivered to user inboxes. See Threat Protection Review and Assertions (September 2018).
- For the added cost of ATP, the service suffers from some important issues. While organizations that meet some use cases may get adequate protection from ATP, the risk landscape means that organizations would be well advised to consider alternative offerings that provide more advanced protection.

Credential Phishing and Email Fraud

About

- Credential phishing and email fraud are social engineering attacks that do not use malicious links or malicious attachments. These attacks are generally targeted at specific people (hence creating very low volumes of messages), use impersonation techniques, and request access to credentials or financial resources with convincing sounding reasons. They are usually malware-free, compelling, and have been very effective at gaining direct financial payments from organizations that have been attacked. Best-in-class tools to address these issues offer a multi-layered approach to these low-volume, malware-free attacks. These solutions go beyond detecting exact-match domain spoofing and basic authentication; they scan email data and content using classifiers to catch suspicious requests and look-alike domains.
- ATP capabilities in Office 365 often cannot stop credential phishing and email fraud because, while the intent of the message is malicious, its contents and any payload are not. Office 365 failed to identify several high profile malware-less attacks during 2017-2018, including the attacks impersonating well-known brands like DocuSign, the Bank of America, and false Office 365 login requests used for credential harvesting.
- [**June 2019**] Research by Barracuda on data from March 2019 showed that 29% of organizations had at least one account compromised in their Office 365 tenant, and these were used to distribute more than 1.5 million malicious and spam emails. See Barracuda on Account Takeover.

Issues for Customers to Consider

- Microsoft does not seem to be able to reliably identify credential phishing attempts that lead to an impersonated Office 365 login screen. During 2018-2019, many such emails have been delivered to end users. Since neither the payload nor link itself is malicious, Advanced Threat Protection offers no benefit. Microsoft appears to lack the ability to reliably identify impersonated message content for its own service.
- Protecting users from being impersonated by others requires manual action by an administrator to create an anti-phishing policy and list each specific sender to protect. This list must be kept up-to-date manually by the administrator, since integration with Azure AD based on job roles is not supported—for example, to protect a new Vice President or CEO. This creates a time consuming and error prone situation.
- Office 365 will notify the recipient of a suspicious message that spoofs the organization's domain name, but the match must be exact. This protection in Exchange Online Protection works without reliance on explicit SPF, DKIM and DMARC settings; the capability was previously called the Exact Domain Spear Phishing Protection service, but that name is not current terminology. Office 365 does not deal with near matches due to similar domains that look or sound similar to the organization's domain (e.g., rnicrosoft.com vs. microsoft.com), and unless the higher priced Office 365 plans are used (e.g., E5), will struggle to identify email fraud messages that have been sent by compromised internal accounts. With impersonation attacks through the takeover of legitimate mailboxes on the rise, Office 365's lack of standard advanced detection capabilities is worrisome.
- Traditional methods of classifying spam based on message volume do not work for classifying credential phishing and email fraud messages. Email fraud may be perpetuated through but a single message.
    - [**July 2019**] Microsoft is introducing greater reliance on the Anti-Phishing Policy for managing anti-spoofing for intra-org spoof and DMARC failures. The change will classify more messages that fail email authentication checks as phishing attempts rather than spam, giving tenant admins the ability to deal with phishing attempts more harshly than plain spam.
- Office 365 does not provide a simple method to remove emails from the mailboxes that have passed through filters. Without reverting to PowerShell, there is no way to remove an email across multiple mailboxes and no simple way to revert any retraction. The same problem applies to DLP in Office 365, since if information is leaked internally there is a need to take action to remove this information.
    - Using the *New-ComplianceSearchAction* PowerShell command for purging phishing emails can only soft delete messages, which leaves phishing emails accessible to end users if they recover deleted items via Outlook or Outlook Web Access.
    - Zero Hour Auto Purge (ZAP) only works with spam and malware-based messages, not phishing and impersonation ones.
- Spoof Intelligence manages users, addresses and domains that are permitted to spoof the organization's domain. This provides protection to their own internal users and any business partner or customer who receives valid or invalid email from their domain. Spoof Intelligence is part of the Security & Compliance Center. It should be noted that granular policy control is not

available for Spoof Intelligence, instead the feature can only be set to “on” or “off”. Additionally, reporting functionality for this tool is limited. Spoof Intelligence was initially released for customers on the Enterprise E5 plan (or those with the ATP add-on), but was made generally available as part of EOP in August 2018.

- Common email authentication mechanisms, such as SPF, DKIM and DMARC, are able to identify brand-spoofing when implemented correctly. They are not, however, so effective at identifying brand-spoofing where look-alike or sound-alike domain names with their own strong email authentication are used. Capturing and appropriately classifying such messages requires going beyond the common email authentication approaches.
- Microsoft analyzes 400 billion emails each month, and of these, only detects 600 million as being malicious. That translates to a malicious identification rate of only 0.0015%. This rate is Microsoft's own assertion as to the malware catch rate of ATP and EOP together. If Office 365 ATP and EOP together only identify 0.0015% of all email as malicious, then its services are fundamentally broken and ineffective. This would explain why end users still receive many malicious emails every day; ATP and EOP just can't see the malicious intent. The services don't work, because 99.9985% of the email stream is flagged as non-malicious. In user terms, assuming 150 million active users of Office 365, that's roughly 2700 emails per person per month, or around 120 per business day (sent and received). Microsoft's catch rate of 0.0015% stops four (4) messages per month per user from getting delivered. Undoubtedly these four messages per month per user are serious threats and should be stopped, but many other threats still get delivered.

Exchange Online Protection

About

- A messaging security service in Office 365. Common acronym is **EOP**. Offers good, basic protection.
- Focused on identifying known threats.
- From September, Microsoft is adding enhanced anti-spoofing capabilities from Advanced Threat Protection into the baseline Exchange Online Protection offering.
- Can be extended through Advanced Threat Protection, which adds protection against unknown and new malware and email threats.
- In September 2018, Microsoft introduced Microsoft Threat Protection. Exchange Online Protection is one of the services in the portfolio.

Issues for Customers to Consider

- EOP does not currently provide a catch-rate aligned with best in class third-party solutions. Improving the performance of EOP requires the addition of custom rules and configurations which are beyond the skills of many IT teams.
- Some customers report poor recognition of phishing attempts, including attacks that impersonate Microsoft products like Office 365, Outlook and SharePoint, which contain links leading to dangerous payloads. Moreover, EOP offers no specific whaling detection tool and first stage-baiting messages are often delivered to end users who may answer them, thereby allowing the spammer to go to the next step.
- The default EOP configuration allows users to easily access their Office 365 junk folder and release any message. Once a message has been released, the user can then click on any dangerous link or open any dangerous attachment it may contain. Since many security breaches are user-based, third party solutions that offer a low false positive rate allowing for centralized quarantine management better protect organizations against their own users.

Identification of Sensitive Data

About

- Sensitive data can be identified using the content inspection capabilities of Data Loss Protection, and the Data Governance capabilities available in Enterprise E1 and Enterprise E3 that can be used to set up labels that end users can manually apply to flag content as sensitive in Office 365.
- More advanced capabilities for sensitive data and data governance require the Enterprise E5 plan, which can automatically label content for retention based on keyword queries and sensitive information types.
- Another added cost option is the new Azure Information Protection service, which can classify and/or protect content based on manual and/or automatic identification of sensitive data at-rest. It is important to select solutions that cover data not only at rest, but also in motion.
- [**October 2018**] Microsoft will add the ability to create a custom sensitive information type using the user interface of the Security & Compliance Center. Previously this could only be accomplished using an XML file. See Office 365 DLP Updates.
- [**March 2019**] Microsoft released to public preview new capabilities for detecting credentials stored in documents, systems and applications without appropriate controls. The initial short list of credentials that can be detected focus exclusively on Azure (with one exception), but wider support on multiple levels is planned. See Credential Detection Using Azure Information Protection.

Issues for Customers to Consider

- Analyzing content for sensitive data relies on the Sensitive Information Types provided by Microsoft, or a custom-definition created by the customer. Sensitive data matching is simple to circumvent to exfiltrate data; the matching algorithms look for exact matches and are easy to trick. For example:
  - Matching a credit card number can be circumvented by changing any one of the 16 digits into the equivalent word. For example, writing the last four digits as "997four" will not match against the credit card regex.
  - Matching a SWIFT code can likewise be circumvented by changing a digit to a word, or a letter to the Air Force alphabet equivalent. For example, instead of writing the SWIFT code of WPACNZ2W (which will be matched against the sensitive information type), writing it as WPACNovemberZ2W will not trigger a match, and therefore not be caught by the DLP rule. This is even when the email subject line and the email body specify that a SWIFT code is included in the message.
  - In summary, matching sensitive data requires too much perfection in how sensitive data is formed in a message, and does not use a balanced evaluation for the presence of sensitive data.
- Even without attempting to deliberately obfuscate the presence of Sensitive Information, messages containing sensitive information are missed by DLP policies if explanatory metadata is missing from the email. For example, an email that contains a Social Security Number but not the explanatory phrase "Social Security Number" does not trigger a DLP policy looking for Social Security Numbers.

Microsoft Cloud App Security

About

- Microsoft's Cloud App Security Broker (CASB). This is the full version of Cloud App Security, and should not be confused with the Office 365 Cloud App Security offering. The latter is scoped to provide enhanced visibility into usage of Office 365 apps, along with details on usage of some third-party cloud apps and productivity apps that work with Office 365.
- Microsoft Cloud App Security is NOT included in any Office 365 plans. It comes as part of Enterprise Mobility + Security, or as part of a Microsoft 365 plan.
- **Other Cloud Platforms**. Microsoft Cloud App Security provides visibility into activities on other cloud applications, including SaaS, IaaS and PaaS offerings.
    - e.g., Amazon Web Services - S3 Buckets. Microsoft Cloud App Security can identify misconfigured S3 buckets (and automatically take a governance action or alert for manual intervention), and record login and other activities.
    - e.g., SharePoint Online in Office 365. For example, a file can be blocked in real-time from download based on the existence of sensitive data in the file.
    - e.g., Files and folders in Box that have public sharing status, and are this vulnerable to brute force scanning.
    - [**May 2019**] Microsoft added a Discovered Resource tab to Microsoft Cloud App Security, for providing visibility into custom applications hosted on Amazon Web Services, Microsoft Azure and the Google Cloud Platform. See Discovered Resources in MCAS.
    - [**May 2019**] Microsoft extended its support for apps running on IaaS and PaaS offerings, including Microsoft Azure, Amazon Web Services, and Google Cloud Platform. The extended support provides visibility into which custom apps are running, and details on storage accounts being created. Data reported includes what resources exist, users who are accessing each resource, and how much traffic is being transmitted.
- **Integration with Windows Defender ATP**. Microsoft introduced an integration between Microsoft Cloud App Security and Windows Defender ATP, so that usage data from Windows 10 devices (that are enrolled) will be fed to Microsoft Cloud App Security. This provides a broader picture of cloud app usage across the organization, irrespective of which network a device is connected to.
    - [**Preview**] September 2018. See Microsoft Cloud App Security and Windows Defender ATP for Discovery
    - [**General Availability**] March 2019. See Microsoft Cloud App Security Updates
    - [**March 2019**] With the broadening of Windows Defender ATP to support macOS devices (and the renaming of the service to Microsoft Defender ATP), it logically follows that usage data from enrolled Mac devices should at some point also be fed to Microsoft Cloud App Security.
- In September 2018, Microsoft introduced Microsoft Threat Protection. Microsoft Cloud App Security is one of the services in the portfolio.
- **OAuth Applications**. Microsoft Cloud App Security can report on OAuth applications that have been approved against Office 365, Salesforce and G Suite. Applications can be blocked by an administrator, and alert policies created to alert on new approvals. See OAuth Threat Monitoring in Microsoft Cloud App Security.
- **Roadmap 2018-2019**. At Ignite 2018, Microsoft offered several insights into the roadmap for Microsoft Cloud App Security, including additional real-time session controls for other Microsoft cloud services, more advanced DLP capabilities, improved integration with Windows Defender ATP, and support for non-browser-based apps, among others. See Microsoft Cloud App Security - Roadmap Updates.
- **Alerts**. From December 2018, alerts related to Office 365 apps and services will also be displayed in the Alerts view in the Office 365 Security & Compliance Center. This will provide a unified alerting plane on Office 365, drawing on the additional signals captured through Microsoft Cloud App Security and Office 365 Cloud App Security. See Microsoft Cloud App Security Alerts.
    - [**May 2019**] Exporting alerts to CSV from the Alerts dashboard now includes the date the alert was resolved or dismissed.
- **Integration with Azure AD Application Proxy**. Microsoft Cloud App Security can be integrated with Azure AD Application Proxy, so as to use the real-time conditional access policies from Microsoft Cloud App Security when accessing on-premises web apps that are connected via Azure AD Application Proxy to Azure AD credentials. See Real-Time Microsoft Cloud App Security Controls for On-Premises Web Apps.
- [**December 2018**] Microsoft added two new policy rules to detect suspicious activities in a user's inbox. The first new policy

alerts on suspicious inbox forwarding rules, and the second on suspicious inbox manipulation rules. See New Rules in Microsoft Cloud App Security. The changes also apply to Office 365 Cloud App Security.

- [**January 2019**] Microsoft added a Session ID field to Exchange Audit Log records, enabling the differentiation of actions performed by a user authenticated against Azure AD. Microsoft Cloud App Security could leverage this new unique field value in policies to automatically detect and alert on potential malicious activity within an Exchange mailbox. See Session ID Added to Exchange Online Audit Logs.
- [**January 2019**] Microsoft Cloud App Security can be set to inspect files protected with Azure Information Protection, thereby looking inside encrypted files to ensure sensitivity data is being appropriately protected and to ensure that sensitive data isn't being exfiltrated through obfuscation. See Inspecting Encrypted Files in Microsoft Cloud App Security.
- [**January 2019**] Alerts raised in Microsoft Cloud App Security can be linked to a Microsoft Flow playbook, for adding workflow intelligence, insight, and human perspective into the appropriate action to take when an alert is generated. Microsoft Flow integration is offered in addition to or instead of current alerts for text message and email notifications. See Security Workflows with Microsoft Flow.
- [**March 2019**] In advance of the RSA Conference 2019, Microsoft announced a plethora of updates to Microsoft Cloud App Security. The updates were grouped into four areas: threat protection, adaptive DLP, integrations, and protecting any cloud app. Updates included:
  - **User Risk Overview with Investigation Priority**. Offers an overall assessment of the security risk of individuals, based on the types of alerts being triggered and the user's overall impact to the organization (see Image 1 above). The investigation priority score offers a way for administrators to focus on the individuals posing the greatest risk. The Investigation Priority Score leverages data and signals from multiple offerings in Microsoft Threat Protection.
  - **Sandbox Detonation of Malware in Cloud Storage Apps**. For cloud storage apps connected to Microsoft Cloud App Security via API, files that are potentially malicious will be automatically checked via detonation in a sandbox. Newly uploaded files are examined automatically, and existing files are checked as well.
  - **New DLP Controls**. New control options to prevent unauthorized access to confidential and sensitive information through the DLP engine in Microsoft Cloud App Security. Options include read-only downloads in zero-trust situations, blocking file uploads under certain conditions, and preventing sensitive information being sent through chat and messaging apps, among others.
  - **Integration with Azure Sentinel**. For integrating Microsoft Cloud App Security data with other data sources in Azure Sentinel, Microsoft's new cloud-based SIEM. Sentinel also allows longer retention times for data, and various data visualization options. For background on Sentinel, see Azure Sentinel and Microsoft Threat Experts.
  - **Integration with Power BI**. For data visualization of Microsoft Cloud App Security data. Additional data attributes can be included for analysis as well, leveraging data from Azure Sentinel.
  - **Expanding Cloud App Support**. Direct support for Cisco WebEx and Dynamics 365, and conditional access support for Azure Portal and LinkedIn Learning. Microsoft also introduced a private preview program for organizations wanting to onboard other web apps to Conditional Access App Control.
- Microsoft Data Classification Services can be used as part of File Policies in Microsoft Cloud App Security for inspecting content.
- [**May 2019**] **Scoped Office 365 Workloads**. Microsoft enabled scoping of the workloads in Office 365 connected to Microsoft Cloud App Security. Previously, all of Office 365 was connected. From May 2019, organizations can now specify which workloads they want to connect (and by implication, which ones to exclude).
- [**August 2019**] Conditional Access App Control was released for any cloud, on-premises or custom app, as long as certain requirements are met. See Expanded Conditional Access in Microsoft Cloud App Security.
- [**Roadmap**] The following changes have been advised for Microsoft Cloud App Security:
  - In Q1 2020 - availability to GCC High customers.

Issues for Customers to Consider

- Cloud apps hosted on cloud services platforms such as Fastly and Amazon Web Services are not broken out into a detailed view. App traffic is aggregated and listed as being with the cloud services platform, not the cloud app directly.
  - [**May 2019**] Microsoft extended its support for apps running on IaaS and PaaS offerings, including Microsoft Azure, Amazon Web Services, and Google Cloud Platform. The extended support provides visibility into which custom apps are running, and details on storage accounts being created. Data reported includes what resources exist, users who are

accessing each resource, and how much traffic is being transmitted.

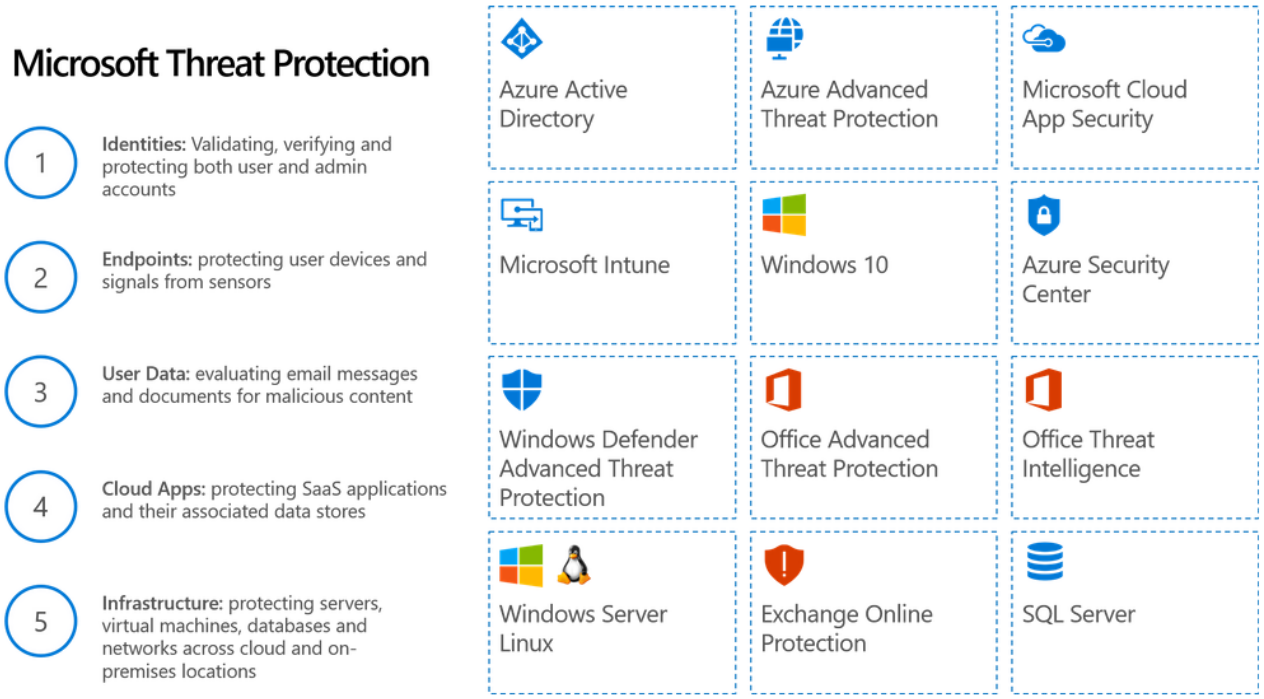
- Microsoft Cloud App Security does not provide a user risk profile, calculated from correlating multiple security threats and events. Microsoft Cloud App Security reports only within the context of the policies that have been configured.
    - While not part of Microsoft Cloud App Security, Microsoft's Azure Advanced Threat Protection service offers a risk-based profile for each user. See Azure Advanced Threat Protection.
- [**January 2019**] **No Cross Tenant Capabilities**. Microsoft Cloud App Security is tied to a tenant, which means that a single instance of Microsoft Cloud App Security is unable to track security events across multiple Office 365 tenants. For instance, in an acquisition situation, security events from the newly acquired organization cannot be fed into the acquirer's Microsoft Cloud App Security instance. Each is standalone. To get a consolidated view, security events from each Microsoft Cloud App Security instance need to be fed into a SIEM or other unifying system.
- [**May 2019**] **Microsoft Cloud App Security Alert Delay**. Several users of Microsoft Cloud App Security (MCAS) have noticed a significant time delay between an event happening and an alert being raised in MCAS. For example, a couple of users say there is at least a 90 minute delay between an impossible travel event being recorded in Office 365 and Azure and the alert being surfaced in MCAS. Similarly, another user commented that uploading a new file containing credit card numbers in contravention of a DLP policy can take up to 2 hours to show in MCAS. See Weekly News Drop (May 17).

Microsoft Defender ATP (Advanced Threat Protection)

About

- Microsoft Defender ATP was previously called **Windows Defender ATP**. It was renamed Microsoft Defender ATP on March 21, 2019.
- Windows Defender ATP is available with the advanced licenses for Windows 10 (Enterprise E5). It is not included in Office 365 plans. It is bundled with the Microsoft 365 Enterprise E5 plan, and is part of the Microsoft Threat Protection framework.
- When a successful attack (malware or other) is identified by Windows Defender ATP, the risk score for the device is increased.
    - **By implication** - in the Windows Defender Security Center, devices with high risk scores are listed at the top of the list, providing a visual alert to an administrator of an active security threat.
    - **By implication** - an elevated risk score is sent to Intune, which in turn advises Azure AD. If configured, Azure AD will enforce Conditional Access restrictions, preventing a high risk machine from accessing sensitive corporate data.
    - **By implication** - if configured, automatic investigation and remediation actions on the compromised machine can be started. Manual investigation and remediation options are also available. Once all active threats have been neutralized and removed, the device will automatically reduce the risk score, which in turn will remove the conditional access restrictions.
- [**February 2019**] Microsoft introduced Microsoft Threat Experts, a managed threat protection service for customers with Windows Defender ATP, that provides access to Microsoft's security professionals for proactive and responsive support with current threats. Threat Experts complement and extend an organization's current security operations center / team. See Azure Sentinel and Microsoft Threat Experts.
- [**March 2019**] The integration announced in September 2018 in preview between Microsoft Cloud App Security and Windows Defender ATP for identifying shadow IT services used directly on Windows devices was released to general availability. The integration means that cloud apps used from Windows 10 devices that don't go through the corporate firewall or other network devices - such as when the device is at an offsite cafe - can still be discovered in Microsoft Cloud App Security. See Microsoft Cloud App Security Updates.
- [**March 2019**] Windows Defender ATP was renamed Microsoft Defender ATP on March 21, 2019. This coincided with Microsoft extending Defender ATP support to macOS devices. See Windows Defender ATP Goes Mac.
    - [**June 2019**] Microsoft released Microsoft Defender ATP for macOS to public preview in June 2019.
    - [**June 2019**] Microsoft Defender ATP for Mac was released to General Availability on June 28, 2019. Supports macOS Mojave, High Sierra, and Sierra.
- [**March 2019**] A security recommendation surfaced in the Microsoft Defender ATP Center can be pushed by a security admin to the admin of Microsoft Intune to request remediation. The remediation request from Microsoft Defender ATP shows in the new Security Tasks node in Intune. Once the Intune admin has approved the remediation request and completed the remediation process, Microsoft Defender ATP is updated to show a reduction of risk across devices.
- [**June 2019**] Microsoft released its new Threat and Vulnerability Management extension to Microsoft Defender ATP to general availability. It adds a risk-based approach to discovering, prioritizing, and remediating endpoint vulnerabilities and misconfigurations.

Microsoft Threat Protection



At Ignite 2018, Microsoft announced Microsoft Threat Protection, a Microsoft 365 offering that creates a single bundle of different Microsoft security and threat protection products. Microsoft Threat Protection is a Microsoft 365 offering, not an Office 365 offering.

Microsoft Threat Protection:

- Relies on the 6.5 trillion daily signals in the Microsoft Intelligent Security Graph.
- Focuses on protecting five categories of threats - identities, endpoints, user data, cloud apps, and infrastructure. Some individual products have a role to play across categories, including Office 365 ATP and Microsoft Cloud App Security.
- Microsoft says that its Threat Protection portfolio includes its own security services, along with specific capabilities from partners. It is not clear which partner offerings are included in Microsoft Threat Protection.
- The customer who spoke at the Ignite session on Microsoft Threat Protection commented on the power of unifying their security services with Microsoft. This was a shift from best-of-breed vendors or no-vendor in each of the respective security categories in the portfolio of offerings that makes up Microsoft Threat Protection.
- Will require security professionals who understand the intricate interlinkages between and across the different products and services in Microsoft Threat Protection.
- [**March 2019**] Signals and data from Azure Advanced Threat Protection, Microsoft Cloud App Security, Azure AD Identity Protection, and Azure Sentinel (if used) are analyzed to calculate an Investigation Priority Score for each user in the tenant. The score gives security analysts a quick way of determining which users should be investigated first based on threat to the business. User and Entity Behavior Analysis (UEBA) is used to create standard baselines for individuals across time and in comparison to their peer groups, and anomalous behavior triggers increased scoring.
- [**May 2019**] Microsoft provided an update on the numbers of threats it is identifying and mitigating every month using the services in the Microsoft Threat Protection portfolio. See Microsoft Threat Protection Update.

Issues for Customers to Consider

- Microsoft asserts - rightly so - that the modern organization faces a wide and diverse attack surface, and also asserts - probably rightly so as well - that no single product or service can secure the entire modern workplace. However, Microsoft has contributed to this problem, by creating such a plethora of product-aligned security services that it can confuse and undermine the ability for customers to ensure protection across the attack surface. The introduction of a unified offering is directionally right for both Microsoft and customers, but it will have to be much more than a bundling of disparate services into a single pane of glass.
- While unification is a good direction for Microsoft, the respective individual services still suffer from various weaknesses, as

noted in the pages in this Analysis Services. Unification alone will not address these weaknesses and drawbacks; that will take a concerted effort by Microsoft's various security-focused product groups to work together more closely.

Mobile Threat Defense

About

- Mobile devices are used widely by employees to access corporate information. Devices that display malicious or threatening behaviors - such as apps leaking data, apps exhibiting malicious behaviors, or apps surreptitiously requesting device or data access privileges that are abnormal - need to be contained. Microsoft Intune, a capability in Enterprise Mobility + Security and Microsoft 365 plans - provides device protection and configuration capabilities.

- Additional threat signals on mobile device apps and behaviors are available if a third-party mobile threat defense vendor is part of the equation. Microsoft Intune can receive threat signals from vendors such as Lookout, Symantec, Check Point and more.
    - [**August 2018**] Microsoft announced a new integration with BETTER Mobile, for sharing threat signals between BETTER ActiveShield and Microsoft Intune. See Threat Defense on Mobile Devices with Intune and BETTER.

Issues for Customers to Consider

- Each tenant can receive additional signals from one-and-only-one Mobile Threat Defense vendor. That is, Microsoft Intune can be integrated with only one additional mobile threat defense offering. It is not possible to mix-and-match capabilities within a single tenant.

No Manual Threat Scan

About

- An option to initiate a manual threat scan enables an administrator to search mailboxes and/or files for malware or indicators of attack.

- A manual scan can be used to:
  - Cleanup or remediate after an attack.
  - Verify there are no existing threats after first installing third-party security software.
  - Perform a risk assessment for compliance.

Issues for Customers to Consider

- Administrators do not have the ability to manually initiate a scan of messages in Exchange Online, nor documents in SharePoint Online and OneDrive for Business, to search for malware and other indicators of attack or compromise.

- Any malware that has not been previously identified will remain in place until it is possibly part of a subsequent successful attack, or perchance happens to be identified as part of an automatic selective scan if the customer has ATP. Administrators cannot, therefore, be sure that they have cleaned up all malicious files after an initial successful attack, nor generate a real-time dashboard of all existing threats in the environment.

Office 365 and GDPR Compliance

About

- The European Union's (EU's) General Data Protection Regulation (GDPR), the soon-to-be-enforced data protection regulation covering personal data on EU data subjects, will have significant impacts for organizations doing business in the EU and elsewhere. Organizations using Office 365 will need to ensure the protections offered in the service are up to standard, or they may face punitive fines under the regulation. A holistic approach to data protection, both within Office 365 and beyond, will be necessary for GDPR compliance.
- While GDPR will be enforced from late May 2018 and Microsoft has been investing heavily to get Office 365 and its other cloud properties ready for GDPR, there is a lot that is unknown about how GDPR will be enforced in practice.

Issues for Customers to Consider

In examining the capabilities offered for security, archiving, encryption, compliance and data protection in Office 365, the following strengths and weaknesses are evident in advance of GDPR's enforcement date:

- Office 365 offers various capabilities for identifying sensitive information across Exchange Online, SharePoint Online, and OneDrive for Business, using the more than 80 pre-built sensitive information types in the Security & Compliance Center. Advanced Data Governance, a service included in Enterprise E5, can proactively and automatically apply sensitivity labels to data as it is being created. For organizations using Enterprise E5, these capabilities will help with the data discovery challenge of GDPR.
- While not part of Office 365, Microsoft's Azure Information Protection Scanner will periodically scan on-premises file servers and repositories for sensitive, confidential and protected data. This will highlight to data controllers what personal data is currently being stored in on-premises systems, and therefore where data protections will be needed. These scan results will also help in planning for migrating to Office 365, Azure or other cloud services, highlighting to where sensitive information will be moving.
- When a DLP policy identifies sensitive information in a document in SharePoint Online or OneDrive for Business, it will block access to the data to everyone but the document owner, last modifier, and the site owner. While this will indeed protect personal data, it will not address use cases where people other than those three have valid business reasons for accessing the personal data in a document contained in a secured SharePoint Online or OneDrive for Business site. Likewise, sensitive data in a document cannot be sanitized while leaving the rest of the document available for review, or partially encrypted to prevent unauthorized access. In summary, Office 365 offers broad and basic ways of applying data protection policies within the organization, but it lacks the nuance, panache and elegance that complying with the GDPR will require.
- DLP policies that identify sensitive information will also lock and block documents in SharePoint Online and OneDrive for Business to prevent them from being shared with external users. This will be the appropriate action to take in some use cases, but not all. For example, there doesn't yet appear to be a way to check if a valid sharing agreement is in place between the organization and external firms or specifically named individuals. End users will need to do out-of-band checks to see whether they can transfer data or not.
- Service integrity and resilience to protect against threats to personal data is a matter of interest in GDPR. From a GDPR compliance perspective, the questions above about whether services like Office 365 ATP are good enough to protect end users from malicious links and attachments become much more than an exercise in comparing feature effectiveness between competitive offerings. If personal data is compromised in Office 365 because ATP is not good enough, that becomes a real problem for organizations.
- Encryption is specifically mentioned in the GDPR as a method of reducing the impact of personal data being breached, stolen, or inadvertently shared with unauthorized recipients. Beyond its role in doing so, it's a good practice for protecting all types of data. Office 365 uses encryption at many levels to protect data in Office 365, offers Office 365 Message Encryption (for user and policy-based encryption, with some provisos as explored above), and customers newly have the choice of bringing their own encryption keys to add a further level of protection. Since the destruction of a customer's encryption key has catastrophic consequences for access to data in Office 365 (which in itself is a problem under GDPR), organizations will need to ensure appropriate controls are in place to ensure the customer's master encryption key is not compromised in a ransomware or credential phishing attack.
- GDPR is a much more expansive issue than just Office 365. Microsoft's own positioning of its offerings for organizations

wanting to work towards GDPR compliance is Microsoft 365, which combines Office 365, Windows 10 (including capabilities like Windows Information Protection), device protection and more. Even Microsoft acknowledges that while Office 365 will need to comply with GDPR requirements, it is not the complete story for organizations.

- Complying with GDPR will require organizations to gain and maintain a holistic and real-time view of data protection threats across all cloud services, applications, endpoints and devices. There is no great gain from a data protection perspective if end users can save documents containing sensitive information to thumb drives or alternative cloud storage locations and use those locations to circumvent Office 365's data protection controls. Microsoft offers some capabilities in these areas, including the Office 365 Cloud App Security and the broader Microsoft Cloud App Security service, as do other vendors. Many employees also grant access to unapproved third-party applications and add-ins that integrate with Office 365 and other SaaS applications. Best-in-class solutions can give organizations visibility and control when it comes to third party applications that may be inappropriately accessing and storing data.
- The data protection requirements of GDPR will bring to light poor data protection practices of modern organizations. For example, storing personal data on customers or subscribers in ad hoc and unsecured Excel spreadsheets is a poor practice compared to using a secured database with field-level encryption and pseudonymization. Perhaps Microsoft's approach to locking and blocking all documents in SharePoint Online and OneDrive for Business that contain sensitive information will prove to be an effective way of forcing organizations to improve their own internal data management and data protection practices.
- The right to be forgotten is one of the core rights of data subjects under GDPR, and means that under certain conditions, all applicable personal data on a given individual must be deleted. However, this requirement is highly nuanced, in that applicability is defined by the legal basis under which the data was originally collected. Applying a blanket deletion to all personal data for the individual is not the intent of the regulation; a highly targeted operation is required instead. Technologies for deleting data in Office 365 will provide brute force capability to ensure a data subject is forgotten, but this must take place only within a strong data governance framework where data provenance requires the deletion action. How Microsoft will address this nuance in Office 365 remains to be seen.
- Until 2017, global organizations were advised to choose one master location for their Office 365 tenant, meaning that all access from outside the region would backhaul across Microsoft's global network. The alternative for organizations with regional compliance and data protection requirements was to try to make multiple tenants work somewhat seamlessly together, which was possible, but messy. With the introduction of Multi-Geo, albeit still in preview, large global organizations have a new possibility for segregating data access, DLP policies, and sharing policies across Office 365. This may prove to be a beneficial change for organizations with significant operations in Europe and other regions of the world, although Multi-Geo is enabled only for some Office 365 workloads, and services like Exchange Online Protection and ATP are not offered in all geographies. Multi-Geo was originally positioned for organizations with more than 10,000 Office 365 users (this minimum was reduced several times during 2018, and a further reduction is due in 2019), but even organizations with 250 employees distributed around the world may benefit from data protection policies and data residency on a regional basis.
- [**February 2019**] A data protection impact assessment (DPIA) undertaken in November 2018 in the Netherlands for the Dutch government raised significant concerns with covert data collection in Office 365 ProPlus. Microsoft committed to addressing (some of?) the concerns raised in the DPIA by the end of April 2019. See Microsoft Response to Dutch DPIA.
    - [**March 2019**] Microsoft announced that Office 365 ProPlus 1904 - the April 2019 release for Windows only - will support new privacy controls to limit the amount of diagnostic and related data sent from Office to Microsoft. See Office 365 ProPlus with Privacy Controls.
- Organizations that need to comply with GDPR would be well advised to consider alternative data protection capabilities beyond those offered in Office 365. While Office 365 will eventually offer more robust and nuanced protections, GDPR needs to be addressed now.

Office 365 Cloud App Security

About

- Office 365 Cloud App Security is a stripped-down edition of Microsoft Cloud App Security that reports on usage of Office 365 services and other services that are similar to Office 365. In December 2018, Microsoft added support for some Dynamics 365 activities.
- Office 365 Cloud App Security is included in Office 365 Enterprise E5, or available via an add-on to Enterprise E3.
- From December 2018, alerts related to Office 365 apps and services will also be displayed in the Alerts view in the Office 365 Security & Compliance Center. This will provide a unified alerting plane on Office 365, drawing on the additional signals captured through Microsoft Cloud App Security and Office 365 Cloud App Security. See Microsoft Cloud App Security Alerts.
- Microsoft releases new capabilities to Office 365 Cloud App Security after releasing them first to Microsoft Cloud App Security. However, only those capabilities relevant to Office 365 Cloud App Security are added; Microsoft Cloud App Security retains a larger capabilities set. During September to December 2018, Microsoft enhanced Office 365 Cloud App Security with:
    - App permission policies can be set to automatically revoke access to an OAuth application that is considered risky. To make the intent of these policies clearer, Microsoft changed the name of App permission policies to OAuth Apps.
    - Cloud Discovery can accept log files from Forcepoint Web Security Cloud, has enhanced support for the i-Filter parser, and features an enhanced custom log parser.
    - Docker on Windows can be used to automatically upload log files; supports Windows 10 (Fall Creators Update and newer) and Windows Server 1709 and later.
    - OAuth app policies can be scoped to groups, to enable greater nuance in how policies are applied.
    - Support for Microsoft Dynamics activities that are supported in the Office 365 audit log.
    - Several new anomaly detection policies, such as data exfiltration, deletion of multiple virtual machines in a single session, and suspicious inbox manipulation rules. These policies provide warning and early detection for data breaches, account compromise, malicious internal actors, and more.
    - Integration with Microsoft Flow, so administrators can create more advanced alert and action pathways.
- [**December 2018**] Microsoft added two new policy rules to detect suspicious activities in a user's inbox. The first new policy alerts on suspicious inbox forwarding rules, and the second on suspicious inbox manipulation rules. See New Rules in Microsoft Cloud App Security. The changes also apply to Microsoft Cloud App Security.
- [**January 2019**] Microsoft added a Session ID field to Exchange Audit Log records, enabling the differentiation of actions performed by a user authenticated against Azure AD. Microsoft Cloud App Security could leverage this new unique field value in policies to automatically detect and alert on potential malicious activity within an Exchange mailbox. See Session ID Added to Exchange Online Audit Logs.
- [**January 2019**] Alerts raised in Office 365 Cloud App Security can be linked to a Microsoft Flow playbook, for adding workflow intelligence, insight, and human perspective into the appropriate action to take when an alert is generated. Microsoft Flow integration is offered in addition to or instead of current alerts for text message and email notifications. See Security Workflows with Microsoft Flow.
- [**February 2019**] Microsoft released to public preview additional app support in Office 365 for conditional access, covering both access and session policies. Conditional access was previously only available for SharePoint Online, but the newly supported apps are Exchange Online, OneDrive for Business, Power BI, Microsoft Teams, and Yammer. Conditional Access App Control in Office 365 Cloud App Security relies on Azure AD Conditional Access, and requires at least Azure AD Premium P1 licensing. Depending on the who (user / group), what (cloud app) and where (locations, networks) of the user session, policies can block access entirely, block downloads, enforce encryption of downloaded documents, increasing monitoring, and more. See Office 365 Cloud App Security Expands Conditional Access.

Issues for Customers to Consider

- Office 365 Cloud App Security does not provide a user risk profile, calculated from correlating multiple security threats and events. Office 365 Cloud App Security reports only within the context of the policies that have been configured.
    - While not part of Office 365 Cloud App Security, Microsoft's Azure Advanced Threat Protection service offers a risk-based profile for each user. See Azure Advanced Threat Protection.
- Office 365 Cloud App Security does not offer integrated data loss protection or file scanning. These functions must be done by

other Office 365 services, such as Office 365 Unified DLP or Exchange Online DLP.

Reporting for Response to Threats

About

- The Security & Compliance Center offers various reports on what has happened due to malicious and unwanted messages.

Issues for Customers to Consider

- The Security & Compliance Center does not offer incident remediation workflows or reporting on how malicious activity was addressed.
- There is no ability to associate events with knowledge articles and similar cases to streamline remediation.

Scoped Administrative Access

About

- Privileged Access Management shifts from an approach of standing access for administrative tasks in Office 365, to an explicitly-scoped, time-bounded, and approved task-based or role-based approach. This approach is called Zero Standing Access. Requests for elevated privileges must be approved before elevated access rights are granted.
- Privileged Access Management was released into by-application-only preview in April 2018. Customers were required to apply for the preview program, rather than it being broadly available for all E5 customers.

Issues for Customers to Consider

- Privileged Access Management was released in preview in April 2018, and still only applies to Exchange Online (at September 2018). Other workloads in Office 365 do not support scoped administrative access. Microsoft said it would expand zero standing access to other workloads, but at September 2018, this has not yet been released.
- Requesting privileged access requires the use of PowerShell and a special PowerShell cmdlet. There is no UI-option within the Admin Center for instantiating a new request.
- Privileged Access is only available in Office 365 E5, or through the Advanced Compliance SKU. Note that the by-application-only preview status is still in place (at September 2018); Privileged Access is not available within the standard E5 license yet.
- Turning on Privileged Access controls for a tenant does nothing to implement task-level or role-level access controls. Specific access policies must be configured. Any task or role that is not covered by an access policy enables standing access for administrators with the right Office 365 access privileges.

Spam Quarantine

About

- While not the default option for handling spam, an administrator can switch on a spam quarantine for the organization. Compared to the default behavior of routing spam to each user's Junk Mail folder (thereby giving each user full access to their spam directly), spam quarantine is an improved defense against spam that carries a malicious payload or ransomware.
- Users must sign into the spam quarantine using a Web browser and their Office 365 credentials.
- Quarantine is part of Exchange Online Protection and Advanced Threat Protection.

Issues for Customers to Consider

- Only 500 messages can be displayed in the spam quarantine – there is no ability to view more. An end user can attempt to filter their list of spam messages to find the valid business emails inadvertently captured as spam, but the interface and message limit does not make this an easy process. It is more likely that valid messages that have been labeled as spam will remain undetected.
- An administrator cannot view all messages held in the quarantine in a single list. They must be divided into the different types of messages that are held in the quarantine, such as spam, malware, phishing, and bulk.
- Quarantined spam messages are retained for a maximum of 30 days, after which they are deleted and not retrievable. Microsoft says that the default duration is also 30 days, but a check of several tenants had the default still set at 15 days. An administrator can decrease, but not increase, this maximum number. If a valid business email is incorrectly labeled as spam and the end user does not review his or her quarantine for more than 30 days, those messages will be irretrievably lost.
- Until September 2018, the maximum was only 15 days. Microsoft increased the maximum to 30 days in September 2018.
- It is not possible to create different policies to deal with different types of spam and bulk messages, such as spam, malware, phishing, and bulk matches. An anti-spam policy can be differentiated based on recipient, but not based on type of message.
- When adding an X-header within a policy, the X-header has to be the same for each type of spam or bulk message; there isn't an option to differentiate the X-header based on type (e.g., spam, malware, phishing, or bulk).
- While spam is only one category of message that might be quarantined, a single setting under anti-spam sets the quarantine period for all categories of messages that are quarantined; there is no option to set a different retention period based on different types of quarantined messages.
- For end users, there is no workflow for releasing spam from the quarantine. If a user wants a message put into their inbox, the action is executed directly. There is no possibility for flagging a message for release and enabling an administrator to check the message before the actual release action is triggered.
- **Spam Notification Message for End Users**. An administrator can turn on spam notifications for end users, which is a once-a-day email message listing messages in the quarantine addressed to the user which were classified as spam. Note that:
    - The notification is for spam only. Other messages sent to the quarantine are excluded.
    - Notifications regarding spam messages held in the quarantine can only be sent to everyone or no one. Office 365 does not have a fine-grained ability to specify which users should receive notifications, nor which users should not.
    - It is not possible to specify the time of day for delivering the spam notification message from the quarantine, nor how frequently it should happen below the unit of days (e.g., there is no possibility to request a notification message every few hours). When the spam notification is received in the middle of the night, users could miss the notification.
    - While messages can be released from the quarantine from the notification message, each one must be handled in turn, necessitating yet another new browser window for each message the user wants to release to his or her inbox.
    - The notification message lists quarantined messages using Universal Coordinated Time (UTC) for all users. It pays no attention to the date/time zone settings for the user, thus displaying messages in a technically-correct but user-irrelevant format.
    - It is not possible to generate a spam notification message as soon as a new spam message is received. Notifications are sent daily, and not more frequently.
- Messages from blocked senders are still sent to the spam quarantine, rather than just being deleted immediately. This overloads the quarantine with possible spam as well as email from blocked senders; it would be much better just to have emails that have not been sent from blocked senders shown in the quarantine.
- The quarantine doesn't share intelligence with users on how many similar messages were received with a similar subject line

and sender by other people in the organization. A higher number would signal the likelihood that the message is spam or a phishing attempt, but this intelligence is not offered to help users make informed decisions about the likelihood of a message carrying malicious intent.

- Microsoft's new Zero-hour Auto Purge (ZAP) feature does not support the spam quarantine. While it can automatically re-classify messages incorrectly classified as spam or mis-classified as clean, and move messages between the user's inbox and Junk Mail folders, it cannot move messages automatically between the spam quarantine and inbox. Plus, ZAP works only with Exchange Online inboxes, which presents a problem for organizations that maintain a hybrid environment.

Limited Support for Hybrid Architectures

About

- Security capabilities in Office 365 are focused on Office 365 workloads and data.

Issues for Customers to Consider

- The security capabilities in Office 365 offer incomplete support for organizations with hybrid architectures.
- Advanced Threat Protection (ATP) lacks hybrid capabilities, meaning that customers with Exchange or SharePoint on-premises, for example, must have a second and separate threat-protection offering. ATP handles only certain Office 365 workloads under specific conditions, and does not address data and systems beyond Office 365. This can cause problems with many customers operating a hybrid environment.
- DLP policies defined in the Security & Compliance Center apply to specific Office 365 workloads only. These policies are not also enforced for on-premises servers from Microsoft or other vendors.
- eDiscovery in the Security & Compliance Center is only for certain Office 365 workloads, and does not work with on-premises Exchange, SharePoint and OneDrive for Business environments.
    - See eDiscovery - Overview
- Any organization investing in Office 365 security capabilities – with all of their associated issues – will still need to acquire and manage a completely separate set of security services for non-Office workloads and data.

Support for Parallel Third-Party Security Solutions

About

- Office 365 has a series of general and specific weaknesses in its security capabilities.
- Customers can benefit from additional assurance and true advanced mitigation capabilities provided by best-in-class third-party security solutions. The ideal for adding layers of security is a collaborative, multi-layer approach, whereby additional layers process incoming threats before handing the message to Office 365 for its own security testing and assurance, and likewise protect internal plus outbound messages with additional complementary layers of security.

Issues for Customers to Consider

- There have been situations where adding layers of security before Office 365 has resulted in the Office 365 security services no longer working; the new front-end security capabilities are treated as trusted delivery mechanisms that render Office 365's own security ineffective.
- In the rapidly evolving threat landscape in which organizations find themselves working, Microsoft needs to offer better possibilities for third-party security vendors to deliver complementary security services that bolster Office 365's security capabilities.

Tenant Architecture and Data Residency

About

- From the beginning of Office 365, the design of the tenant architecture was that each organization used one and only one tenant, homed in one geographical region, and to which all out-of-region traffic would route for access to the organization's data. This design works perfectly for organizations that are solely active in one geographical region, but can cause significant data sovereignty and data residency challenges for multi-national and cross-regional organizations. The sole tenant location for the organization is set when the organization first signs up for Office 365, and even then, some content types in Office 365 have only been served out of the North American region, regardless of the organization's master region, although this is slowly changing over time.
    - [**Example**] For a tenant created in Canada, various data has been stored in the United States, including Microsoft Teams, Planner, and Yammer.
    - [**August 2018**] Microsoft announced that conversation and chat data in Microsoft Teams is available in-country for new three new countries. See Teams Data Residency in Canada with Others to Come and Teams Data Residency in Australia and Japan.
    - [**March 2018**] Microsoft added France to the list of countries offering in-country data residency for conversation and chat data in Microsoft Teams. See Data Residency in France for Microsoft Teams.
- What this means, therefore, is that under the original design, an organization with significant operations in multiple geographies cannot geo-ring fence content into local Office 365 data centers, which has implications for legal cases, government access, and compliance with data protection regulations. Organizations dissatisfied with the original design have until recently had only one other option, and that was to try to make multiple tenants homed in different geographical regions work as one. Setting up multiple, inter-related Office 365 tenants is a non-trivial technical undertaking, and has several negatives for actual usability. Microsoft has, in general, advised organizations not to pursue this route.
- **Multi-Geo**. Microsoft used its Ignite 2017 conference to introduce a second and more tenable option for organizations for which one tenant was not a workable answer: Multi-Geo. This new option enabled a single tenant to have data stored in different geographies, based on settings configured for each individual.
    - Multi-Geo initially required a minimum seat threshold of 10,000. This was reduced to 5,000 in April 2018, and to 2,500 in October 2018. In order to be able to use Multi-Geo, the tenant must have a minimum of 5% of total seats licensed for Multi-Geo; hence at a 2,500 minimum, this would mean 125 seats would need to be licensed for Multi-Geo. Microsoft is working to reduce this minimum number even further, but has in general used the minimum seat threshold to give itself time to get the service and its associated support processes right before opening it to the masses.
    - Microsoft intends to reduce the minimum seat count even further in mid-2019. Specific numbers have not been announced yet.
    - [**May 2019**] Microsoft announced a further reduction to 500 users, effective June 1, 2019. See SharePoint Security and Compliance Updates.
- Multi-Geo is priced at US$2 per user per month, for users who are homed in one of the satellite geos. Users homed in the master geography are not liable for the US$2 per user per month.
- Multi-Geo was initially enabled for individual-level workloads in phase 1, specifically Exchange Online and OneDrive for Business. Both of these services have a single owner, and therefore can be easily homed in a specific geo. Phase 2, announced at Ignite 2018, added support for two workloads that can have multiple owners, specifically SharePoint Online and the SharePoint site and mailbox components of Office 365 Groups. These are due for release in 1Q2019. See Multi-Geo for SharePoint and Office 365 Groups (October 2018).
    - [**March 27, 2019**] Multi-Geo for SharePoint and Office 365 Groups were released to General Availability.
    - [**May 2019**] At the SharePoint Conference 2019, Microsoft said Multi-Geo for SharePoint and Office 365 Groups were released to General Availability. It is unclear why this was restated given the March 2019 release. See SharePoint Security and Compliance Updates.
    - [**August 2019**] Two new Multi-Geo regions were brought online: South Africa and the United Arab Emirates. New datacenters have recently been activated in both geographies.
- **Geo-Level Policies**. After setting up additional geographies in a tenant, customers will gain the ability to tailor various policies at the geo level. This includes sharing policies in OneDrive and SharePoint, DLP policies in the Security & Compliance Center,

and even eDiscovery managers.

- **SharePoint Online**. Availability of SharePoint Online for Multi-Geo was released in late March 2019. Each geo offers:
  - A geo-scoped admin center.
  - A geo-scoped policy for specifying sharing rules for external domains.
  - Search indexes and content for each geo.
  - Automatic creation of new sites in the geo where the user creating the site is located. If required, an administrator can move the site to another geo.
  - Geo-scoped eDiscovery.
  - A globally-managed taxonomy term store that is replicated to each individual geo.
- **Yammer**. Microsoft announced that Yammer is gaining new data residency options. The guiding principle is that Yammer message bodies and files attached to Yammer messages will be stored at rest in the geographical area in which the Office 365 tenant is enrolled. There is no mention of Multi-Geo options for Yammer. See Yammer in Europe and eDiscovery.
  - [**April 2019**] Data residency for Yammer Enterprise in Europe was released to preview. Some capabilities are not available, such as external messaging.
  - [**May 2019**] Microsoft released in-geo data residency in Europe for Yammer. Only applies to new Office 365 enterprise customers. Still no mention of migration options.

Issues for Customers to Consider

- SharePoint Online is targeted as the third workload for Multi-Geo, but unlike Exchange and OneDrive, which are user-focused services, SharePoint is a team- or group-focused service, which makes some flow-on decisions about data access and data rights more complicated. Each geo-enabled location with SharePoint will have a unique URL namespace, which means that SharePoint access will be less seamless than for Exchange and OneDrive. And organizations with cross-geographical collaboration between employees will constantly have to ask which SharePoint location is the correct one for each new site. With the current design, a new SharePoint site or Office 365 Group will be homed in the original owner's preferred data location / geo.
- Some critical services, such as Exchange Online Protection, are not currently targeted as being Multi-Geo enabled. The current intent is that EOP processing will always happen in the tenant's default geo location, rather than being distributed out to each individual geo. Having all email route through scanning services in another geo location may not be good enough for large organizations.
- **Only Partial Workload Support**. Multi-Geo is a good step in the right direction, but it doesn't yet deal with all of the workloads in Office 365. Multi-Geo customers will still need to figure out their data residency approach for Microsoft Teams, Skype for Business, Yammer, and other Office 365 workloads. And some workloads - such as Azure AD - are non-regional or global services that will defy being homed exclusively in a specific region.
- **Some Unique Designs**. Microsoft's approach to Office 365 data centers is broadly consistent across the world, but some countries have unique arrangements. For example:
  - [**Germany**] Germany has an isolated Office 365 approach, to ensure data residency. Microsoft Cloud Germany is different from the rest of the world, is run by a German data trustee, and does not provide the full complement of Office 365 services. Starting late 2019, Microsoft will introduce new data centers in Germany that bring the German service offering in line with the rest of the world. See Microsoft Announced New Data Centers for Germany.
  - [**China**] Office 365 is run by 21Vianet, a Chinese company to whom Microsoft licenses Office 365. Not all Office 365 services are offered by 21Vianet. Office 365 data is resident within China, and the service is subject to Chinese laws.
- **Cascading Effects**. Despite having a global network of data centers, an outage event in one specific data center can have cascading effects beyond the local region. This can be caused by service requests being re-routed to another region, thereby causing spikes in demand that degrade service more broadly. It can also be caused by non-regional services, such as Azure AD, being negatively affected by a regional outage. It can also be caused by legacy data management strategies where customer data is not distributed more broadly across multiple data centers. For example:
  - [**September 2018**] A lightning strike in Texas on September 4, 2018, disrupted the cooling systems at the US South Central data center in San Antonio. This had a major impact on both Office 365 and Azure services, with customers outside of the US South Central region experiencing Azure AD authentication problems. In addition, certain data for Visual Studio Team Services (VSTS) was authoritatively stored in San Antonio, and the outage there caused disruption for VSTS customers across the world, including in Europe. Clearly Microsoft has several weaknesses in its engineering

design for Office 365 if a problem in one data center causes major disruption across the world. See Data Center Outage in US South Central.

Lack of Unified Visibility of Attack Vectors

About

- A unified view of malware and non-malware attacks allows an administrator to gain a consolidated and integrated view of current and emerging threats and threat patterns.
- It is useful if an administrator can correlate current and emerging threats across both email and cloud applications.

Issues for Customers to Consider

- The various threat reports in the Security & Compliance Center provide a piecemeal view of the threats facing an organization across malware and non-malware attack vectors, but not a consolidated view. The various separate reports are focused on specific types of attacks, meaning that a security administrator must manually correlate what is happening across the entire organization in order to gain a “big picture” view.
- Office 365 offers the following piecemeal threat reports via Threat Explorer (Threat Management > Explorer):
  - **Malware** (in email messages). Shows malware threats that have been detected in email via anti-virus scan, ATP detonation, or reputation detection. Shows top malware families and top users who are being targeted by malware.
  - **Phish**. Shows email messages containing malicious URLs, and notes how they were detected (by URL, by reputation, by heuristic, or by Machine Learning). Also displays which URLs were clicked, and whether the URLs in question have been blocked or not.
  - **User-reported**. Displays messages that users have reported for re-classification, for example, an email that was delivered but the user believes it is a phishing email or contains malware. Also displays submissions for false positives, in which a user asserts that a message classified as junk is not so.
  - **All email**. Displays a list of all email activity between users and all email messages sent from external sources into the Office 365 tenant.
  - **Malware** (in files). Lists the files stored in Office 365 that have been detected as malware through the Advanced Threat Protection file detonation process. This only includes files that have been analyzed through ATP file detonation; it is not as assertion about all files in existence (e.g., such as those which have not been detonated or checked).
  - There is no ability to view a single consolidated list of all threat types, and then to sub-filter using facets.

Update Log - Security

September 2019

September 2 - Expanded Conditional Access in Microsoft Cloud App Security

August 2019

August 19 - Microsoft Cloud App Security Updates - 151 to 153

August 15 - Netherlands on Data Privacy Risks

August 1 - Azure AD Identity Protection Updates

July 2019

July 30 - Monotonic Machine Learning Models

July 30 - BlueTalon Acquired

July 25 - Symantec on BEC Numbers

July 17 - Admin Submissions for Suspicious Emails

July 4 - Threat Explorer Hunting Updates

July 2 - Anti-Phishing Policy Update

July 2 - Synchronous URL Detonation

June 2019

June 27 - Microsoft Cloud App Security Updates

June 24 - FlawedAmmyy Trojan

June 19 - Data Centers in Middle East

June 6 - Discovered Resources in MCAS

June 4 - Barracuda on Account Takeover

June 3 - Free DMARC Discovery for Office 365

May 2019

May 29 - Compliance Manager 2019

May 28 - Can't Change Office 365 Tenant Name

May 24 - Identity Secure Score Released

May 22 - SharePoint Security and Compliance Updates

May 15 - Avanan Global Phish Report 2019

May 15 - Microsoft Threat Protection Update

May 13 - Microsoft Secure Score Updates

May 10 - Identity Security at Microsoft

April 2019

April 30 - Data Investigations

April 19 - Yammer in Europe and eDiscovery

April 15 - Attacking Microsoft Office Vulnerabilities

April 8 - EDPS Investigation of Microsoft re Data Protection

April 4 - Automated Incident Response Playbooks at Public Preview

April 2 - State of Cybersecurity

March 2019

March 29 - Threat Explorer Updates

March 26 - Office 365 ProPlus with Privacy Controls

March 25 - Windows Defender ATP Goes Mac

March 18 - Data Residency in France for Microsoft Teams

March 18 - Update on Microsoft Threat Protection

March 13 - Microsoft Cloud App Security Updates

March 11 - Azure Sentinel and Microsoft Threat Experts

March 5 - Credential Detection Using Azure Information Protection

February 2019

February 27 - Office 365 Cloud App Security Expands Conditional Access

February 8 - Microsoft Response to Dutch DPIA

January 2019

January 31 - Security Workflows with Microsoft Flow

January 29 - Inspecting Encrypted Files with Microsoft Cloud App Security

January 22 - Role-Based Access to Alerts in Office 365 Security & Compliance Center

January 22 - New Rules in Microsoft Cloud App Security (also applies to Office 365 Cloud Security)

January 21 - Azure Advanced Threat Protection

January 16 - Policy Service for Office 365 ProPlus

January 14 - ATP Splitting Into Two Plans

January 4 - Session ID Added to Exchange Online Audit Logs

January 2 - Standalone Upgrades for Microsoft 365 E3

December 2018

December 26 - Office 365 Cloud App Security Updates

December 21 - Multi-Geo Available in India

November 2018

November 30 - Real-Time Microsoft Cloud App Security Controls for On-Premises Web Apps

November 26 - Microsoft Cloud App Security Alerts

November 14 - Microsoft Cloud App Security - Roadmap Updates

November 6 - Hosted Apps Obfuscated to Microsoft Cloud App Security

November 2 - Microsoft Secure Score Updates

October 2018

October 30 - Office 365 Cloud App Security Updates (August/September 2018)

October 25 - OAuth Threat Monitoring in Microsoft Cloud App Security

October 17 - Microsoft's Phish Miss Rate - From Highest to Lowest?

October 15 - Safe Links in Microsoft Teams

October 10 - Updates to Information Protection

October 8 - Verified Businesses in Outlook.com

October 4 - Microsoft Threat Protection

October 1 - Multi-Geo for SharePoint Online and Office 365 Groups

September 2018

September 27 - Microsoft Cloud App Security and Windows Defender ATP for Discovery

September 24 - Threat Protection Review and Assertions

September 24 - Windows Virtual Desktop

September 19 - Specific Admin Roles for Microsoft Teams

September 5 - Maximum Spam Quarantine Period Increased to 30 Days

September 4 - Data Center Outage in US South Central

August 2018

August 31 - New Data Centres for Germany from late 2019

August 27 - Teams Data Residency in Australia and Japan

August 24 - Threat Defense on Mobile Devices with Intune and BETTER

August 16 - Anti-Spoofing Added to All Exchange Online Protection Plans

August 10 - Teams Data Residency in Canada with Others to Come

August 3 - Microsoft Cloud App Security can track Amazon Web Services S3

August 2 - Customer Lockbox Access Approver Role added to Office 365

June 2018

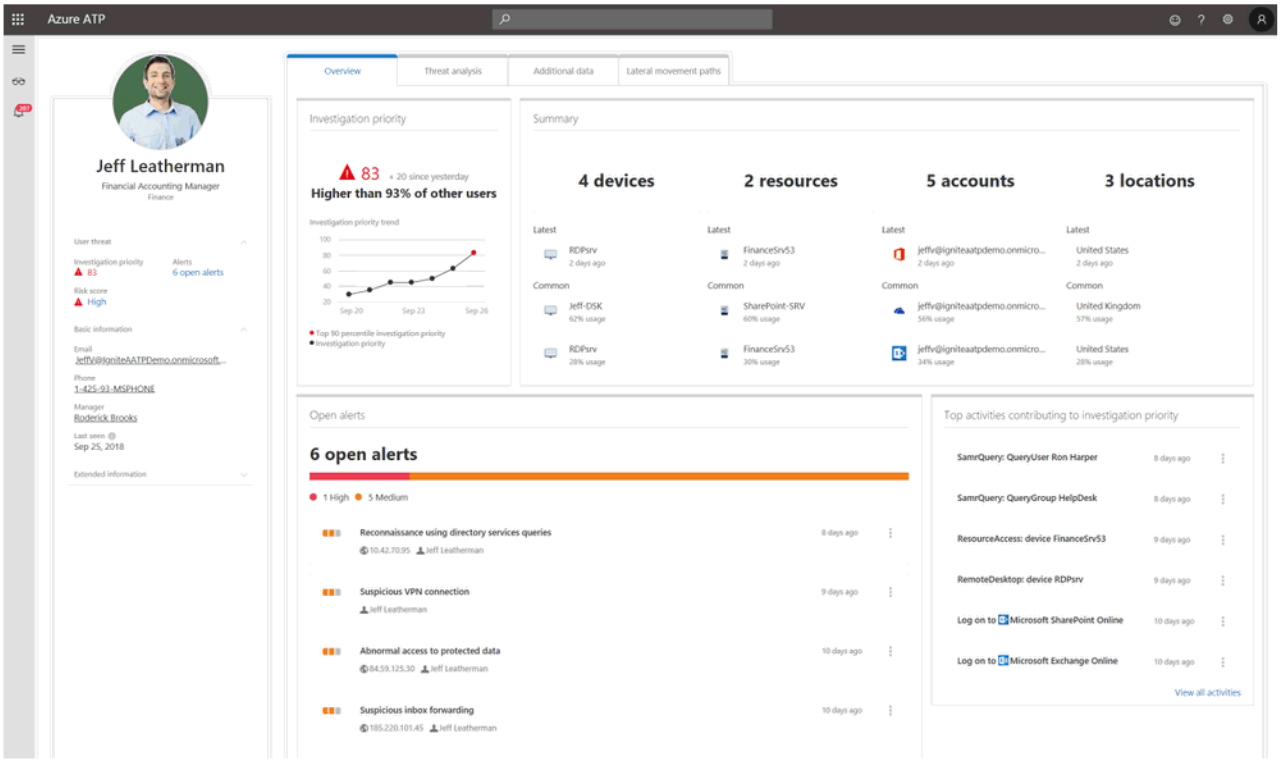
June 19 - General Availability - Five New Sensitive Information Types for GDPR. Microsoft released 5 new sensitive information types for identifying personal data relevant to GDPR. These are available for individual use in DLP or data governance policies. Microsoft also released a new GDPR template, which groups all EU-relevant sensitive information types together, for use as a single entity in policies. The new data types are: EU passport number, EU national identification number, EU driver's license number, EU tax identification number (TIN), and EU social security number (SSN) or equivalent ID. See Data Loss Protection. Announced via Security, Privacy and Compliance Blog.

Azure AD B2B Collaboration

About

- A component of Azure AD Premium, offering identity and authentication options for external parties. Azure AD B2B Collaboration is not included in the version of Azure AD that comes with Office 365.
- Offers several ways of federating with external identities, including Google account federation and direct federation with any identity provider that supports SAML or WS-Fed. External users in these identity systems can sign-in using their credentials; they do not have to create a separate Microsoft account, for example, to sign-in to an organization's systems.
- Users who do not have a federated account can gain access using a one-time passcode. They do not have to create a new account in an identity system in order to sign-in.
- Offers lifecycle management capabilities for guest accounts.
- Offers the ability to audit what access a guest has to an organization's systems, using the Access Reviews capability of Azure AD.
- Works with multi-factor authentication and conditional access to further safeguard organizational systems.

Azure Advanced Threat Protection



About

- A cloud service in Azure for detecting and investigating advanced attacks and insider threats across users, servers and endpoints. Azure ATP provides protections in the cloud and for on-premises servers, endpoints and user accounts in Active Directory.
- Aggregates and correlates activity and security signals to create a behavioral profile for each user. Relies on multiple data sources, including group members and permissions, network traffic, event logs, VPN data, IP address (for location signals), and more. Uses multiple methods for identifying suspicious user and device behavior, including known-technique detection and behavioral analytics. For example, if a user account is used to log in using a previously unseen device from a previously unvisited location, the risk of a compromised user account is quite high.
- Receives signals from Windows Defender ATP with data on specific actions taken on an endpoint. A SecOps analyst can pivot from Azure ATP to Windows Defender ATP to investigate a specific device.
- Provides proactive recommendations on identity configurations and security settings to reduce the potential attack surface.
- [**September 2018**] Integrates with Azure AD Identity Protection, which adds activity and security signals from Azure AD. The combined service - Azure ATP with Azure AD IP - enables the calculation of an overall risk score on a user-by-user basis, which in turn can be leveraged by SecOps analysts in prioritizing mitigations for users and risk situations. For example, in the screenshot above, Jeff has a risk score that is 93% higher than all other users in the firm.
- [**September 2018**] Microsoft claims that Azure ATP is protecting "millions of users" at organizations worldwide.
- [**March 2019**] Signals and data from Azure Advanced Threat Protection, Microsoft Cloud App Security, Azure AD Identity Protection, and Azure Sentinel (if used) are analyzed to calculate an Investigation Priority Score for each user in the tenant. The score gives security analysts a quick way of determining which users should be investigated first based on threat to the business. User and Entity Behavior Analysis (UEBA) is used to create standard baselines for individuals across time and in comparison to their peer groups, and anomalous behavior triggers increased scoring.

Analysis

- The concept of a risk-based user profile across multiple signals is an idea that shows up in the capabilities of Cloud Access Security Brokers (CASB) of third-party vendors. It is not something that is available natively in Office 365 Cloud App Security or Microsoft Cloud App Security, the two CASBs on offer from Microsoft. However, Azure ATP offers this complementary view of

user risk, and this is being surfaced in Microsoft Cloud App Security to enable SecOps analysts to prioritize remediation actions for risky users.

Azure AD Identity Protection

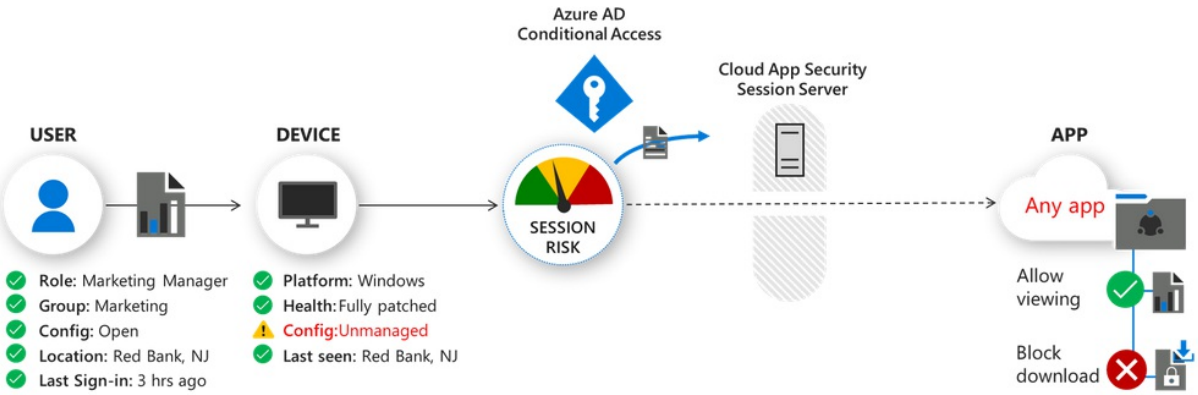
Entity	Automation?	Insightful reports?	Public APIs?	Enhanced machine learning?
Risky users	✓ User risk policy	✓ Risky users	✓ Risky user's API	✓ Yes
Risky sign-ins	✓ Sign-in risk policy	✓ Risky sign-ins	✓ Sign-ins API (with risk info)	✓ Yes

About

- A service that detects and protects an organization from identity attacks, using dynamic intelligence and machine learning. The service profiles users for risk, highlights risky sign-ins, and risk events such as leaked credentials on other sites.
- The capabilities available to customers depend on licensing level for Azure AD. Premium P2 customers gain access to all capabilities, while P1 and AD Basic/Free receive lower capability sets.
- [**September 2018**] Integrates with Azure Advanced Threat Protection, supplying activity and security signals from Azure AD. The combined service - Azure ATP with Azure AD IP - enables the calculation of an overall risk score on a user-by-user basis, which in turn can be leveraged by SecOps analysts in prioritizing mitigations for users and risk situations.
- Offers APIs for incorporating signal data from Azure AD Identity Protection into other systems including SIEM, storage, ticketing, and alerting.
- [**March 2019**] Signals and data from Azure Advanced Threat Protection, Microsoft Cloud App Security, Azure AD Identity Protection, and Azure Sentinel (if used) are analyzed to calculate an Investigation Priority Score for each user in the tenant. The score gives security analysts a quick way of determining which users should be investigated first based on threat to the business. User and Entity Behavior Analysis (UEBA) is used to create standard baselines for individuals across time and in comparison to their peer groups, and anomalous behavior triggers increased scoring.
- [**August 2019**] Microsoft upleveled the number of behaviors its analyzes as part of the Unfamiliar Sign-In Properties attack monitor, which resulted in doubling its ability to detect compromised sign-ins and reduced false positives by 30%. See Azure AD Identity Protection Updates.

Expanded Conditional Access in Microsoft Cloud App Security

Description



Microsoft announced the expansion of its ability in Microsoft Cloud App Security to enforce conditional access on apps, with support to enforce sessions controls for any cloud app, on-premises app or custom app that meet specific requirements. In the example above, the user's device is unmanaged, and therefore a conditional access app control policy blocks downloading of content while still enabling viewing of that content by the Marketing Manager.

Specifics include:

- Admins can onboard any app and gain a standardized set of monitoring capabilities and controls.
- For cloud apps, the requirements for onboarding are the use of SAML 2.0 or Open ID Connect, and that single sign-on is via Azure AD (and its Conditional Access capabilities).
- For on-premises apps, the requirements for onboarding are the use of the Azure AD App Proxy and Kerberos Constrained Delegation (KCD).
- Data exfiltration controls are available to block download, block copy and cut, block print, and apply Azure Information Protection labels on download.
- Data infiltration controls are available to block upload and block paste.
- The activity log page in Microsoft Cloud App Security provides details for review and analysis by authorized administrators, including filter and search capabilities to focus on particular activities or files.

Analysis

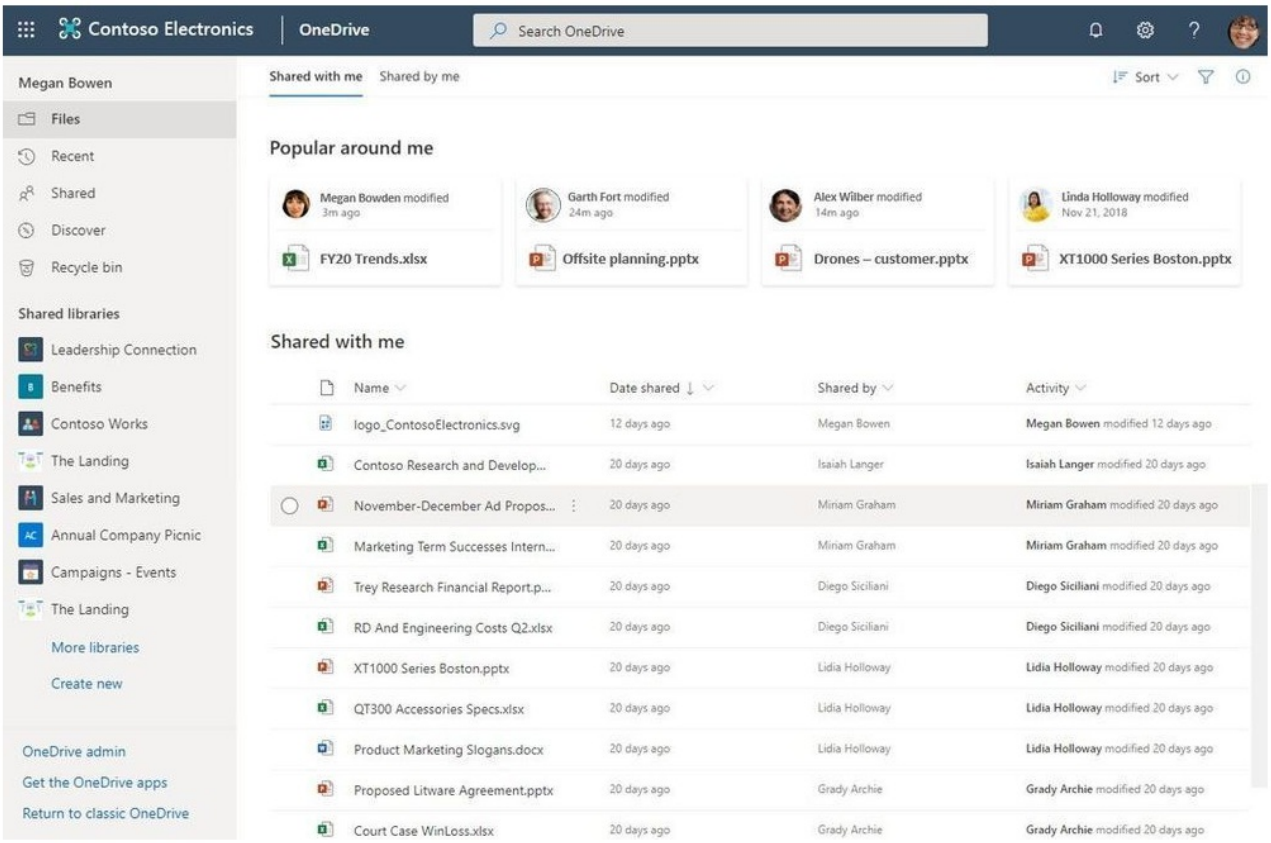
- As long as the requirements are met, it's a strong value proposition for organizations: onboard any app and gain fine-tuned controls for enforcing conditions on behavior.
- The "Cloud App" naming in Microsoft Cloud App Security is now reflective of only a part of its overall functionality. Microsoft may move to rebrand the offering.

About

- **Date** - September 2, 2019
- Advanced Security for Any App in Your Organization (Enterprise Mobility + Security Blog, August 28)
- **Tag** - Security
- **Implication** - Microsoft Cloud App Security

Shared With Me in OneDrive

Description



Microsoft added a view to OneDrive of files that have been shared with a given user, enabling quick access to such files. The view also shows files that are popular around the user, or trending in interest among work colleagues.

Analysis

- I'm sure there used to be a view of documents that had been shared with a user, but it was deprecated because Microsoft thought it unnecessary. Sounds like it was too useful, and it's back again.

About

- **Date** - September 3, 2019
- SharePoint Roadmap Pitstop: August 2019 (SharePoint Blog, September 3)
- **Tag** - File Sharing

Weekly News Drop - September 6, 2019

Roundup of recent Office 365 news:

- **Data Centers in Switzerland**. Microsoft released its two new data centers in Switzerland - located in Zurich and Geneva - for usage with Azure workloads. Support for Office 365, Dynamics 365 and the Power Platform are on the roadmap but not yet released. Microsoft says about 30 customers and partners are already using Azure, including UBS Group, Swiss Re, and Swisscom, the latter of which will be offering ExpressRoute connections for customers. Microsoft Azure Available from New Cloud Regions in Switzerland (Azure Blog, August 28).

Weekly News Drop - August 2, 2019

Roundup of recent Office 365 news:

- **Azure Information Protection Unified Labeling Client at General Availability**. Microsoft released the new unified labeling client for Azure Information Protection to general availability during July; it was released to preview in June. The GA client supports labels with user-defined permissions that prompt for custom permissions, multiple languages, and multiple device types (Windows, Mac, iOS and Android). The classic client - for Windows only - was also updated. Azure Information Protection Documentation Update for July 2019 (Azure Information Protection Blog, July 31).
- **Yammer Mobile Client Upgrades**. The mobile clients on iOS and Android for Yammer have been updated. New features include the feed as the landing page, reduced visual clutter and improved readability, support for Live Events, and improved search capabilities within the scope of a given group, among others. Most new features are available immediately, while some are still rolling out. New Features and a New Look for Yammer Mobile (Yammer Blog, July 30).

Azure AD Identity Protection Updates

Description

Microsoft updated its Azure AD Identity Protection service, which seeks to protect organizations from identity attacks. The major update is the addition of new discrete events that are analyzed as part of the Unfamiliar Sign-In Properties attack monitor. Details include:

- The list of behaviors analyzed include device identifiers, IP address, location, tenant corporate IP addresses, IP carriers, available browser sessions, and the Exchange Active Sync Mail Client ID, among others.
- The traffic pattern of IP addresses seen by Azure AD are automatically captured and fed into the Identity Protection service, as part of reducing false positives.
- The separate behaviors are analyzed and grouped into one of four risk categories. The risk score for a given sign-in attempt is either high, medium, low or nothing detected. Conditional access policies can be set up that are responsive to different levels of sign-in risk.
- Microsoft claims that these changes have doubled its ability to detect compromised sign-ins (which seems right given the collection and consumption of additional signals), and also reduced its false positive rate by 30%.

Using the above capabilities requires Azure AD Premium P2 licensing.

Analysis

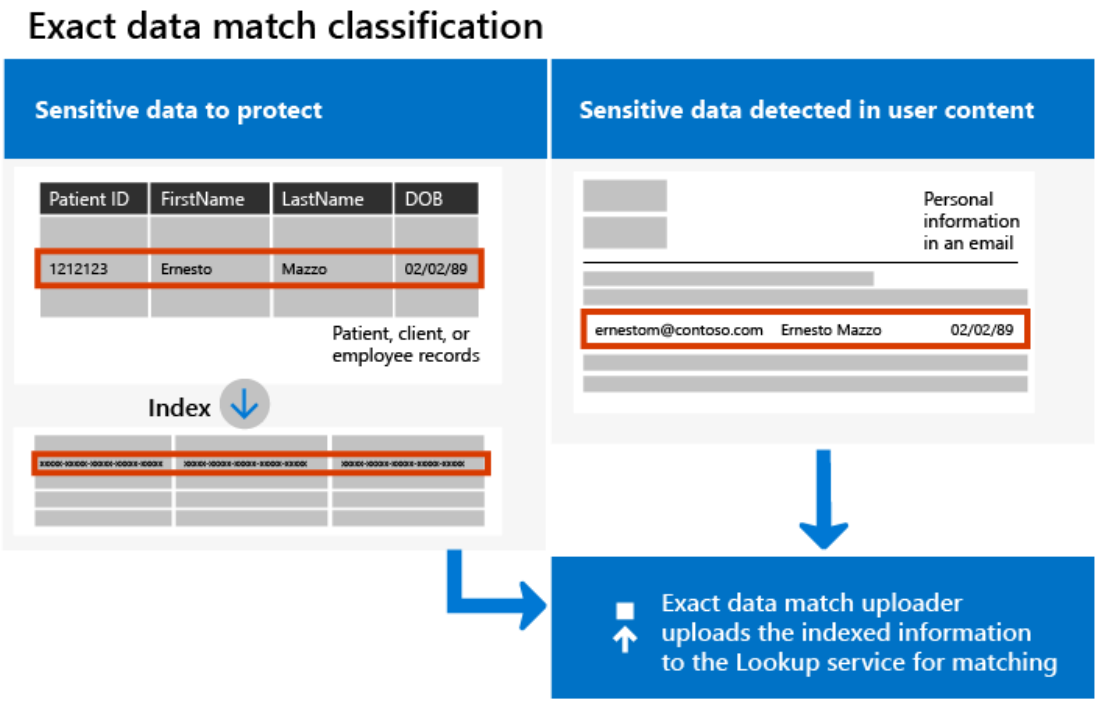
- The ability to create a differential conditional access policy based on the automatically computed risk score category is a compelling addition to Microsoft's playbook. Other vendors have had this ability for several years, and hence this has been missing-in-action from Microsoft's offering. Of particular note is the ability to drive an MFA prompt based on risk score.

About

- **Date** - August 1, 2019
- Presenting the New Unfamiliar Sign-In Properties (Azure AD Identity Blog, August 1)
- What is Azure Active Directory Identity Protection (Refreshed) (Microsoft Azure Docs)
- **Tag** - Security
- **Implication** - Azure AD Identity Protection

Exact Data Match in DLP

Description



Microsoft added the ability to use Office 365 DLP policies and Microsoft Cloud App Security DLP policies to match for exact data. The intent is to enable an organization to specify its sensitive data held in structured systems - for example, patient records, customer details, bank account numbers, etc. - and then give DLP policies the permission to attempt an exact lookup match of content in email messages and files against the authoritative structured systems. The new Exact Data Match option is an extension of the current custom sensitive information types in Office 365. Details include:

- Requires the organisation to upload its sensitive content to Microsoft, for indexing and storage in the Microsoft cloud.
- Works with Office 365 DLP policies for content in Exchange Online, OneDrive for Business, and Teams, along with the DLP policy engine in Microsoft Cloud App Security (as part of Microsoft 365 E5). SharePoint is not yet supported.
- Policy tips will be displayed for exact matches to warn a user that what they are attempting to do is in violation of an Office 365 DLP policy, starting with Outlook on the web. Support for other Office apps will be added in the future.

Analysis

- Exact Data Match is a good extension to the current matching approaches used in Office 365 DLP policies, which are based on matching against regular expressions. The ability to say precisely that a patient record or customer account is being inappropriately referenced in an email message is useful.
- The red flag in this new capability is the requirement to upload a customer's sensitive information to Microsoft, for indexing and availability for real-time lookup. This is also not a one-time requirement, because customer data will need to be kept up-to-date for the exact data match to work. Whether an organization is willing to hand over its complete collection of sensitive information to Microsoft for DLP policies remains to be seen, but we don't imagine the path to be an easy one.

About

- **Date** - August 8, 2019
- New Exact Data Match (EDM) Classification Helps You Better Detect and Protect Sensitive Information (Security, Privacy and Compliance Blog, August 7)
- **Tag** - DLP
- **Implication** - DLP in Security & Compliance Center

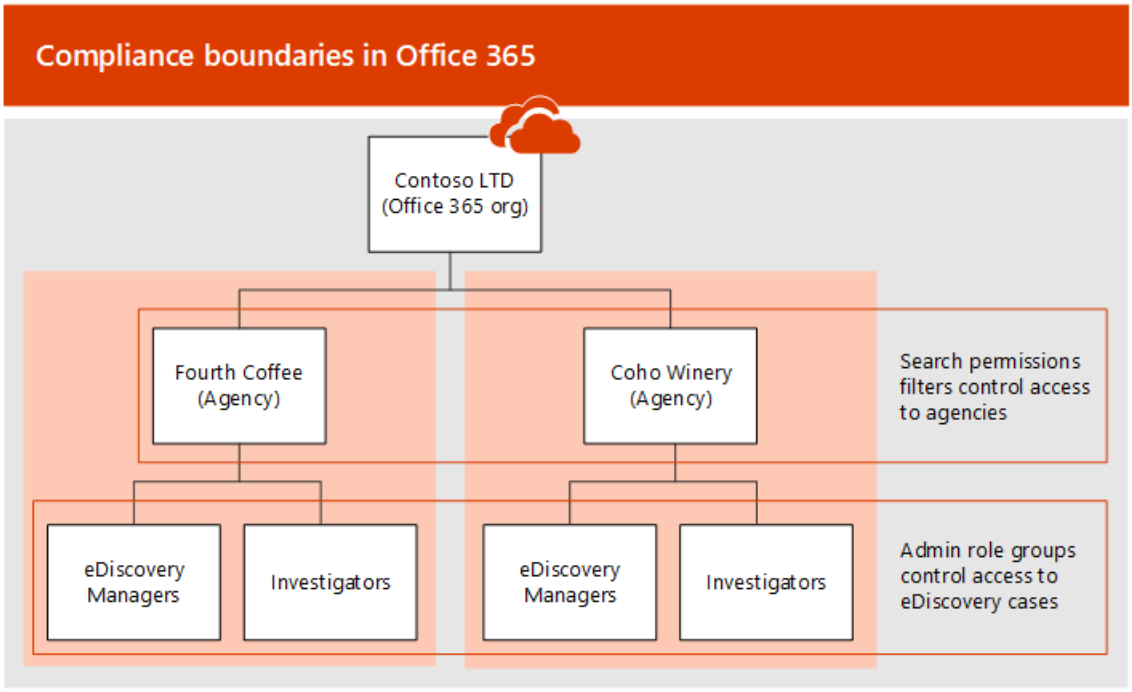
Weekly News Drop - August 9, 2019

Roundup of recent Office 365 news:

- **Single Day Retention of Teams Chats**. From September, Compliance Administrators will be able to set retention policies for Teams chats as low as a single day. Microsoft Teams - Shorter Retention (Microsoft 365 Roadmap 53936, July 30).
- **Microsoft Cloud App Security for GCC High**. Microsoft Cloud App Security, the CASB in Microsoft 365 (not Office 365) plans, will be made available to GCC High customers during Q1 of 2020. GCC High is one of the higher security cloud offerings from Microsoft to meet US Department of Defence requirements, including validation to access requirements and background check processes for users. Microsoft Cloud App Security for GCC High Customers (Microsoft 365 Roadmap 54016, August 1).
- **Azure ATP for GCC High**. Azure Advanced Threat Protection, a cloud service for detecting and investigating identity attacks and threats, will also be made available to GCC High customers in Q1 2020. Azure ATP for GCC High Customers (Microsoft 365 Roadmap 54017, August 1).
- **Phishing Detection (In)Effectiveness**. University of Plymouth academics tested the effectiveness of phishing controls across several email providers, and found that 75% of linkless phishing messages and 64% of phishing messages with links were not labelled as malicious in any way and went to the user's inbox. It is unclear which providers hosted the target mailboxes, and which domain was used for sending the messages (and thus what standing reputation for the email sending infrastructure was in place). Tech Companies Not Doing Enough to Protect Users from Phishing Scams (EurekAlert, July 30).
- **South Korea Data Residency for Microsoft Teams**. Effective July 9, Micosoft started offering in-country data residency for new Microsoft Teams customers in South Korea, from its two data centers in Seoul and Busan. Existing customers already using Microsoft Teams will continue to have data served from the current data centers. Microsoft Teams Launches South Korea Data Residency (Microsoft Teams Blog, August 6).
- **Azure AD Basic Deprecated**. Azure AD Basic was introduced in 2014 as the first step above the free Azure AD capabilities included in Office 365; priced at $1 per user per month, the Basic edition offered identity access to up to 10 apps per user. From July 1, Microsoft has removed the Basic service tier for new customers, but current customers can continue with the offering for the foreseeable future. Microsoft Is Phasing Out the Basic Edition of Azure Active Directory (ZDNet Microsoft, August 9).

Compliance Boundaries

Description



Microsoft enhanced the capabilities in Office 365 for creating logical boundaries to separate content locations that eDiscovery Managers can search. The same controls can be used to limit who can access eDiscovery cases. The intent is to support organizations who must comply with different regulations in different geographical areas, such as multi-national corporations and governments made up of multiple agencies.

Compliance Boundaries are enabled using PowerShell, via the search permissions filtering cmdlets.

- An organization wanting to create compliance boundaries must first nominate a user-level attribute in Azure AD that can be used to divide individuals into separate logical groupings, such as by department, company, office, or other. Microsoft has a specific list of attributes that can be used, in order to enable support across Exchange, SharePoint and OneDrive. Clearly, good processes will need to be in-place to ensure the nominated attribute is kept current for all employees.
- A support request must be filed with Microsoft Support to sync the nominated Azure AD attribute to all OneDrive accounts. This will also map the attribute to SharePoint as a hidden managed property. The completion of this support request can take 4-6 weeks.
- Role groups must be created in the Security & Compliance Center, in order to divide people with eDiscovery Managers rights into separate groups for accessing the separate agencies, departments or other groupings. When a new eDiscovery case is created, the correct role group needs to be given access rights.
- A PowerShell cmdlet is used to tie together a nominated attribute value and a specific eDiscovery Managers role group.
- For organizations using Multi-Geo, an additional parameter in the cmdlets can also be used to specify additional search constraints and which datacenter is used for exporting data. This provides further capability to keep relevant data within a specified geographical boundary. The use of Multi-Geo with compliance boundaries also introduces some implications for the search rights of eDiscovery Managers.
- There are still some anomalies that Microsoft needs to fix over time. For example, while the cmdlets will prevent the return of search results of content locations in a different boundary, an eDiscovery case can still include content locations beyond the boundary. The boundary is enforced below the level of the user experience, which could lead to confusion as a consequence of eDiscovery Managers selecting locations they don't actually have permissions to search. Secondly, compliance boundaries are ignored for legal holds, meaning that an eDiscovery Manager in one boundary can still put users in other boundaries on legal hold. Third, compliance boundaries do not apply to Exchange Public Folders.

Analysis

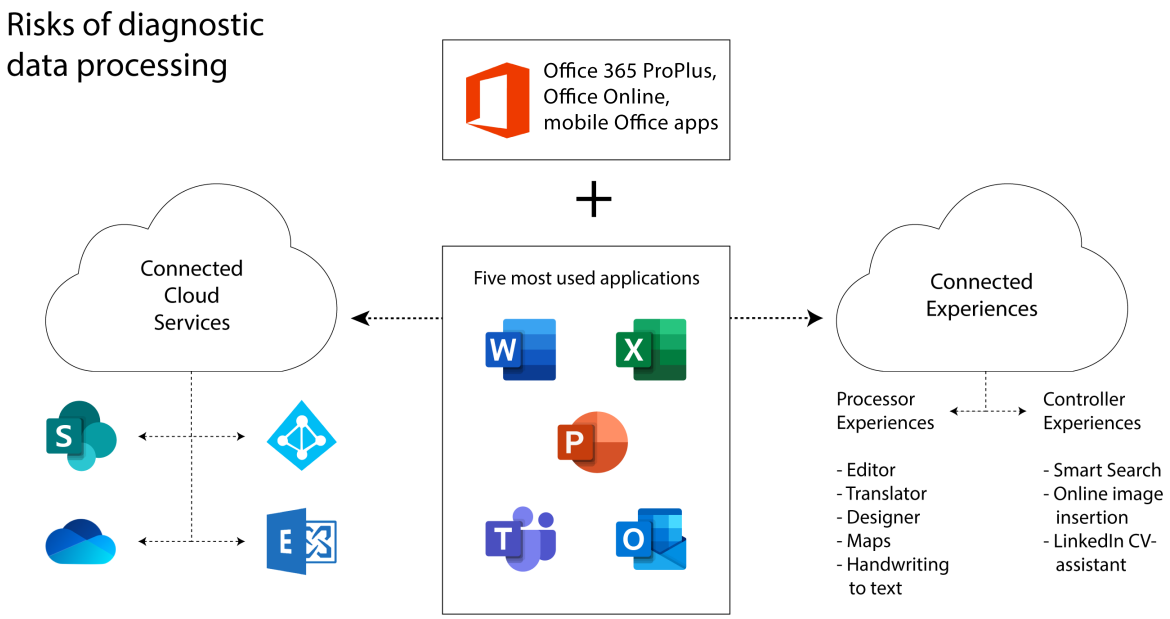
- Having a structured way to enforce logical boundaries between content is important for large, complex organizations when moving to the cloud. The architecture of a single worldwide tenant with or without Multi-Geo support comes with the requirement to create boundaries in some way; previously this would be done with separate physical infrastructure and therefore separate physical boundaries in an on-premises world.
- Since the user-level attribute offers a real-time status of the boundary affilitation of a user, it is unclear how Microsoft handles eDiscovery searches for previous time periods where the user was affiliated with another boundary. For example, if a 2019 case requires searches against Department1 data locations from calendar year 2017 when User1 was in that department but User1 moved to Department2 in 2018, will User1's data sources still be searched? It would appear the answer is no, and therefore potentially responsive material will be excluded by design.

About

- Date - August 12, 2019
- Set Up Compliance Boundaries for eDiscovery Investigations in Office 365 (Microsoft Docs)
- **Tag** - eDiscovery

Netherlands on Data Privacy Risks

Description



In a follow-up to its earlier DPIA on Office 365 ProPlus, The Privacy Company in the Netherlands published three additional DPIAs looking at the data privacy risks in Office Online, the mobile Office apps, and Windows 10 Enterprise. The Privacy Company noted that Microsoft has fully addressed the eight privacy risks identified in Office 365 ProPlus in November 2018 through a combination of technical, organizational and contractual measures, but observes that these measures have not been applied to Office Online, the mobile Office apps, and Windows 10 Enterprise. For example:

- At least three of the mobile Office apps on iOS - Word, Excel, and PowerPoint - send data about the use of these apps to an American marketing company for predictive profiling.
- System-generated logs and the various telemetry clients regularly send diagnostic data on the use of Office and Windows 10 Enterprise to Microsoft's servers in the United States. Such diagnostic data includes personal data about user behavior.
- Microsoft processes diagnostic data for Windows 10 Enterprise for many broad and undefined purposes, which is contrary to the GDPR principle of purpose limitation; Microsoft has no legal basis for undertaking such processing.
- Unlike the measures introduced for Office 365 ProPlus, similar measures are not available for Office Online, the mobile Office apps, and Windows 10 Enterprise. For example, there is no similar opt-out option for the collection of diagnostic data for an administrator covering Office Online and the mobile Office apps.

The DPIAs were carried out on the behalf of the Netherlands government. The government has also secured audit rights of Microsoft's practices, offering an annual snapshot of compliance with the agreements in place. The findings of this annual audit - as executed by an independent third-party - will be published by SLM Rijk (the government agency responsible for the Microsoft relationship).

The conclusions and recommendations raised by The Privacy Company include:

- That government agencies avoid the use of Office Online, the mobile Office apps on iOS and Android devices, and set the data collection level in Windows 10 Enterprise to the lowest possible setting.
- Private sector organizations in the Netherlands should likewise be cautious, and should negotiate privacy guarantees from Microsoft, although this is probably better handled through an umbrella agreement via an industry body or professional association rather than one-by-one with Microsoft.

Analysis

- The Privacy Company was very clear in its earlier DPIA that only Office 365 ProPlus was covered. Once Microsoft committed to responding to the identified data privacy risks from the first DPIA, it was only a matter of time before the scope of analysis

extended to other parts of Microsoft's offering.
- Microsoft rolled out at least three of the improvements to Office 365 ProPlus to a much broader market than just the Netherlands. The contractual agreements, however, are currently only operational in the Netherlands, but in essence, are there for the taking by any government in Europe or beyond that wants to follow a similar approach. But this will require negotiation.

About

- **Date** - August 15, 2019
- New DPIA on Microsoft Office and Windows Software: Still Privacy Risks Remaining (Long Blog) (The Privacy Company, July 29)
- Windows 10, Office Online Users Get New Warning Over Data Privacy (ZDNet, July 30)
- **Tag** - Security

Weekly News Drop - August 16, 2019

Roundup of recent Office 365 news:

- **Azure AD Provisioning Updates**. Microsoft announced additional third-party app support in Azure AD Provisioning, enabling policy-based provisioning from Azure AD to apps such as Oracle Fusion ERP, Envoy, Federated Directory, Zoom, and others. It also announced new insights for managing and monitoring the status and progress of provisioning cycles. Azure AD Provisioning, Now with More Apps and Better Insights (Azure AD Identity Blog, August 12).
- **New Multi-Geo Locations**. Following on from the recent release of datacenter capabilities in South Africa and the United Arab Emirates, Microsoft announced that these locations are now active for Multi-Geo across Exchange Online, OneDrive, SharePoint Online, and Office 365 Groups data. Multi-Geo Capabilities in Office Now Available in South Africa and the United Arab Emirates (SharePoint Blog, August 12).
- **Advanced Hunting in Microsoft Threat Protection**. Microsoft added the ability to hunt for threats across endpoints and email using query language in Microsoft Threat Protection. Various query templates are offered to support hunting. The capability builds off the threat hunting experience already available in Microsoft Defender ATP. The Evolution of Microsoft Threat Protection - July Update (Microsoft Security Blog, July 29).

Microsoft Cloud App Security Updates (151 to 153)

Description

Microsoft released multiple updates to Microsoft Cloud App Security, spanning three releases from June 9 to July 7. The updates included:

- Tightening of admin access, including new read-only admin roles, 90-day audit data on all admin activity, and a configurable timeframe for automatic sign-out of admin sessions.
- For anomaly detection policies - files identified as malware by automated scanning but subsequently confirmed as safe by manual review can be marked as authorised (clean) ... which removes it from the malware detection report and suppresses future matches on the file.
- The presence of a disaster recovery plan was added as a new risk factor to the Cloud App Catalog. The intent is to enable the assessment of apps for business continuity.
- Conditional Access App Control was released to general availability for OneDrive for Business, SharePoint Online, Azure DevOps, Exchange Online, and Power BI. Conditional Access App Control enables the enforcement of conditions on users, networks, devices and more in order to grant access to apps.
- Linking any web app with session and sessions policies using Conditional Access App Control was released to preview.
- File policies now support the use of the trash governance action, for automatically moving files to the trash folder. This action was enabled for files in Google Drive and Dropbox.
- The Investigation Priority Score was enhanced to pick up activities and actions that on their own are not suspicious enough to trigger alerts. The aggregation of all risk events - regardless of size - is intended to show threat-laden happenings.
- Support for connecting with Microsoft Flow was released to general availability, enabling SecOps teams to develop a customized workflow for alerts.
- The integration with Azure ATP was released to general availability, for providing a single view of identity activities across both cloud apps and the on-premises network. The intent of the integration is to prevent identity threats on the on-premises network hiding from Microsoft Cloud App Security and thus preventing a comprehensive analysis of identity threats facing the customer.

Analysis

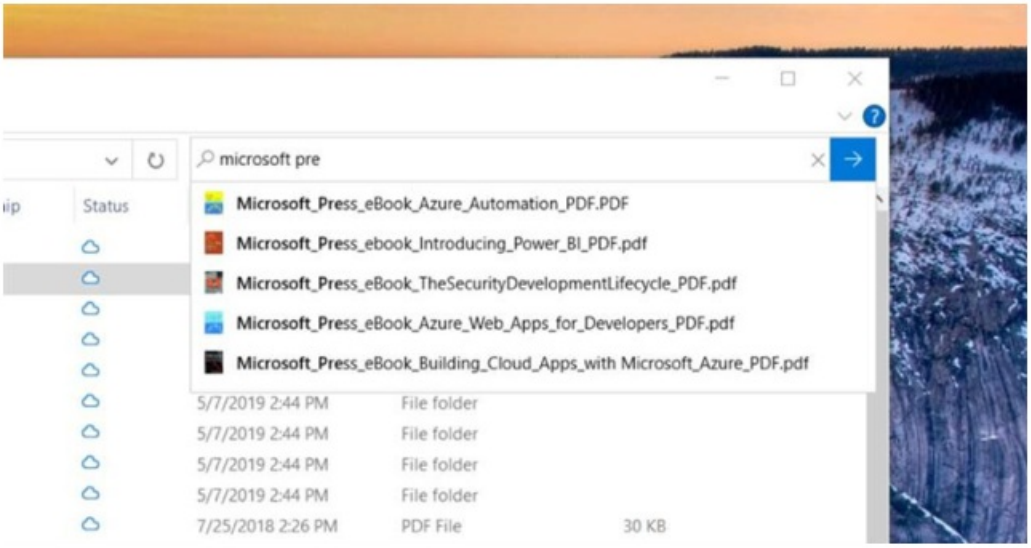
- Microsoft continues to enhance and refine its top-end cloud access security broker. Some of these capabilities are likely to find their way into the Office 365 Cloud App Security offering too.

About

- **Date** - August 19, 2019
- What's New with Microsoft Cloud App Security - Updates 141 to 153 (July 7, 2019)
- **Tag** - Security

File Explorer Search in Windows 10

Description



The most recent Windows Insider Preview Build of Windows 10 includes a change in the search approach used in File Explorer. The search box in File Explorer is now powered by Windows Search, which means that the overall search results combine local files stored on the device in combination with files stored in a user's OneDrive account.

Analysis

- Online file storage services eliminate the need for a user to store all their files on a given device. This supports easier movement between a collection of devices across a business day. The seamless integration of local search results with OneDrive search results gives the right signal to the user: it's all your content, and you have access to all of it from one place.

About

- **Date** - August 21, 2019
- Announcing Windows 10 Insider Preview Build 18362.10014 and 18362.10015 (19H2) (Windows Blog, August 19)
- **Tag** - File Sharing
- **Implication** - File Sharing - Overview

SharePoint Files Restore Failure

Description

After suffering a ransomware attack, the administrator of an Office 365 tenant in Asia attempted to use the SharePoint Files Restore feature to roll-back a document library to its pre-encrypted state. It didn't work very well. Details:

- The ransomware infection encrypted over 32,000 documents in the Projects subfolder of a document library.
- The restore point date slider in SharePoint Files Restore became unresponsive when the administrator attempted to drag it back to a date/time that was pre-attack. The admin machine needed to be restarted several times, but despite multiple attempts, the admin was unable to select the preferred date.
- The admin had to opt for a restore point two days after the infection began. Files were restored, but many of these files were still encrypted.
- The admin still could not use the slider to select the preferred date/time, so had to opt for a canned timeframe that was significantly before the infection began. This meant the loss of multiple files and changes to files.

Analysis

- Large document libraries (and subfolders in such libraries) are not well-supported by SharePoint Files Restore. The customer in this instance apparently lost about two weeks worth of new files and file changes due to the inability of Files Restore to work as advertised. The customer is hopeful that lost files can be recovered from other repositories, or lost files and file changes can be recreated.

About

- **Date** - August 22, 2019
- When Technology Fails: Woes With SharePoint Online Restore this Library (Petri, August 20)
- **Tag** - File Sharing
- **Implication** - SharePoint Files Restore

Weekly News Drop - August 23, 2019

Roundup of recent Office 365 news:

- **Office 365 ATP Automated Incident Response Data Availability**. Microsoft announced that information about AIR investigations will be exposed through the Office 365 Management Activity API, so that customers can leverage AIR intelligence in custom tools; event data will be sent each time the status of an investigation changes. Event data will include investigation metadata, a link to the investigation, and high-level information about actions and associated entities. Office ATP AIR - Exposing Investigation Data Through Management Activity API (Microsoft 365 Roadmap 53624, August 15).
- **Reviewing Errors in Advanced eDiscovery Review Sets**. From September 2019, eDiscovery Managers will be able to remediate or ignore errors within a review set one by one, rather than as a group. The intent is to improve the review experience by enabling reviewers to see more detailed information about documents before making a decision to take further action or ignore the error. Advanced eDiscovery Single Item Error Remediation (Microsoft 365 Roadmap 54398, August 15).
- **Phishing Detection on Microsoft Forms**. Microsoft is extending its phishing detection for Microsoft Forms to include forms used within an organization. This change will be enabled in September 2019, and is in addition to the recently released phishing detection for public forms. Automatic Phishing Detection for Enterprise In-Org Forms (Microsoft 365 Roadmap 54433, August 16).
- **Microsoft Graph Security API Add-on for Splunk**. Microsoft released a new way of integrating security alerts with Splunk Enterprise, with alerts being streamed from a range of Azure, Microsoft 365 and Office 365 security services into Splunk. The new offering replaces the earlier Azure Monitor add-on for Splunk. Introducing the New Microsoft Graph Security API add-on for Splunk (Security, Privacy and Compliance Blog, August 21)

Weekly News Drop - August 30, 2019

Roundup of recent Office 365 news:

- **User Templates in Microsoft 365 Admin Center**. Microsoft announced that in September 2019, it will introduce the ability to define templates for creating new users in the Microsoft 365 Admin Center. Default attributes in the user template are automatically applied when creating a new user from the template. Create Users with Templates in the Microsoft 365 Admin Center (Microsoft 365 Roadmap 54434, August 23).
- **Irish DPA Investigating Data Collection in Windows 10**. The data protection agency in the Netherlands raised concerns regarding the collection of non-diagnostic data in Windows 10, and has asked its counterpart in Ireland to evaluate further. The Irish DPA is the lead DPA for Microsoft, since Microsoft's European operations are headquartered in that country. Microsoft Improves Privacy Protection But Further Investigation Needed (Dutch DPA, August 27).

Synchronous URL Detonation

Description

Microsoft is adding a new policy option to ATP Safe Links policies, which if enabled, will mean that URLs in email messages are tested for malicious behavior before delivery to the recipient.

- Enabling the setting will mean that users will not see the notification page advising them that the URL they clicked is being scanned.
- If a message contains a malicious URL, the email will be routed to the user's Junk Folder (the default setting), or another location based on the policy setting.

Synchronous URL detonation is expected to be available in July 2019.

Analysis

- If a URL is malicious at the time a message is received, preventing the message from landing in a user's inbox is essential.
- The roadmap item for synchronous URL detonation makes no mention of time-of-click URL detonation in addition to pre-delivery URL detonation, but with attackers able to weaponize URLs after the delivery of a message (in order to circumvent pre-delivery checking), it is almost certain that pre-delivery clearance will have no impact on post-delivery time-of-click checking. It would be pure madness on Microsoft's behalf to assume that a pre-delivery check was sufficient.
- On the other hand, since the intent of the setting is to prevent the user from seeing the "we're scanning the URL" notification page, perhaps enabling this setting will turn off subsequent time-of-click URL detonation until the URL is re-classified as malicious.
- Let's assume 100 recipients at an organization receive the same message. For the first 99 recipients, pre-delivery URL checks turn up no malicious behavior and therefore the email is delivered to each recipient's inbox. By the time the final message is received and scanned, however, the URL has been weaponized and the final message is delivered to the recipient's Junk Folder. It is unclear whether the first 99 messages will be automatically reclassified as malicious and moved to Junk by Zero Hour Auto-Purge (ZAP), or if they will remain in inboxes but in a newly weaponized state.

About

- **Date** - July 2, 2019
- Synchronous URL Detonation in Office 365 ATP (Microsoft 365 Roadmap 52683, June 27)
- **Tag** - Security
- **Implication** - Advanced Threat Protection

Anti-Phishing Policy Update

Description

In February 2019, Microsoft announced a forthcoming change to the handling of intra-org spoof and DMARC failures, for delivery before the end of March 2019 (see Microsoft 365 Roadmap Updates - March 25). Those changes were not implemented on that timeline, and are now scheduled to begin by the end of July, for completion during August 2019.

The changes mean that:

- The Anti-Phishing policy will continue to manage cross-organization spoof situations.
- The Anti-Phishing policy will newly also manage intra-organization spoof and DMARC failures. This was previously handled by the Anti-Spam policy.
- All email messages will newly be stamped with a composite authentication result that gives Microsoft's verdict on the authentication of the email message. Options for the compauth header are pass, fail or none. A reason will also be given.
- Some messages that would previously have been classified as spam will now be marked as spoofing attempts, and will therefore be dealt with according to the spoof action, not the spam action. This is likely to reduce the quantity of spam in a user's Junk Folder, for example.

Analysis

- Microsoft is hoping that tenant administrators will become more intentional about email authentication and spoofing settings, in order to give richer signals about who is validly allowed to spoof their domain name.
- While spam is annoying, phishing is dangerous. Lost credentials due to a successful phishing lure can result in unauthorized access to data, high-reputation spam and phishing, business email compromise, and more. Tightening the screws is a good move.

About

- **Date** - July 2, 2019
- Updated Feature: We're making some changes to anti-spoofing enforcement actions (Office 365 Message Center MC183701, June 28)
- **Tag** - Security

Threat Explorer Hunting Updates

Description

Microsoft made several changes to the hunting experience in Threat Explorer, in order to improve the manual threat hunting experience for security administrators. Changes are:

- The previous singular value of delivery status has been split into multiple values. Delivery Status is renamed Delivery Action, with values of Delivered, Junked, Blocked, or Replaced. Delivery Location - a new column - specifies where the email is currently located, with options of Inbox/folder, On-prem/external, Junk folder, Deleted items folder, Quarantine, Failed, or Dropped). Special Action - another new column - specifies any events that occurred after delivery of the email (e.g., ZAP, Dynamic Delivery). In combination, the three values are intended to help an admin know what actions were taken on an email and where it is currently located.
- A new timeline view is being added to Threat Explorer. When available, the timeline view will show the thread of multiple events happening to an email message.
- Admins will have the ability to view and download malicious email messages for further analysis.

The above changes are expected to be available worldwide by end July 2019.

Analysis

- Simplifying the ability to understand current threats is a good move. The previous setup carried too much information in a single column value, decreasing the ability for an administrator to understand what was happening and take appropriate remediation actions.

About

- **Date** - July 4, 2019
- Improvements to Threat Explorer For Better Hunting Experience (Microsoft 365 Roadmap 52595, June 27)
- **Tag** - Security

Weekly News Drop - July 5, 2019

Roundup of recent Office 365 news:

- **Office 365 in Virtualized Environments**. Microsoft announced a series of improvements in Office 365 ProPlus in multi-user virtual environments. ProPlus will be supported on Windows Server 2019, in order to provide virtual desktop services to users. Windows Server 2019 will also support OneDrive Files On-Demand, allows users to have quick access to their most frequently used and preferred files, while minimizing disk storage requirements. The improvements are based on the virtualization technology acquired via FSLogix. Improving the Office App Experience in Virtual Environments (Microsoft 365 Blog, July 1).
- **New Storage Providers in Outlook on the Web**. Outlook on the web will support new storage providers - e.g., personal OneDrive, Google Drive and Facebook - and these options are available by default; due for release in July 2019. Outlook on the Web with 3rd Party Storage Providers (Microsoft 365 Roadmap 525297, June 24).
- **More Microsoft 365 Integrated Goodness**. Microsoft's 2020 fiscal year started on July 1. One strand of Microsoft's strategy over the coming year is to drive greater integration across the previously separate capabilities of Office 365, Windows 10, and Enterprise Mobility + Security that were bundled as Microsoft 365. From now on, it's less about bundling and more about integration and cohesiveness. Microsoft Wants to Start Marketing Microsoft 365 as a Single Product in its New Fiscal Year (ZDNet Microsoft, July 2).
- **ATP Plan 1 Gets Custom Phish Alert Option**. Customers on ATP Plan 1 will be able to create a custom phishing alert for the activity type "Phishing email detected at time of delivery." This was previously only available in ATP Plan 2 (and by implication, for customers using E5). The alert can be further scoped using several configuration options. Roll-out starts July 1, and is intended to be available worldwide by July 19. Ability to Create Custom Phish Alerts for Customers with Office 365 ATP P1 (Microsoft 365 Roadmap 52769, June 28).
- **Threat and Vulnerability Management Released**. Microsoft released its new Threat and Vulnerability Management extension to Microsoft Defender ATP to general availability on June 30, 2019. It adds a risk-based approach to discovering, prioritizing, and remediating endpoint vulnerabilities and misconfigurations, and relies on continuous vulnerability scanning. Microsoft's Threat & Vulnerability Management Now Helps Thousands of Customers to DIscover, Prioritize, and Remediate Vulnerabilities in Real Time (Microsoft Security Blog, July 2).

Automatic Guest Account Creation in Azure AD

Description

Microsoft announced the preview of an integration between SharePoint / OneDrive and Azure AD B2B for external sharing. Instead of SharePoint / OneDrive separately handling external sharing, Azure AD B2B is now in charge of the process. Details are:

- When a user shares an item from SharePoint or OneDrive with an external user, a new guest account is immediately created for the new external user in Azure AD. If an account already exists for the external user, this is used instead of creating a new one.
- Applies to the sharing of files and folders across both OneDrive and SharePoint. Additionally, it applies to list items, document libraries, and sites in SharePoint.
- The preview was released at the end of June 2019, and will be available everywhere by the end of July 2019.
- The benefit of these changes is that new control sign-in and access options are available over a guest account as defined in Azure AD, such as conditional access policies. There will also be fewer places to check for guest users with access to resources in the tenant.

Analysis

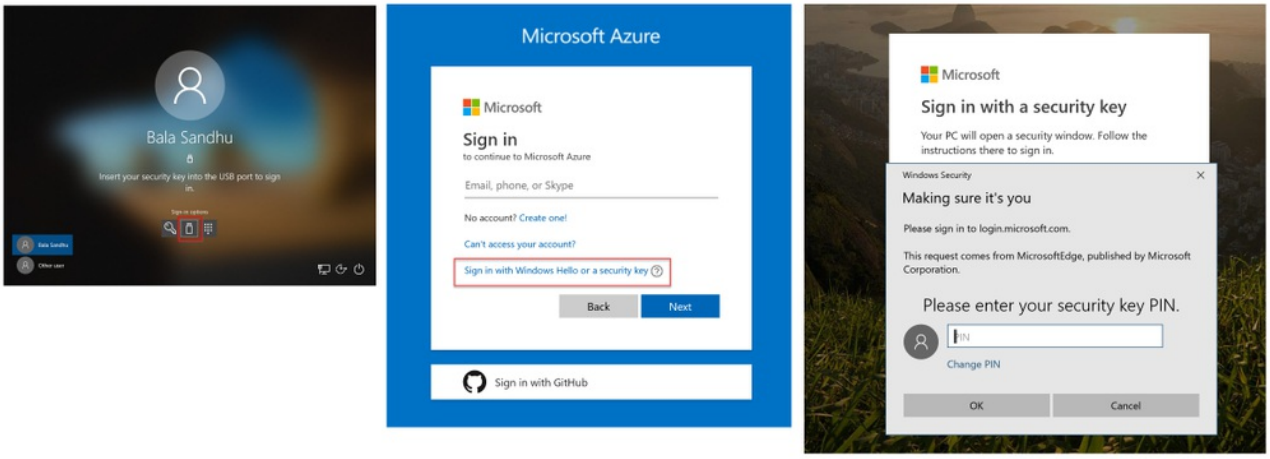
- Streamlining external sharing options into Azure AD enables customers to benefit from the massive investments Microsoft is making into that identity platform. For example, administrators should have the ability to now enforce some lifecycle controls over all guest accounts.

About

- **Date** - July 5, 2019
- New Feature: OneDrive & SharePoint Integration with Azure AD B2B (Preview) (Office 365 Message Center MC183679)
- SharePoint and OneDrive Integration with Azure AD B2B (Preview) (Microsoft Docs, July 3).
- **Tag** - File Sharing

Passwordless with Azure AD

Description



Microsoft released the public preview of passwordless authentication with Azure AD using FIDO2-based security keys, including the Microsoft Authenticator app. Microsoft argues that passwords are no longer an effective security mechanism, and something very different is necessary. Details of passwordless authentication include:

- Once set up, users will be able to sign-in to Azure AD-connected apps and services without using a password. Each user will require a FIDO2-based security key, the Microsoft Authenticator app, or Windows Hello. Or multiples thereof.
- Microsoft updated the admin portal for Azure AD, adding a new Authentication Method Policy blade in public preview. This enables an Azure AD administrator to configure users for passwordless authentication.
- Once enabled for passwordless authentication by an admin, users can add authentication methods including security keys.
- While Microsoft Authenticator is a valid FIDO2-based authenticator, Microsoft has also partnered with security key hardware providers to support other form factors. The initial three partners are Feitian Technologies, Yubico, and HID Global.

The public preview is available immediately.

Analysis

- This announcement covers accounts in Azure AD, such as Office 365 work and school accounts. Microsoft released passwordless authentication for Microsoft accounts in June. See Weekly News Drop - June 14.
- Many of the security tools in Microsoft's toolkit aim to mitigate the effects of a compromised password or identify when a compromised password is being used by an attacker. By going back to the root of the problem and offering ways to eliminate passwords entirely, a complete set of follow-on problems should eliminated or greatly reduced.
- Loss of a phone or security key is going to be annoying. Administrators will have the ability to reissue keys, but the cost of "resetting my password" is going to leap from only a call to the help desk to a call to the help desk plus the cost of a new physical security key. This cost will, however, be less than the cost of a security breach.

About

- **Date** - July 10, 2019
- Announcing the Public Preview of Azure AD Support for FIDO2-Based Passwordless Sign-In (Azure AD Identity Blog, July 10)
- Microsoft Passwordless Partnership Leads to Innovation and Great Customer Experiences (Azure AD Identity Blog, July 10)
- Your Pa$$word Doesn't Matter (Azure AD Identity Blog, July 9)
- What is Passwordless? (Microsoft Docs, July 9)
- **Tag** - Authentication
- **Implication** - Passwordless Authentication with Azure AD

Weekly News Drop - July 12, 2019

Roundup of recent Office 365 news:

- **More About Teams, Less About Windows**. As Microsoft's 2020 financial year begins, indications are that the company and its sales force will focus more on pushing Microsoft Teams than Windows upgrades. Teams is expected to be a major focus at the upcoming Inspire 2019 conference for Microsoft partners as well. Microsoft Shifts Sales Focus From Windows to Teams (Petri, July 8).
- **Roles Page in Office 365 Admin Center**. Microsoft is adding an admin roles page to the modern Office 365 Admin Center, in order to give clearer visibility into who has what admin rights in a given tenant. "*We're improving how you manage admin roles in the Microsoft 365 admin center. It will be easier to see who has admin access and to assign roles that grant the right level of access to your admins. We are rolling out this feature to Targeted Release customers and will begin rolling it out to worldwide production in July. Today, you can view, add, or remove admin roles for a specific user from the Active users page. We're adding a Roles page accessible from the left navigation pane in the new admin center to extend your capabilities. With this experience you can export a list of all admins in your org who are assigned Azure Active Directory roles that apply to Microsoft 365 services. You can view all admins assigned to a specific role, add or remove admins from a specific role, search for roles by name and keyword, and learn more about what each role allows a user to do.*" Updated Feature: Manage Admin Roles in the Microsoft 365 Admin Center (Microsoft 365 Roadmap 52624, June 24).
- **Microsoft Teams at 13 Million Daily Active Users**. Microsoft changed its way of reporting user numbers for Microsoft Teams, which has previously been about use at X thousands of organizations. Now that the daily active user count for Microsoft Teams is greater than Slack, Microsoft announced a number of 13 million active daily users after 2 years in market, compared to 10 million for Slack at its most recent public disclosure. Microsoft also announced several in-progress and forthcoming updates to Teams, including announcement posts, geo-fenced time clock for clock-in and clock-out at a work site, and policy packages for IT admins. Microsoft Teams Reaches 13 Million Daily Active Users, Introduces 4 New Ways for Teams to Work Better Together (Microsoft 365 Blog, July 11).
- **Microsoft Virus Initiative Joins Microsoft Intelligent Security Association**. The Microsoft Virus Initiative, founded more than 20 years ago to enable Microsoft and antivirus / antimalware vendors to collaborate on security solution development, has been folded into The Microsoft Intelligent Security Association. Microsoft says that antivirus and antimalware technologies "have long been the backbone of security solutions," and wants these capabilities reflected in the newer Intelligent Security Association. Microsoft Intelligent Security Association Welcomes Members of the Microsoft Virus Initiative (Microsoft Security Blog, July 11).
- **Automated Phishing Detection in Microsoft Forms**. Microsoft said it will be adding automated phishing detection to Microsoft Forms in July, to prevent customers from losing sensitive data via phishing forms. The Microsoft Office Support article about the change notes that Microsoft has "automated machine reviews" for detecting malicious password collection, and there is also a manual option whereby an end user can report a form for suspected phishing (if, for example, it requests a password). Automated Phishing Detection (Microsoft 365 Roadmap 52927, July 12).

Authentication Methods Reporting

Description

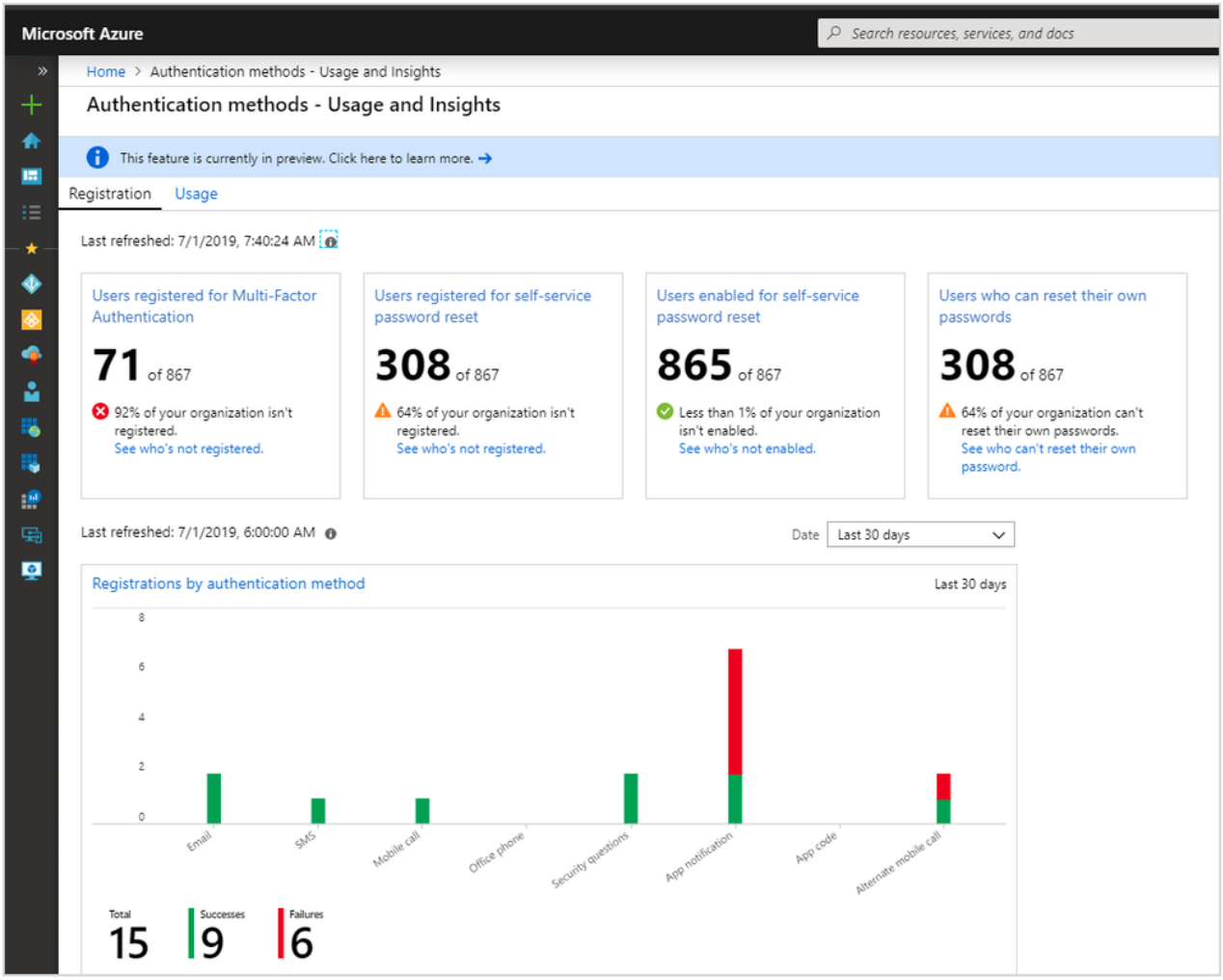


Figure 1. Authentication Methods Registration overview.

Microsoft announced new reporting capabilities for authentication methods and usage in Azure AD, focused on multi-factor authentication and self-service password reset. The new capabilities entered public preview on July 11, 2019.

The reports:

- Show the number of users registered for MFA and SSPR, and users enabled for SSPR.
- Offer summary data (above) as well as detailed reports at a per user level.
- Provide visual data on resets and account unlocks by method.

Analysis

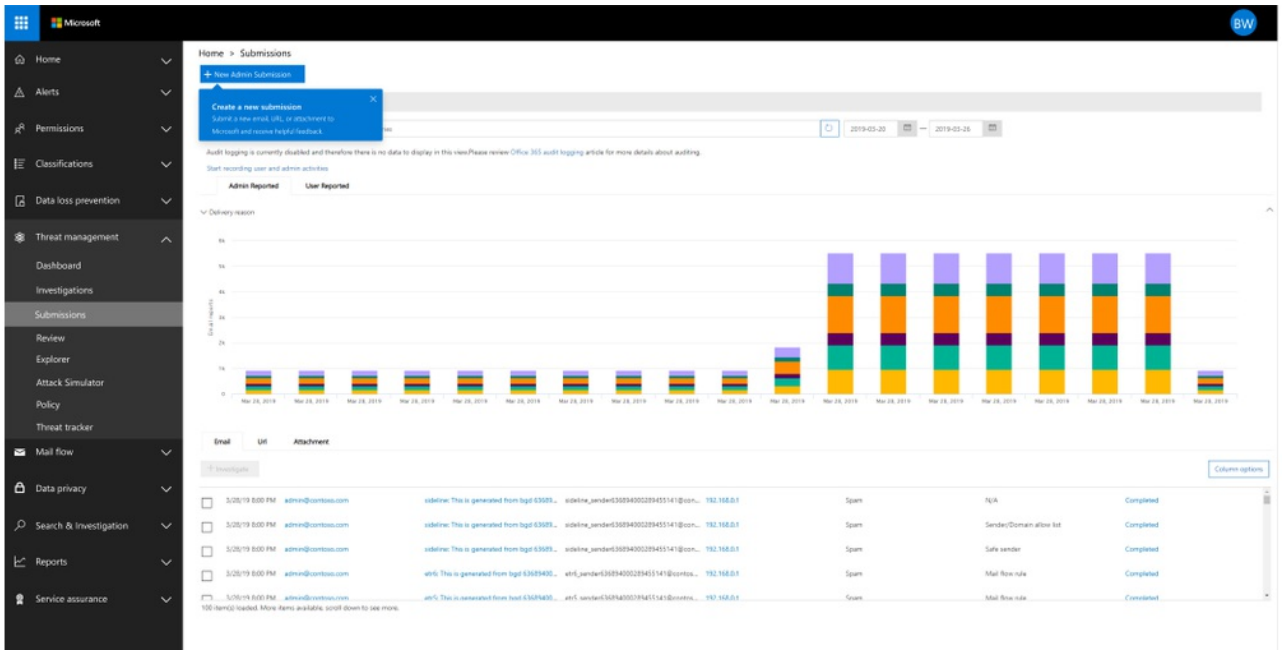
- The capability is only at public preview. Before being released, Microsoft will need to more cleanly differentiate between internal users and other types that are currently tracked (e.g., shared mailboxes, guest accounts, users with blocked sign-in). The current reports also do not report on passwordless users, although this is apparently in progress / under development.

About

- **Date** - July 15, 2019
- Authentication Methods - Usage & Insights (Azure AD Identity Blog, July 11)
- **Tag** - Authentication

Admin Submissions for Suspicious Emails

Description



Microsoft added the ability for a security administrator to submit suspicious emails and content to Microsoft for analysis, in order to determine why a message was or was not delivered to an end user. Microsoft's analysis is promised to pinpoint the specific cause, offering admins visibility into the correct next step to tighter or loosen a policy setting, or speak to an end user about one of their policy settings in Outlook.

Analysis

- Controlled submissions to Microsoft with direct feedback on the explanation for behavior is a good addition to the threat management capabilities in Office 365. Microsoft's greater visibility enables an admin to better protect their own organization, and is reflective of the type of dance necessary between the cloud provider and the organizational tenant in a shared security model.
- In explaining the reasoning for the new capability, Microsoft said "*some organizations don't want their users to submit emails directly to Microsoft, as they may contain sensitive information - and therefore want their security team to review the emails before they are submitted to Microsoft.*" There does not seem to be, however, the ability for an admin to turn off direct reporting of end user submissions to Microsoft, only the addition of admin reporting.
- Microsoft indicated that a future version will "automatically fix" config-related issues for the tenant, a potential minefield for crossing the boundary in the shared security model.

About

- **Date** - July 17, 2019
- Empower Security Teams to Easily Report Suspicious Emails & Content and Receive Instant Feedback (Security, Privacy and Compliance Blog, July 12)
- Admin Submissions in Office 365 (Microsoft Docs, July 9).
- **Tag** - Security

Weekly News Drop - July 19, 2019

Roundup of recent Office 365 news:

- **Warning Pages for ATP Safe Links Updated**. Microsoft updated the color scheme and design of its warning pages for ATP Safe Links, for when ATP is scanning a link, a URL is in a suspicious email message, the URL is in a message identified as a phishing attempt, a site has been identified as malicious, a site is blocked, or some other kind of error has occurred. The new designs have bolder color differentiations, more details on what is happening, and offers the ability for the user to proceed to a site regardless of the warning and recommendation to steer clear. Office 365 ATP Safe Links Warning Pages (Microsoft Docs, July 10).
- **Revised Expiration Policy for Office 365 Groups**. Microsoft announced the private preview of a revised expiration policy for Office 365 Groups. Expiration policies previously worked on the basis of explicit action by an owner to renew the group. The new approach adds automatic renewal based on owner or user activity within an app connected to the Office 365 Group, e.g., viewing a document in a SharePoint document library automatically renews the lifetime of the group. Other conditions remain unchanged, such as that groups are soft-deleted for 30 days before being hard-deleted if not recovered in that timeframe. Participation in the private preview is available to selected customers with Azure AD Premium. User Activity Based Expiration Policy for Office 365 Groups is Now in Private Preview (Office 365 Blog, July 18).

Symantec on BEC Numbers

Description

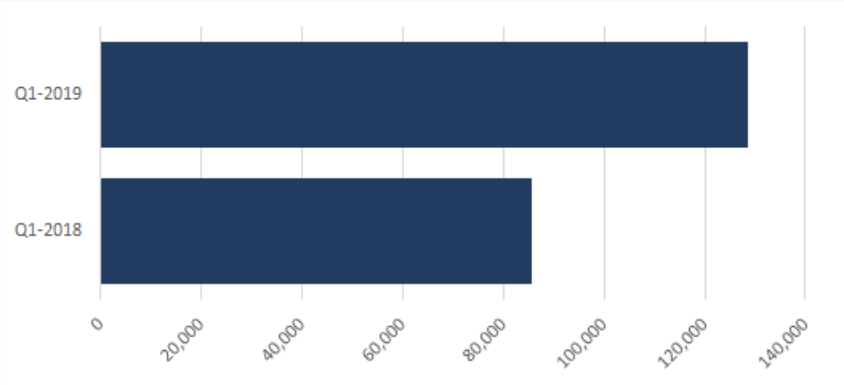


Figure 1. BEC average daily volume was 50 percent higher in Q1 2019 than Q1 2018

Symantec offered a review of the numbers for business email compromise scams over the past 12 months. Key numbers from Symantec's telemetry:

- Average daily BEC email volume increased 50% year-on-year for the three months January-March 2018 and January-March 2019. Symantec says the volume went from 85,000 in 1Q 2018 to 129,000 in 1Q 2019.
- These BEC threats are focused on around 6,000 organizations per month.
- On average, a business is receiving five BEC email scams per month.
- Organizations in the US and UK are the most heavily targeted by BEC scammers.

The FBI's Internet Crime Complaint Center reported losses from BEC scams at US$1.3 billion for 2018; this is on the basis of reported BEC losses only, so the actual number including non-reported losses will be much higher. Regardless, it's a lucrative scam.

Analysis

- BEC scams require looking for the proverbial very small needle in a haystack. With only five BEC threats per business per month, pinpoint accuracy in detection is essential. Symantec also highlights the need for complementary security awareness training to increase human wariness of this threat vector.

About

- **Date** - July 25, 2019
- BEC Scams Remain a Billion-Dollar Enterprise, Targeting 6K Businesses Monthly (Symantec Threat Intelligence Blog
- **Tag** - Security

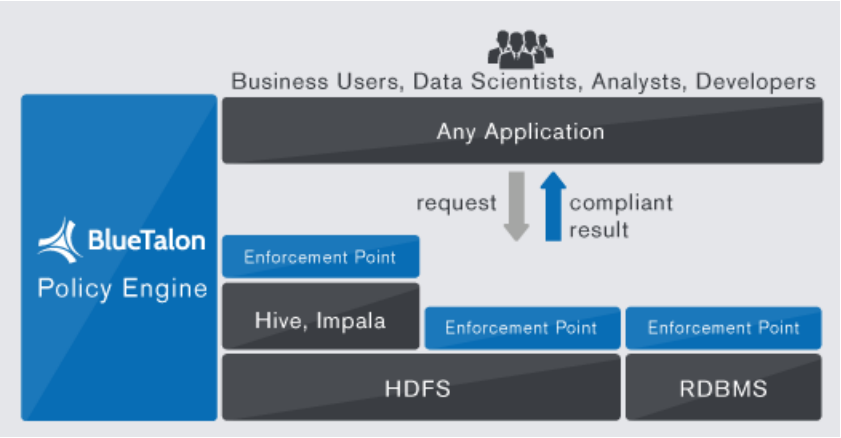
Weekly News Drop - July 26, 2019

Roundup of recent Office 365 news:

- **Changes to Yammer Groups in 2020**. Microsoft announced several forthcoming changes to Yammer groups in the first quarter of 2020. Changes include the ability for an admin to require that all Yammer groups are Office 365 Connected Groups, the ability to set permissions on who can and cannot create new Yammer Groups, and the ability to prevent Yammer groups from being hidden from the groups directory. Due before the end of March 2020. Enforce All Yammer Groups are Office 365 Connected Groups (Microsoft 365 Roadmap 53550, July 16), Enforce Yammer Group Creation Rights (Microsoft 365 Roadmap 53629, July 17), Prevent Yammer Groups From Being Hidden From the Directory (Microsoft 365 Roadmap 53635, July 17).
- **Changes to Office 365 Client Licensing and Activation**. Microsoft announced that licensing and activation for Office 365 subscription-based clients will shift to a rolling process of automatic activation and deactivation across multiple devices, in order to make the process seamless and transparent for the end-user. Reporting for admins will improve too, with reports in the Activation Report changing to be user-specific per device. The changes will start rolling out from August 2019 and be completed by January 2020. Office 365 Client Licensing and Activation Improvements (Office 365 Blog, July 22).
- **No More Office Online**. Microsoft said it is dropping the "Online" naming convention for the browser-based versions of Word, Excel, PowerPoint, Outlook, etc., because it doesn't want to use platform-specific sub-brands anymore. The change does not apply to the server products offered in Office 365 such as Exchange Online and SharePoint Online. Microsoft's proffered reason for introducing the naming change appears nonsensical. Why Office Online is Now Simply Office (Office Apps Blog, July 24).
- **South Africa Datacenters Offering Office 365**. Microsoft's new datacenters in South Africa are now also offering Office 365. Azure was the first workload (March 2019), Office 365 has gone live in July (in line with the original promise for 3Q 2019), and Dynamics 365 and Power Platform are scheduled for 4Q 2019. Office 365 support includes Exchange Online, SharePoint Online, and conversation and chat data in Microsoft Teams (with particular specifications, as per usual data residency conditions and prerequisites). Microsoft Office 365 Now Available from New South Africa Cloud Datacenters (Microsoft 365 Blog, July 25) and Microsoft Teams Launches South Africa Data Residency (Microsoft Teams Blog, July 28).

BlueTalon Acquired

Description



Microsoft announced the acquisition of BlueTalon, for its data access control technology that works across on-premises and cloud data repositories (the so-called "modern data estate"). BlueTalon has been working with Fortune 100 companies to improve data security, data access visibility, and data control. BlueTalon's IP and people will join the Azure Data group to improve data governance.

BlueTalon's technology:

- Uses a Policy Engine for the unified definition of access policies, along with enforcement points that sit between data repositories and the applications and users that request the data.
- Enables the explicit definition of the scope of access that users should have to business data. Policies can be role, attribute, or purpose-based, and can control data at the column, row, cell or partial cell basis.
- Includes full auditing capabilities over policies and user access to data, offering visibility into who accessed what data, when, and for what reasons. Access that should not have happened are also captured.
- Offers on-the-fly data masking to protect sensitive data.
- Offers stealth analytics, a term that is not clearly explained, but is likely to mean the ability to perform analytics on a masked set of data thus protecting the individual data elements while still accurately creating summary statistics and data-based insights for decision making.

Terms of the acquisition were not disclosed.

Analysis

- Microsoft said the increased complexity of data platforms plus regulations such as GDPR and CCPA contributed to the need for the acquisition.
- There is a deep focus in BlueTalon on structured data. There appears to be less of a focus on unstructured data in email messages, Word documents and PowerPoint presentations, which makes up the majority of data in Office 365. It is unclear how the BlueTalon acquisition will impact Microsoft's GDPR compliance aspirations in Office 365.

About

- **Date** - July 30, 2019
- Microsoft Acquires BlueTalon, Simplifying Data Privacy and Governance Across Modern Data Estates (Official Microsoft Blog, July 29)
- Microsoft Acquires BlueTalon: Building the Next Generation of Cloud Data Governance Together (BlueTalon Blog, July 29)
- BlueTalon Policy Engine
- BlueTalon Resources (whitepapers)
- **Tag** - Security

Monotonic Machine Learning Models

Description

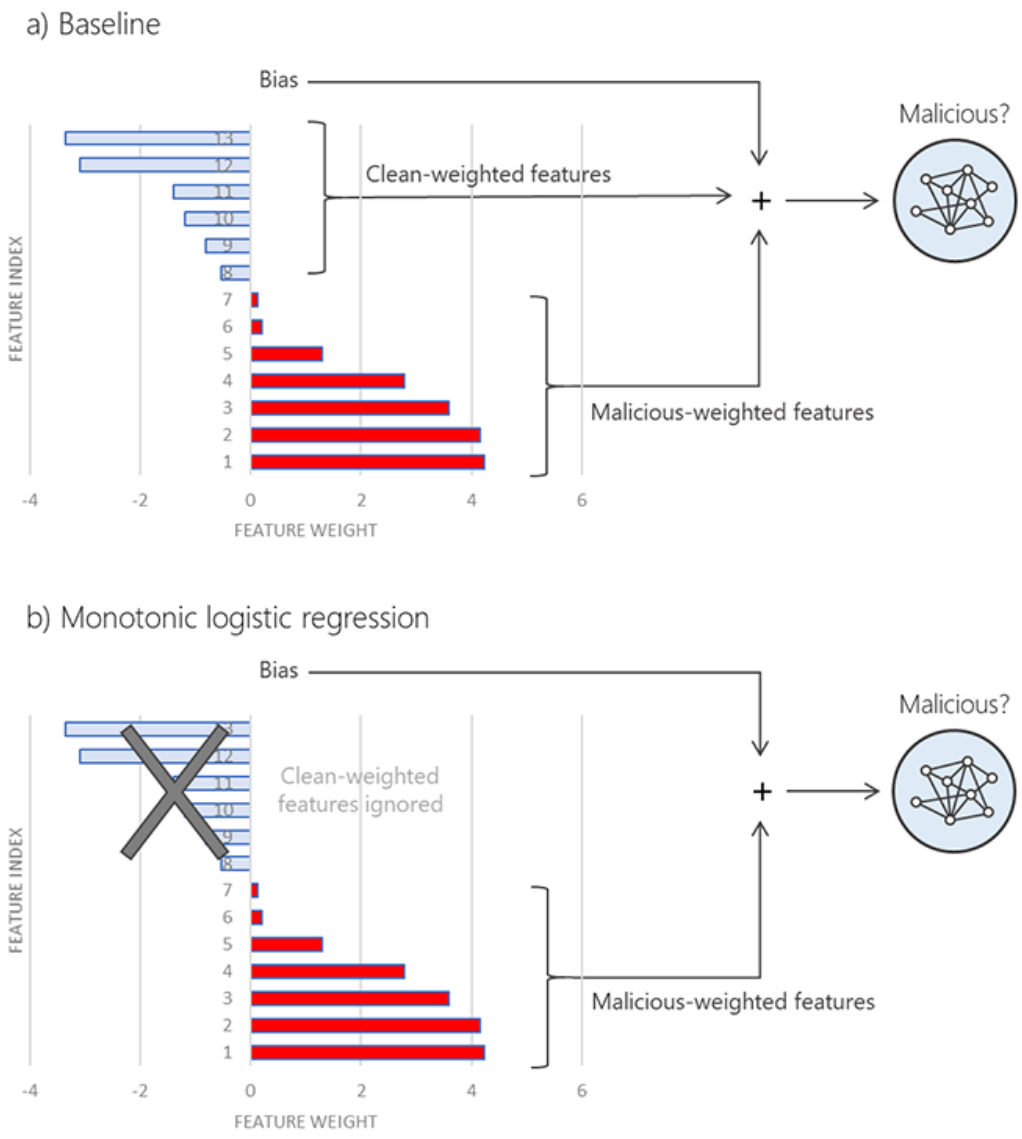


Figure 1. Features used by a baseline versus a monotonic constrained logistic regression classifier. The monotonic classifier does not use cleanly-weighted features so that it's more robust to adversaries.

Since late 2018, Microsoft has added three separate monotonic machine learning models to its cloud-based anti-malware detection models for Microsoft Defender ATP's Antivirus. While a baseline model weighs both the clean and malicious factors in a campaign to determine an overall malicious ranking, monotonic models discard the clean factors and only evaluate the malicious factors. By using these new monotonic models in addition to the current classifiers, Microsoft claims it has been able to detect additional malware campaigns that would have otherwise been missed. Specifically, Microsoft says that one of its monotonic models blocks malware on an average of 200,000 distinct devices every month; these would previously have been missed.

Microsoft was careful to point out that its new monotonic machine learning models are deployed in addition to the current baseline models that evaluate both clean and malicious factors.

Analysis

- Clearly more is better in this case, but while more of the same is just repetition, more of a different kind is resulting in better overall detection rates.

About

- **Date** - July 30, 2019
- New Machine Learning Model Sifts Through the Good to Unearth the Bad in Evasive Malware (Microsoft Security Blog, July 25)
- **Tag** - Security

Free DMARC Discovery for Office 365

Description

Microsoft partnered with Valimail, so that Office 365 tenants can get free access to the Valimail Monitor for Office 365 service. The service offers an automated analysis of all third-party services sending email on their behalf, in line with the DMARC standard for email authentication. The intent is to create human-readable reports, rather than expecting someone to interpret XML-based aggregate reports on email traffic.

- Valimail claims the setup process is very simple: fill out a form on their web site, and then spend five minutes updating the DNS settings.
- Valimail Monitor provides a report of which senders are using the tenant's domain. After the initial analysis period, this is kept up-to-date in real-time.
- Valimail offers an upgrade (not free) to its Valimail Enforce service, which automates DMARC enforcement so that unauthenticated traffic is blocked. An Office 365 administrator can take the necessary enforcement steps manually as well.

Valimail is a member of the Microsoft Intelligent Security Association.

Analysis

- Reducing the unauthorized use of an organization's domain name in email traffic reduces the likelihood of it being used in phishing attacks, because unauthorized traffic is marked as invalid.
- Strong email authentication with SPF, DKIM and DMARC is one important part of reducing the attack space, but it will do nothing if a valid user's account is compromised. While strong email authentication is an important component of an overall security posture, it is not the only defense necessary.

About

- **Date** - June 3, 2019
- Secure Your Journey to the Cloud with Free DMARC Monitoring for Office 365 (Microsoft Security Blog, June 3)
- **Tag** - Security

Barracuda on Account Takeover

Description

Barracuda analyzed its data set on Office 365 customers in March 2019, and noted the following:

- 29% of organizations had at least one account in their Office 365 tenant compromised.
- 4,000 compromised accounts were identified.
- More than 1.5 million malicious and spam emails were sent from these compromised accounts in March 2019.
- 34% of compromised accounts had malicious rules created to hide hacker activity.

Barracuda recommended five mitigations:

- Don't rely solely on security technology that looks for malicious links and attachments (e.g., Office 365 Advanced Threat Protection). Use something more, such as machine learning that analyzes standard communication patterns and highlights anomolies.
- Have the ability to identify when an account has been compromised, and then alert the users and automatically remove malicious emails sent from compromised accounts.
- Use multi-factor authentication, so that a username and password isn't enough to gain access to an account.
- Use something like a cloud access security broker (CASB) to monitor for suspicious activity, such as logins from unusual locations, and the creation of malicious inbox rules.
- Educate users via security awareness training. Do phishing simulations to test efficacy. Create additional rules on confirming potentially-suspicious email requests, such as wire transfers and purchasing gift cards.

In a separate report (registration required), Barracuda looks in more detail at three spear phishing attack types: brand impersonation, blackmail, and business email compromise.

Analysis

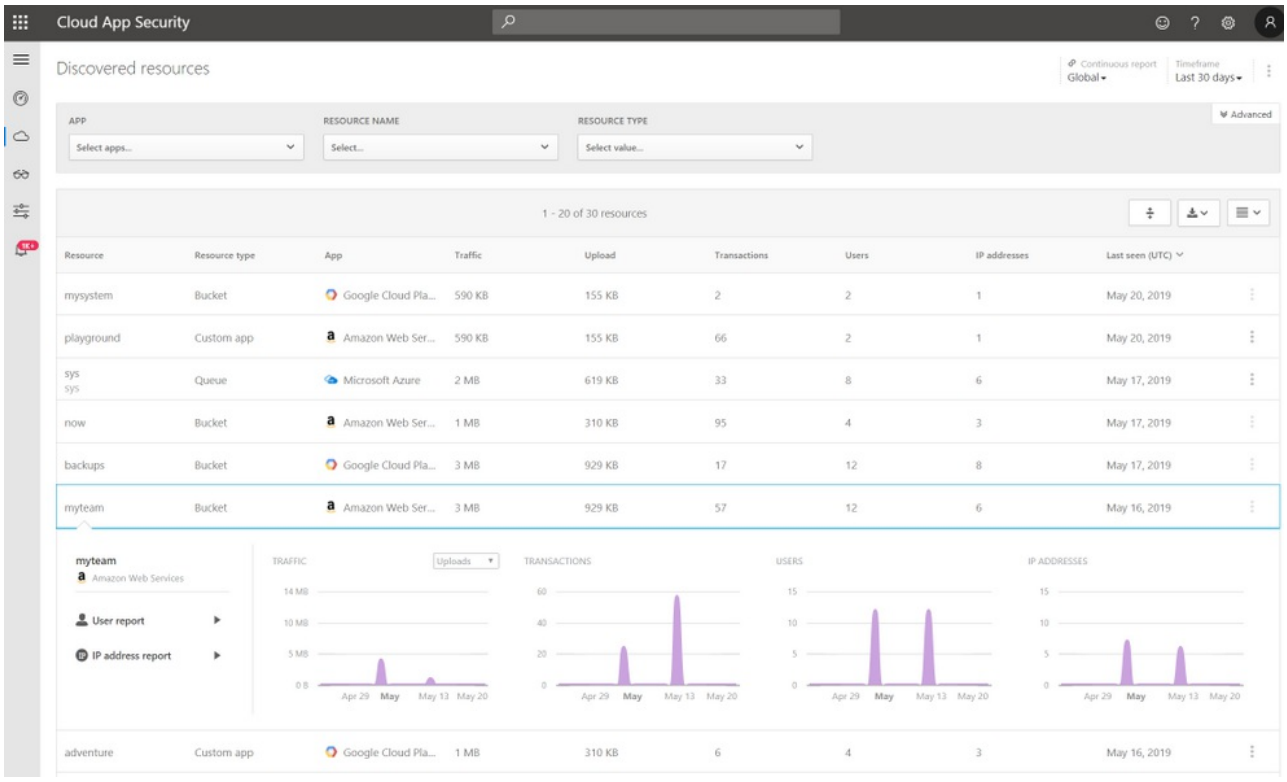
- Barracuda's recommendations are fairly standard and generally appropriate. Some of its recommendations can be met with Microsoft's higher-end Office 365 and Microsoft 365 plans (e.g., Advanced Threat Protection in E5). Other suggestions touch on features not in Microsoft's stack (e.g., machine learning that analyzes standard communication patterns and highlights anomolies).

About

- **Date** - June 4, 2019
- Threat Spotlight: Account Takeover (Barracuda Blog, May 2)
- Spear Phishing: Top Threats and Trends (Barracuda Report, 13 pages, registration required)
- **Tag** - Security
- **Implication** - Credential Phishing and Email Fraud

Discovered Resources in MCAS

Description



Microsoft added a new Discovered Resources tab to Microsoft Cloud App Security, its CASB in Enterprise Mobility + Security E5 or Microsoft 365 E5 plans. Resources hosted on Microsoft Azure, Amazon Web Services and the Google Cloud Platform that are identified through URL data captured on firewalls and proxies will be displayed, along with details on traffic, transactions, user numbers (along with specific identities through the user report), and IP addresses. A discovered resource can be named as a custom app, which means it is then included in the Cloud Discovery dashboard

Microsoft said it intends to add support for additional cloud platforms, but no details nor timeframes were disclosed.

Analysis

- The promise of CASBs is the ability to identify everything and enforce governance actions to secure resources, mitigate risks, and control an organization's complete digital estate. Microsoft's new Discovered Resources capabilities allows for the identification of potentially risky data and system resources, with visibility the first step to governance and control.

About

- **Date** - June 6, 2019
- Discover Shadow IT Across IaaS and PaaS with Microsoft's CASB (Enterprise Mobility + Security, May 29)
- Discover Resources and Custom Apps (Microsoft Docs, May 23)
- **Tag** - Security
- **Implication** - Microsoft Cloud App Security

Weekly News Drop - June 7, 2019

Roundup of recent Office 365 news:

- **Password Hash Sync**. The Microsoft DART Team (Detection and Response) outlined the design principles and tenant-benefits of using password hash sync, including non-access to passwords by Microsoft, linkage with Azure AD Smart Lockout and the Leaked Credentials Service, and shielding of denial of service and password spray attacks by Microsoft (instead of on-premises AD FS). Demystifying Password Hash Sync (Microsoft Security Blog, May 30).
- **Office 365 for Windows Desktop 1905**. Microsoft released version 1905 (May 2019) of Office 365 for Windows on May 29. Highlight capabilities: live captions and subtitles in PowerPoint (12 languages supported as voice input, and 62 languages as translated subtitles), easier switching between Office 365 work and personal accounts, @mentions in comments in Word, Excel and PowerPoint, and improved co-authoring support in Microsoft Excel. Version 1905 is available translated into 44 languages. Office 365 for Windows Desktop - May 2019 Release Details (Office International Blog, May 31).
- **Stocks in Excel with More Real-Time Information**. Microsoft announced new agreements with Nasdaq and Refinitiv for pulling current financial information on US exchange-listed equities into the Stocks data type in Microsoft Excel for Office 365. New financial data available includes bitcoin, bonds, international currencies, and more. The intent is to offer improved access to market data for everyday investors. Microsoft, Nasdaq, and Refinitiv Empower Everyday Investors with Real-Time Data and Insights in Excel (Microsoft 365 Blog, June 5).
- **Google Cloud Outage**. A serious networking issue at Level 3, an ISP that provides connectivity to Google data centers, disrupted many Google services (YouTube, Gmail, Search, Google Drive, and more) and many companies that rely on Google services (including Snapchat, Shopify, Discord, and more). The outage lasted 4 hours on June 2. Google Gloud Goes Down, Taking YouTube, Gmail, Snapchat, and Others With It (ZDNet, June 2). An Update on Sunday's Service Disruption (Inside Google Cloud, June 4).

Weekly News Drop - June 14, 2019

Roundup of recent Office 365 news:

- **Another CVE-2017-11882 Exploit**. Threat actors are leveraging the CVE-2017-11882 vulnerability in older versions of Equation Editor in a spam campaign targeted at European users. If the user has an unpatched device and opens the weaponized RTF document in the email, a backdoor trojan is downloaded and installed on their device. The vulnerability was addressed in a patch in November 2017, but many devices remain unpatched. Microsoft Warns About Email Spam Campaign Abusing Office Vulnerability (ZDNet Microsoft, June 9).
- **Passwordless in Windows 10 1903**. Windows 10 version 1903 includes new options for passwordless access to Windows and a Microsoft account on the web. One new option is creating a Microsoft account based on a phone number, with no password to enter, using the Microsoft Authenticator app or an SMS code for security setup. Another option is logging into Windows for the first time using a Microsoft account linked with the Microsoft Authenticator app. A third is the use of Windows Hello for signing in to a Microsoft account and other websites supporting FIDO authentication on the web. These advances don't yet apply to Work and School accounts in Office 365. Advancing Windows 10 as a Passwordless Platform (Microsoft Security, June 10).
- **Conditional Access Rights Added to Microsoft 365 Business**. Microsoft added Conditional Access to its Microsoft 365 Business plans, so that small and medium-sized businesses (the Business plans max out at 300 users) can better control how company resources are accessed. The conditional access capabilities are the same as those in Azure AD Premium P1, but all of the capabilities in P1 were not released to the Business plans. Conditional Access is Now Part of Microsoft 365 Business (Microsoft 365 Business Blog, June 12).
- **More Pre-Integrated Apps with Azure AD**. Microsoft added 25 new pre-integrated third-party applications that support single sign-on and/or automated user provisioning to Azure AD during May 2019. Pre-integrated apps included Marketo Sales Engage, webMethods Integration Suite, and JobHub. Automated user provisioning is supported for Dropbox for Business, Zoom, and Dynamic Signal, among others. New Pre-Integrated Apps Available in Azure AD June 2019 (Azure AD Identity Blog, June 13).

Data Centers in Middle East

Description

Microsoft announced its first data center region in the Middle East, with two new data centers in the United Arab Emirates (in Abu Dhabi and Dubai). The new data centers currently offer Azure and Office 365 capabilities to customers in the region, and by the end of the year will also offer Dynamics 365 and the Power Platform.

Linked with the announcement of the new data center region, Microsoft announced that it achieved the Dubai Electronic Security Center (DESC) certification, which means government and semi-government entities are permitted to use the new data centers.

Analysis

- Microsoft continues to build out its data center footprint across the globe, enabling both in-country data residency and supporting local certifications necessary for securing customers.
- There was no word about migration of data for current customers.

About

- **Date** - June 19, 2019
- First Microsoft Cloud Regions in Middle East Now Available (Microsoft Azure Blog, June 18)
- **Tag** - Security

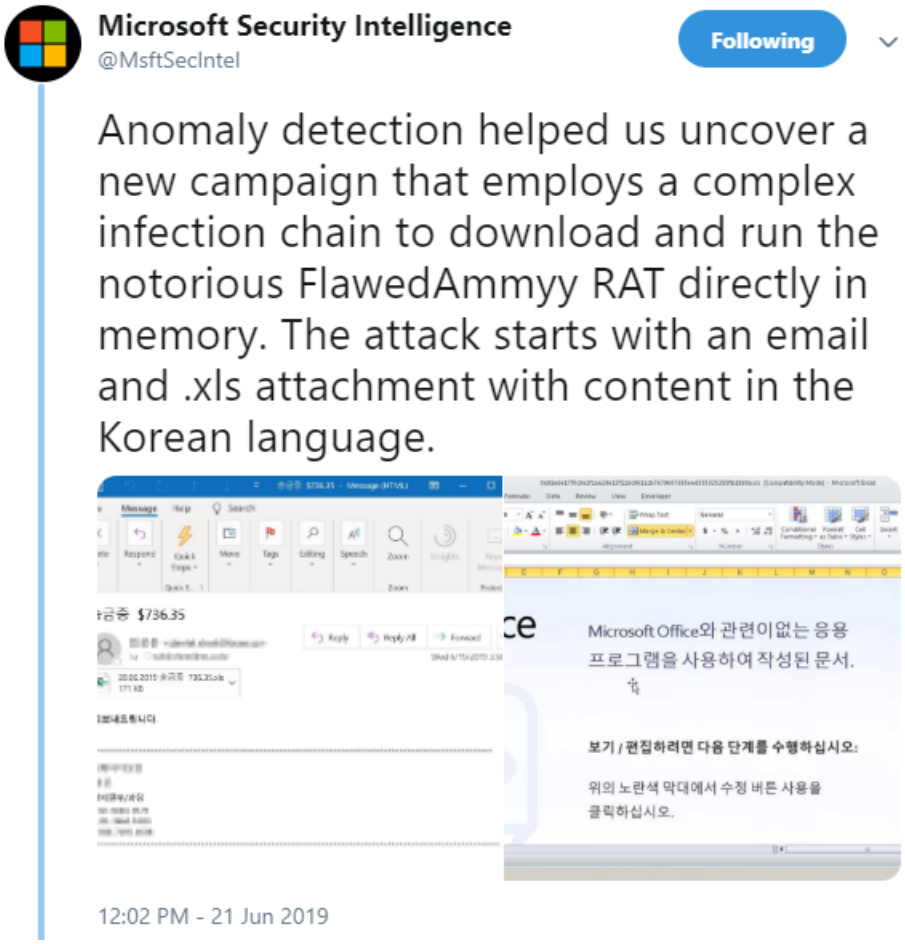
Weekly News Drop - June 21, 2019

Roundup of recent Office 365 news:

- **PowerPoint Designer Updates, and Presenter Coach**. Microsoft announced that its AI-powered PowerPoint Designer service has been used to enhance more than 1 billion slides. New capabilities added to PowerPoint Designer include support for branded templates, theme recommendations, and relatable references for large numerical values. It also announced Presenter Coach, a forthcoming service initially for PowerPoint Online that offers a rehearsal mode with on-screen guidance on pacing, language, and style. Presenter Coach is due later in 3Q 2019. PowerPoint AI Gets an Upgrade and Designer Surpasses a Major Milestone of 1 Billion Slides (Microsoft 365 Blog, June 18).
- **AutoSave Dramas**. Numerous customers are struggling with the default behavior of AutoSave. For example, customers starting a new document based on an old one are finding that AutoSave results in the loss of the original document. Others complain that merely opening a document will in some cases result in a save operation that overwrites the last saved date. Microsoft offered several approaches for minimizing the negative effects of AutoSave. Disable the New AutoSave By Default, As It Can Lead to a Loss of Data (Office 365 UserVoice, April 29).
- **Information Barriers Due June 2019**. Microsoft announced that Information Barriers, its new ethical walls service initially for Microsoft Teams, will be released in June 2019. "*Avoid conflicts of interest within your organization by limiting which individuals can communicate and collaborate with each other in Microsoft Teams. This helps limit the disclosure of information by controlling communication between the holders of information and colleagues representing different interests, for example, in Firstline Worker scenarios. This is particularly helpful for organizations that need to adhere to Ethical Wall requirements and other related industry standards and regulations*." Microsoft 365 Roadmap 50586 (June 10).
- **Authentication Session Management for Outlook on the Web**. Microsoft is adding controls for authentication persistence for Outlook on the Web. Due by end June 2019. "*Authentication Session Management allows you to control the frequency at which your users are required to enter their credentials. Admins will be able to configure both the Sign-in frequency as well as if sessions will persist after Outlook on the web is closed*." Microsoft 365 Roadmap 52371 (June 13).
- **User Investigation Priority Released**. Microsoft released the new investigation priority experience in Microsoft Cloud App Security, which draws on identity threat signals from Azure ATP, Azure AD Identity Protection, and Microsoft Cloud App Security. The method for calculating who is a top risk is now determined by all recent user activities and alerts that indicate an active attack or insider threat. Prioritize User Investigations in Cloud App Security (Enterprise Mobility + Security Blog, June 20).

FlawedAmmyy Trojan

Description



Microsoft Security Intelligence highlighted a current malware campaign that uses compromised Excel attachments to distribute the FlawedAmmyy remote-access trojan through a complex chain of infection. The chain includes activities that run solely in memory on Windows devices, in order to avoid anti-virus software that only analyze files. The compromised attachment uses macros to initiate the infection, and can compromise even fully patched Windows PCs. Once the file is opened, macro functions are automatically run.

Microsoft said that its Threat Protection customers running Microsoft Defender ATP and/or Office 365 ATP were protected from infection. Specifically, it claimed that "*Microsoft Threat Protection defends customers from this attack. Cloud-based machine learning protections in Microsoft Defender ATP blocked all of the components of this attack at first sight, including the FlawedAmmyy RAT payload. Office 365 ATP detects the email campaign.*"

Analysis

- Taken at face value, Microsoft's advanced tools are effective at stopping emerging malware threats. While the above is an example of an attack that was detected "at first sight" (to use Microsoft's language), it is unclear how many other attacks get through the various levels of defence offered by Microsoft.
- Microsoft Defender ATP requires Windows 10 advanced licensing, and is offered as part of Microsoft 365 plans. It is not available as part of any Office 365-only plans.

About

- **Date** - June 24, 2019
- Update from Microsoft Security Intelligence (Twitter, June 21)
- Microsoft: We're Fighting Windows Malware Spread via Excel in Email with Bad Macro (ZDNet Microsoft, June 24)
- **Tag** - Security

Preservation Hold Library Update

Description

When a retention policy applies to content in a SharePoint site, changes to and deletions of documents are tracked through a hidden Preservation Hold Library in the site. The earlier version of a document undergoing change is saved to the preservation hold library. A deleted document is moved from its source document library to the preservation hold library. Once the retention period has expired, earlier versions and deleted documents are purged from the preservation hold library and moved to the first-stage recycle bin, where they are held for 93-days before being irrevocably purged from SharePoint Online.

However, when a retention policy enforcing a hold on content is deactivated incorrectly or inappropriately by an administrator. Under this situation, content is moved to the first-stage recycle bin (as per the normal process), but for any content that was deleted more than 93-days previously, an irrevocable purge happens immediately.

To reduce the likelihood of inadvertent data loss, Microsoft announced two forthcoming changes:

- When a retention policy is removed from a site, any documents on hold in the site will remain on hold for a further 30-days. This is called a grace period.
- Once items are deleted from the Preservation Hold Library, they will be moved to the second-stage recycle bin, instead of being irrevocably purged immediately. Deleted content in the second-stage recycle bin can be recovered by an administrator for a short time period. In order to be different from the first-stage recycle bin - where the deletion trigger is the number of days that have elapsed since the original document was deleted - the second-stage recycle bin must restart the deletion trigger to be the number of days since the content was put into the second-stage recycle bin.

These changes will begin rolling out in July 2019, and are expected to be available worldwide to all customers by the end of August 2019.

Analysis

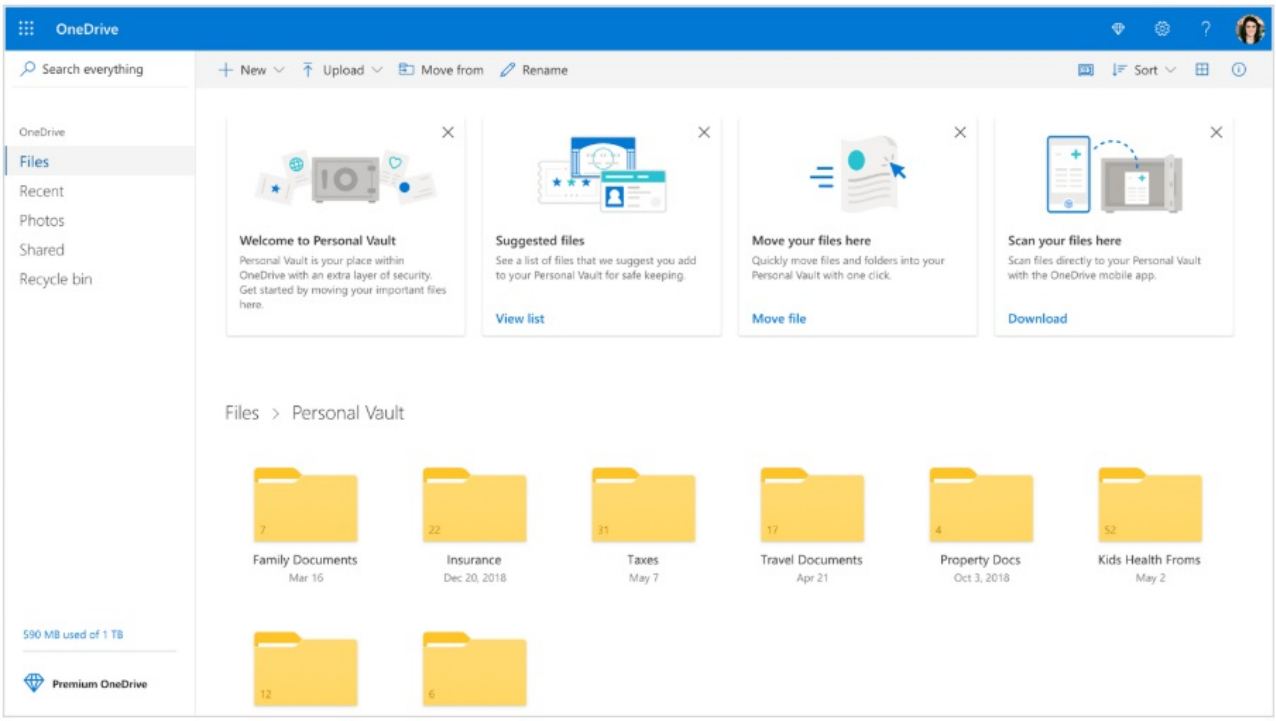
- Some customers must have experienced data loss from this situation in order for this change to be made.
- With this change, some content will be held for longer than it needs to be. For example, if a retention policy is intentionally and correctly lifted, content will remain available for at least another 120 days. There does not appear to be a way to diffentiate between a policy inappropriately lifted, and one that is correctly lifted.

About

- **Date** - June 25, 2019
- Enhancements to SPO Preservation Library (Microsoft 365 Roadmap, June 18)
- Important Change to SharePoint Online Retention Policy Processing (Office 365 IT Pros, June 20)
- **Tag** - Archiving

OneDrive Personal Vault

Description



The OneDrive personal service - available standalone to consumers or as part of a consumer subscription to Office 365 - is gaining new protections for files. Microsoft announced a new Personal Vault segment of OneDrive, which has additional access protections compared to other storage segments in a user's OneDrive account. The design goal of Personal Vault is to provide further protections for sensitive and important files.

Specifically:

- To access the Personal Vault folder, a strong authentication method (e.g., Microsoft Authenticator app) or a second step of identity verification (e.g., fingerprint, face, PIN or SMS code) is required.
- Once opened, the Personal Vault folder will auto-lock after a specified period of time. The account owner can change the lock period. Likewise, any files opened from within the Personal Vault folder will be locked after a defined time has elapsed.
- On Windows 10 PCs, the Personal Vault folder and its contents are synced to a BitLocker-encrypted area of the local hard drive.
- On mobile devices, the OneDrive app can be used for scanning documents, taking pictures, or shooting video directly into the Personal Vault area. Doing so bypasses the local storage on the mobile device, e.g., new pictures are not stored on the camera roll. This is the same capability as offered in Teams for healthcare.
- All content stored in Personal Vault is accessible from OneDrive on the web or via a OneDrive client or app.
- Customers with an Office 365 consumer subscription can use Personal Vault for all of their files (up to their storage allocation). Customers with a free account or standalone OneDrive subscription will be able to store a certain number of files in Personal Vault, but not everything.

The above changes do not apply to OneDrive for Business as part of business and enterprise Office 365 plans.

Personal Vault will roll out first to customers in Australia, New Zealand and Canada. It is expected to be available worldwide by the end of 2019.

Analysis

- For customers using multi-factor authentication on their personal OneDrive account, the added protection of Personal Vault is nice but not essential. For customers not using MFA at the account level, having the option of extra protection for sensitive and important files is a good addition to the service.

- It is unclear how an open protected file will be obfuscated from view when auto-locked. Auto-locking for additional edits will be essential, but auto-locking must also go beyond that to prevent an reading activity.
- It is unclear how additional identity verification will be enforced for people invited to share a document stored in Personal Vault, or indeed, if this capability will be offered at all.

About

- **Date** - June 25, 2019
- OneDrive Personal Vault Brings Added Security to Your Most Important Files and OneDrive Gets Additional Storage Options (Microsoft 365 Blog, June 25)
- **Tag** - File Sharing

Microsoft Cloud App Security Updates

Description

Microsoft continues to update its cloud access security broker in Enterprise Mobility + Security and Microsoft 365 plans. Recent updates to Microsoft Cloud App Security include:

- The impossible travel anomaly detection policy has been extended to be aware of neighboring countries.
- Access to Discovery reports can be scoped, allowing security analysts to be given access to discovery data for specific sites and business units, instead of all data captured by Microsoft Cloud App Security.
- The Azure AD Global Reader role can be assigned to a security analyst. This provides full read-only access to the data in Microsoft Cloud App Security, but does not confer the right to make any changes to settings or take any actions.
- Sessions policies have new abilities to use the Data Classification Service for identifying sensitive information in files, download permissions can be automatically applied per user (e.g., read-only), and if files are too large to scan on download, the administrator can specify whether such downloads are blocked or allowed.

Analysis

- Microsoft continues to tweak and extend Microsoft Cloud App Security, addressing the real-world concerns faced by customers. None of the above changes are revolutionary, but each adds to the ability to tailor the service for users and situations.

About

- **Date** - June 27, 2019
- What's New with Microsoft Cloud App Security (Microsoft Docs, June 20)
- **Tag** - Security

Weekly News Drop - June 28, 2019

Roundup of recent Office 365 news:

- **S/MIME for Outlook for Android and iOS**. S/MIME signing and encrypting of email messages via Outlook for Android and Outlook for iOS is under development, and is expected to be released during July 2019. Requires that customers are using the updated Microsoft sync technology architecture. Outlook for Android and S/MIME (Microsoft 365 Roadmap 32569, June 24) and Outlook for iOS and S/MIME (Microsoft 365 Roadmap 32570, June 24).
- **OneDrive Consumer Storage Plans**. Microsoft announced that its standalone OneDrive consumer subscription will double its storage allocation from 50 GB to 100 GB for no additional cost (still $1.99 per month). In addition, Office 365 consumer subscribers - not business or enterprise ones - will be able to purchase up to another 1 TB of storage space. OneDrive Personal Vault Brings Added Security to Your Most Important Files and OneDrive Gets Additional Storage Options (Microsoft 365 Blog, June 25).
- **Files Channel Tab Removes View Limit**. The new Files Channel Tab in Microsoft Teams uses more of the native capabilities from SharePoint, including the ability to display up to 30 million documents in a view. The original cut-down Files Channel Tab in Teams had an arbitrary limit of 300 documents. Availability of the new tab is still rolling out. New Teams Files Channel Tab Solves View Limit (Office 365 for IT Pros, June 26).
- **Microsoft Teams for Existing Customers**. Existing installations of Office 365 Business and Office 365 ProPlus on the monthly update channel will be updated to include Microsoft Teams, beginning July 9. The Teams client will be kept up-to-date after the initial installation. For organizations that do not want to deploy Teams, the Teams client can be excluded from the standard installation. Teams is Coming to Office 365 Business & Office 365 ProPlus Monthly (Microsoft Teams Blog, June 28).

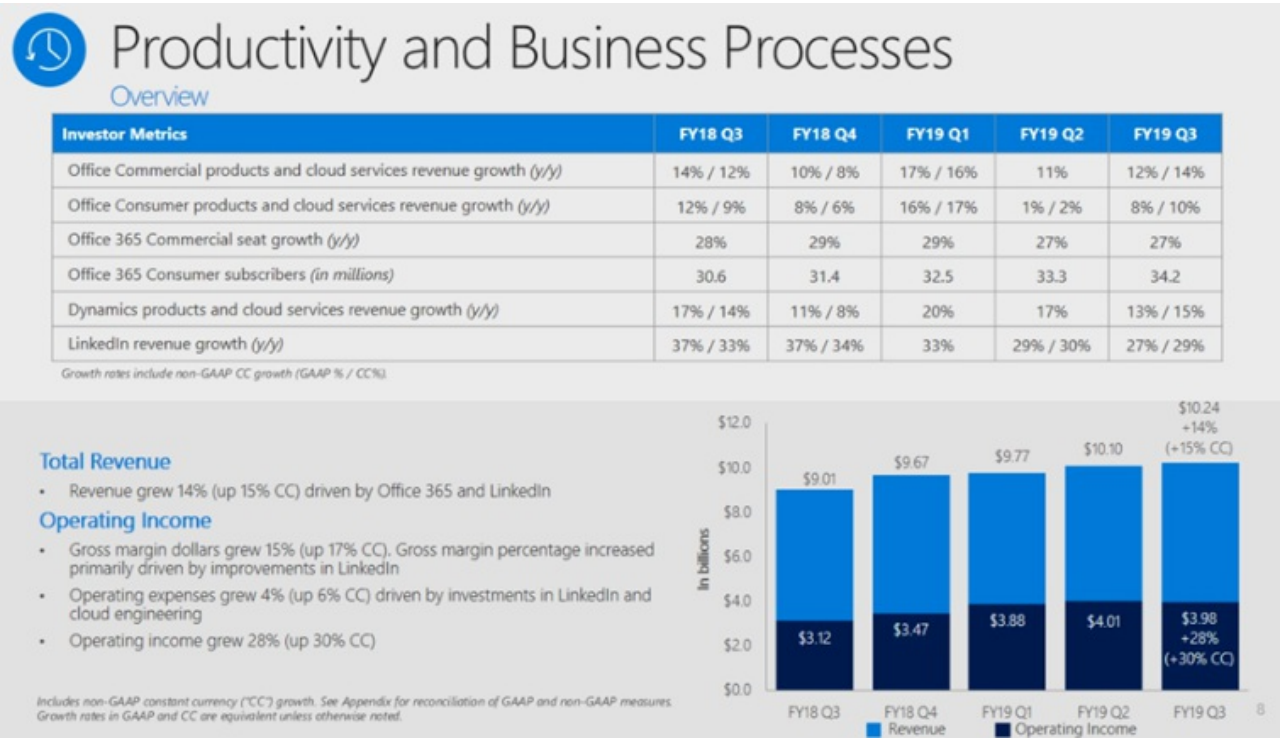
Weekly News Drop - May 3, 2019

Roundup of recent Office 365 news:

- **Principles for Customer Control over Data**. Microsoft announced three new principles that will guide its strategy on transparency and customer control over data. Principle one is that all data collected from major products on devices will be categorized as required or optional. Principle two is that product documentation will be improved to describe required and optional data types, and why required data is viewed that way. Principle three is that Microsoft will report twice a year on data privacy, including new required data, deprecated data collection, and the impact of new data privacy laws, among others. Increasing Transparency and Customer Control Over Data (Microsoft On the Issues, April 30).
- **New Privacy Controls for Office 365 ProPlus on Windows**. Microsoft introduced a new version of Office 365 ProPlus on Windows, with new privacy controls to allow the IT administrator for an Office 365 work or school tenant to control which connected experiences are available. Connected experiences include analyzing content for design recommendations, downloading online content, and document collaboration, among others. Microsoft Office Brings You New Privacy Controls (Microsoft 365 Blog, May 1).
- **Advanced eDiscovery Updates at GA**. The updates to Advanced eDiscovery announced in January 2019 were released to general availability on April 30. These include "*a custodian based approach to holding content, ability to communicate with custodians with hold notices and escalations, a static set of content to work with once a case is established and the ability to review and update content prior to export*." Advanced eDiscovery General Availability (Security, Privacy and Compliance Blog, April 30).
- **DNS Update Takes Down Microsoft Cloud Services**. For almost two hours on Thursday May 2, a failed DNS update took down several high profile Microsoft cloud services, including Office 365, Skype, and Xbox. Microsoft was attempting to migrate from its legacy DNS to one hosted on Azure, when a faulty name server delegation setting wrought havoc across the world. Networking Outage Disrupts Microsoft's Cloud Platform In Nearly Every Region (Petri, May 2) and Azure Global Outage: Our DNS Update Mangled Domain Records, Says Microsoft (ZDNet, May 3).
- **Office 365 Achieves ISO 22301**. Microsoft announced ISO 22301 certification for Office 365, which addresses business continuity preparedness and restoration cadence. The certification includes how to prevent, mitigate, respond to, and recover from disruptive events. The certification was announced on the same day as the above outage - which was therefore a real-life example of ISO 22301 in action, or just really, really bad timing. ISO 22301 Highlights Office 365's Unmatched Business Continuity & Disaster Recovery Preparedness (Security, Privacy and Compliance Blog, May 2).

Office 365 Market Snapshot - Microsoft's Q3 2019

Description



Productivity and Business Processes

Overview

Investor Metrics	FY18 Q3	FY18 Q4	FY19 Q1	FY19 Q2	FY19 Q3
Office Commercial products and cloud services revenue growth *(y/y)*	14% / 12%	10% / 8%	17% / 16%	11%	12% / 14%
Office Consumer products and cloud services revenue growth *(y/y)*	12% / 9%	8% / 6%	16% / 17%	1% / 2%	8% / 10%
Office 365 Commercial seat growth *(y/y)*	28%	29%	29%	27%	27%
Office 365 Consumer subscribers *(in millions)*	30.6	31.4	32.5	33.3	34.2
Dynamics products and cloud services revenue growth *(y/y)*	17% / 14%	11% / 8%	20%	17%	13% / 15%
LinkedIn revenue growth *(y/y)*	37% / 33%	37% / 34%	33%	29% / 30%	27% / 29%

Growth rates include non-GAAP CC growth (GAAP % / CC%).

Total Revenue

- Revenue grew 14% (up 15% CC) driven by Office 365 and LinkedIn

Operating Income

- Gross margin dollars grew 15% (up 17% CC). Gross margin percentage increased primarily driven by improvements in LinkedIn
- Operating expenses grew 4% (up 6% CC) driven by investments in LinkedIn and cloud engineering
- Operating income grew 28% (up 30% CC)

Includes non-GAAP constant currency ("CC") growth. See Appendix for reconciliation of GAAP and non-GAAP measures. Growth rates in GAAP and CC are equivalent unless otherwise noted.

Microsoft announced its Q3 results for end March 2019. Key highlights:

- Revenue from Office 365 and other Microsoft cloud services continues to grow strongly.
- The number of monthly active users of Office 365 has grown to 180 million. The previous official number was 155 million at end September 2018.
- Office 365 consumer users grew to 34.2 million, up from 33.3 million at the end of January 2019.
- 100 million users also have a subscription to Microsoft's Enterprise Mobility and Security stack of services. The breakdown between users having both an Office 365 subscription and an EMS one versus users with the combined Microsoft 365 plan (which has both, along with Windows 10 licensing) was not disclosed.

Analysis

- There hasn't been an explicit breakdown of Office 365 vs. Microsoft 365 numbers before, and this earnings report doesn't give any strong indications either. However, it does signal 100 million users of Enterprise Mobility and Security, most of which has to be due to organizations migrating to Microsoft 365 versus staying purely on Office 365 plans. As we have previously signaled in this service, Microsoft 365 is the bigger picture.

About

- **Date** - April 25, 2019
- Microsoft Cloud Strength Drives Third Quarter Results (Microsoft Investor Relations, April 24)
- Office 365 Reaches 180 Million Monthly Active Users (Office 365 IT Pros, April 25)
- Microsoft's Q3 Earnings Jump 14% on Office and Cloud Growth (Petri, April 24)
- **Implication** - Office 365 - Overview

Microsoft Build 2019

Description

At Microsoft's annual Build conference for developers, Microsoft announced several new and updated capabilities coming to Office 365 and Microsoft 365, including:

- **Microsoft Graph Data Connect**. Allows an organization to extract productivity data from the Microsoft Graph and combine it with internal performance data, using Azure Data Factory. The combination is intended to help organizations identify common patterns in productivity and performance that can be enacted more widely.
- **Fluid Framework**. A new way of enabling multi-person co-authoring on web content and within documents, as well as the use of a componentized document model for new kinds of documents that aren't constrained by current document paradigms (e.g., a Word document is by definition a self-contained document). The framework will also enable intelligent agents to work side-by-side with human authors, on tasks such as text translation, suggesting edits, and performing compliance checks, among others. These capabilities will be integrated into experiences such as Microsoft Teams, Microsoft Word, and Outlook, among others. An initial version of the framework will be available later in 2019.
- **Focus Plan in MyAnalytics**. Coaching within MyAnalytics on the need to schedule focus time for getting work done, in order to cultivate a different culture that doesn't rely on back-to-back meetings and never-ending interrupt-driven electronic communications. Once a user has booked focus time, notifications will be held back to reduce / eliminate interruptions.
- **Microsoft Search at GA**. The general availability of Microsoft Search was announced, as mentioned in our Weekly News Drop for this week.
- **Microsoft Edge Updates**. The forthcoming Chromium-based version of Edge will offer compatibility with Internet Explorer apps (by opening IE in a tab), privacy controls for limiting the use of tracking tokens by third-parties, and the ability to create collections of web pages and resources. These capabilities are available in preview for developers; general market availability has not been relaesed yet.
- **Conversational AI in Virtual Agents**. Based on the acquisition of Semantic Machines in 2018, Microsoft is working on the next generation of conversation agents. These will support multi-turn, multi-domain, and multi-agent experiences that learn from their interactions with individuals and can carry forward earlier learning into future actions. Microsoft's work in this area will be integrated into Cortana at some point in the future.

Analysis

- Build offers a forum that Microsoft uses to signal future intent and possibilities. Announcements and directions at Build conferences don't always make it to market - either at all or on-time. But it is always interesting to see what is being worked on for the future of work.

About

- **Date** - May 6, 2019
- New People-Centered Experiences in Microsoft 365, The World's Productivity Cloud (Microsoft 365 Blog, May 6)
- On Microsoft Edge - Chromium-based Edge: What's Coming Next in Microsoft's Open-Source Browser (ZDNet, May 6)
- On Conversational AI - Here's Microsoft's New Plan to Keep Cortana Alive and Differentiated (ZDNet, May 8)

Advanced eDiscovery Updates for Q4 2019

Description

Microsoft announced a couple of changes on the roadmap for Advanced eDiscovery, both for delivery later in 2019:

- **Advanced eDiscovery Delegated Access**. "*Now add external counsel to a specific case within Advanced eDiscovery. This feature will help organizations ensure their partners of choice are able to execute eDiscovery related tasks within Microsoft 365 directly.*" Due Q4 2019.
- **Advanced eDiscovery Threaded Chat and Email Review**. "*Now eDiscovery managers can review chats and emails in context of the thread and full context of the collaboration or discussion. This will help speed the efficiency of the review process with communications in full context of the conversation.*" Due Q4 2019.

Analysis

- Delegated access is an important addition to eDiscovery, since it reduces the need to export sensitive data and release it for wider consumption in other eDiscovery tools. Facilitating secure review and collaboration by external users elevates the integrated workflow capabilities in Advanced eDiscovery.
- Regarding threaded chat and email review - about time. Wider context is essential in understanding whether a given conversational turn is responsive or not.

About

- **Date** - May 8, 2019
- Advanced eDiscovery Delegated Access (Microsoft 365 Roadmap 50754, April 25)
- Advanced eDiscovery Threaded Chat and Email Review (Microsoft 365 Roadmap 50755, April 25)
- **Implication** - eDiscovery Workflow
- **Tag** - eDiscovery

Weekly News Drop - May 10, 2019

Roundup of recent Office 365 news:

- **Microsoft Search at General Availability**. After its release to targeted customers in September 2018, Microsoft announced the general availability of its new intelligent search experience on May 6. Microsoft Search offers a consistent and unified search experience, meaning that every search box provides access to the same personalized results for each individual, the same search box is integrated into each application, and the search box offers both content results and access to task information and insights. Microsoft Search can be integrated with Bing, in order to merge public information with organizational results, while maintaining data security. Microsoft Search gives each user rapid access to their recent documents, relevant people, and recommended content, which while being a boost for productivity, will also streamline data breach conditions if an account is compromised. Welcome to Microsoft Search, Intelligent Search for the Modern Workplace (The SharePoint Community Blog, May 6).
- **BitLocker Management using Intune**. Microsoft announced that Intune will offer expanded management capabilities for BitLocker before the end of 2019. Admins will be able to configure 38 BitLocker encryption settings via Intune policies, and access reports on device encryption status and recovery key access. Admins will also be able to set policies in Intune to prevent access to corporate resources if encryption requirements are not met. These expanded capabilities are due before the end of calendar year 2019. Microsoft Expands BitLocker Management Capabilities for the Enterprise (Enterprise Mobility and Security Blog, May 8).
- **Third-Party App Usage of Microsoft Identities**. Microsoft continues to improve its Identity Platform for developers, enabling the integration of third-party applications with Azure AD accounts and personal Microsoft accounts for identity. This replaces the need to create and manage a separate identity system for applications, thereby reducing complexity and account credential sprawl. Among other updates, Microsoft released the unified app registration portal for Azure AD so that organizations can register and manage their applications built with the Microsoft Identity Platform. Microsoft also noted that over 1 million third-party apps are actively using its Identity Platform every month. Build 2019: Celebrating 1M third-party active apps, the Microsoft identity platform, and more (Azure AD Identity Blog, May 6).
- **Records Management in the Compliance Center**. Records management capabilities in Office 365 will be available in the new Microsoft Compliance Center in May 2019. "*Now take advantage of Microsoft 365 records management capabilities in one place with specific permissions model and tailored experience for records management including file plan, event-based retention, and defensible disposition. Enable your records management requirements in-place within Microsoft 365.*" Microsoft 365 Roadmap 50795 (April 26).
- **Advanced Record Versioning in Advanced Data Governance**. Microsoft is playing with the concept of what makes something a record, and whether records can or cannot be changed. "*Now users with correct permissions can lock and un-lock a record to enable collaboration on records within SharePoint Online. Use the advanced record versioning feature to ensure records retention policies are met, while supporting collaboration and productivity on records in your organization. At each lock or un-lock action a snapshot of the record is taken and preserved to ensure records retention requirements are met.*" Due June 2019 in Advanced Data Governance. Microsoft 365 Roadmap 50794 (April 25).
- **Microsoft Defender ATP for Detecting Credential Theft**. Microsoft outlined the capability of Microsoft Defender ATP to detect credential dumping, with a specific focus on how modelling memory access to a particular process will generate a highly predictable cluser of activity for non-legitimate accesses. This can be used to trigger an alert for investigation by SecOps. Detecting Credential Theft Through Memory Access Modelling with Microsoft Defender ATP (Microsoft Security Blog, May 9).

Identity Security at Microsoft

Description

The internal Security Team at Microsoft outlined three investments being made to improve identity management at Microsoft. The three areas are:

- **Securing administrator accounts**. Methods include limiting the number of people with access to admin capabilities, separating admin user accounts from day-to-day worker accounts, and using request-and-approval-based time-limited access to admin accounts for just-in-time access privileges. Microsoft also has separate admin-only devices, which are kept up-to-date with the latest upgrades and patches, and does not support remote execution of admin tasks.
- **Eliminating passwords**. Reduce the reliance on passwords, and ideally eliminate passwords altogether. Microsoft recommends the use of multi-factor authentication, the use of newer authentication workflows (that permit the use of biometrics), the reduction in use of legacy authentication workflows, and storing passwords in as few identity systems as possible.
- **Simplifying identity provisioning**. Analyze worker roles to understand specific access privileges required by each worker role, and assign privileges on the basis of role not user. This simplifies the task of managing access privileges over time as people move from role-to-role, and ensures that older access privileges are not just carried forward into new roles.

Microsoft's security team says these three investments reduce the risk of compromised accounts.

Analysis

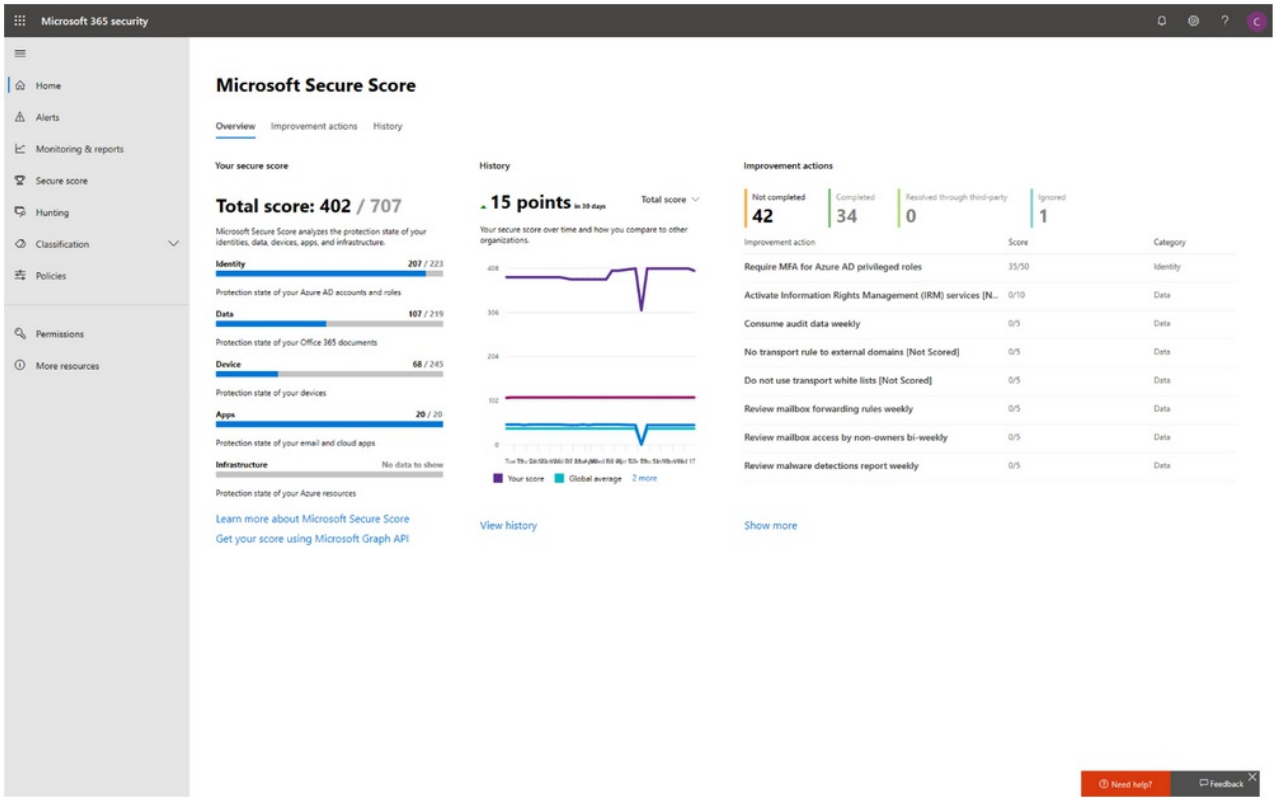
- These investment areas internally match the customer-facing best practice guidance being advocated by Microsoft.
- Some of these capabilities are already available in various forms in Office 365 and Microsoft 365. Undoubtedly more capabilities are coming.

About

- **Date** - May 8, 2019
- 3 Investments Microsoft is Making to Improve Identity Management (Microsoft Security Blog, May 8)
- **Tag** - Security

Microsoft Secure Score Updates

Description



Microsoft announced that its Secure Score dashboard is now available in the new Microsoft 365 Security Center. The previous standalone experience for Secure Score will be available until end May 2019, after which it will be deprecated.

The new Secure Score:

- Is organized around threat entities, rather than Microsoft products. The threat entities are the same as in Microsoft Threat Protection--identity, data, devices, apps and infrastructure.
- Offers an overview pane with your current score, history snapshot, and high priority recommended improvement actions.
- Lists improvement actions that could be done to increase the organization's Secure Score, with properties that include user impact, implementation cost, and status. An administrator can sort and filter the list of recommended actions.
- Includes a more comprehensive picture of the organization's secure score over time, rather than just offering a point-in-time snapshot as previously. Comparative trend lines are offered against the global average, industry average, and other organizations with a similar number of licensed Office 365 seats.
- Is available through API, which has been released to general availability.

Analysis

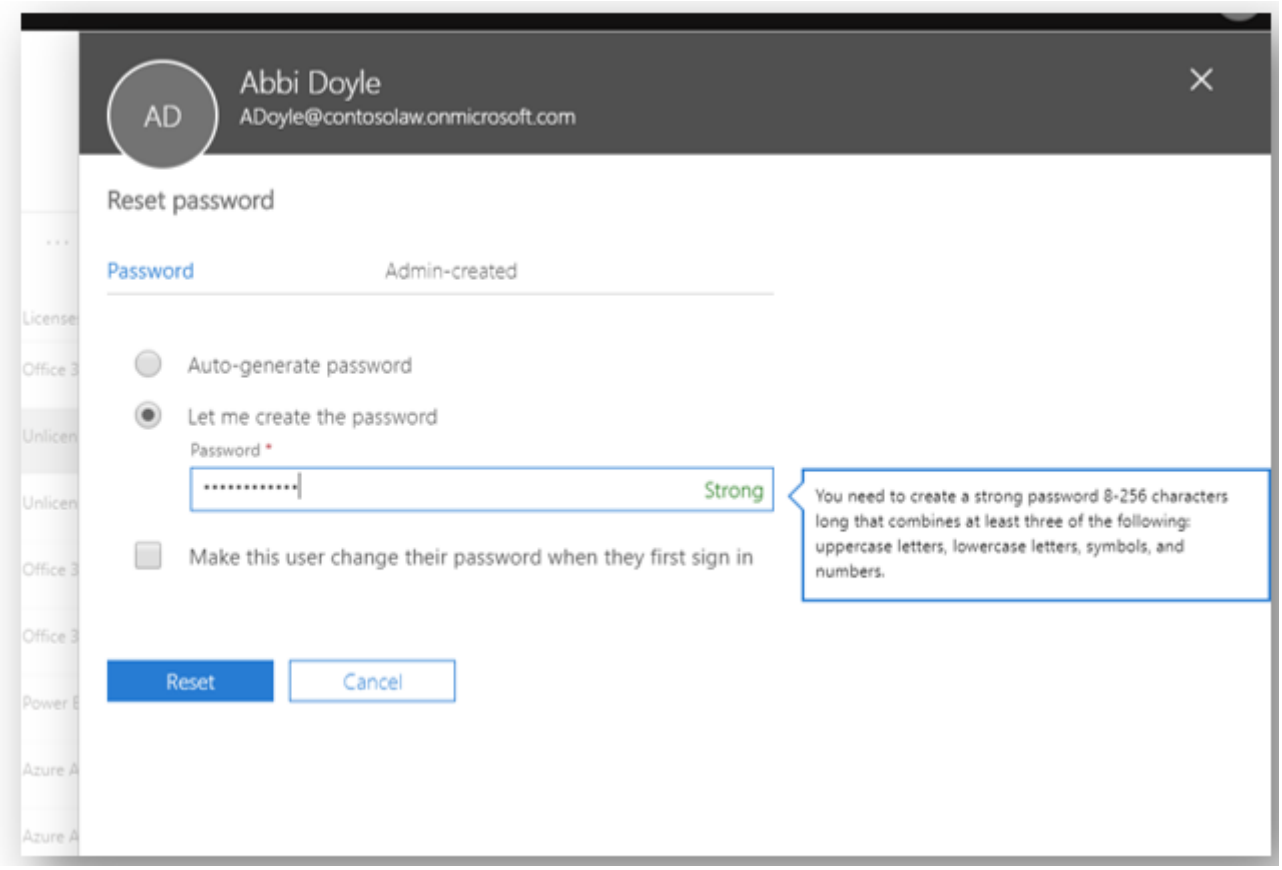
- With many different products and capabilities on offer from Microsoft and third-party vendors, and many different threat vectors facing organizations on a daily basis, having a structured way of scoring a security baseline and gaining insight into how to improve that baseline is a good use of intelligence. Historical trend lines over time in comparison to other sets of customers offers social pressure to improve.
- It is in Microsoft's best interest to have a highly secured service, and to minimize the number of times a customer is breached, hacked, or otherwise compromised. But with a shared security model, Microsoft can only do so much directly without crossing into actions that are the customer's responsibility. Secure Score offers an indirect pathway for elevating overall security for customers.

About

- **Date** - May 10, 2019
- A New Home and an All-New Look for Microsoft Secure Score (Security, Privacy and Compliance Blog, May 10)
- **Tag** - Security

Support for Longer Passwords

Description



Microsoft eliminated the previous limitation of a 16-character maximum password length in Office 365 and Azure AD. Passwords now have a maximum length of 256-characters, and must meet at least three of the complexity requirements: uppercase letters, lowercase letters, symbols, and numbers. Spaces are also supported, which opens the use of passphrases rather than passwords. Passphrases are easier to remember than a password with a difficult pattern. For example, a passphrase could be "I am Clarke Kent and I am Superman." This is a 34-character "password" that is simultaneously easy-to-remember for the end user but, due to its length, harder for an attacker to guess or crack.

Microsoft also introduced support for password writeback from Azure AD to on-premises Active Directory using Azure AD Connect. This allows an administrator to change a user's password in Azure AD, and have this propagated back to Active Directory. Password writeback requires Azure AD Premium licensing.

Analysis

- The absence of support for passwords longer than 16 characters has been a key shortcoming in Office 365 and Azure AD. These changes address this long overdue problem.
- Longer password length has been a critical recommendation for strengthening the username / password combination for authentication. However, regardless of password length, a breached password is still a breached password, whether it is 16-characters or 78-characters. Office 365 tenants need additional layers of account protection, such as multi-factor authentication and passwordless approaches that rely on public key cryptography.

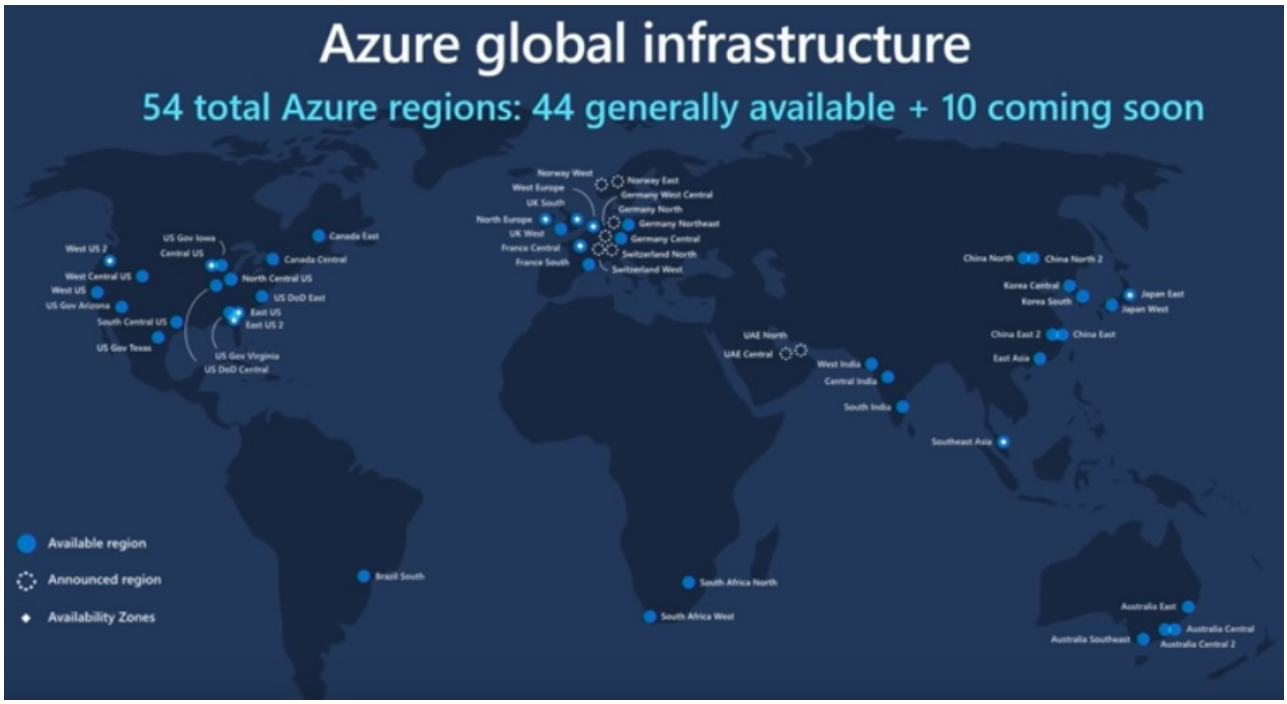
About

- **Date** - May 8, 2019
- What's New in Microsoft 365 User Management for April 2019 (Microsoft 365 Blog, May 8)
- Reset Password in the Microsoft 365 Admin Center (Microsoft 365 Roadmap 51332, May 9)
- Removal of the 16-Character Limit for Passwords in Azure AD (Azure AD Identity Blog, May 15)
- Password Policies That Only Apply to Cloud User Accounts (Microsoft Docs)

- **Tag** - Authentication
- **Implication** - Authentication - Overview

Azure Durability

Description



At its Build 2019 conference last week, Microsoft talked about several investments in improving the durability of its Azure data centers. Investments include:

- The ability for a cloud app to survive platform failure, without having to reboot virtual machines. This allows virtual machines to keep running even if the host platform is disrupted, with the VMs coming back on line when the host platform is re-established.
- The greater use of availability zones to improve reliability if a given Azure data center was knocked out of action due to a localized event, e.g., an earthquake. Availability zones offer independent power, networking and cooling facilities within an Azure region.

Analysis

- Improving the resiliency and durability of Azure is essential as customers migrate more and more workloads to Azure and Office 365 (which runs on Azure infrastructure).
- While Azure is greater than just Azure AD, Office 365 customers have experienced several major service disruptions due to lack of resiliency in Azure AD. This means that Microsoft's current architecture for Azure has not yet delivered a fail safe cloud-based authentication service. For example, a lightning strike in Texas in September 2018 disrupted the cooling systems at the US South Central data center which impacted both Office 365 and Azure services, with customers outside of the US South Central region experiencing Azure AD authentication problems.

About

- **Date** - May 14, 2019
- Build 2019 - Inside Azure Datacenter Architecture with Mark Russinovich (Youtube, May 8)
- Microsoft Wants Its Azure Servers to be as Durable as Tardigrades (ZDNet Microsoft, May 14)
- **Tag** - Authentication
- **Implication** - Authentication - Overview

Microsoft Threat Protection Update

Description

Microsoft provided an update on its protection statistics with Microsoft Threat Protection, its range of services for security and protection - such as Microsoft Defender ATP, Office 365 ATP and Azure ATP. Statistics included:

- 5 billion phishing emails blocked in 2018.
- Microsoft's security analysts analyzed 300,000 phishing campaigns during 2018.
- 14 million malicious sign-in attempts blocked every year.
- 470 billion emails analyzed, up from 400 billion a year ago.
- 1 billion Azure AD user accounts, up from 750 million a year ago.
- Millions of new attacks every day that run for 60 minutes or less.

Microsoft claims the signals it gathers across the multiple products in the Microsoft Threat Protection portfolio enable it to offer superior protection compared to third-party vendors, and gives the example of its ability to identify a threat in a PDF document that no-one else was able to see.

Analysis

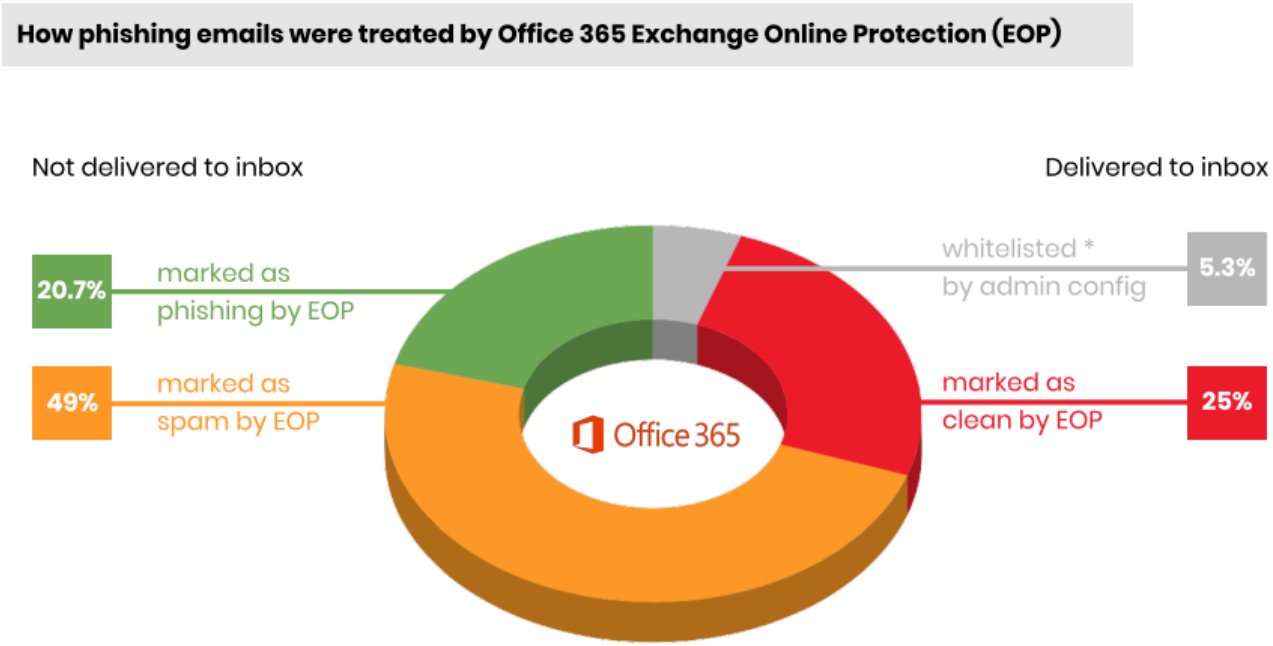
- The cross-product signal sharing and protection leveraging capabilities in Microsoft Threat Protection due to the Intelligent Security Graph is a golden asset for Microsoft. Having visibility into so many threat episodes offers an unparalleled body of threat knowledge.
- While impressive, the services in Microsoft Threat Protection are not perfect (e.g., see Avanan's Global Phish Report 2019). Threats still get through, as evidenced by phishing messages that still get delivered to a user inbox. It also points to the need for multi-layered protection, including account and identity protection.

About

- **Date** - May 14, 2019
- Executing on the Vision of Microsoft Threat Protection (Microsoft Security Blog, May 14)
- Announcing Microsoft Threat Protection (Security, Privacy and Compliance Blog, September 2018)
- **Tag** - Security
- **Implication** - Microsoft Threat Protection

Avanan Global Phish Report 2019

Description



Avanan reported on the phishing trends it has seen with Office 365 and Google G Suite:

- Avanan detects twice as many phishing attacks on Office 365 (1.04%) compared to Google G Suite (0.5%). With over 180 million actively monthly users of Office 365, it provides a much greater set of potential phishing victims compared to G Suite.
- Avanan claims that 25% of the phishing attacks it analyzed were not detected by the threat protection capabilities in Office 365.
- Avanan breaks phishing into four categories: malware delivery (50.7%), credential harvesting (40.9%), extortion (8%), and spearphishing (0.4%).
- 1 out of every 25 branded emails is a phishing email - with Microsoft being the most impersonated brand over the course of a year.

Analysis

- In total, Avanan claims that 1 in every 99 emails is a phishing email (1.01%), and for Office 365 it is 1.04%. This is consistent with Microsoft's most recent phishing statistics: 5 billion phishing emails in 2018 out of 470 billion email messages (1.06%). See Microsoft Threat Protection Update.
- Avanan's tests were with Exchange Online Protection only, which was able to identify and block just under 70% of threat-ladened messages. Microsoft Threat Protection offers a variety of services that kick in after EOP, such as Office 365 Advanced Threat Protection and Microsoft Defender ATP, the impact of which were not modelled in the Avanan report.

About

- **Date** - May 15, 2019
- Avanan Global Phish Report 2019 (Avanan, April 10)
- **Tag** - Security

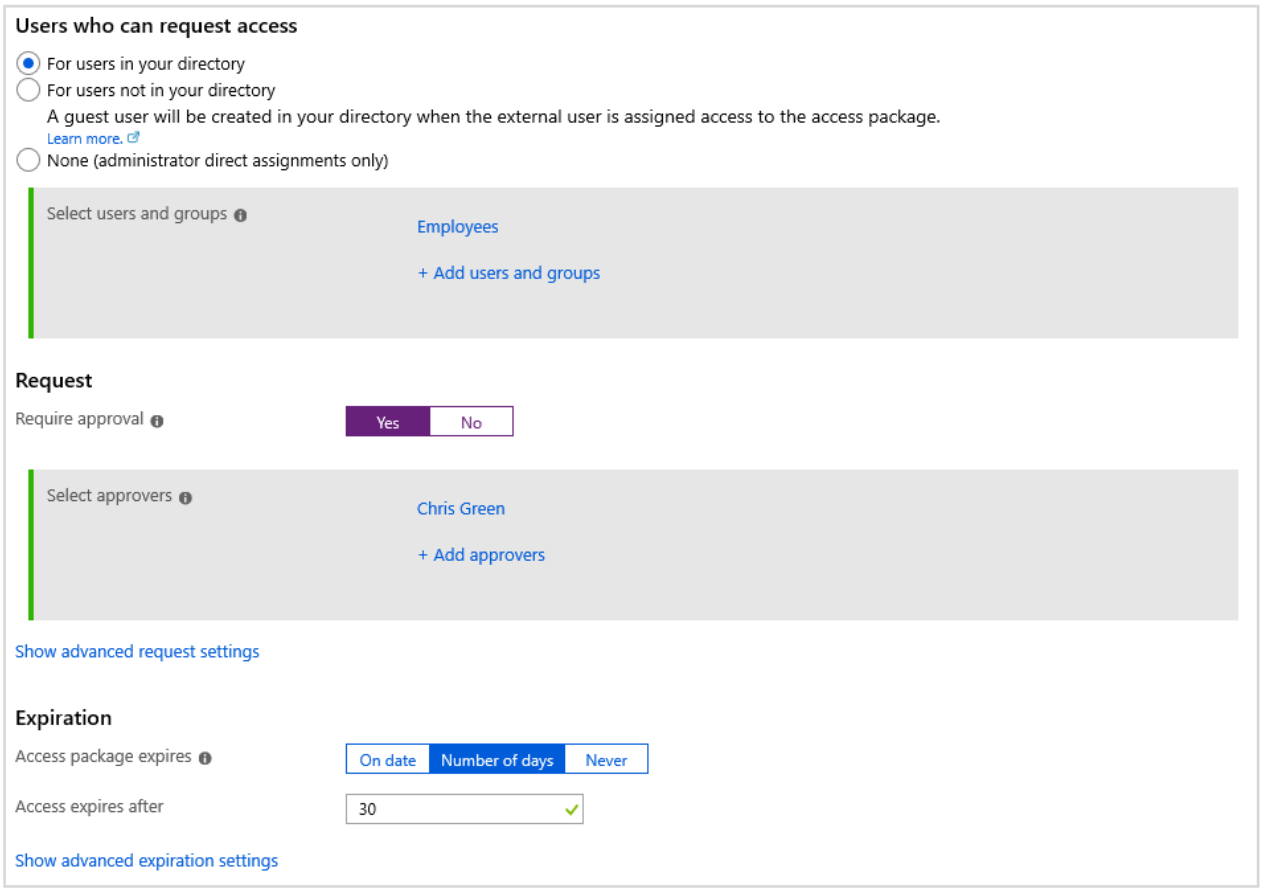
Weekly News Drop - May 17, 2019

Roundup of recent Office 365 news:

- **Microsoft Cloud App Security Alert Delay**. Several users of Microsoft Cloud App Security (MCAS) have noticed a significant time delay between an event happening and an alert being raised in MCAS. For example, a couple of users say there is at least a 90 minute delay between an impossible travel event being recorded in Office 365 and Azure and the alert being surfaced in MCAS. Similarly, another user commented that uploading a new file containing credit card numbers in contravention of a DLP policy can take up to 2 hours to show in MCAS. Cloud App Security Alerts Not in Realtime? (Microsoft Cloud App Security, May 9).
- **SharePoint Servers Under Attack**. SharePoint servers on-premises are under attack due to a security flaw that permits remote code execution. Microsoft has fixed the vulnerability in updates released in February, March and April 2019, but customers must apply these patches to on-premises servers. Active attacks have been identity across multiple sectors, and if servers are not patched, could result in one of the biggest vulnerabilities in SharePoint in recent years. The vulnerability does not affect SharePoint Online. Microsoft SharePoint Servers are Under Attack (ZDNet Zero Day, May 10).
- **Audit Log Truncation Resolved**. The truncation of Office 365 Audit Events was finally resolved in early May 2019, some 8 months after being reported to Microsoft. Truncated records will not be corrected by Microsoft. The Sad Case of Truncated Office 365 Audit Events (Office 365 IT Pros, May 10).
- **Shareable Links in Microsoft Teams**. Users will gain the ability to create a shareable link to any file stored in Microsoft Teams, and be able to set the appropriate permissions directly when doing so. "*The copied link can then be shared with others, by pasting it into a chat or channel. On pasting the plain lengthy link, this feature converts the link into a file chiclet object (same as the ones already available in Teams, when you upload a file into a chat or a channel). The sender can also set permissions on the file link that they are sharing, at the time of composing the message itself, so that the recipients do not run into access issues*." Due by the end of June 2019. Microsoft Teams - Shared Links (Microsoft 365 Roadmap 51230, May 7).
- **Ovum Consulting on Microsoft Security Stack**. Ovum Consulting published a report in early April 2019 that calls out the benefits of using Microsoft's security stack, including Azure AD, Microsoft Threat Protection, Microsoft Information Protection, and Azure Sentinel. Ovum Recommends Microsoft Security to Safeguard your Hybrid and Multi-Cloud Environments (Microsoft Security Blog, May 16). Microsoft's licensed the report (PDF, 13 pages).
- **US Government on Office 365 Security Misconfigurations**. The Cybersecurity and Infrastructure Security Agency (CISA) analyzed the configuration settings for organizations migrating to Office 365, and noted four vulnerabilities. CISA recommends addressing the following: multi-factor authentication for administrator accounts, mailbox auditing, password sync with Azure AD Connect, and authentication using legacy email protocols. While the recommendations are important, each is fairly basic to implement. No mention was made of newer security capabilities in Office 365 and Microsoft 365, such as message encryption, information protection, and cloud access security, among others. Analysis Report 19-133A - Microsoft Office 365 Security Observations (CISA, May 13).

Azure AD Entitlement Management

Description



Microsoft released the public preview of Azure AD Entitlement Management, a policy-based approach to giving employees and guests (external users) controlled access to resources such as Office 365 apps, third-party cloud applications, and internal line-of-business applications that have been integrated with Azure AD.

- **Access Packages**. Creates a grouping of target applications that people assigned the package can access. Access packages support Office 365 and Azure AD security groups, third-party and internal applications that have been integrated with Azure AD for authentication, and SharePoint Online sites.
- **Support for Multiple Request Policies per Access Package**. Policies specify who can request the access package, if approval is required, and when/if access rights are automatically revoked. Each access policy supports multiple request policies, so for example, people in one group are automatically provisioned with access, while people in another group must be have their request authorized prior to gaining access.
- **Permission to Request**. Defines who the policy applies to. Options are a specified users in your directory, external users not in your directory, and none. None means that an administrator must directly assign access; no one can request it.
- **Need to Approve**. Who (individuals or groups) must approve an access request. Advanced options include requiring a justification by requester and/or the approver, and the time-out period for the request. If approval is required, access is automatically provisioned once approved. If approval is not required, the request is fulfilled as soon as possible after being submitted by the requester.
- **Automatic Expiration**. When the bundle of access rights in the package expire for the user, in order to automatically withdraw access rights. Options are on a specified date, after a specified number of days, or never.

Microsoft says that Entitlement Management is one of the four modules in its Identity Governance portfolio for Azure AD, with the other three being Privileged Identity Management, Terms of Use, and Access Reviews. Entitlement Management requires Azure AD Premium P2 licensing, which is available separately, as part of Enterprise Mobility and Security E5, or Microsoft 365 E5.

Analysis

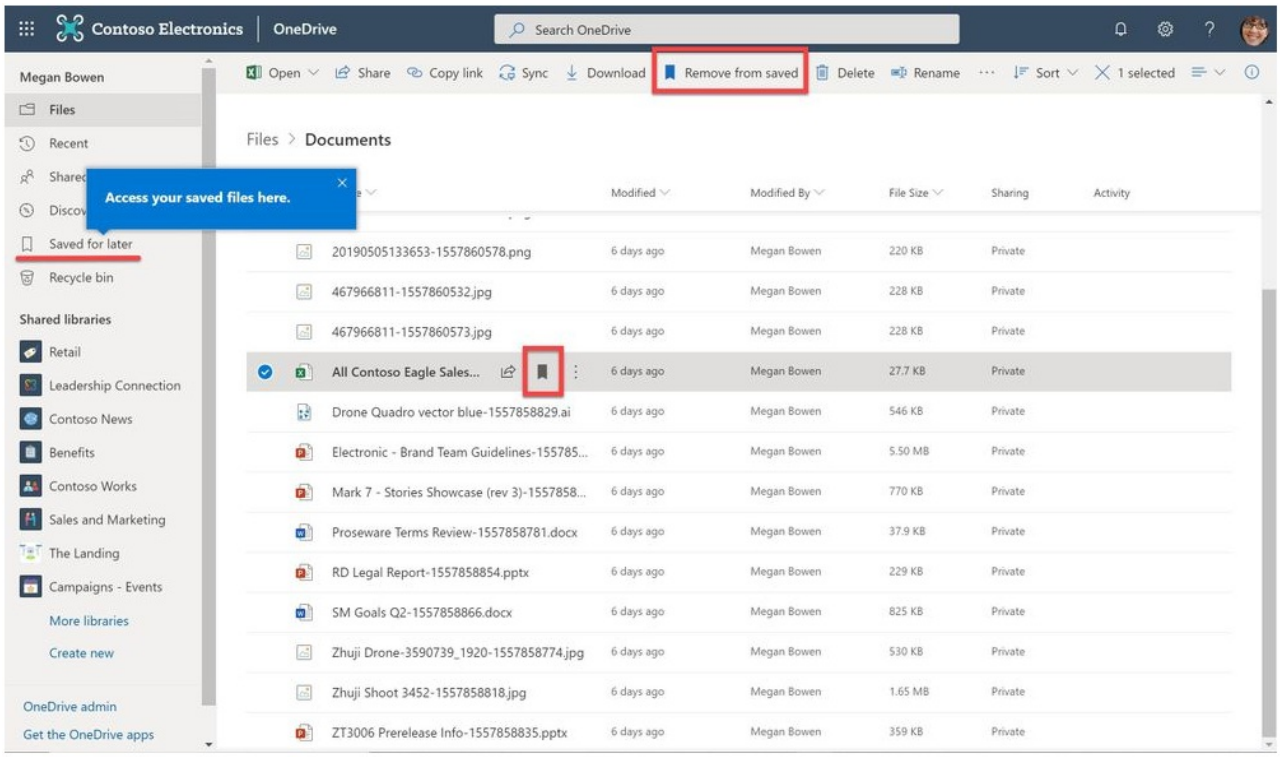
- Having the ability to wrap some formality and auditability around provisioning access to organizational systems and data repositories is increasingly important, due to new and emerging data protection regulations. Being able to show formality of process based on user roles and explicit authorization steps means organizations can show they have the "organizational measures" (per GDPR language) in place.
- Entitlement Management will immediately be attractive to large organizations for their own internal processes, as well as organizations working with a changing roster of external people. However, the due process it enforces for access rights should also make it highly attractive to smaller organizations.

About

- **Date** - May 20, 2019
- Announcing a New Azure AD Identity Governance Preview - Entitlement Management (Azure AD Identity Blog, April 30)
- What is Azure AD Entitlement Management? (Microsoft Azure Docs, April 27)
- **Tag** - Authentication
- **Implication** - Authentication - Overview

OneDrive Updates at SharePoint Conference 2019

Description



Microsoft announced a plethora of updates for OneDrive, what it is now calling its files app for Microsoft 365 (although "files app for Office 365" would be more correct). Updates included:

- The current consistent sharing experience is coming to MIcrosoft Teams. It is currently available in OneDrive, Office desktop and mobile apps, SharePoint document libraries, desktop Windows Explorer and Mac Finder.
- A sharing link pasted into Outlook Web App will be transformed into a more visual link to the file. It will include the ability to change the default sharing privileges.
- A new recommended files view at the top of the UI in OneDrive on the web. Recommended files are included based on signals such as recent edits by a collaborator, files you opened recently, and general file activity trends.
- The on-hover file card in OneDrive on the web now includes intelligence on the file, such as time to read and a quick summary based on a table of contents created by AI.
- The ability to save documents for reviewing later (see image above). Saved documents display in the Saved for Later view.
- Shared libraries in OneDrive have more functionality, such as the ability to create new documents, pin documents, and manage metadata, among others. The intent is to offer "full-fidelity" with the SharePoint experience.
- The ability to create a new shared library directly in OneDrive on the web. Creating a new shared library creates an Office 365 group to manage access.
- In-line previewing of AutoCAD DWG files in OneDrive on the web.
- In-line rendering and previewing of 360 degree images.
- The ability to send a collaborator a link to a folder, asking them to upload documents into a specific place. The recipient can add their files to the folder, and by default only sees the files they have uploaded.
- The OneDrive sync client will gain expanded support for differential file sync later in 2019. Currently differential sync is support for modern Office files; it's coming for a whole lot more file types in 2019.
- The file picking experience on Outlook mobile will become consistent with the experience in Outlook web app.
- In the OneDrive mobile apps, Microsoft is improving the recent files experience and improving its annotation options for marking up a PDF.

Analysis

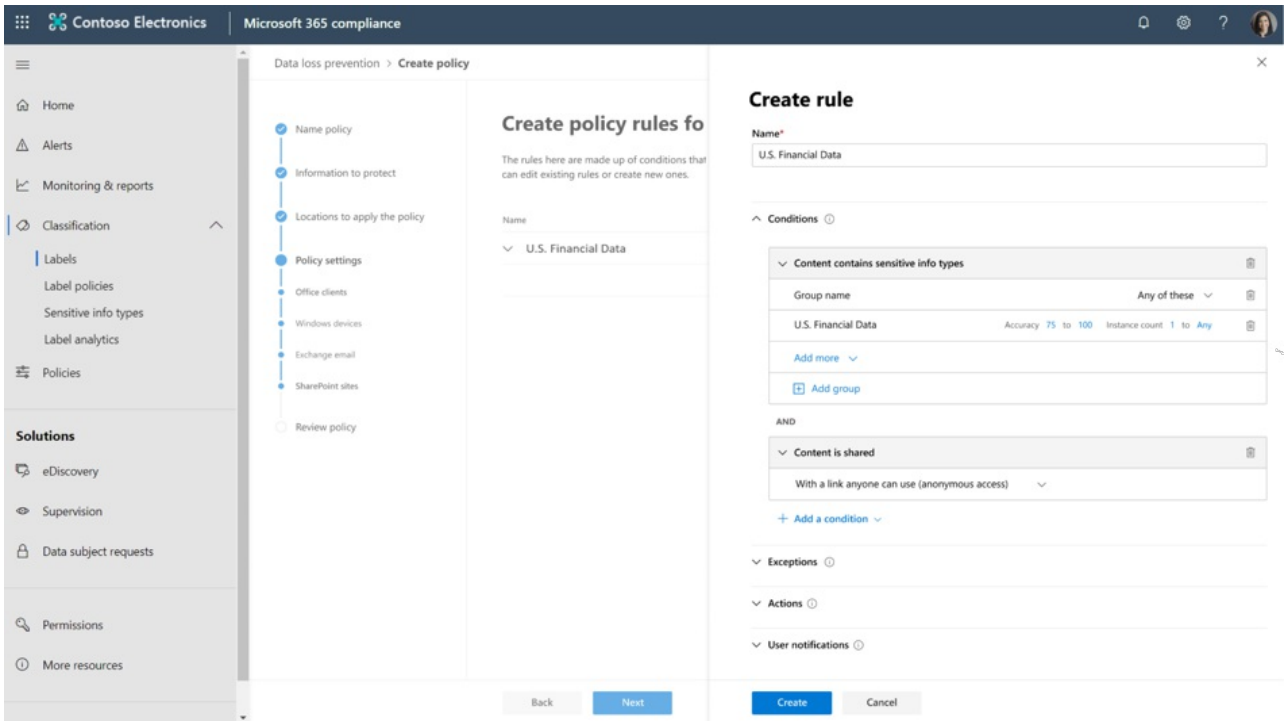
- The announcements add up to a good list of incremental and minor improvements to experience and usability.

About

- **Date** - May 21, 2019
- OneDrive Announcements - SharePoint Conference 2019 (OneDrive Blog, May 21)
- **Tag** - File Sharing

SharePoint Security and Compliance Updates

Description



At the SharePoint Conference 2019, Microsoft announced a long list of security and compliance updates for SharePoint Online:

- Multi-Geo is now generally available for SharePoint Online and Office 365 Groups.
- Licensing requirements for Multi-Geo has been reduced to only 500 users in a tenant. This is effective from June 1, 2019.
- Sensitivity labels can be applied to a SharePoint site as a complete unit. Any content in the site will be automatically labelled. Available in Private Preview.
- Office files protected with sensitivity labels will be available for access in Office Online for opening, editing and co-authoring, if the policy allows it.
- Documents protected with sensitivity labels will be available for full text search by eDiscovery.
- DLP policies will be able to see inside documents protected with a sensitivity label.
- For the complete tenant, a SharePoint administrator can specify an automatic expiration period for site access for new external guests. Access will be automatically revoked after the period elapses, unless the user is granted extended access or sent a new sharing invitation.
- Various updates to the SharePoint Admin Center, including the ability to work with both modern and classic SharePoint in a consolidated view, bulk actions, site renaming, and root site switching (to support the new SharePoint Home Site).

Many of these capabilities were announced or put into private preview, but not actually released to market as generally available.

Analysis

- Multi-Geo was announced as being generally availllable in late March 2019. It is unclear why this announcement was made again at the SharePoint Conference.
- Microsoft is slowly but surely working across the wide implications of new productivity and security features, such as making documents with sensitivity labels available to eDiscovery and DLP.

About

- **Date** - May 21, 2019
- Updates to SharePoint Security, Administration and Migration (SharePoint Community Blog, May 21).
- **Tag** - Security, eDiscovery, Data Loss Protection

- **Implication** - Tenant Architecture
- **Implication** - Indexing File Types
- **Implication** - Sensitivity Labels

Identity Data in Europe

Description

In 2018, Microsoft modified where identity data in Azure AD was stored for European customers, moving identity data to data centers in Europe if the customer (i.e., an Office 365 tenant) provided a leading address in Europe. Microsoft announced that it will also now store all personally-identifiable information (PII - an American term, not a European one) within datacenters in Europe.

Microsoft noted several exclusions, including:

- All two-factor authentication using phone calls or SMS originate from US data centers, and are routed by global providers.
- Push notifications using Microsoft Authenticator originate from US datacenters.
- Device vendor specific services may also be used, and these may be outside Europe.
- OATH codes are always validated in the US.
- For Azure AD B2B, invitations with redeem link and redirect URL information is stored in US datacenters.
- For Azure AD B2B, email addresses of users who unsubscribe from receiving B2B invitations are stored in US datacenters.

Analysis

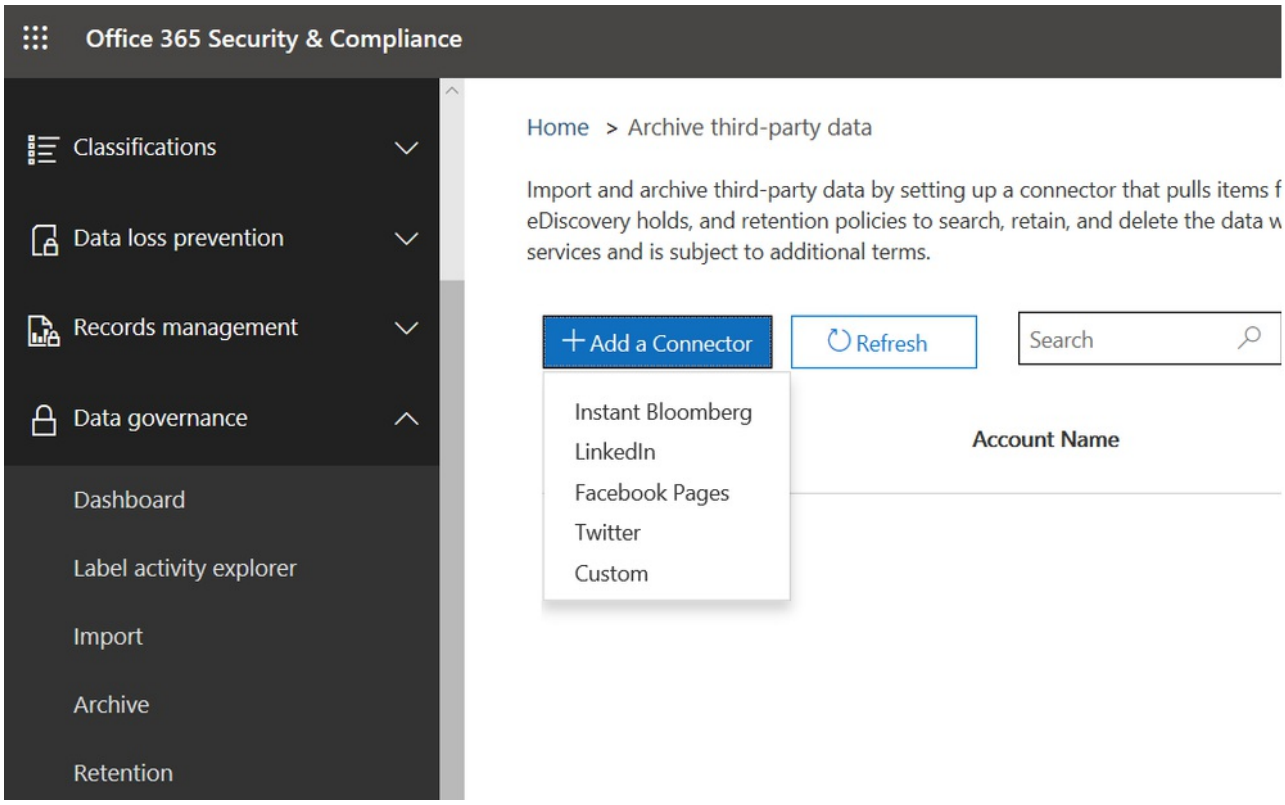
- There does not appear to be a Multi-Geo angle to where identity data is stored. For example, for an Office 365 tenant with a leading address anywhere except Europe who then lights up a Europe satelitte using Multi-Geo, the identity data and PII attributes for the European subset of users will still be stored in Azure AD outside Europe.

About

- **Date** - May 23, 2019
- Identity Data for European Customers (Azure AD Identity Blog, May 23)
- Identity Data Storage for European Customers in Azure Active Directory (Microsoft Docs, March 3)
- **Tag** - Authentication

Records Management

Description



Microsoft said it introduced a new records management solution in Microsoft 365. In reality, it introduced a new heading called "Records Management" in the Office 365 Security & Compliance Center, and moved several current capabilities under the heading. Capabilities are:

- Importing of third-party data using native connectors. Working with a third-party provider for third-party data ingestion has been required previously.
- The File Plan has moved under the Records Management heading, along with disposition review.
- A list of disposed items can be exported to provide proof of disposal.
- The ability to collaborate on records was released to public preview. If enabled, users can continue to edit and modify a declared record, because changes are automatically stored as a new record version.

Analysis

- The author highlighted that these capabilities had come to "Microsoft 365 Compliance," and yet all the screenshots were from the current Office 365 Security & Compliance Center. As usual, the marketing rhetoric is ahead of the engineering reality.
- The Facebook pages native connector still requires installation of code from GitHub. It's "native" in the sense that it comes from Microsoft, but it's not native in the sense that it's completely integrated into the Office 365 code base.
- Ingested data is still converted into an email message format and stored in an Exchange mailbox.

About

- **Date** - May 23, 2019
- New Records Management Solution and Machine Learning Updates Come to Microsoft 365 Compliance (Securiy, Privacy and Compliance Blog, May 21)
- Records Management in Microsoft 365 (Microsoft Docs, May 22)
- Archive Third-Party Data in Office 365 (Microsoft Docs, May 18)
- **Tag** - Archiving
- **Implication** - Lack of Archiving for Some Content Types

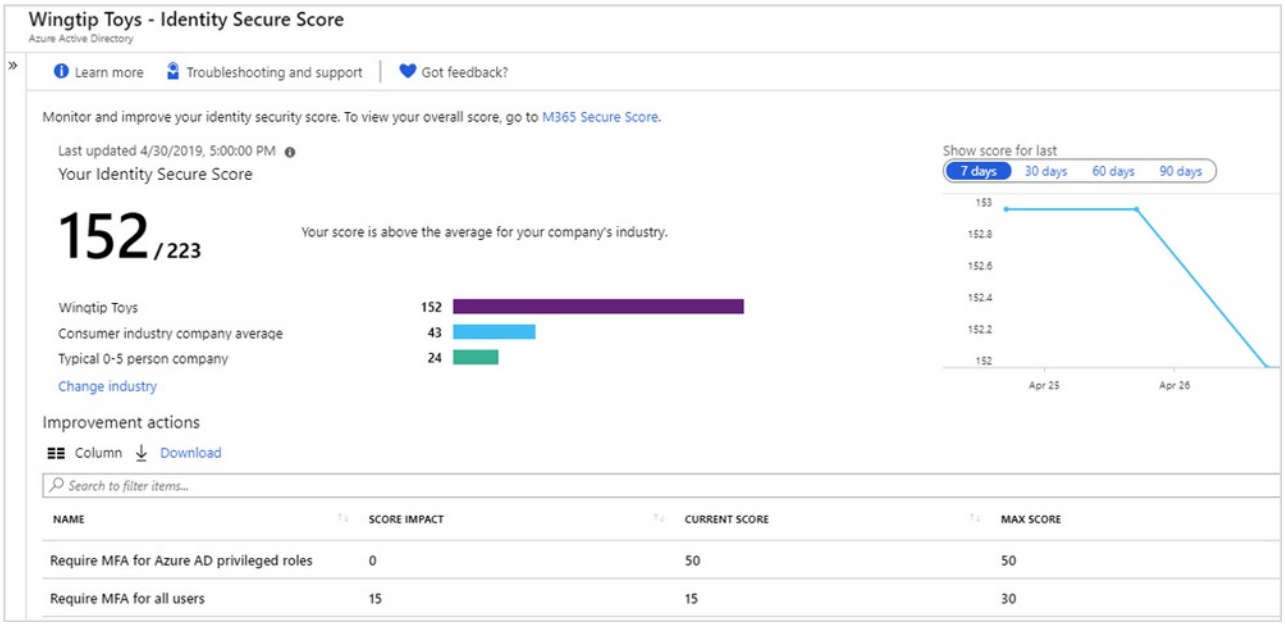
Weekly News Drop - May 24, 2019

Roundup of recent Office 365 news:

- **More SharePoint in Teams Files**. Microsoft will add additional current SharePoint capabilities into the Files tab in Microsoft Teams; the current experience offers only a reduced set of capabilities. Forthcoming capabilities include the ability to sync files, additional view options, lifecycle signals on files, pinning files, and checking out of files. Due by end June 2019. Microsoft Teams - Improved Channel File Tab Experience (Microsoft 365 Roadmap 51234, May 17).
- **Inclusiveness and Accessibility**. Microsoft highlighted its business and cultural drive to become more inclusive, which includes diversity of talent and recruiting people with disabilities. Microsoft's internal approaches to this include a recruitment program for people with disabilities, training for managers working with visible and non-visible disabilities, more flexible job role assessment methods, and sign language interpreters, among others. Microsoft also highlighted its accessibility features for PowerPoint and Microsoft Teams Meetings, specifically live captions and subtitles based on spoken speech. Building the Inclusive Workplace We Imagine, Together (Microsoft 365 Blog, May 15).
- **Identity Provider Support for Chinese Social Platforms**. Microsoft announced support for Chinese social platforms (Weibo, QQ and WeChat) to provide identity services in Azure AD B2C. Azure AD B2C offers a secure way of enabling authentication using existing identity providers for consumer apps, thereby eliminating the need to create a separate identity service for each app. Public Preview of Azure Active Directory B2C in China (Azure AD Identity Blog, May 21).
- **Yammer In-Geo Residency for Europe at General Availability**. At the SharePoint Conference, Microsoft announced that in-geo data residency for Europe for Yammer is now generally available. Only applies to new Office 365 enterprise customers. Microsoft offered no insight into migration options for existing European customers with Yammer data stored in the United States. New Yammer Investments Announced at SharePoint Conference Add Engagement and Compliance Capabilities (Yammer Blog, May 21).
- **Microsoft Search Coming Soon**. Microsoft's new enterprise search experience is almost at general availability. It expands the range of search results available through the search bar, including recent tasks, people, and even anonymized results from Bing. Search That Works - Wherever You're Working (SharePoint Community Blog, May 21).
- **New Setup Experience in Microsoft 365 Admin Center**. Microsoft announced a new setup experience for the apps and services available in a tenant. The new Setup page lists setup tasks to complete that are appropriate to the user's admin role, and quick access to indepth learning resources. Availability is expected for all tenants by early-to-mid June 2019. Optimize Microsoft 365 with the New Setup Experience (Microsoft 365 Blog, May 24). Microsoft 365 Roadmap 51623 (May 21).
- **Compliance Workspaces in SharePoint Online**. Something called a Compliance Workspace is coming to SharePoint Online in Q3 2019. Microsoft's information-light description says: "*Compliance workspaces allow you to review content grouped by label, regardless of type or container – meaning, across files, conversations, emails and more. Libraries have long provided version management for collaborative content. For compliant and regulated industries, sometimes particular versions of a file have distinctive needs for retention, records management and the like. Compliance workspaces will allow you to drill into single versions of files and manage renditions, movement/curation, or retention policies. Many files go through dozens or hundreds of versions with only a handful subject to retention. Workspaces will let you label these versions and even transfer them to centralized stores, allowing you to groom information architecture and containers over time.*" Optimizing Business Solutions with SharePoint and Office 365 at SPC19 (The SharePoint Community Blog, May 21).

Identity Secure Score Released

Description



Microsoft released to general availability its Identity Secure Score dashboard for Azure AD. Identity Secure Score offers a numerical analysis of an organization's security posture for identity, based on the settings within Azure AD that have and have not been enabled. Capabilities include:

- The organization's current identity secure score, compared with the potential maximum score. Trend line analysis of recent changes (7 days, 30 days, 60 days and 90 days) is available.
- Comparative analysis of the organization's current identity secure score with other organizations in the same industry, as well as a cross-industry view of organizations with a similar size.
- Specific recommendations on improvement actions that will increase the organization's identity secure score. The top recommendation (which awards the greatest number of points) is to require MFA for Azure AD privileged roles. The second highest ranking recommendation is to require MFA for all users.
- API access for integrating secure score data with other systems.

Actions that improve an organization's identity secure score also impact the organization's overall Secure Score.

Analysis

- Offering a numerical analysis of security posture along with specific directed recommendations means admins have clear insight into what is required to strengthen their defenses. With the proliferation of new security services and apps in Office 365, Enterprise Mobility and Security, and other Microsoft offerings, being able to see which security capabilities are core and fundamental to security posture is helpful for admins.
- The risk for Microsoft is that it loses the differentiation between security fundamentals and product marketing. If product marketing teams got access to the logic underlying Identity Secure Score., it would be easy to inflate the denominator by recommending an ever growing set of security solutions.

About

- **Date** - May 24, 2019
- Identity Secure Score is Now Generally Available (Azure AD Identity Blog, May 21)
- **Tag** - Security

Can't Change Office 365 Tenant Name

Description

Microsoft offers no way for an Office 365 tenant to change their original tenant name, e.g., the **tenantname**.onmicrosoft.com part. While this whole address space can be hidden from view due to domain mapping, the tenantname part is still displayed in several high profile places in Office 365, irrespective of domain name mappings. For example, the tenantname part is prepended to SharePoint Online and OneDrive addresses, as in tenantname.sharepoint.com. These addresses are visible in web links and sharing links for gifting access to documents and other content.

Office 365 customers note the following reasons for wanting to change a tenant name:

- The original tenant name was inadvertently spelt incorrectly, and not noticed until significant content and usage was in place.
- The company has changed its name, and now wants the sharing addresses it uses from Office 365 to reflect the new name.
- The company has been purchased by another entity, and the new entity wants to change the original tenant name.
- An admin started a demo / trial tenant, and then wants to move the tenant name to a production tenant.

Microsoft's only option currently for customers who want to change their original tenant name is to create a brand new Office 365 tenant with the new correct name, and engage a third-party migration vendor to facilitate data migration from the old tenant to the new one.

However, Microsoft is apparently working on a solution. For example:

- A research project gathering requirements and customer needs, in the context of SharePoint renaming. See SharePoint Tenant Rename Research Survey (March 2019).
- Acknowledgement that the feature is being built, for delivery during 2019. It is unclear whether this is for the complete tenant - tenantname.onmicrosoft.com - or just the SharePoint tenant name, e.g., tenantname.sharepoint.com. See Enabling Renaming the Site Collection URLs (SharePoint UserVoice, March 2019).

Analysis

- The ability to change the Office 365 tenant name is the highest voted item on the Office 365 Admin space on UserVoice (with almost 7000 votes at end May 2019), with comments and votes going back to October 2015. Microsoft personnel have made no official comment on the request in UserVoice.
- Forcing customers to migrate to a new tenant in order to achieve a tenant name change will become more difficult / less effective over time due to encrypted messages and documents.
- Being able to rename the tenant name is only one solution available to Microsoft. Tying accessible URLs to a given tenant name is bad form in multi-tenant cloud services. It would be much better if the tenant name was completely invisible and an alias or vanity name was used if required, or the customer's domain name could be displayed instead.

About

- **Date** - May 28, 2019
- Make It Possible to Change Tenant Name in Office 365 (Office 365 Admin on UserVoice, October 2015)
- Change Your SharePoint Domain Name (Microsoft Docs, February 2018)
- **Tag** - Security

Azure AD Provisioning Updates

Description

Microsoft announced several changes for its identity provisioning services that work with Azure AD. Specifically:

- A user account created in Workday and provisioned through Active Directory to Azure AD can now be updated from Azure AD through Active Directory to Workday if the original username field in Workday needs to be updated. The username writeback ensures the Azure AD userPrincipalName attribute is written back to Workday so the username field in Workday is the same, with the Azure AD attribute being authoritative.
- Access to several new cloud applications can be automatically provisioned from Azure AD, such as Dynamic Signal, Keeper Password Manager and Digital Vault, and Comeet Recruiting Software. Provisioning is based on the SCIM open standard, which Microsoft hopes to make greater use of.
- In Azure AD Connect 1.3.20.0, released end April 2019, writeback of an Office 365 group as defined in Azure AD to Active Directory on-premises is now generally available. Writeback enables users with an on-premises Exchange mailbox to send and receive emails from these groups.

Analysis

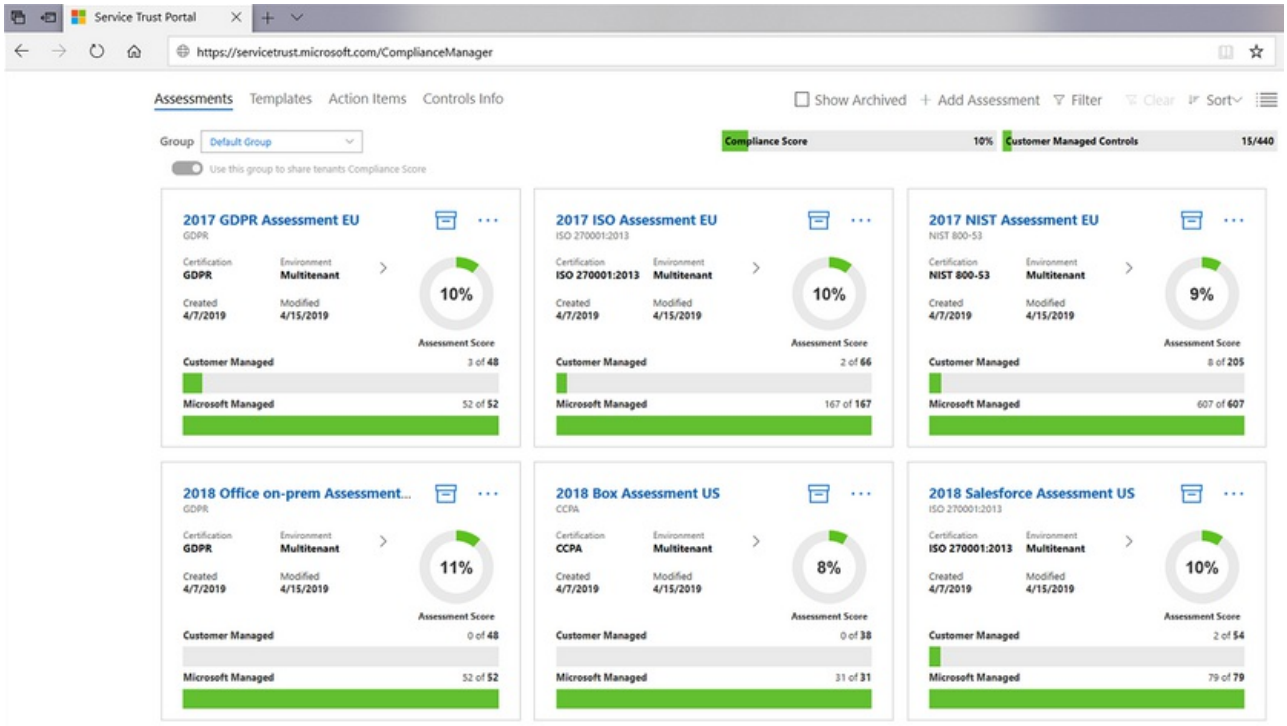
- Rule-based automated provisioning reduces errors, streamlines moves/add/changes, and elevates the ability of a firm to ensure only valid people have current access to systems. As systems proliferate, having linked up provisioning becomes more important.

About

- **Date** - May 28, 2019
- Build a Strong Identity Foundation with Azure AD Provisioning (Azure AD Identity Blog, May 20)
- **Tag** - Authentication

Compliance Manager (2019)

Description



Microsoft released to public preview a new version of Compliance Manager in the Service Trust Portal, with the ability to create assessments and with greater integration with other Microsoft solutions. Microsoft hopes that the new version will become the centralized compliance management tool for an organization.

New capabilities include:

- The ability for an organization to create their own assessments for apps and services, including on-premises and non-Microsoft offerings. Assessments can be created using templates.
- The ability to customize assessments, with new controls and actions that make sense for the organization.
- Automated control assessments, where changes in underlying controls are automatically reflected in Compliance Manager. This is still in early stages, with integration with Microsoft Secure Score as the first integration. Secure Score will provide "continuous updates" - which in practice means once every 24 hours - to Compliance Manager.
- Specific details on the actions to take to deliver the controls required, instead of focusing on the controls as in the previous version.
- A re-thinking of the assessment score, so that it now only reflects the score for actions under the control of the customer. The assessment score is also noted in percentage terms, not as a purely numeric value. Actions under the control of Microsoft (or any other vendor for non-Microsoft apps and services) are not included in the assessment score.
- Support for various regulations and standards related to Office 365 and Intune, with a GDPR assessment apparently forthcoming.

The previous version of Compliance Manager, released in 2018, will retain its data for at least 12 months after Microsoft releases the new version to General Availability.

Analysis

- As commented on Identity Secure Score, a numerical analysis of current status with clarity on actions to take to improve that status is very helpful for administrators and compliance professionals. Separating out the value of the Microsoft actions is a good move on Microsoft's side, since a customer can do nothing to influence those actions or value.

About

- **Date** - May 29, 2019
- Manage Compliance from One Place Beyond Microsoft Cloud with Compliance Manager (Security, Privacy and Compliance Blog, April 29)
- **Tag** - Security

Weekly News Drop - May 31, 2019

Roundup of recent Office 365 news:

- **Analog Data to Digital**. Microsoft announced several new ways of bringing analog data into the digital world, including converting a photo of a table of data to an Excel spreadsheet in Microsoft Excel, converting a photo of a whiteboard to digital ink in the Microsoft Whiteboard app, and streaming data from sensors directly into Microsoft Excel. Take Your Analog Data Digital For a Faster, More Efficient Way to Work (Microsoft 365 Blog, May 29).
- **Channel Moderation in Microsoft Teams**. "Channel moderation gives team owners and members who have been added as moderators exclusive rights to create new posts in the channel and control whether team members can reply." Due June 2019. Microsoft 365 Roadmap 51786 (May 28)

State of Cybersecurity

Description

ZDNet ran an article on the state of cybersecurity over the weekend. It highlights the problems with cybersecurity, putting the blame on the part of:

- Police forces that lack the time, money and skill to catch the crooks and scammers. That is, few consequences.
- Tech companies that release products to market that have not been security hardened. That is, many opportunities.
- Organizations lacking skills and processes for the simple things, such as patching identified flaws. That is, even more opportunities
- Individual end users who have not been vocal enough in demanding better security practices from corporate giants. That is, few consequences.

The article spawned a long comment thread, some of which are nonsensical, while others raise good points, such as:

- Security experts who don't study, learn, and get better - in practical terms - to protect their organization from current and evolving threats. When faced with threat actors who do study, learn, and get better to undermine security defenses, it is no surprise that the bad guys win.
- Security experts who can't translate security needs into terminology that management understands.
- End users who have no sense of security threats, let alone how to do simple every day tasks on their devices.

Analysis

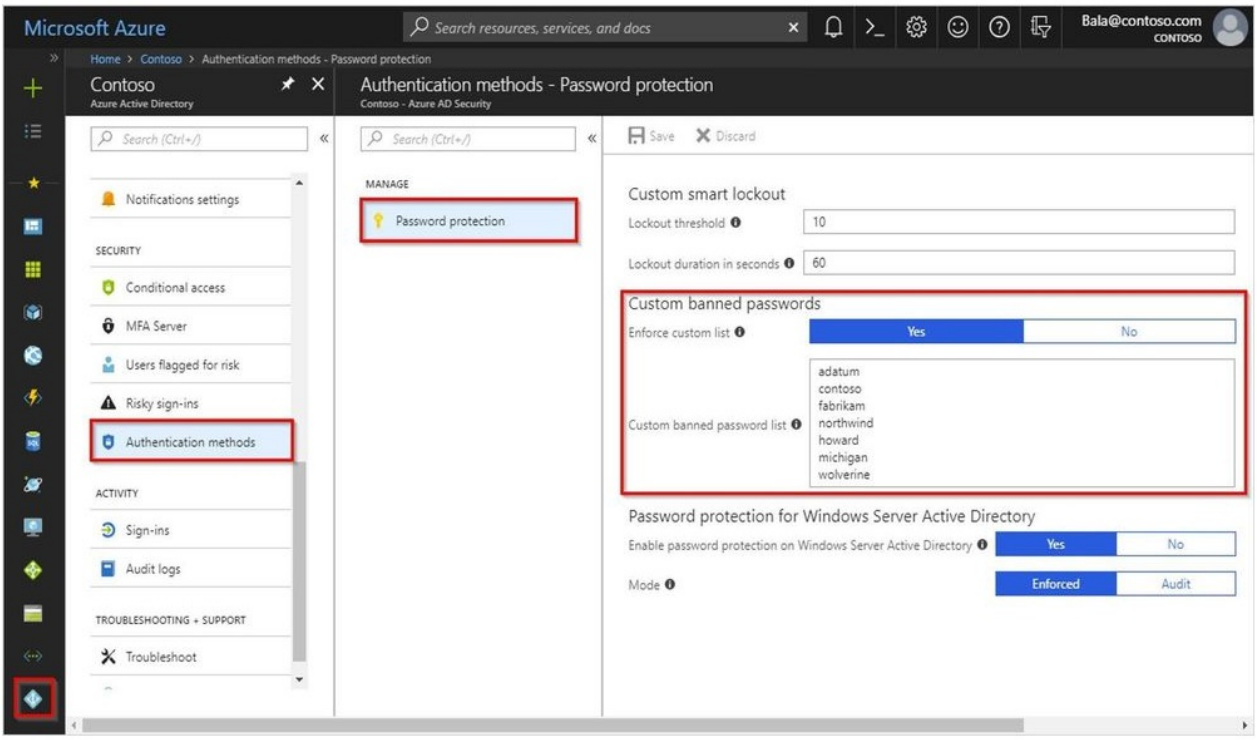
We don't normally run non-Office 365 news in this service, but given the importance of security in Office 365 and the variety of perspectives advocated in the article and comment thread, the above article is worth a (quick) read.

About

- **Date** - March 31, 2019
- Cybersecurity is Broken: Here's How We Start to Fix It (ZDNet, March 31)
- **Tag** - Security

Azure AD Password Protection Released to GA

Description



Microsoft released the Password Protection settings page for Azure AD to general availability; the service earlier entered public preview in September 2018. The intent is to provide organizations with a degree of control over password lockout settings, block specific words from being used in passwords, and allow integration with Windows Server Active Directory for organizations using a hybrid setup. These settings are part of Microsoft's approach for reducing the success rate of password spray attacks.

Specifics:

- Words in the custom banned list are not allowed to be used in a password, subject to a complexity rule applied by Microsoft. This means the list of "banned passwords" is really a list of banned words that can't be used in a password, rather than defining complete passwords that can't be used.
- If the password a user attempts to use includes words in the banned list, the password will be checked for overall complexity through the combination of other characters and letters. Microsoft calculates a complexity score for each password, and if it gets less than 5 points of complexity, the password is rejected. For example, "adatumcontoso" would score only 2 points and be rejected. "adatum@45contoso!" would score 5 or 6 points, and be accepted.
- All passwords are normalized before being checked for complexity.
- Any passwords entered in the custom banned passwords list are banned in combination with several other password banning methods already enforced by Microsoft at a global Azure AD service level. The custom banned passwords are not the only passwords banned; they are just the custom ones that a given organization wishes to prevent. Microsoft suggests organizations enter the "brands and products that their users identify with."
- The explanatory pop-up for the Custom Banned Password list reads "*A list of words, one per line, to prevent your users from using in their passwords. You should include words specific to your organization, such as your products, trademarks, industries, local cities and towns, and local sports teams. Your list can contain up to 1000 words. These are case insensitive, and common character substitutions (o for 0, etc) are automatically considered.*"
- Access to the custom banned password list requires Azure AD Premium P1 or P2 licensing, as does extending password protection to Windows Server Active Directory users.

The list of custom banned passwords is limited to 1000 words.

Analysis

- Microsoft does not currently offer organizations the ability to set a higher complexity score for passwords. Several commenters on the announcement requested this ability.
- Tenants without P1 or P2 licensing still appear able to enter a list of custom banned passwords (words), but there is no warning given that P1 or P2 licensing is actually required. Using the custom list without P1 or P2 licensing will put the customer into violation of licensing terms, but there is nothing in the product to alert a customer to this.
- Password Protection only evaluates a password when a user changes their password. Current passwords are not checked or assessed.

About

- **Date** - April 3, 2019
- Azure AD Password Protection is Now Generally Available (Azure AD Identity Blog, April 3)
- Eliminate Bad Passwords in Your Organization (Microsoft Docs, November 7)
- **Implications** - Authentication - Overview
- **Tag** - Authentication

Weekly News Drop - April 5, 2019

Roundup of recent Office 365 news:

- **Restricted Users in Security & Compliance Center**. Microsoft moved the Action Center from the Exchange Admin Center to the Security & Compliance Center, with a new name of Restricted Users (under Threat Management / Review). The new view lists users who have been restricted from sending mail to external users due to suspicious activity. Admins can unblock user accounts if appropriate. Microsoft said that future updates to Restricted Users will include recommendations on remediation, including changing passwords and enabling MFA. Action Center is Now SCC Restricted Users (Microsoft 365 Roadmap 31546, March 8). See also Message Center MC176246 (March 21, 2019).
- **Native Labeling in Office 365 ProPlus**. Microsoft re-affirmed its intent to release native support for sensitivity labels in the Office 365 ProPlus for Windows applications in the second half of 2019. This will remove the need for also deploying the Azure Information Protection client for labeling, unless the additional capabilities of the Azure IP client are required. Office Apps to Get Native Support for Office 365 Sensitivity Labels (Petri, April 4). See also Microsoft 365 Roadmap 44920 (March 8, 2019) which says 3Q 2019.
- **Kaizala Global Roll-out and Teams Integration**. Microsoft released Kaizala to all eligible Microsoft 365 and Office 365 commercial customers, and is offering in-region data residency for new customers. Over the next 12-18 months, Kaizala will also be integrated with Microsoft Teams for empowering and engaging with people outside the organization's directory. Microsoft Kaizala Rolls Out to Office 365 Customers Globally and Will Become Part of Microsoft Teams (Microsoft Kaizala Blog, March 4).
- **Automated Incident Response Playbooks at Public Preview**. As previously signaled on March 18 (see Update on Microsoft Threat Protection), Microsoft released its first two initial playbooks for Automated Incident Response in Office 365 Advanced Threat Protection into public preview. The two playbooks are User Reported Messages (for phishing) and Weaponized URL (for malicious links). The playbooks automatically react to a threat, gather evidence, and implement mitigations to resolve or neutralize the threat. Playbooks can also be manually triggered by an admin. The intent of the playbooks is to leverage the intelligence in Office 365 to automatically neutralize threats, rather than relying on security professionals undertaking time-consuming investigations. See Optimize SecOps Efficiency with new Automated Incident Response in Office 365 ATP (Security, Privacy and Compliance Blog, April 4).

Retention Labels Meltdown

Description

Details of Office 365 Incident FO176096

Microsoft Information Protection labels went missing in Office 365 for several weeks during March 2019, affecting at least the Retention Labels capability.

- Existing retention labels disappeared from documents in SharePoint Online and OneDrive for Business.
- Users were unable to add new labels to any documents, as this functionality was turned off by Microsoft during the incident.
- Labeling capabilities were switched on again starting March 25, 2019. Auto-label policies began to re-apply the appropriate label to documents.
- Retention labels that had been explicitly applied earlier to documents remained invisible for another week. These were reinstated as part of the restoration process on April 2, 2019.
- It is unclear how many tenants were affected by the disappearing labels, and it is unclear if the retention periods for affected documents remain correct after the reinstatement.

Analysis

- Breakdowns in functionality that are being relied on by customers to meet compliance mandates is a serious matter. Not being able to use compliance functionality to add new labels is annoying, but to have previous compliance decisions disappear is at the extreme end of the concern curve.

About

- **Date** - April 8, 2019
- The Case of SharePoint Online's Missing Retention Labels (Office 365 IT Pros, April 8)
- **Tag** - Data Loss Protection

Microsoft 365 Roadmap Updates - April 8, 2019

Recent updates to the Microsoft 365 Roadmap:

- **Office 365 Groups via Security Groups**. "This feature will provide the ability for Group Owners to add a Security Group as a member of an Office 365 Group. The Security Group can then be used to drive membership inside an Office 365 Group, simplifying membership management scenarios where membership is already be managed within Security Groups." Due Q1 2020. Microsoft 365 Roadmap 50002 (April 2, 2019).
- **Office 365 Groups Activity-Based Expiry Renewal**. "This feature will provide the ability to automatically renew Office 365 Groups which are about to expire when recent activity has been detected within services attached to the Office 365 Group." Due Q1 2020. Microsoft 365 Roadmap 50007 (April 2, 2019).
- **Expiry Notifications Within Office 365 Groups Applications**. "This feature will generate an Expiry Date that can be consumed by end user applications built on Office 365 Groups. Applications built on Office 365 Groups will then have the ability to display notifications within the context of their app to notify a user that a group will expire. Rather than rely strictly on email notifications, users will be notified in the context of their apps, upon which they can take action to renew the group." Due Q1 2020. Microsoft 365 Roadmap 50012 (April 4, 2019).
- **Microsoft Information Protection Labels - Classification Driven Policies with Office 365 Groups**. "We are developing consistent Office 365 Groups classification to make it easier to protect sensitive data. Tenant administrators can now better govern groups created in their respective tenants by enforcing policies on those groups using classification labels in a streamlined and proactive manner." Due Q1 2020. Microsoft 365 Roadmap 50293 (April 5, 2019).
- **Groups Administrator Role**. "This feature will provide a new role for Groups administration. Members of this role can create and manage Groups, create and manage groups settings such as naming and expiration policies, and view groups activity and audit reports." Due Q3 2019. Microsoft 365 Roadmap 50228 (April 4, 2019).

EDPS Investigation of Microsoft re Data Protection

Description

The European Data Protection Supervisor (EDPS) has begun an investigation into the contractual agreements between EU institutions and Microsoft for Microsoft software. The investigation is in light of the new European data protection regulation - Regulation 2018/1725 - that brings the data protection rules for EU institutions in line with the rules defined in the GDPR for other organizations and businesses operating in the EU. The new regulation:

- Makes EU institutions accountable for any data processing carried out on their behalf by third-party service providers.
- Imposes a duty on EU institutions to ensure any contractual arrangements with third-party service providers are in line with the requirements of Regulation 2018/1725, and that any risks are identified and mitigated.
- Assigns the role of data protection supervisory authority for EU institutions to the EDPS. This role requires that the EDPS monitors compliance by EU institutions with Regulation 2018/1725, raises public awareness of relevant risks, and works closely with national data protection authorities (per GDPR) and other relevant national bodies to mitigate these risks.

In light of the data protection impact assessment under GDPR carried out for the Dutch Ministry of Justice and Security, the EDPS is now investigating Microsoft for its compliance under Regulation 2018/1725 in relation to EU institutions.

Analysis

- Until Regulation 2018/1725 came into force, the requirements of GDPR did not apply to EU institutions.
- In light of the eight issues raised by the Dutch report and Microsoft's subsequent addressing of only two of those issues, it is certain the EDPS will identify risks and issues that need to be mitigated by EU institutions or resolved by Microsoft. The higher level of investigation by the EDPS should lead to additional changes by Microsoft that are beyond what Microsoft released in response to the Dutch DPIA.

About

- **Date** - April 8, 2019
- EDPS Investigates Contractual Agreements Concerning Software Used by EU Institutions (EDPS, April 8)
- **See Also** - Microsoft Response to Dutch DPIA (February 2019)
- **See Also** - Office 365 ProPlus with Privacy Controls (March 2019)
- **Tag** - Security

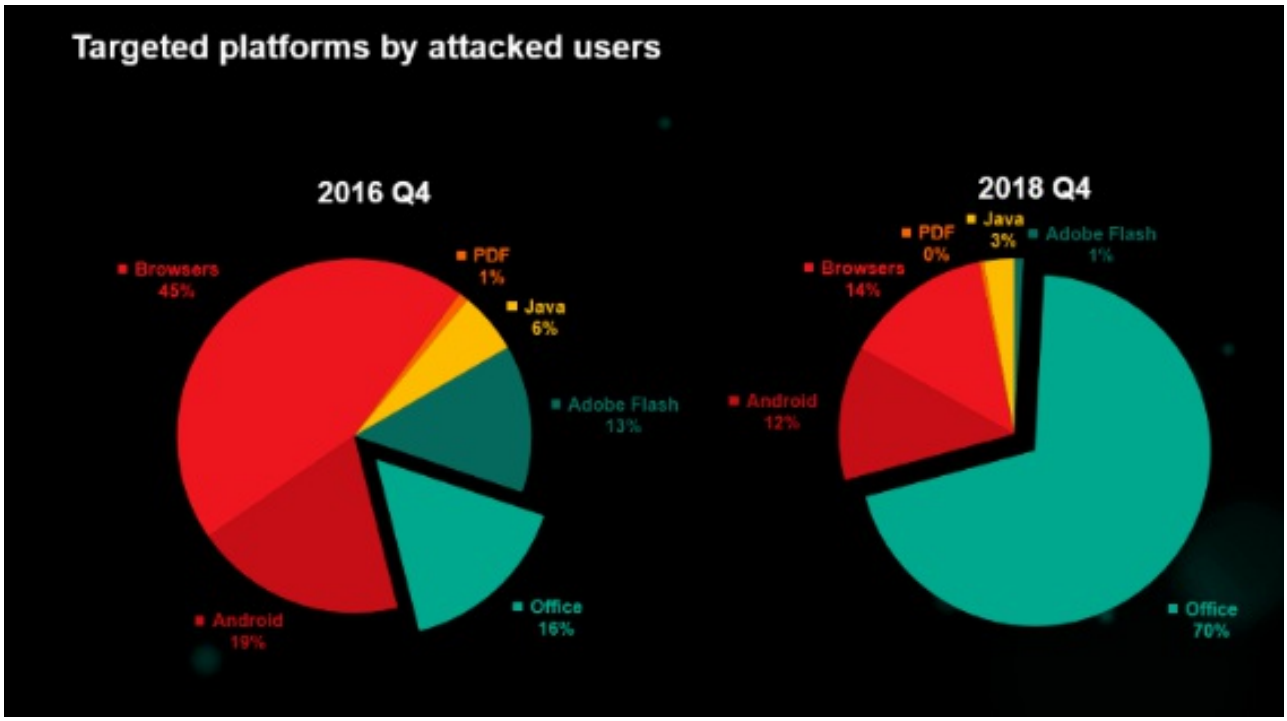
Weekly News Drop - April 12, 2019

Roundup of recent Office 365 news:

- **Teams Admin Center Updates**. Microsoft added a couple of new capabilities to the Microsoft Teams Admin Center, including the ability to delete and archive teams. An archived team can be reactivated. The Teams Administrator can also customize their view of the Teams Admin Center by adding or removing informational columns in views, including privacy and classification. Teams Admin Center Adds Delete and Archive Capabilities (Office 365 IT Pros, April 10).
- **Compound Detection in Azure Sentinel**. Microsoft described in broad terms some of the machine learning capabilities in Azure Sentinel, its recently announced cloud-native SIEM. Using what it is calling Fusion technology, the major intent is to reduce the number of discrete alerts by grouping them through analysis into higher-level cases, thereby reducing the number of alerts and alert fatigue on the behalf of security analysts. Building the Security Operations Center of Tomorrow - Better Insights with Compound Detection (Microsoft Security, April 10), Reducing Security Alert Fatigue Using Machine Learning in Azure Sentinel (Microsoft Azure Security Blog, March 19).
- **Modern SharePoint Admin Center by Default**. Microsoft has completed the rollout of the modern SharePoint Admin Center to all Office 365 tenants with 50 or fewer licenses. During April and May, it will roll out the modern experience as the default experience for the remaining tenants, with the process expected to be completed by the end of May 2019. An admin can switch back to the classic experience on-demand, and the tenant can also be set to keep using the classic experience for all administrators via the Settings page in the SharePoint Admin Center. SharePoint Admin Center Experience Updates (Microsoft 365 Roadmap 46375, April 9), We're Changing Your Default SharePoint Admin Center Experience (Office 365 Message Center MC177501, April 10).

Attacking Microsoft Office Vulnerabilities

Description



At its Security Analysts Summit last week, Kaspersky claimed that 70% of the attacks its security products identified during Q4 2018 were focused on Microsoft Office. That is, attacks attempt to exploit known vulnerabilities in Office and related components, such as the Equation Editor in Microsoft Word, the Windows VBScript engine, and the Internet Explorer scripting engine.

- 70% of attacks in Q4 2018 is four times as high as the number of attacks in Q4 2016, only two years ago.
- Microsoft Office is attractive because the vulnerabilities exist widely across the market, and deeply across many versions of Microsoft Office.

Kaspersky's conclusion echoes similar findings from another security analysis firm, Recorded Future, that last month noted that six of the top 10 exploited vulnerabilities in 2018 were flaws in Microsoft Office.

Analysis

- Given the high degree of focus on exploiting vulnerabilities in Microsoft Office, if you can't get rid of the target, then you have to invest to protect the target. This partly explains Microsoft's high focus on offering its own security services in Office 365 (e.g., Advanced Threat Protection) and Microsoft 365 (e.g., Microsoft Defender ATP, Cloud App Security, etc.).
- Office 365 ProPlus - the cloud delivered and frequently updated version of Microsoft Office - offers the potential for rapidly decreasing the presence of known vulnerabilities as long as [1] Microsoft doesn't re-introduce earlier vulnerabilities and [2] organizations stay close to the forefront of the updating cycle.
- For organizations with a fleet of Office installations that aren't updated by Office 365, keeping up-to-date with software patches is critical.

About

- **Date** - April 15, 2019
- Kaspersky: 70 Percent of Attacks Now Target Office Vulnerabilities (ZDNet Zero Day, April 15)
- Microsoft Targeted by 8 of 10 Top Vulnerabilities in 2018 (Recorded Future, March 19)
- **Tag** - Security

Weekly News Drop - April 19, 2019

Roundup of recent Office 365 news:

- **Microsoft Data Breach**. A customer support agent at Microsoft was subject to account compromise, which resulted in the hackers being potentially able to access some user accounts on Microsoft's web email services (msn.com and hotmail.com, but not Office 365 according to Microsoft). Affected users were notified by email last week; it was recommended that affected users change their password. Some users were told email contents and attachments were not breached, while others were told they were. See Microsoft: Hackers Compromised Support Agent's Credentials to Access Customer Email Accounts (TechCrunch, April 13).
- **Azure Information Protection Unified Labeling Client**. Microsoft released the new Azure Information Protection Unified Labeling Client to general availability. The new client downloads labels and policy settings from the Office 365 Security & Compliance Center (or the new Microsoft 365 Security Center and the new Microsoft 365 Compliance Center). The non-unified labeling client downloads labels and policy settings from the Azure Portal. The new Unified Labeling Client does not have feature parity with the earlier client, and customers requiring capabilities not yet in the new Unified Labeling Client should stick with the earlier client. Microsoft expects 90% feature parity by the end of 2019. See The Azure Information Protection Unified Labeling Client is Now Generally Available (Azure Information Protection Blog, April 16).
- **Migrate Google G Suite to Office 365**. Office 365 tenants will soon have the ability to migrate mail, calendar and contact data from Google G Suite to Office 365, using Microsoft Exchange Mailbox Replication Services to do the migration. Data from G Suite can be migrated all in one go (subject to throughput limitations imposed by Google), or in batches for a staged migration. Some data is not migrated, and since Exchange doesn't support mail labels in the same way that Google does for organizing mail items in Gmail, a translation between labels and folders is done as part of the migration process. See Introducing the New Migration Experience from Google G Suite (Microsoft Exchange Team Blog, April 16).
- **Enterprise Name Dropping**. Microsoft is removing the word "enterprise" from the license display names of the Office 365 Enterprise plans from April 30, 2019. What used to be called "Office 365 Enterprise E3" will now just be called "Office 365 E3." See Message Center Update MC177651 (April 12).
- **Changing Authentication Flow**. "Azure Active Directory (Azure AD) sign-in uses a process to determine where to send a user to authenticate after they enter their username on the sign-in screen. This process will be updated with an upgraded user look up behavior. The new behavior will pave the path towards a passwordless future by enabling alternative credentials like FIDO2. Additionally, this behavior will introduce new and improved error messaging on the sign-in pages if the username the user entered does not match an account in the respective domain. This feature will begin rolling out in May 2019 for managed domains (cloud-only) and for federated domains by end of 2019." See Azure AD Sign-In Process Behavior and Error Messaging Updates (Microsoft 365 Roadmap 33845, April 19).

Yammer in Europe and eDiscovery

Description

Microsoft announced two upcoming changes for Yammer: new data residency options, and support for eDiscovery on Yammer messages.

- **Data Residency**. Microsoft announced its commitment to offer new data residency options for Yammer, with the principle that message bodies and files attached to Yammer messages will be stored at rest in a specific geographical area. Up until this point, Yammer has been provided only out of the United States since Microsoft acquired the company in 2012. For new customers in Europe, creating a new Office 365 tenant provides the opportunity to home Yammer data in the EU; this is in preview currently.
- **eDiscovery**. Microsoft will offer eDiscovery capabilities for Yammer by the end of 2019. Details are sparse, but this should mean that Yammer as a data source can be scoped within current eDiscovery cases in the Office 365 Security & Compliance Center (or the new Microsoft 365 Compliance Center as that becomes more functionally ready).

Both capabilities are scheduled for release in Q4 2019, so probably December 2019 at this point.

Analysis

These are long overdue features for Yammer. Microsoft acquired the product in 2012, and that it has taken 7 years to add these security and compliance features is not good enough. Yammer was the poster child of social technology at Microsoft for several immediate years after the acquisition, but the extended timeframe taken by Microsoft to add necessary capabilities on the user and productivity side - let alone the security and compliance ones - eventually gave the impression that Yammer was on the downwards slide out of Microsoft. Microsoft has attempted over the past 18 months to reinforce the notion that Yammer is both strategic in Office 365 and staying that way.

There is no mention of Multi-Geo support for Yammer data residency, whereby message bodies and Yammer files can be stored in geo-appropriate locations. However, as a first step, gaining the ability to home Yammer data in Europe, for example, is a good move.

There is no mention of migration options at the current time, whereby a current customer could select a new geo-homing location for Yammer data. This is bound to come over time in line with Microsoft's general approach of offering data migration options when new geo-options are introduced - such as with Microsoft Teams - it just hasn't been officially signaled for Yammer yet.

Given the integrations of Yammer with other services in Office 365, not all data surfaced in Yammer will actually be stored in the selected geo for Yammer data residency. Microsoft was very clear to differentiate between files attached to a Yammer message (which will be stored in the geo per Yammer) and files actually stored in SharePoint Online that are surfaced in Yammer (which will be stored in the geo according to the SharePoint data residency policy).

About

- **Date** - April 19, 2019
- Yammer Data Residency in Europe (Microsoft 365 Roadmap 50554, April 19)
- eDiscovery for Yammer (Microsoft 365 Roadmap 50555, April 19)
- Data Residency in Yammer (Microsoft Docs, March 28)
- **Tag** - Security, eDiscovery
- **Implication** - eDiscovery Workflow
- **Implication** - Tenant Architecture and Data Residency

Archiving with Native Connectors

Description

Microsoft currently offers the ability for customers to archive third-party data into Office 365 using customer-arranged agreements with third-party data aggregators, such as Actiance. Microsoft has recently announced that it will add native connectors into the Microsoft 365 Compliance Center for archiving third-party data into Office 365, negating the need for third-party agreements. Once the data is inside Office 365, it will be available for analysis using compliance solutions such as Supervision and Advanced eDiscovery, among others.

Analysis

Offering native connectors will decrease the cost for customers requiring third-party data inside Office 365.

Third-party data archived into Office 365 is currently transformed from its native format into an Exchange email message format, which results in the loss of some content fidelity. Under the forthcoming approach with native connectors, no mention was made about moving away from storing all items as email messages.

About

- **Date** - April 19, 2019
- Native Connectors to 3rd Party Data for Archiving (Microsoft 365 Roadmap 48506, April 19)
- **Tag** - Archiving
- **Implication** - No Archiving for Some Content Types

Supervision 2019 Updates

Description

Microsoft announced several new upcoming capabilities for the latest version of Supervision, which we call Supervision 2019 to differentiate it from the earlier version (Supervision 2017). New capabilities are:

- The ability to include chat messages from Skype for Business Online in policies. Due May 2019.
- The ability to exclude specific email domains from policies, so that email messages sent from those domains are excluded from the supervision set. This is intended to be used to stop automated notices such as email newsletters from being captured for review. Due May 2019.
- By the end of Q4 2019, the review experience will be enhanced to support threaded email and chat conversations, thereby offering contextual analysis options.
- By the end of Q4 2019, the option to escalate messages within a review to another supervisor will be added.
- By the end of Q4 2019, the creation of supervision policies will be upgraded to include pre-configured templates for common policies. The policy creation flow will also be improved through a new wizard.

Analysis

- Microsoft's supervision capabilities languished without a lot of attention from 2015 to early 2019. The announcement of the new Supervision 2019 raised the game on what Microsoft has to offer, including support for Microsoft Teams messages. The above announcements continue this momentum, although there are still many workloads in Office 365 that are excluded from Supervision 2019, such as Yammer.

About

- **Date** - April 23, 2019
- M365 Supervision Now Includes Skype for Business Online Chat and Email Domain Exclusions (Microsoft 365 Roadmap 50585, April 19)
- New M365 Supervision Policy Creation Experience in Microsoft 365 Compliance Center (Microsoft 365 Roadmap 50684, April 19)
- New M365 Supervision Review Experience (Microsoft 365 Roadmap 50686, April 19)
- **Tag** - eDiscovery
- **Implication** - Supervision 2019

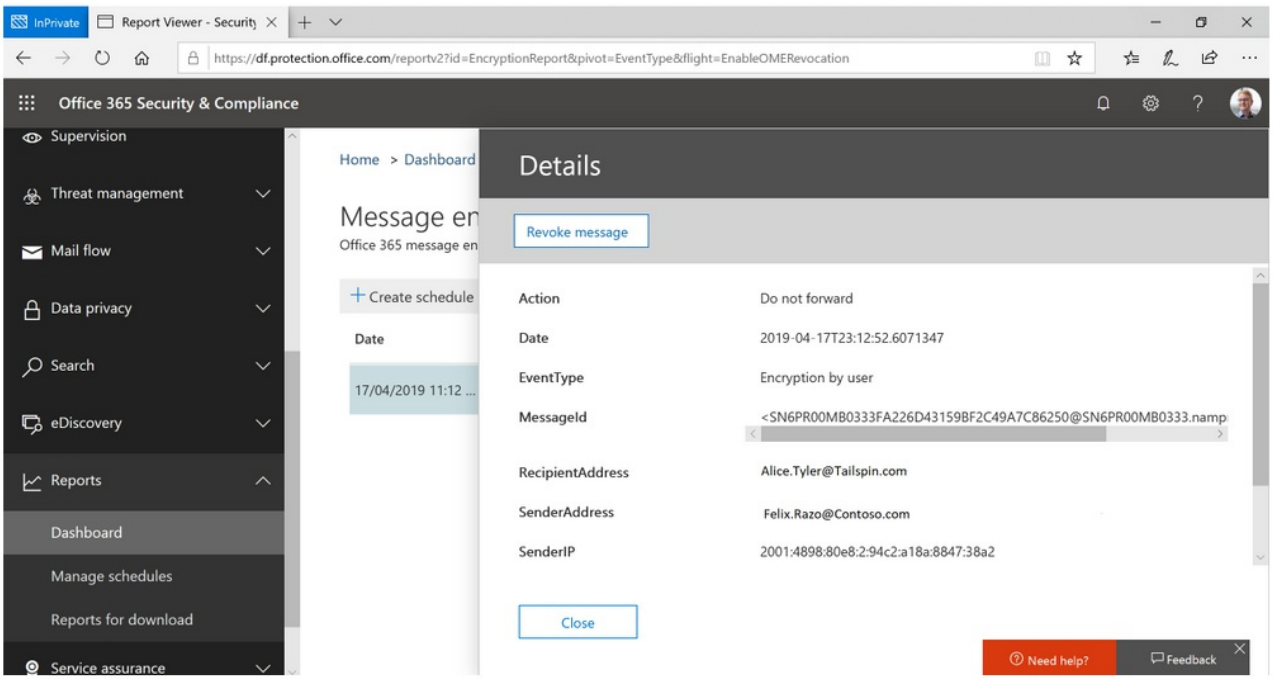
Weekly News Drop - April 26, 2019

Roundup of recent Office 365 news:

- **Compliance and Security Virtual Conference**. In conjunction with KPMG, Microsoft is hosting a virtual conference on its Compliance and Security capabilities on May 14, 2019. The focus is on organizations in Canada and the United States, and addresses topics such as personal privacy, risk assessment, data protection, and responding to regulatory requests. Registration required. Don't Miss the Compliance & Security Virtual Conference on May 14 (Security, Privacy and Compliance Blog, April 24).
- **Files Restore for SharePoint**. Microsoft released Files Restore for SharePoint and Microsoft Teams, with the initial roll-out focused on Targeted Release customers in April. Microsoft expects all customers will have Files Restore available by the end of May 2019. The functionality is targeted at mass deletion, corruption or infection of files, such as through a malware attack or malicious deletion by an employee. Files Restore for SharePoint and Microsoft Teams (SharePoint Community Blog, April 22).
- **Office Cloud Policy Service**. Microsoft released the new Office Cloud Policy Service to general availability. The service offers a new way of defining and assigning security policies to Office 365 ProPlus on Windows; it was announced in January 2019. The New Cloud-Based Policy Management Service for Office 365 ProPlus Has Been Released (Office 365 Blog, April 23).
- **Security Policy Advisor**. In parallel with the release to GA of the new Office Cloud Policy Service (above), Microsoft introduced the Security Policy Advisor service. Security Policy Advisor profiles your organization's use of Office 365 ProPlus, and recommends security policies that would improve overall security. The recommendations are backed by data on how many people would be affected by the change. Available in public preview (English only), with broader availability scheduled in early-to-mid May 2019. Introducing Security Policy Advisor - A New Service to Manage Your Office 365 Security Policies (Microsoft 365 Blog, April 23)

Office 365 Advanced Message Encryption

Description



Following the announcement of branded templates, message expiration and message revocation in September 2018, Microsoft released these features in an advanced add-on to Office 365 Message Encryption, called Office 365 Advanced Message Encryption. The new capabilities are only available in Office 365 E5 (or E3 plans with the Advanced Compliance add-on), and it is expected that they will be fully available by the end of May 2019.

New capabilities are:

- The ability to define one or more custom email templates for business-to-consumer encrypted emails, for the situation when the recipient receives a link-based version of the encrypted message (does not support Outlook in-line decryption). A custom template must be defined using PowerShell, and includes options for logo, color and explanatory text. Templates can also include an expiration date.
- Custom email templates are applied using a Mail Flow rule in the Exchange Admin Center. Microsoft said this would be based on matching to a condition, such as the use of a trigger word in a given language to signal the need to use a particular template, but there are many condition matching options in Mail Flow rules.
- As noted above, custom email templates can include an expiration date. If the custom email template is applied to an outbound email message that is accessed via the Office 365 web portal, the message will no longer be accessible once the expiration date has passed.
- An administrator can use the Office 365 Security & Compliance Center to report on encrypted messages that have been sent. The administrator has the option to revoke a given message.

Analysis

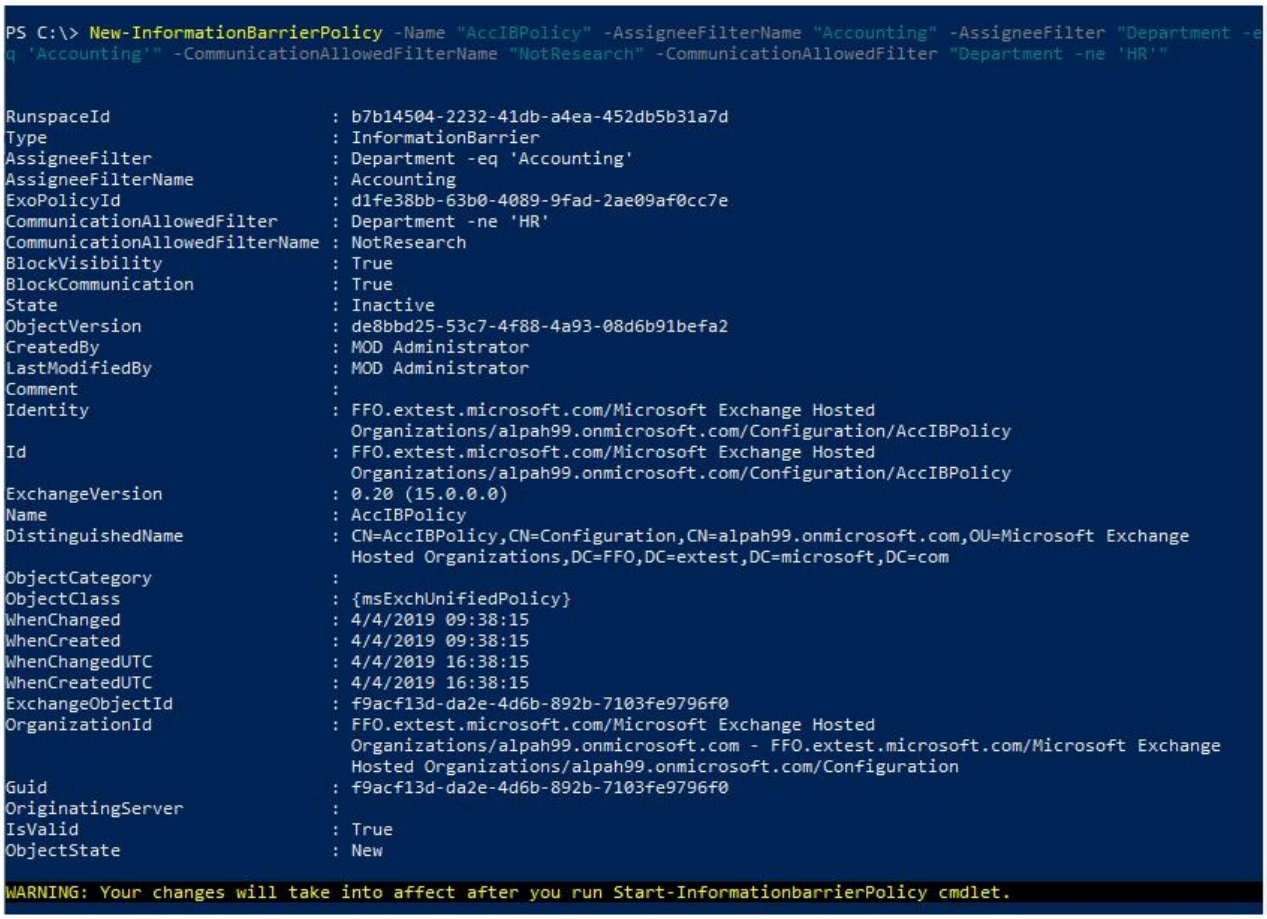
- When these capabilities were announced in September 2018, there was no indication that they would only be available in an advanced plan. It is unclear whether this is a measure to throttle initial demand, or just another attempt to get users to upgrade to higher-priced Office 365 plans.
- Message expiration dates and message revocation only applies to messages accessed through the Office 365 web portal. These new capabilities do not apply to encrypted messages accessed in-line through Outlook.
- Message revocation is an administrator-only capability. End users cannot revoke their encrypted messages from the Sent folder in Outlook.

About

- **Date** - April 30, 2019
- Announcing Office 365 Advanced Message Encryption (Security, Privacy and Compliance Blog, April 1).
- **Tag** - Encryption
- **Implication** - Office 365 Message Encryption - Version 2

Information Barriers in Microsoft Teams

Description



Microsoft announced Information Barriers for Microsoft Teams, for enforcing ethical walls between users in the same tenant. Ethical walls provide policy-enforced methods of preventing specific people from interacting through the tool. Information Barriers was released to preview on April 30.

Capabilities include:

- A new Information Barrier Policy is created using PowerShell cmdlets (above). The policy defines the rules on people who can't interact or share a chat thread, voice call or the same workspace in Microsoft Teams. In the above policy, it seems as through people who work in the Accounting department are being prevented from interacting with anyone who works in the HR department.
- Attempts to cross the Information Barrier - on purpose or accidentally - will be blocked in the user interface. For example, attempting to add a new member to a team who is prohibited by an Information Barrier from joining, will fail because the user will not show in the search results. Likewise, attempting to start a new private chat with a prohibited colleague will fail, and an error message will be displayed.
- Existing communications are checked when a new Information Barrier is created. If violations are identified, corrective action is taken to ensure nothing further is shared, for example, by changed one-to-one chats to read-only, or removing a user from a group chat.
- When released to general availability, Information Barriers will require E5 licensing (Office 365 or Microsoft 365), or an E3 plan with the Advanced Compliance add-on.

Analysis

- Ethical wall requirements are mandatory in certain industries, such as particular financial services areas. The absence of ethical wall capabilities in Microsoft Teams will have prevented some firms from embracing the toolset, and thus these new capabilities

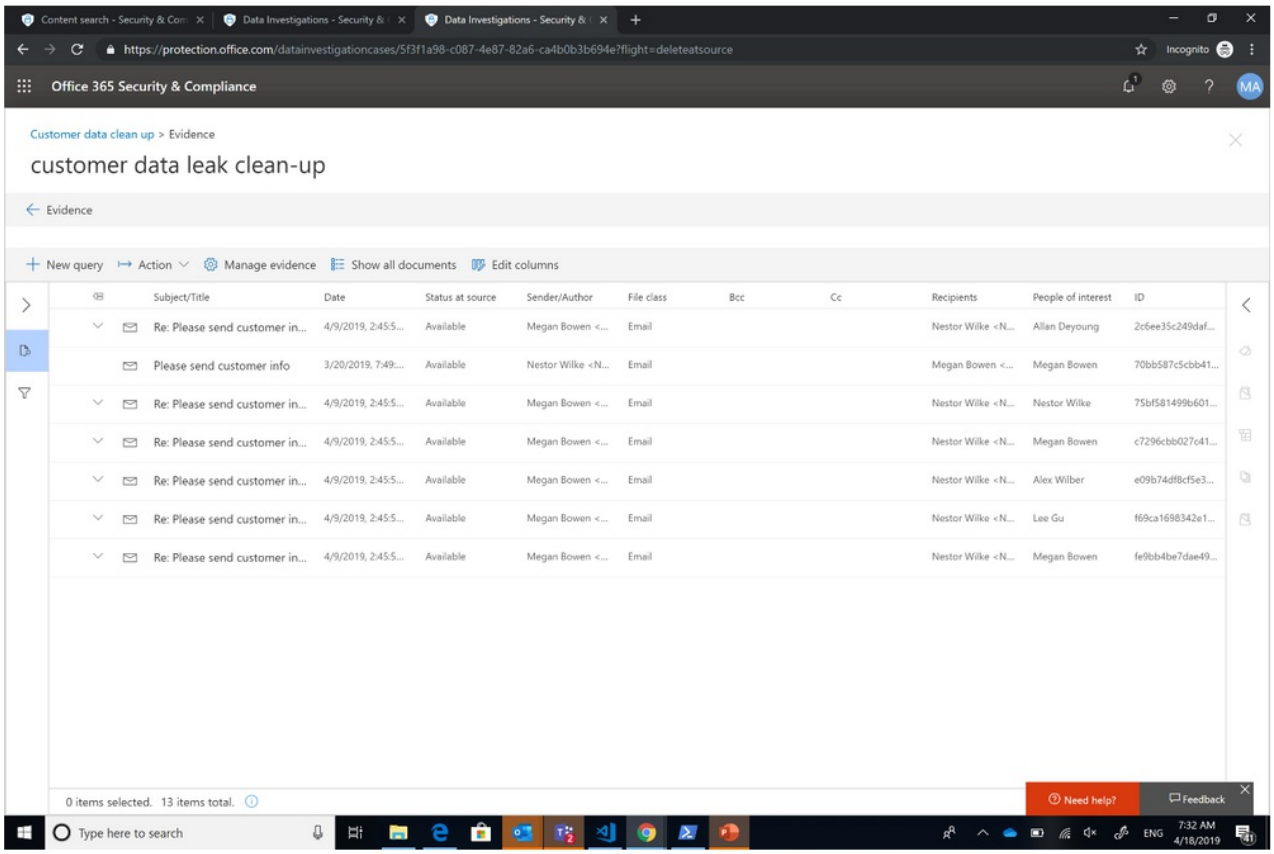
will remove this obstacle.
- Defining via PowerShell is okay for the initial release, but hopefully a GUI approach won't be too far off.
- Ethical walls go much further than just access control. Any Microsoft Team can be configured with limited access rights, therefore preventing people excluded from the access rights list from being able to participate in the content and conversation in the workspace. But access rights can be changed by an administrator at any time. Ethical walls enforce the separation until removed.
- There is no mention of error logging of attempts to cross the Information Barrier. The action is blocked for the user in the user interface, but it is unclear whether the failed attempt is also logged for administrator review.
- Exchange Online also includes ethical wall options, but policies defined for Exchange Online are separate from Information Barriers for Microsoft Teams. It remains to be seen whether Information Barriers is a Teams-only approach for ethical walls in Office 365, or if it becomes an Office 365-wide approach to ethical walls, with Teams merely being the first workload to receive the capability.

About

- **Date** - April 30, 2019
- Information Barriers Preview (Microsoft Teams Blog, April 30)
- Information Barriers in Microsoft Teams Preview (Microsoft Docs, April 30)
- **Tag** - eDiscovery
- **Implications** - Information Barriers in Teams

Data Investigations

Description



Leveraging core capabilities from Advanced eDiscovery, Microsoft announced the preview of Data Investigations. The new security service is designed to search for sensitive, malicious or misplaced data across Office 365, and once identified, facilitate the deletion of offending content.

Capabilities include:

- Defining search criteria for spilled data, using constructs such as keywords, conditions (message and document properties), and other advanced search capabilities.
- Data that matches the search criteria is pulled into a data investigation case for review within the Security & Compliance Center. Individual messages and documents can be analyzed / reviewed by a human reviewer, and tagged for deletion, for example, if it represents an actual data spillage.
- Messages or documents that have been spilled inappropriately can be deleted using PowerShell commands for hard deletion. Messages in Exchange Online will be deleted immediately, unless the mailbox is subject to a legal hold or single item recovery is enabled. Documents in OneDrive and SharePoint will be moved to the site collection recycle bin, and will be deleted after 93 days.

Data Investigations was released to public preview on April 30, 2019.

Analysis

- Data Investigations works with content in Exchange Online, OneDrive for Business, and SharePoint Online. It does not address other content or communication workloads in Office 365 such as Yammer and Microsoft Teams.
- Data Investigations can only contain or mitigate data within the Office 365 tenant in which the Data Investigation case is created. It cannot contain or mitigate messages or documents spilled beyond the tenant.
- With the emphasis on irrevokably deleting messages and documents that represent a data spillage, it is unclear whether Microsoft is aiding and abetting a customer to destroy evidence of a data breach.
- Deletion is the only mitigation offered. Microsoft does not offer the ability to limit access to the spilled data through encryption,

for example.

About

- **Date** - April 30, 2019
- Data Investigation Capabilities in Office 365 in Public Preview (Security, Privacy and Compliance Blog, April 30)
- Manage a Data Spillage Incident in Microsoft 365 (Microsoft Docs, April 2)
- **Tag** - Security

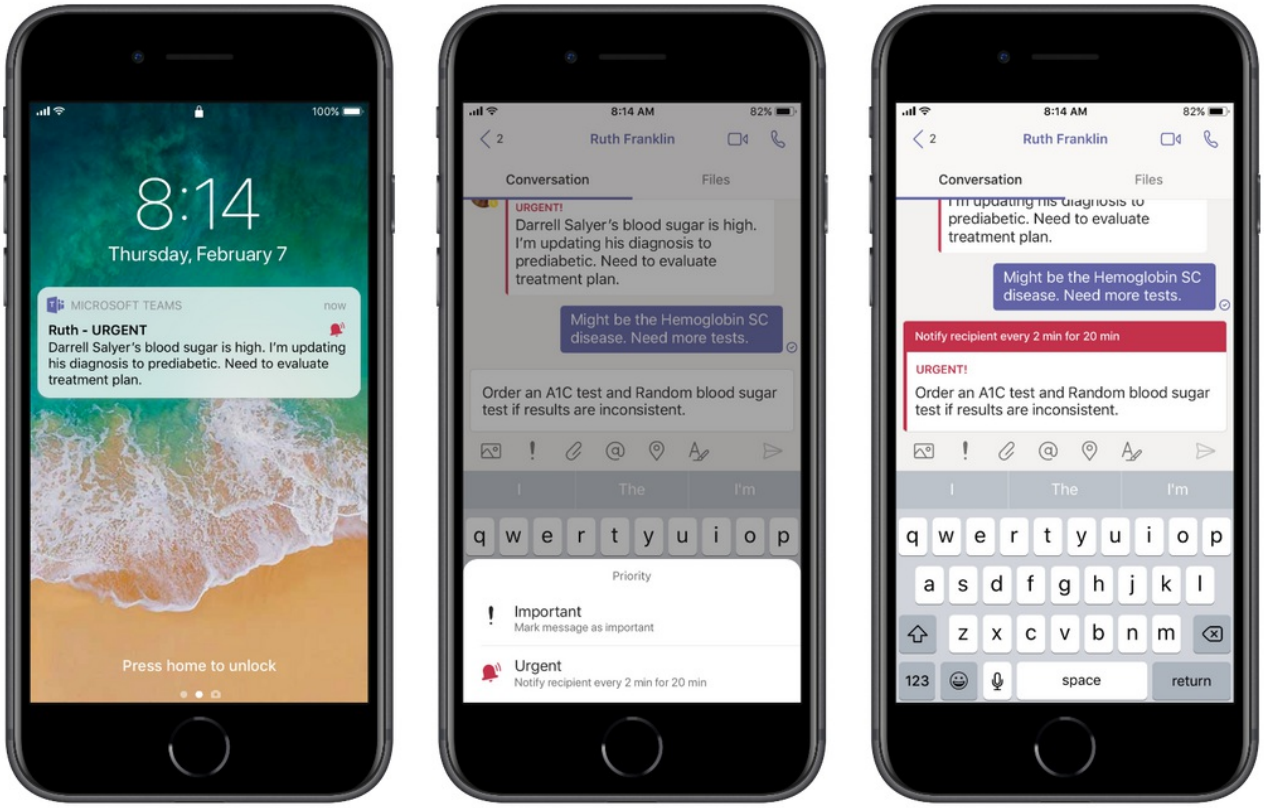
Weekly News Drop - March 1, 2019

Roundup of recent Office 365 news:

- **Office App Released**. Microsoft released to general availability the new Office app for Windows 10, which provides a single screen interface to Office apps, recent documents, and learning resources on Office apps. Office replaces MyOffice, which is installed with Windows 10. The experience is essentially the same as visiting Office.com as a user and signing in. Supports both online and offline modes, and if certain Office apps are not installed on a user's device, the Office app will open the associated version from Office Online. Customization options are available for organizational use, including branding, integration with third-party apps, and access to Microsoft Search. NEW! The Office app for Windows 10 Now Available to Everyone (Office Apps Blog, February 20).
- **AccountGuard in Europe**. Microsoft made its AccountGuard service available in 12 additional countries in Europe, bringing the total to 14 markets in advance of EU and member state elections in Europe during 2019. AccountGuard offers heightened protection for spearphishing and related attacks against email accounts in Office 365, Hotmail, and Outlook.com, with cyber threat notification, best practice security guidance, and additional services for organizations involved in democratic processes. AccountGuard is free of charge to eligible democratic organizations, but they must be using Office 365 to register for the service. New Steps to Protect Europe from Continued Cyber Threats (Microsoft EU Policy Blog, February 20).

Healthcare Enablement

Description



Clinicians get repeated notices about urgent messages in need of acknowledgment and response

During February 2019, Microsoft announced and released several capabilities for Microsoft Teams as part of its focus on the healthcare market. Enabling firstline workers - those who do not sit (or stand) behind a desktop computer all day - is a general top-level focus for Microsoft (because it has already won the lion's share of the desk, as in Microsoft's original vision of "a computer on every desk"), and healthcare workers are part of the firstline workforce.

Announcements included:

- In Microsoft Teams, the ability to mark a chat message as urgent. Doing so means the message alerts the recipient every 2 minutes for up to 20 minutes, or earlier if the recipient accepts the alert. Urgent messaging is in public preview.
- In Microsoft Teams, the ability to assign a delegate when unavailable. Microsoft calls this "message delegation," but all it practically means is that an out-of-office style message is shown in the Microsoft Teams chat interface when someone begins to write a chat message to the busy recipient. There is no auto-routing of chat messages to the delegate; messages must be manually re-directed. This means the original recipient does not have access to the chat messages sent to their delegate when they become available again.
- In Microsoft Teams, support for smart camera (so images are only ever stored in Teams, and not on device local storage), shift scheduling and coordination, and cross-tenant message federation. The first two capabilities are from Microsoft's earlier capability improvements for Teams; they are not specific to healthcare.
- In Microsoft Teams, the ability to integrate with electronic health records that align with a particular standard (FHIR - HL7 Fast Healthcare Interoperability Resources). Several early interoperability partners were announced.
- In Microsoft Teams, the availability of templates for healthcare teams. New templates are available for running a ward and running a hospital.

The capabilities were announced as part of Microsoft's focus on healthcare, but the innovations in Microsoft Teams will be available more generally to all Microsoft Teams tenants.

The above capabilities in Microsoft Teams are complemented by a wider healthcare focus, including:

- The Microsoft Healthcare Bot, for building and deploying virtual assistants in the healthcare space.

- FHIR interoperability investments in Azure.
- Precision healthcare investments, including partnerships with several other healthcare tech providers.

Analysis

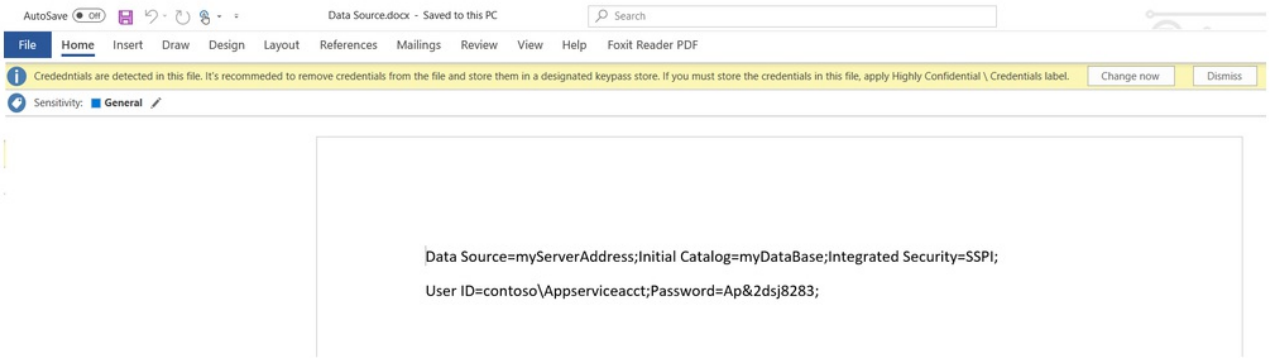
- Generally speaking, the capabilities announced for Microsoft Teams are good stepwise improvements to the service. Some capabilities - with "message delegation" being the prime culprit - are way oversold in terms of language. If message delegation is truly required, there is a lot of scope for improving what is actually offered.
- There are data protection and data privacy issues with some of the capabilities, e.g., urgent messaging. On devices that display an alert generally on the lock screen for anyone to read - rather than newer devices that require authorization before being displayed - private patient information could be unintentionally compromised.
- Other capabilities reflect a deep awareness of the data protection and data privacy issues in healthcare, e.g., the Smart Camera. Having the ability to bypass local photo storage on a device and only store a new photo image in Teams offers an important capability.

About

- Date - March 1, 2019
- Microsoft for Healthcare: Technology and Collaboration for Better Experiences, Insights and Care (Microsoft Official Blog, February 7)
- New Capabilities in Microsoft 365 Empower Healthcare Professionals (Microsoft 365 Blog, February 7)
- Empower Healthcare Organizations with New Capabilities in Microsoft Teams (Microsoft Teams Blog, February 11)
- Integrate Electronic Healthcare Records Into Microsoft Teams Care Coordination Through FHIR (Microsoft Teams Blog, February 12)
- Get Started with Microsoft Teams Healthcare Templates (Microsoft Docs, February 7)
- Implications for -
- Tagged as -

Credential Detection Using Azure Information Protection

Description



Microsoft introduced new capabilities in Azure Information Protection for the automatic detection of credentials inappropriately stored in systems, documents and applications. The detection capabilities extend Microsoft's sensitive information types, and the first batch of credentials - all focused on Azure except one SQL Server credential - are enabled for the Azure Information Protection Client and the Azure Information Protection Scanner.

- Detection via the client can be configured to automatically apply a label with heightened restrictions, or alternatively to recommend that the user does so.
- Detection via the scanner for on-premises file repositories can equally apply a label with heightened restrictions if required. Scanning results are published to the Azure Information Protection Analytics dashboard for analysis and remediation.

The above credential detection capabilities were released to public preview.

Microsoft indicated future plans for credential detection, such as:

- Availability in other Microsoft Information Protection services, such as Microsoft Cloud App Security and Office 365 DLP.
- Availability of additional credential types, beyond the initial short list focused mainly on Azure.

Not indicated but highly likely is the ability to use the new native integration of sensitivity labelling in Office 365 apps, rather than relying on the use of the Azure Information Protection client that works solely with Office for Windows.

Analysis

- Credentials are both sensitive and very powerful, the latter of which explains the rise in attempts for credential compromise through phishing and other means. Automated capabilities for identifying where credentials are stored without appropriate protection is an important new capability for Microsoft's Information Protection portfolio.
- The above announcements lack an Office 365 story in the short term (unless Azure Information Protection is also licensed), both in terms of credentials that can be detected and the ability to use the new native sensitivity labeling in Office apps. But Microsoft has to start somewhere and learn from the market, and the aforementioned future plans signal good things ahead for Office 365 customers.

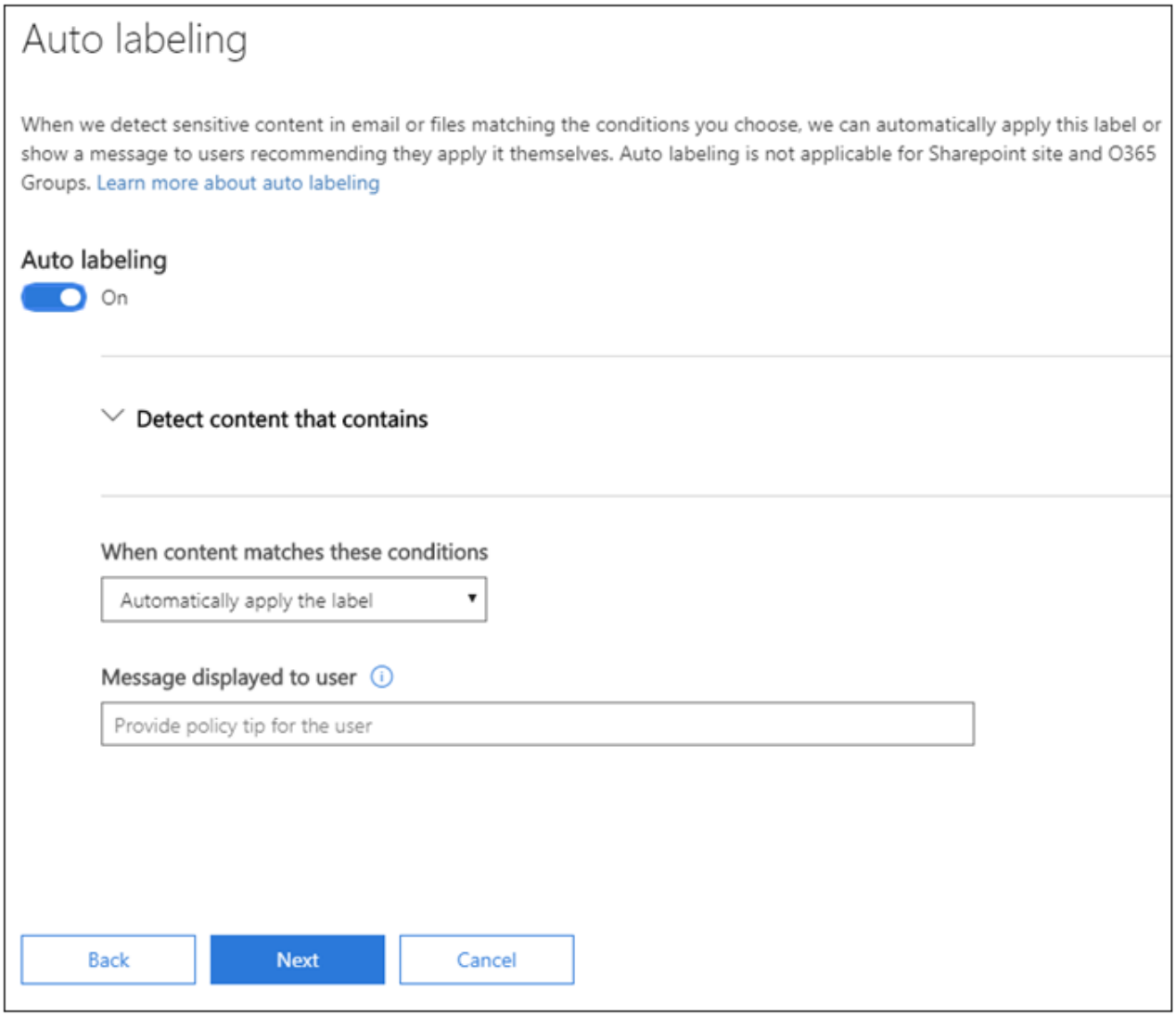
About

- Date - March 5, 2019
- Azure Information Protection Helps You to Be More Secure By Automatically Discovering Credentials (Azure Information Protection Blog, March 5)
- Tagged as - Data Loss Protection, Security
- Implications for - Azure Information Protection, Identification of Sensitive Data

Information Protection Updates, and Auto-Labeling of Sensitivity Labels

Description

Microsoft announced the addition of new Information Protection service plans to Office 365 E3 and E5, as well as to the Advanced Protection and Compliance SKUs. The Information Protection service plans are available at two subscription levels - Standard and Premium - with auto-labeling one of the Premium features. Based on these two levels, it would follow that Information Protection Standard will be added to Office 365 E3, and the Premium tier to E5 and the Advanced SKU. These changes will roll-out during March 2019.



The inclusion of the new Information Protection Premium subscription in Office 365 E5 and the Advanced SKU means that sensitivity labels can now be applied automatically to content in Office 365. The auto-application is defined in the sensitivity label based on the identification of sensitive information using Microsoft's sensitive information types. Auto-labeling currently only works with Office 365 for Windows, due to the requirement to have the Azure Information Protection unified labeling client installed (which is a Windows-only offering). Support for the newer native labeling options in Office apps on Mac, iOS and Android are not supported yet, although such support is coming.

Analysis

- Auto-labeling of content is the holy grail of data governance. Manual labeling has too many risks - such as incorrect labeling and forgotten labeling.
- Sensitivity Labels only work on the basis of Microsoft's sensitive information types. Other methods of matching content are not supported.

- Auto-labeling only supports email messages and files. Auto-labeling is not yet available for documents in SharePoint sites or messages in Office 365 Groups. Auto-labeling will detect text in an email message, but does not analyze the subject line or any email attachments for the presence of sensitive information.
- Auto-labeling offers two options: automatic or recommended. Recommended labeling currently only works with Word, Excel and PowerPoint. Outlook is not supported yet.
- If an email or document already has a sensitivity label, auto-labeling will respect the current label as long as the current label has a higher sensitivity rating than the auto-label alternative. In other words, auto-labeling will not downgrade current sensitivity labels, but it will upgrade from lower rated sensitivity labels.

About

- **Date** - February 20, 2019
- MC173614 Information Protection updates to the existing Office 365 E3, E5, Advanced Compliance and Information Protection (Office 365 Message Center Update)
- New Information Protection Service Plans for Office 365 (Office 365 IT Pros, February 25)
- Apply a Sensitivity Label to Content Automatically (Microsoft Docs, March 7)
- Azure Information Protection Unified Labeling Client: Version Release Information (Microsoft Docs, February 28)
- **Tag** - Data Loss Protection
- **Implications** - Office 365 Sensitivity Labels

Weekly News Drop - March 8, 2019

Roundup of recent Office 365 news:

- **Avoiding the Unintended Consequences of Delve**. Delve uses signals captured by the Microsoft Graph to suggest potential linkages between people and content. In situations where sensitive personal topics are being discussed - for example, between an employee and a company counsellor - Delve's ability to suggest content linkages could inadvertently result in the compromise of sensitive situations. One option is to use discardable Office 365 accounts for sensitive discussions of this nature, with the Delve settings for capturing and analyzing signals disabled. Using Discardable Office 365 Accounts to Preserve User Privacy (Petri, February 26).
- **From Windows 7 to Windows 10 and Microsoft 365**. Microsoft re-iterated the resources available to help organizations migrate from Windows 7 devices to Windows 10 and Microsoft 365, including the Modern Desktop Deployment Center, the Desktop App Assure program, and as a last resort, the Extended Security Updates offer for Windows 7 that will also support Office 365 ProPlus through to 2023. Now is the Time to Make the Shift to Microsoft 365 (Microsoft 365 Blog, March 1).
- **Exchange Online Mailbox Auditing by Default**. Microsoft completed its work to enable the default auditing of activity within Exchange Online Mailboxes to the audit log in the Exchange Admin Center. Audit logs for mailboxes are now captured by default, whereas previously an administrator had to enable auditing on a per mailbox basis. Audit log entries are not yet automatically logged to the Unified Audit Log in the Security & Compliance Center, but [1] that work is still in progress, and [2] administrators still have the option of enabling auditing to this location manually. Exchange Online Mailbox Auditing Enabled by Default (Security, Privacy and Compliance Blog, March 6).
- **Two New Data Centers in Africa**. Microsoft's two new data centers in South Africa are now operational, with Azure being offered at general availability to customers. Office 365 will be available from the two new data centers in the third quarter of 2019, and Dynamics 365 in the fourth quarter. The new data centers are located in Cape Town and Johannesburg. Microsoft Opens First Dataceners in Africa with General Availability of Microsoft Azure (Microsoft Azure Blog, March 6).

Azure Sentinel and Microsoft Threat Experts

Description

Microsoft announced two new security services: Azure Sentinel and Microsoft Threat Experts. The first provides enhanced visibility into security threats facing an organization, and the second offers proactive and responsive access to Microsoft's security personnel.

- **Azure Sentinel**. A cloud-based SIEM that captures security signals from multiple systems (including Office 365), offers a consolidated view of what's happening across the network, and uses AI to highlight the critical incidents. Early adopters of Azure Sentinel have noted a 90% reduction in alert fatigue among security professionals. Available in preview from February 28, 2019. Pricing has not been disclosed.
- **Microsoft Threat Experts**. A managed threat protection service for organizations using Windows Defender ATP, providing access to Microsoft's security professionals. Threat Experts will offer proactive support in identifying the most important risks, and responsive support when asked for help via Windows Defender ATP (using the "Ask a Threat Expert" menu option). Available in preview from February 28, 2019. Pricing has not been disclosed.

Analysis

- Given the breadth of services across Microsoft's portfolio that could be compromised and thus carry indicators of compromise and threat, even if Azure Sentinel only provides a consolidated view with prioritized and actionable advice it is an important step forward for Microsoft and customers. The ability to integrate with security systems from other vendors via open standards and the Microsoft Intelligent Security Association extends the value opportunity.
- While Windows Defender ATP offers important telemetry and capability for organizations when identifying and responding to threats, the complexity of current security threats and attacks combined with the lack of well-trained security professionals puts many organizations at risk. Access to a managed service for security within Windows Defender ATP gives organizations new options for building a security operations strategy that combines internal and external expertise, and also provides Microsoft with greater detail into threats and attacks against individual customers/organizations that can be integrated into its wider security stack to benefit all customers and organizations.
- Microsoft stated in mid-March that Microsoft Threat Experts is initially limited to Windows Defender ATP, but that it will "soon" be extended to cover additional components of the overall Microsoft Threat Protection offering set. See Update on Microsoft Threat Protection (March 18).

About

- **Date** - February 28, 2019
- Announcing New Cloud-Based Technology to Empower Cyber Defenders (Microsoft Official Blog, February 28)

- Announcing Microsoft Threat Experts (Microsoft Security Blog, February 28)
- Microsoft Threat Experts: Case Studies for Managed Threat Hunting Service (Windows Defender ATP Blog, February 28)
- **Tag** - Security
- **Implications** - Windows Defender ATP

OneDrive and Granular Restore

Description and Analysis

Microsoft offers OneDrive Files Restore, a capability for restoring an entire OneDrive account to a previous point in time during the previous 30 days for Office 365 subscribers. Restoring OneDrive to a specific point in time must be done via the OneDrive browser client; it cannot be done via the OneDrive sync client. Files Restore relies on version history and the recycle bin, so if the Recycle Bin has been emptied, files may not be available. Net-net is that restoring an entire OneDrive account is subject to several limitations and weaknesses, making it a "best-efforts" restoration not a guaranteed one.

Microsoft also offers selective or granular restoration of individual files, subject to certain provisions and restrictions. These include the use of version history and/or the use of the recycle bin. This means that:

- If versioning is turned on and the user needs an earlier version, then a user can granularly roll-back to a previous version without restoring their entire OneDrive.
- If a document has been deleted and the recycle bin has not been emptied, a user can granularly recover a deleted file from their recycle bin.

However, as with an entire restoration, this is a "best-efforts" / "hope it works" restoration, not a guaranteed one. For example:

- If a file is deleted from OneDrive in the browser UI, the deleted file will go into the Recycle Bin (first stage), and then into the second stage recycle bin (if enabled, will retain for 93 days). This duration may be long enough for recovering a misplaced file, but once deleted, it is unrecoverable.
- If the file is deleted via the OneDrive for Business sync app on PC or Mac, the deleted file is moved to the recycle bin of the local device, and does not show in the recycle bin accessible via the OneDrive browser UI. Once the recycle bin on the local device is emptied, the file is gone. It is not available via the first-stage or second-stage recycle bin.

In summary, OneDrive does offer some selective / granular restoration capabilities, but it is only a best-efforts "maybe" approach.

About

- **Date** - March 12, 2019
- Restore Your OneDrive (Microsoft Office Support)
- Restore Deleted Files or Folders in OneDrive (Microsoft Office Support)
- Restore a Previous Version of a File in OneDrive (Microsoft Office Support)
- **Tag** - File Sharing
- **Implications** - OneDrive Files Restore

Microsoft Cloud App Security Updates

Description

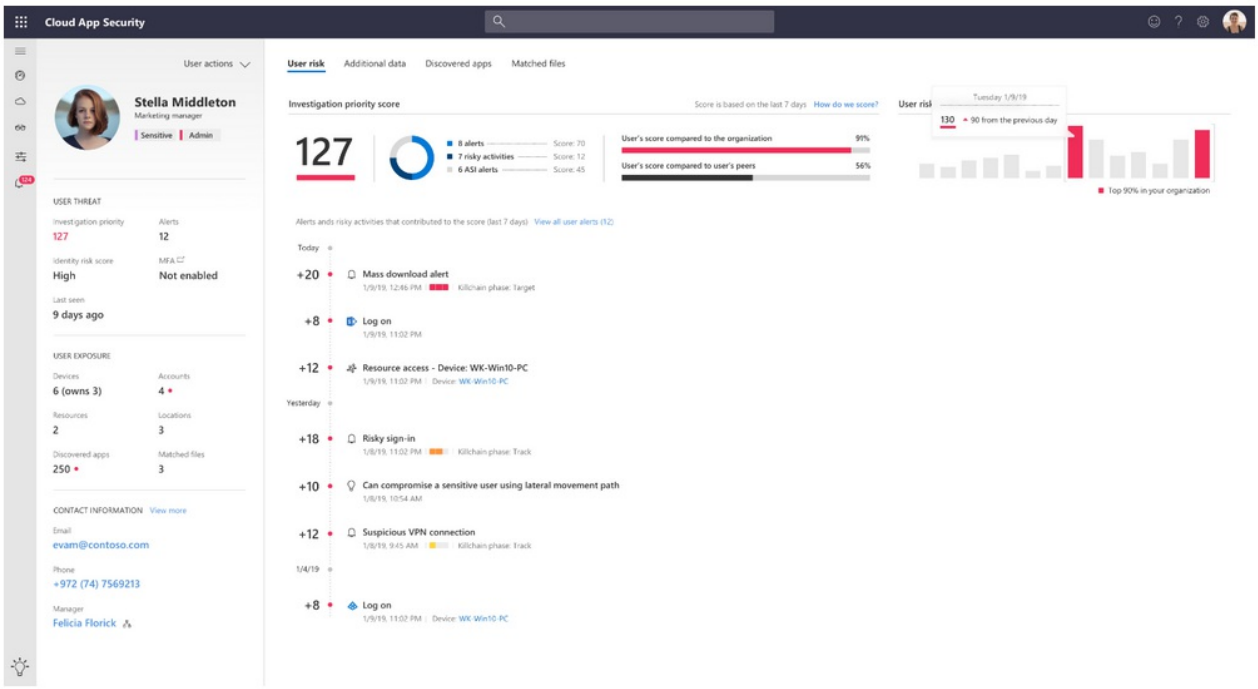


Image 1: The new User risk overview provides you with User Investigation Priority and timeline of suspicious alerts and activities

In advance of the RSA Conference 2019, Microsoft announced a plethora of updates to Microsoft Cloud App Security. The updates were grouped into four areas: threat protection, adaptive DLP, integrations, and protecting any cloud app. Updates included:

- **User Risk Overview with Investigation Priority**. Offers an overall assessment of the security risk of individuals, based on the types of alerts being triggered and the user's overall impact to the organization (see Image 1 above). The investigation priority score offers a way for administrators to focus on the individuals posing the greatest risk.
- **Sandbox Detonation of Malware in Cloud Storage Apps**. For cloud storage apps connected to Microsoft Cloud App Security via API, files that are potentially malicious will be automatically checked via detonation in a sandbox. Newly uploaded files are examined automatically, and existing files are checked as well.
- **Adaptive DLP Controls**. New control options to prevent unauthorized access to confidential and sensitive information through the DLP engine in Microsoft Cloud App Security. Options include read-only downloads in zero-trust situations, blocking file uploads under certain conditions, and preventing sensitive information being sent through chat and messaging apps, among others.
- **Integration with Azure Sentinel**. For integrating Microsoft Cloud App Security data with other data sources in Azure Sentinel, Microsoft's new cloud-based SIEM. Sentinel also allows longer retention times for data, and various data visualization options. For background on Sentinel, see Azure Sentinel and Microsoft Threat Experts.
- **Integration with Power BI**. For data visualization of Microsoft Cloud App Security data. Additional data attributes can be included for analysis as well, leveraging data from Azure Sentinel.
- **Integration with Windows Defender ATP**. The integration announced in September 2018 in preview between Microsoft Cloud App Security and Windows Defender ATP for identifying shadow IT services used directly on Windows devices was released to general availability. The integration means that cloud apps used from Windows 10 devices that don't go through the corporate firewall or other network devices - such as when the device is at an offsite cafe - can still be discovered in Microsoft Cloud App Security. See Microsoft Cloud App Security and Windows Defender ATP for Discovery.
- **Expanding Cloud App Support**. Direct support for Cisco WebEx and Dynamics 365, and conditional access support for Azure Portal and LinkedIn Learning. Microsoft also introduced a private preview program for organizations wanting to onboard other web apps to Conditional Access App Control.

Analysis

- The introduction of the new User Risk Overview is long overdue in Microsoft Cloud App Security. Until the release of this capability, user risk was only interpreted within the strict confines of defined policies. The overview steps up what Microsoft Cloud App Security can deliver, and addresses a shortcoming in relation to other third-party CASBs on the market.
- DLP policies that take a wider set of contextual conditions into consideration are a good forward step for Microsoft Cloud App Security. Being able to vary how a DLP policy is enforced based on context is an important capability (although it will require security professionals who can wisely model differential context factors).
- The option to integrate Microsoft Cloud App Security with Azure Sentinel will enable organizations to overcome the design limitation of Microsoft Cloud App Security being tied to a single tenant. Azure Sentinel should be able to take a data feed from multiple Microsoft Cloud App Security instances, thereby providing a super-view across multiple tenants in a merger and acquisition scenario, or anytime an organization uses multiple individiual Office 365 / Microsoft 365 tenants rather than Multi-Geo.

About

- **Date** - March 6, 2019
- Microsoft Cloud App Security @RSAC 2019 (Enterprise Mobility + Security Blog, March 6)
- Introducing Investigation Priority Built on User and Entity Behavior Analytics (Enterprise Mobility + Security Blog, March 6)
- **Tag** - Security
- **Implications** - Microsoft Cloud App Security, Windows Defender ATP

Microsoft 365 Roadmap Updates - March 14, 2019

Recent updates to the Microsoft 365 Roadmap:

- **Manage Face Detection in Microsoft Stream**. "A new administration control to turn off the face detection feature on a tenant level will be available in the Stream admin portal." Due March 2019. Microsoft 365 Roadmap 48379 (February 26).
- **Data Investigations Solution**. "The new data investigations solution provides IT admins with the ability to search for specific content in their organization and take action to remediate that content. This is helpful in the case that an organization needs to isolate and remove malicious or sensitive content." Due March 2019. Microsoft 365 Roadmap 48504 (February 26).
- **Intelligent Classification for Advanced Data Governance**. "Advanced Compliance customers will now be able to utilize out of the box machine learned classifiers or train their own custom machine learned models to help classify, protect and govern sensitive or business relevant content." Due April 2019. Microsoft 365 Roadmap 48505 (February 26).
- **Updates to File Hover Card - OneDrive and SharePoint**. "Across OneDrive for Business and SharePoint Online, the updated file card can now help you keep track of activity around all files (not just Office). Guest and Anonymous file viewers will also be included in the list. Lifecycle signals such as checked-out file, malware, DLP and missing metadata will also be reflected." Due March 2019. Microsoft 365 Roadmap 49092 (March 4).
- **Full-Fidelity Shared Libraries in OneDrive**. "Not only can you sync shared libraries from SharePoint and Microsoft Teams to your PC or Mac using OneDrive, you can now view shared libraries in OneDrive on the web with support for viewing file metadata. Initial capabilities include viewing, sorting and grouping by custom metadata and changing your file view to any previously saved file view." Due April 2019. Microsoft 365 Roadmap 49093 (March 4).
- **Customized Help Link for External Sharing in OneDrive for Business**. "When a user is blocked from sharing externally by policy, IT administrators can how provide a "learn more" link that will be surfaced in the error message. This link can be used to explain company policies on external sharing or even to direct users to internal portals to request policy changes." Due March 2019. Microsoft 365 Roadmap 49288 (March 7).
- **Staged User Rollout to Azure AD Cloud Authentication**. "Migrate ussers from federated authentication to Azure AD cloud authentication in groups or phases and manage from the Azure AD portal. Cloud authentication (Pass-through authentication or Password Hash Sync) enables benefits such as no real-time dependency on existing on-premises infrastructure, leaked credential protection, and seamless single-sign on." Due April 2019. Microsoft 365 Roadmap 32838 (March 8).
- **Mail Flow Insights - Phase 2**. "In this update we are adding multiple new reports and tools to the mail flow dashboard in the Office 365 Security & Compliance Center to help discover trends and insights and allow you to take actions to fix issues related to mail flow in your Office 365 organization. We are adding reports to understand domain health status in your organization (such as identify expired or incorrectly configured domain that prevents it from accepting emails); what messages sent by your users are being rejected at their destination; spot messages coming from your own on-premises server might be from compromised machines and user accounts; or identity mails being sent from your on-premises servers and attributed to your organization but not coming from configured accepted domains. We’re also adding a mail flow map, a graphical report showing the characteristics of your organization’s mail flow coming into and leaving Office 365. This report helps an admin understand mail routing pattern for their organization and can help identify anomalies and fix issues. Lastly, we’re providing an SMTP Client Auth report displaying your organization's usage of SMTP Authenticated Submission (SMTP Auth) protocol for the past 7 days. This is a legacy protocol therefore user accounts are more susceptible to being compromised and used to send spam emails." Due April 2019. Microsoft 365 Roadmap 49361 (March 8).

Office 365 for the US Government

Description

Microsoft announced several capabilities in Office 365 (and other Microsoft cloud services) are now available for the US Government via the Government Community Cloud High (GCC High) and Department of Defense (DoD) cloud platforms offered by Microsoft. These two cloud platforms offer higher grade security than the standard Government Community Cloud (GCC) offering from Microsoft.

New capabilities are:

- **Microsoft Teams**. Now generally available on GCC High and the DoD clouds. Teams was previously released to GCC.
- **Microsoft Power Platform**. Power Platform is made up of Power BI (data analysis), PowerApps (app development) and Flow (workflow automation). The platform is now generally available on GCC.
- **Dynamics 365 Customer Engagement**. In April, several Dynamics 365 applications will be released for government usage.
- **Outlook Mobile**. Now generally available on GCC High and DoD clouds. Microsoft had to change the architecture of Outlook Mobile in order for it to meet the security and compliance requirements of the US government (although these changes have been previously made available more generally).
- **Automated Investigation and Remediation in Advanced Threat Protection**. Microsoft is adding automated investigation and remediation capabilities in Office 365 Advanced Threat Protection. It will offer a graphical representation of a security threat and automation options for resolving the threat. Will be available for government customers "shortly" (on GCC; specific date not disclosed).

The above capabilities are contextualized within the broader Microsoft strategy of helping government agencies to fully embrace the potential of cloud services in order to have a greater impact on mission success.

Analysis

- Availability of cloud capabilities for government customers is generally on a slower cadence than general commercial customers, due to higher security and compliance requirements. None of these announcements are earth shattering, but are important to government agencies and workers who have until now been denied access to newer innovations from Microsoft.

About

- **Date** - March 13, 2019.
- New Microsoft 365 and Business Applications Technologies Enable Government to Modernize for the Mission (Official Microsoft Blog, March 13)
- New Teamwork and Security Capabilities for Microsoft 365 Government (Microsoft 365 Blog, March 13)
- Announcing Power Platform and Dynamics 365 Updates for Microsoft Government Cloud (Microsoft Industry Blogs, March 13)

Weekly News Drop - March 15, 2019

Roundup of recent Office 365 news:

- **Naming Policy for Office 365 Groups**. Microsoft released the Naming Policy feature for new Office 365 Groups, enabling both automatic prefix- and suffix-based additions to a group name, and the prevention of particular words from being used in group names. The naming policy must be set using PowerShell (there is no UI-option), and requires Azure AD Premium licensing. Only new groups are affected; current groups are not automatically updated to enforce the naming policy. New Feature: Office 365 Groups Naming Policy is Generally Available (Office 365 Groups, March 8).
- **MileIQ with Azure Active Directory**. MileIQ, an automatic mileage tracking service that works on iOS and Android devices and that is included in Office 365 Business Premium and Microsoft 365 Business plans, now allows authentication using Azure Active Directory credentials. The service tracks business drives in the background, and makes it easy for users to submit business drives for reimbursement or tax purposes. Available in the United States, Canada and the United Kingdom. MileIQ Now Supports Azure Active Directory (Office 365 Blog, March 5).
- **User Count of Teams vs. Slack and Workplace by Facebook**. Microsoft claims over 420,000 organizations are using Microsoft Teams, although does not break out those using Teams for free compared to those using Teams as part of a paid Office 365 subscription. Recent user numbers from other players in the market put Slack at 85,000 paying organizations and 10 million overall (paid and unpaid) monthly active users, and Workplace by Facebook at over 2 million paid users with at least 1.5 million of these coming from the 150 organizations who have more than 10,000 users each. Teams User Count Outpaces Slack and Workplace (Office 365 IT Pros, March 4).
- **Flagged Emails in Microsoft To-Do**. Microsoft introduced an integration between Microsoft Outlook and Microsoft To-Do, its task planning app. Messages flagged in Outlook automatically display in the Flagged Email list in To-Do. As is true for any to-do item in To-Do, users can add steps (sub-tasks) to a Flagged Message. Flagged Emails Come to Microsoft To-Do (Microsoft To-Do Blog, March 13).
- **Update to Exchange 2019 or Not?** Tony Redmond reviews the pros and cons of upgrading to Exchange 2019, and concludes that support timeframes are the most compelling reason. He also asks when an on-premises Exchange Server will become unnecessary for Microsoft to deliver. Stick or Stay: Should I Upgrade to Exchange 2019? (Petri, March 14).

Update on Microsoft Threat Protection (March 2019)

Description

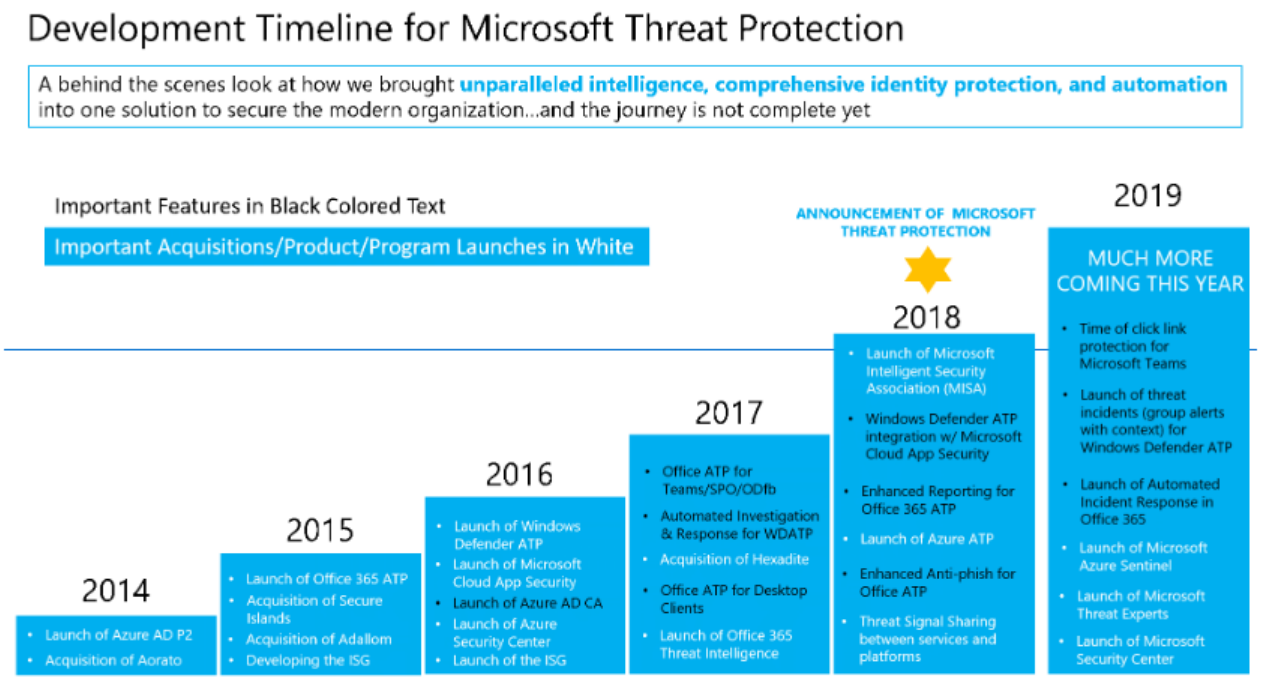


Figure 1. The development timeline of Microsoft Threat Protection.

Microsoft offered a strategic overview of its Microsoft Threat Protection offering set, and a historical look at the development timeframe from 2014. Microsoft Threat Protection offers both protections for end users and various tools and capabilities to reduce complexity for security professionals.

- Microsoft's overall intent with Microsoft Threat Protection is to "provide organizations with seamless, integrated and comprehensive security across multiple attack vectors." Microsoft's Intelligent Security Graph plays a major role in correlating security and threat signals across Microsoft's offerings.
- Microsoft leveraged the RSA Conference last week to announce the next steps in the Microsoft Threat Protection journey, including Azure Sentinel and Microsoft Threat Experts.
- Microsoft noted that its new Threat Experts service is currently limited to Windows Defender ATP, but soon it will be extended to cover more components of the overall Microsoft Threat Protection offering set. The initial linkage of Threat Experts with Windows Defender ATP is a learning constraint for Microsoft, not the final statement of service coverage.
- Microsoft is almost ready to release its initial Automated Incident Response playbooks to Office 365 Advanced Threat Protection. The two playbooks almost ready for release are User Reported Phish and Weaponized URL, and the intent of each playbook is to automatically collect additional insight, correlate threat signals, and neutralize the threat.

Analysis

- Microsoft offers multiple point solutions / services to address security threats in Office 365 and other Microsoft capabilities. Painting the higher level picture is helpful, and the integration of threat signals through the Intelligent Security Graph potentially hands Microsoft a massive advantage in environments that adhere to the Microsoft stack. Correlation of signals helps with identifying complex threats, and correlation also helps in automated response situations.
- A commonly cited fact in security circles is about the general lack of security professionals who can help organizations shore up their defenses and mitigate security threats of all kinds. Capabilities like the ones offered by Microsoft provide a level of automated analysis and execution to help address this gap, but also to optimize the time and focus of currently overworked and overloaded professionals in SecOps teams.

About

- **Date** - March 18, 2019
- The Evolution of Microsoft Threat Protection: RSA Edition Part 1 (Microsoft Security, March 14)
- The Evolution of Microsoft Threat Protection: RSA Edition Part 2 (Microsoft Security, March 14)
- **Tag** - Security
- **Implications** - Advanced Threat Protection

Data Residency in France for Microsoft Teams

Description

Microsoft turned on data residency for some Microsoft Teams data for France Office 365 tenants, effective March 18, 2019. Data residency for Teams data applies to [1] conversation and chat data stored at rest, and [2] only to new customers - those new to Office 365, or for current customers who have never activated Microsoft Teams in their Office 365 tenant. Microsoft plans to offer migration options for current customers who have Teams data stored in other EMEA data center locations.

There are various exceptions to data residency for Microsoft Teams, as is standard with how Microsoft approaches data residency for the overall Office 365 service.

Analysis

- Data residency in France is the continuation of Microsoft's moves towards more in-country data storage. See previous coverage of data residency for Microsoft Teams for Canada and Australia and Japan.

About

- **Date** - March 18, 2019
- Microsoft Teams Launches France Data Residency (Microsoft Teams Blog, March 18)
- **Tag** - Security
- **Implications** - Tenant Architecture

Weekly News Drop - March 22, 2019

Roundup of recent Office 365 news:

- **Disable Basic Authentication**. Microsoft's research says that disabling basic authentication for Exchange Online reduces account compromise rates by 67%. Condititonal Access policies in Azure AD Premium can be used to force modern authentication. Alex Weinert on Basic Authentication (Twitter, March 17).
- **Microsoft Cloud App Security and Box**. After recent disclosures about inadvertent data breaches through oversharing of links to files and folders in Box accounts, Microsoft explained the capabilities in Microsoft Cloud App Security to both provide visibility to sharing threats and to proactively enforce governance actions to mitigate sharing threats. Automated governance actions (via File Policies) can label sensitive files (using an Azure Information Protection classification label), change sharing permissions, or quarantine the file. Protect Your Data in Box Environments with Microsoft Cloud App Security (Enterprise Mobility + Security, March 20).
- **Disaster Recovery with Office 365**. Tony Redmond reviews the impact of a disaster happening with Office 365, and concludes there is "not a lot" companies can do to avoid significant impact if such an event were to happen. Recent incidents such as the lightning strike to the San Antonio datacenter (September 2018) were irritating, but only resulted in Office 365 being affected for less than 24 hours. For something longer - a multi-day outage for example - organizations don't have many practical options given the design of Office 365, the availability of services in Office 365 with no on-premises equivalent, and the near impossibility of migrating to an equivalent service under disaster situations. If an Office 365 Disaster Happened, What Would You Do? (Petri, March 19).

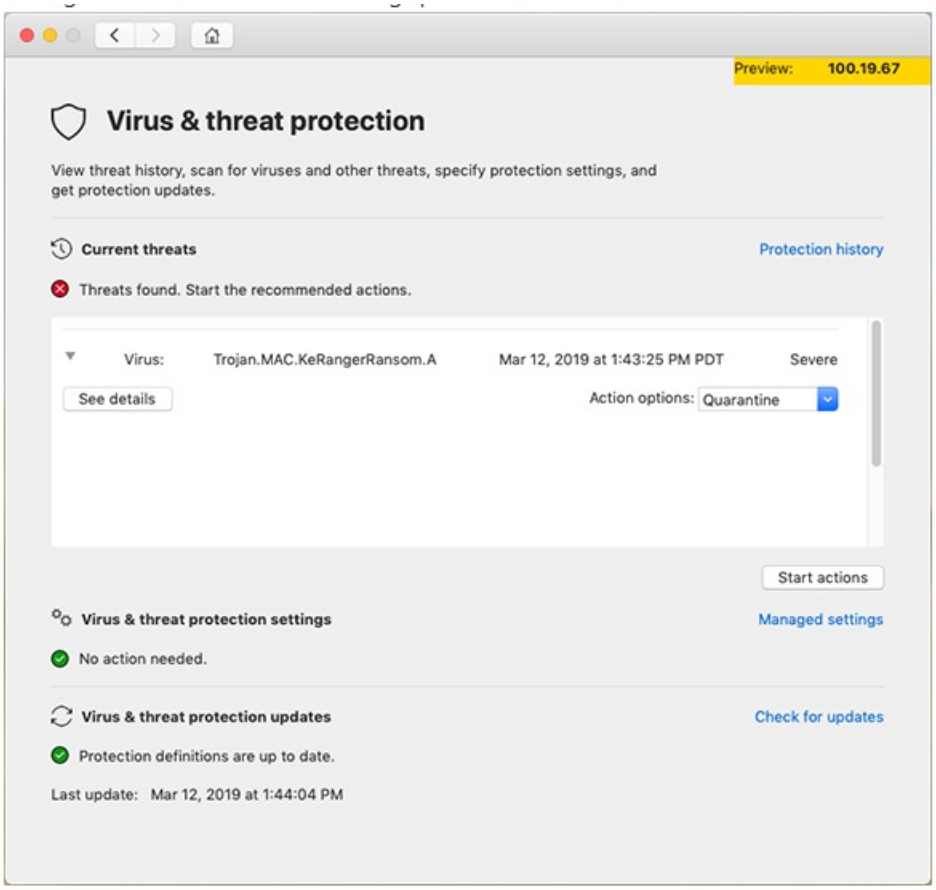
Microsoft 365 Roadmap Updates - March 25, 2019

Recent updates to the Microsoft 365 Roadmap:

- **SharePoint Files Restore**. "Files restore for SharePoint and Microsoft Teams is a complete self-service recovery solution that allows administrators and end users to restore files from any point in time during the last 30 days. If a user suspects their files have been compromised, they can investigate file changes and allow content owners to go back in time to any second in the last 30 days. Now your users and your administrators can rewind changes using activity data to find the exact moment to revert to." Due March 2019. Microsoft 365 Roadmap 33714 (March 21). See also SharePoint Files Restore.
- **Intra-Org Spoof and DMARC Failures**. "Intra-Org Spoof and DMARC Failures – We are simplifying the way that our customer manage anti-spoofing by consolidating all spoof actions and management under one policy: the Anti-Phishing policy. This means that we will no longer take the Spam action, as dictated in the Anti-Spam policy, for intra-org spoof and DMARC failures. Cross-org spoof will continue to be managed by the Anti-Phishing policy without changes. Additionally, we have further simplified anti-spoofing protection management by stamping all mails, including intra-org spoof, with a Composite Authentication result in the headers. This makes it much easier to quickly decipher our verdict on the authentication of the mail and whether we deemed the mail spoof, and why. This may result in some messages that were previously marked as spam will start getting marked as phish (CAT:SPOOF). In still other cases, customers that were moving all spam to the junk folder and phish to the quarantine would now see them going to quarantine. We'll be gradually rolling these features out over the course of the next few weeks, and we expect the rollout to be complete by end of February." Due March 2019. Microsoft 365 Roadmap 46841 (February 19).
    - **Update (July 2019)** - these changes were rescheduled to begin in late July, for completion in August 2019. See Anti-Phishing Policy Update.
- **Recommended View on Web**. "Leveraging Office's new intelligent services, we're pleased to introduce the new "Recommended View". This view will help you get you to your files faster by recommending files to you based on how you work and how you collaborate with others. It also brings attention to important files relevant to you, that you may not want to miss." Due April 2019. Microsoft 365 Roadmap 49094 (March 12).
- **Per Machine Install of Sync Client**. "Today, the OneDrive sync client installs per-user, meaning OneDrive.exe is installed for every user account on the machine under %localappdata%. With the new per-machine install, admins will be able to install OneDrive under the Program Files (x86) directory. Other than where the sync client is installed, everything else stays the same. The per-machine client will be helpful especially for multi-user machines (kiosks, schools, VDI etc.) and in cases where admins do not want exe files running from the user profile. Over time, we plan to migrate more and more of our install base to per-machine." Due 3Q2019. Microsoft 365 Roadmap 49424 (March 12).
- **Time to Read and Inside Look to Files**. "You can get deeper information like Key Points from documents and the average time to read. This information can help you make quick decisions about which content to read and how to best prioritize your day." Due 4Q2019. Microsoft 365 Roadmap 49423 (March 12).
- **Updated Microsoft 365 Admin Center**. "The Microsoft 365 admin center, available at admin.microsoft.com, is the common entry point for managing all your Microsoft 365 services. We'll begin rolling out an updated version with new features and functionality in April. During this time, admins will still have access to the old version. All IT admin tasks that can be completed in the admin center today will be supported. With the change, there is a simplified admin experience with enhancements made in the following areas: [1] Improved user, groups, and settings management to make common, everyday tasks more efficient; [2] Targeted, intelligent recommendations and actionable insights to help your org get the most out of your Microsoft 365; [3] Tailored admin center experiences for your organization and admin role to provide a focused environment. If you'd like to experience it before general availability, join Targeted Release or click on the toggle in the upper right corner of the admin center dashboard to access the preview." Due April 2019. Microsoft 365 Roadmap 48639 (March 13).

Windows Defender ATP Goes Mac

Description



Microsoft renamed Windows Defender ATP, its endpoint protection platform, to Microsoft Defender ATP, and introduced a version of Microsoft Defender ATP for macOS devices.

- Threat signals from Mac devices are surfaced alongside threat signals from Windows devices in the Microsoft Defender ATP portal, also renamed from the Windows Defender ATP portal. Alerts and detections in the portal include the context of the device and the alert process tree.
- Threats identified via Microsoft Defender ATP can be quarantined, removed, or permitted (allowed) to run.
- Several advanced settings can be set by end users on a device-by-device basis, unless the Microsoft Defender ATP administrator has disabled the setting of these options.
- Supports macOS Mojave, High Sierra and Sierra. Microsoft Defender ATP is kept up-to-date via Microsoft AutoUpdate.
- During the preview, although not avaliable immediately, Microsoft's new Threat and Vulnerability Management capabilities will also be added to the Mac version. These new capabilities enable the prioritization and remediation of threats and vulnerabilities. These are due for release in the first several weeks of April 2019.

Microsoft Defender ATP for Mac was released into limited preview. Customers wanting to be involved in the limited preview must apply for the program.

Analysis

- As a Windows-only offering, Windows Defender ATP was a mark against Microsoft's ambitions in the security market. Extending to macOS is essential for customers with heterogeneous environments. Microsoft has signaled its intent to support Linux too, but there are no timeframes or specifics available at this time.
- Microsoft Defender ATP adds a more generalized set of security and antimalware capabilities to Windows and Mac devices, and given it is only available in the higher priced Microsoft 365 plans, should complement the Office 365 Advanced Threat Protection offering. It will be interesting to see where Microsoft will take Office 365 ATP over the next year, in relation to

Microsoft Defender ATP.

- With the broadening of Windows Defender ATP to support macOS devices (and the renaming of the service to Microsoft Defender ATP), it logically follows that usage data from enrolled Mac devices should at some point also be fed to Microsoft Cloud App Security, just as can happen with enrolled Windows 10 devices running Windows Defender ATP. Capturing cloud app usage data directly at an endpoint level enables a global viewpoint of app usage across the organization, not just when devices are connected to a managed network.

About

- **Date** - March 21, 2019
- Announcing Microsoft Defender ATP for Mac and new Threat and Vulnerability Management Capabilities (Microsoft Security, March 21)
- Announcing Microsoft Defender ATP for Mac (Windows Defender ATP Blog, March 21)
- **Tag** - Security
- **Implications** - Microsoft Defender ATP, Microsoft Cloud App Security

Office 365 ProPlus with Privacy Controls

Description

Microsoft announced that the next major release of Office 365 ProPlus (for Windows only) will include new privacy controls, so that at a tenant-level, an administrator can specify how much diagnostic and related data is sent back to Microsoft. The new privacy controls are in response to the Dutch Data Protection Impact Assessment published about Office 365 in late 2018.

Specifics include:

- At a tenant-level, an administrator can select the level of diagnostic data to be sent to Microsoft. The default is everything, meaning the administrator can opt-out of everything and select a lower level.
- Using a yet-to-be-released tool, an administrator will be able to view the data being sent to Microsoft.
- The settings can be controlled using the new Office Client Policy Service (in public preview) or Group Policy.
- The privacy controls initially only apply to Office 365 ProPlus for Windows. Office for Mac is excluded, as are the mobile apps and Office Online.
- There is no insight into how Microsoft may provide similar privacy settings for server apps in Office 365, such as SharePoint Online, Exchange Online, Microsoft Teams, and more.
- Microsoft warns that reducing the amount of diagnostic data shared with Microsoft is likely to have negative implications for the organization, such as reduced capabilities in Office apps and services, and greater difficulties in troubleshooting problems.

The ability to control privacy settings is due to ship with Office 365 ProPlus version 1904, due in April 2019. The privacy settings will initially be released into the Monthly Channel and the Monthly Channel (Targeted) for Windows.

Analysis

- The ability to limit sharing of diagnostic and related data with Microsoft is a needed change in light of new regulations. The initial capabilities offer a solid first step, but clearly there is much more that needs to be addressed yet across a much broader set of Office 365 capabilities.
- The Dutch DPIA raised eight risk areas. The new privacy controls slated for end April 2019 address the first two risks, but do not appear to yet address the remaining six risks, such as data storage outside of Europe for diagnostic data that is sent to Microsoft (risk 7).
- The Office Client Policy Service enables policy settings to be defined for sub-groups, which means different people in a tenant could be subject to different privacy controls for Office.

About

- **Date** - March 26, 2019
- Giving Your Organization More Transparency and Control Over Microsoft 365 Cloud Connected Experiences for Office (Message Center Update MC176396, March 25)
- Overview of Privacy Controls for Office 365 ProPlus (Microsoft Docs, March 26)
- Transparency and Control over Microsoft 365 Cloud Connected Experiences for Office (Microsoft Roadmap 49779, March 25)
- Microsoft Responds to Dutch DPIA with Privacy Control for Office ProPlus (Petri, March 26)
- **Tag** - Security
- **Implications** - Office 365 and GDPR

Weekly News Drop - March 29, 2019

Roundup of recent Office 365 news:

- **Customer Advisory Board Meeting for Microsoft Cloud Security**. Microsoft is hosting a Customer Advisory Board meeting in Redmond from April 30 to May 2, with a focus on its cloud security offerings including Microsoft Cloud App Security. The Board is made up of customers from different industries, sizes, geopolitical requirements, and security needs. Interested in Joining Our Customer Advisory Board? (Enterprise Mobility + Security, March 22).
- **DKIM Keys at 2048-Bits**. Despite being a security recommendation for several years, Office 365 does not support a DKIM key length of longer than 1024-bits. Security audits are increasingly flagging the risks of shorter key lengths, due to increased computing power that can break the key and thus spoof email. The US DoD rejects encrypted email signed with a DKIM key of less than or equal to 1024-bits. The Office 365 Security Team has signaled that a longer key length of 2048-bits will be available to all customers by the end of June 2019; the increased key length is currently in private preview. Note that there are other best practice recommendations for the use of DKIM keys that increases security, such as more frequent rotation of DKIM keys. Set DKIM Key Size to 2048 By Default (Office 365 Admin on UserVoice, March 27).
- **Tamper Protection in Microsoft Defender ATP**. Microsoft is adding a tamper protection setting to Microsoft Defender ATP, which can be set by an Intune administrator to ensure managed devices remain in a protected state. If the Intune administrator has turned tamper protection on for the device fleet, then neither the local device admin nor any malicious apps - in theory - can disable real-time protection, cloud-delivered protection, behavior monitoring, deletion of security intelligence updates, and more. The setting is off by default. The capability is also being offered to WIndows home users, with the setting defaulted to on. Tamper Protection in Microsoft Defender ATP (Windows Defender ATP Blog, March 27).
- **Microsoft 365 Security Center at General Availability**. Microsoft announced that its new Microsoft 365 Security Center is now at general availability. The new Security Center was announced two months ago, with a release date of "before end March 2019." Microsoft just made it. However, as one of the commenters on the announcement notes, the new offering is not finished yet, so the announcement is the first step with many more to come yet. Unlike during the preview stage where the availability of the Security Center was limited to Microsoft 365 E3 and E5 subscribers, the new Center is generally available across Office 365 subscribers only too. Microsoft 365 Security Center Reaches General Availability (Security, Privacy and Compliance Blog, March 28).
- **Microsoft 365 Compliance Center at General Availability**. Microsoft also pushed the Microsoft 365 Compliance Center into general availability, which was also announced in January. As with the Security Center, it was limited to just Microsoft 365 E3 and E5 subscribers, but is now more broadly available across Office 365-only plans. Your Specialized Compliance Workspace - Microsoft 365 Compliance Center (Security, Privacy and Compliance Blog, March 28).

Threat Explorer Updates

Description

In Roadmap ID 49537, Microsoft signaled several updates coming to Threat Explorer in the short-term:

- The updates focus on the Phish and All Email views in Threat Explorer - for customers with Advanced Threat Protection P2 and Office 365 E5 customers.
- New details on URLs in messages will support drill down analysis, and filtering based on URLs included in messages will be offered.
- URL information will be displayed in the graphs.
- Time-of-click data from Safe Links will be included, such as which clicks were allowed vs. blocked.
- New alerts will be created in the Security & Compliance Center Alerts dashboard for admins when the post-denotation reputation of a potentially malicious URL changes, or when a potentially malicious URL is clicked. The alert will include details outlining what the admin needs to do to address the new threat.

The Office 365 Management API was also updated, with new events related to email phish and URL clicks.

The updates to Threat Explorer will be rolled out worldwide starting end March 2019, and due for completion by end April 2019.

Analysis

- With phishing being used so frequently to compromise account credentials and lay the foundation for future persistent threats, strengthening the ability of administrators to detect, manage and mitigate phishing threats is critically important.
- The changes signaled increase the reporting and insights available to administrators in Office 365, but not necessarily the underlying security technology to reduce the rate of successful phishing attempts. Both go hand-in-hand and both are necessary.

About

- **Date** - March 15, 2019
- Enhancements to URL Views in Threat Explorer (Microsoft 365 Roadmap 49537, March 15)
- **Implications** - Advanced Threat Protection
- **Tag** - Security

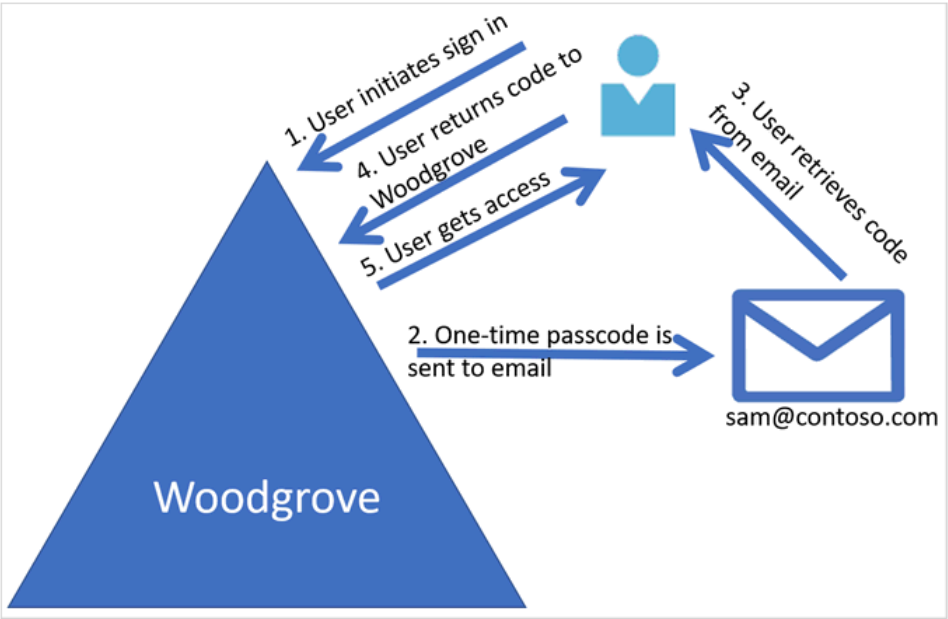
Weekly News Drop - February 1, 2019

Roundup of recent Office 365 news:

- **Tuning of Anomaly Detection Policies**. Microsoft added advanced tuning controls to anomaly detection policies in Office 365 Cloud App Security. For example, there is a new slider in the Impossible Travel policy which determines the level of anomalous behavior needed before an alert is triggered; this is analyzed according to the baseline for the user and the tenant. Four of the anomaly detection policies can be set to look at both successful and failed logins or only successful logins in triggering alerts. See Office 365 Cloud App Security releases 139 and 140 (Microsoft Docs, January 22, 2019).
- **Updates for the Azure Information Protection Scanner**. Microsoft released the new user interface for the Azure Information Protection Scanner, providing visibility into all scanner nodes and scanning statistics, along with admin control over incremental and full rescans. The update also supports a single SQL Server database per scanning profile, rather than requiring one per scanner node, and supports additional file formats (PDF, ZIP, and TIFF with OCR). Finally, central management of scanner configuration and scanned repositories was put into Public Preview. See Azure Information Protection Scanner Gets New Central Management, and Many New Other Features (Azure Information Protection Blog, January 22, 2019).
- **Drop Failure Rate in Microsoft Teams**. Microsoft Teams has been reporting dropped calls and unclassified calls when two users have an ad hoc screen-sharing session. Since there is no audio call associated with these sessions, Microsoft will no longer collect audio data on these calls for the Call Quality Dashboard from February 1, 2019. See The Rise of Drop Failure Rate and Unclassified Streams: Explained (Microsoft Teams Blog, January 29, 2019).
- **Another Azure AD Outage**. Issues with authentication via Azure AD ed to a global outage affecting users and services in Office 365, Azure and Dynamics 365. Users attempting to log into new sessions were unable to do so; those with cached log in sessions were able to keep working. See Microsoft Cloud Services See Global Authentication Outage (ZDNet, January 29, 2019).
- **Alerts Updates**. Several updates were added to the Office 365 Alerts capability in the Security & Compliance Center, including inclusion of Office 365-related alerts from Microsoft Cloud App Security, retrieval of Alerts using the Office 365 Management API, role-based permissions for viewing alerts, and access to insight signals through the Management Activity API or an email alert to an administrator. Insight signals show a trend, weakness or area of vulnerability in how Office 365 has been set up or is being used, such as users being targeted by a phishing campaign. See Maintain Visibility More Effectively with Updates to Alert Policies and Insights (Security, Privacy and Compliance Blog, January 29, 2019).
- **Security Baselines in Microsoft Intune**. Microsoft added mobile-device management security baselines in Microsoft Intune, offering broadly known and well-tested configurations that provide intelligent recommendations tailored to each organization. A security baseline can be deployed as is or customized to take account of specific needs. Intune can report the status of an organization's fleet of Windows 10 devices against the recommendations in the security baseline. See Microsoft Intune Introduces MDM Security Baselines to Secure the Modern Workplace (Enterprise Mobility + Security Blog, January 31, 2019).

20190207 Support of Email OTP in Azure AD

Description



Microsoft released the public preview of email-based one time passcodes (OTP) for guest access to resources in Office 365, controlled by Azure AD. When inviting a guest user outside the tenant to access a resource, if Azure AD is unable to locate a Microsoft account, Azure AD account, or federated account for the tenant, it will fall back to Email OTP. This means:

- If Email OTP is enabled for the tenant, users who can invite guests can invite guests irrespective of their email address.
- Guests can use an existing email identity for access and collaboration. They do not have to create a Microsoft account just to redeem a sharing invitation.
- When a guest receives the initial sharing invitation, they click the link to claim access. Azure AD will then send a second email to the same email address, this time containing a time-limited one time passcode. If the guest applies the OTP within 30 minutes, they gain access to the resource for 24 hours. Gaining access for additional 24 hour time periods requires going through the OTP process again. Microsoft implemented this control to ensure the guest retains access to their email account - for example, that they are still employed by the organization who owns the email domain.
- The service is in public preview, and some details are still to be worked out. For example, once a user gains access through an email OTP, they will continue to use email OTP for all future access even if they subsequently obtain a Microsoft account or Azure AD account with that same email address. The service does not currently make any future checks for the presence of a new Microsoft or Azure AD account. This flow can be broken by deleting the email OTP account in the tenant's Azure AD, which then forces the guest to re-authenticate using his or her new account.
- Email OTP is less secure than having a Microsoft or Azure AD account, because both the initial sharing email and OTPs are delivered to the same email address. If the guest's email account has been compromised, an attacker will be able to access resources shared by another organization. To mitigate this risk, Microsoft said it is possible to use conditional access or multi-factor authentication with guest accounts using email OTP.
- This new Azure AD-based email OTP service will replace the current email OTP option in SharePoint Online. Microsoft says "soon," but has not definitely a timeframe.

Analysis

- There is always a trade-off between "seamless collaboration" and security. Email OTP enables easy and quick access for guests regardless of their email address - thus delivering on the seamless collaboration ideal - but comes with weak security due to both the username (email address) and password (passcode delivered to the same email address) being available to an attacker if the guest's email account is compromised. Email OTP is currently set to off as the default, meaning that administrators have to make a deliberate change to enable the feature.
- An all-of-service approach for email OTP is preferrable to a service-specific approach. Having this homed in Azure AD makes

much more sense than limiting it to SharePoint Online.

About

- Date - January 29, 2019
- Announced via - Azure Active Directory Identity Blog
- Implications for -
- Tagged as - Authentication

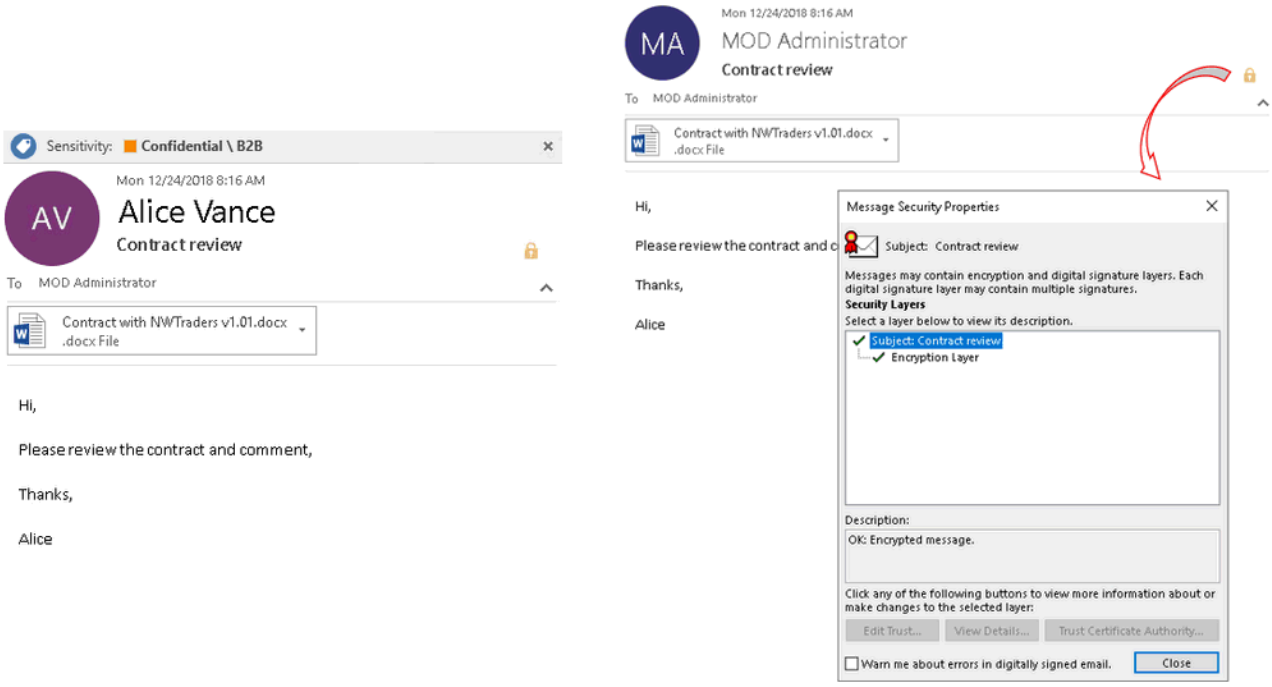
Weekly News Drop - February 8, 2019

Roundup of recent Office 365 news:

- **Updated OWA Generally Available**. The updated version of Outlook Web App is now generally available to all Office 365 tenants. Some features from the previous version have not yet made it across to the new version. See New OWA Now Generally Available to Office 365 Tenants (Office 365 IT Pros, February 6).
- **SharePoint Conference 2019**. Microsoft's 2019 SharePoint Conference is happening in May in Las Vegas. Despite the SharePoint nomeclature, the event more broadly addresses Office 365 services, Microsoft Teams, security and compliance, governance and adoption, and more. See Why Go To the 2019 SharePoint Conference? (SharePoint Community Blog, February 1).
- **Legal Requests for User Data at GitHub**. Legal requests for user data from GitHub more than doubled from 51 in 2017 to 122 in 2018, with the vast majority also being subject to a gag order to prevent notification to the user. Only in 9% of cases was GitHub not subject to a gag order, down from 42% in 2015. See Microsoft's GitHub: Requests for User Data Double in 2018, but Gag Orders Grow Faster (ZDNet, January 24).
- **Megamenu Navigation in SharePoint Online**. Microsoft announced that megamenu navigation will roll out to SharePoint Online Communication Sites starting in February 2019. Megamenu navigation is in addition to the current cascading navigation design. Other pending changes include site headers, site footers, and a site design panel for site owners. See Organize Your SharePoint Sites with Megamenu Navigation and New "Change the Look" Options (SharePoint Community Blog, January 30).

Sensitivity Labels with S/MIME Option

Description



Microsoft added the ability to sign and/or encrypt email messages with S/MIME based on a user selecting a sensitivity label for an email message in Outlook. The ability to trigger S/MIME from a sensitivity label means the process is tied to an easy-to-understand user activity (applying a label), with the label definition responsible for the background signing and/or encrypting process.

Using S/MIME instead of Office 365 Message Encryption is only available for email messages and attachments in Outlook for Windows, and only for customers with Azure Information Protection (and the add-in client for Outlook). Microsoft's stated preference is that customers make use of Office 365 Message Encryption instead of S/MIME, but have added S/MIME support to address the requirements of customers with an existing S/MIME infrastructure.

Analysis

- Using S/MIME is targeted at a limited market, and comes with several restrictions. The customer must have a working S/MIME infrastructure, and the labeling experience will only work in Outlook for Windows with the Azure Information Protection add-in client. Microsoft states it has no plans to support S/MIME signing and/or encryption in the new native labeling experiences in Mac, iOS, and Android.
- While Microsoft supports S/MIME as an option, the configuration for a sensitivity label is not point-and-click. It requires an administrator to set an advanced client setting in the Azure portal - which could also reflect the idea that while the functionality is essential for a few select customers, only a few will actually make use of it. While it is possible to use S/MIME, it is not a simple set up process. On the other hand, Microsoft says that migrating from S/MIME to Office 365 Message Encryption can be done with a single click in the label policy.
- While S/MIME is offered as an option, Microsoft is very clear that it would prefer customers to use Office 365 Message Encryption.

About

- Date - February 5, 2018
- Announced via - Azure Information Protection Blog
- Implications for - Sensitivity Labels
- Tagged as - Encryption, Data Loss Protection

Weekly News Drop - February 15, 2019

Roundup of recent Office 365 news:

- **Teams Support 5,000 Members**. Microsoft doubled the maximum number of members who can access a single team in Microsoft Teams. The previous limit was 2,500, but the new limit of 5,000 is now generally available to all existing and new teams. See Teams Membership Limit Raised to 5,000 (per team) (Office 365 IT Pros, February 8).
- **Fewer Code Exploits, More Social Engineering**. A Microsoft security engineer claims that Microsoft's security investments have reduced the attack surface available to hackers from code exploits, and that widespread attacks are uncommon. What is common, however, are targeted attacks and social engineering efforts that don't involve code exploitation. See Microsoft: Improved Security Features are Delaying Hackers from Attacking Windows Users (ZDNet Microsoft, February 10).
- **Deployment Guide for Azure Information Protection**. The Information Protection Customer Experience Engineering Team released a deployment guide for Azure IP. The guide is intended to help business decision makers and IT implementers follow a proven deployment process and mininimize mistakes that could derail the initiative. See Azure Information Protection Deployment Acceleration Guide (Azure IP Blog, February 11).
- **Microsoft Teams Admin Center**. Microsoft rebranded the Teams and Skype for Business Admin Center as just the Microsoft Teams Admin Center. The newly rebranded center also offers several usage reports on users, devices and team workspaces. See It's Now the Teams Admin Center ... And Some New Teams Usage Reports (Office 365 IT Pros, February 14).
- **Document Signals in SharePoint Online**. Microsoft is adding new visual cues to views in SharePoint, called Signals. These small icons convey important security information about a file, such as the presence of malware, that sharing access is blocked by a DLP policy, and that a DLP policy has triggered a warning about a file. Other signals address common SharePoint status points about a file, including checkout status, missing metadata, and that the document is newly created or uploaded. See January 2019 SharePoint Modernization News (The SharePoint Community Blog, January 24).

Microsoft Response to Dutch DPIA

Description

Nr	Risk	Possible measure Microsoft	Possible measure per tenant
1	Lack of transparency	Public documentation and data viewer tool	Use tool when it becomes available
2	No possibility to influence or end the collection of telemetry data	a. Temporary settings to minimise the processing	Use temporary minimisation settings
			Do not use SharePoint/OneDrive
			Do not use web-only Office 365
		b. Permanent settings for telemetry levels	Use setting telemetry Off when switch is available
3	Unlawful collection and storage of sensitive/ classified/special categories of data	*a. Option to delete historical diagnostic data by Device ID*	Consider deleting some specific users and creating new accounts for them
		b. Guarantee never to store content data in telemetry data or in other system-generated event logs unless strictly necessary	Prohibit users from sending personal data to Microsoft to 'improve' Office
			Consider pilot with other software for some functionality (after conducting a separate DPIA)
4	Incorrect qualification Microsoft as data processor	*a. Minimisation of purposes to be able to act as a processor OR New framework agreement as joint controller*	Endorse new framework agreement as processor or joint controller
		b. Only process data from voluntary Connected Services as a data processor OR change default for voluntary Connected Services to 'Off'	Prohibit voluntary Connected Services unless Microsoft offers these services as a processor
5	Not enough control over sub-processors and factual processing	*More audit rights*	Consider stand-alone deployment without Microsoft account for confidential/sensitive data
6	The lack of purpose limitation	*Processing only for strictly necessary purposes for which the tenants have a legal ground*	- no specific measure, see above
7	The transfer of data outside of the EEA	*New contractual guarantees and/or storage of diagnostic data within the EU*	- no specific measure, see above
8	The indefinite retention period of diagnostic data	*Determine necessary retention periods*	- no specific measure, see above

In mid-November 2018, The Privacy Company in the Netherlands published the data protection impact assessment (DPIA) it had undertaken on behalf of SLM Rijk (the Dutch Ministry of Security and Justice). The DPIA investigated the use of Office 365 ProPlus, which encompassed Office 2016 MSI, Office 365 click-to-run, and Office Online. SLM Rijk oversees the relationship between Microsoft and the Dutch government, which includes upwards of 300,000 employees.

The Privacy Company drew several conclusions:

- Microsoft systematically collects and stores personal data on the behaviour of individual employees on a large scale. There is no public documentation on what is collected. The fact of covert collection of such large scale data was labeled as "alarming."
- Customers have no choice on the collection and storage of telemetry data (covering 23,000 to 25,000 events in Office), which almost certainly includes several types of personal data (and is thus a GDPR issue). No choice extends in three directions: no choice on the amount of data, no choice on whether the collection happens or not, and no choice to see what data is collected.
- Because Microsoft defines the types of data collected and the purposes of this data collection, Microsoft should not be considered a data processor but rather a joint data controller. The burden of compliance is higher for the latter.
- Microsoft's approach with Office ProPlus raises eight significant concerns (see table above). Before the release of the DPIA,

Microsoft worked with The Privacy Company and SLM Rijk to offer new capabilities to address the first two concerns (including a so-called "zero-exhaust setting" that could be enabled for Dutch government agencies by Microsoft), but did not agree to further changes to address concerns 3-8.

On February 8, Politico ran a story stating that Microsoft has agreed to address "a series of privacy concerns raised" in the above report. These changes will be offered before the end of April 2019, but the specifics as to how Microsoft will address the eight issues are unclear. The specific statements from Microsoft are vague:

- "*We feel good about what we're doing to give customers transparency and choice on the diagnostic data they share with us, but we always want to do more.*"
- "*In the coming weeks we will take additional steps to make it easier for customers to understand what data needs to go to Microsoft to run our services and why, and where data-sharing is optional.*" This could address concerns 1 and 2.

The Irish Data Protection Commission - who is the lead supervisory authority in Europe for Microsoft - is monitoring the situation, and if the need arises because the mitigations offered are insufficient, has the option of beginning an investigation under GDPR.

Analysis

- GDPR provides due cause (for organizations) and due force (for vendors and suppliers) to examine data protection approaches, issues, concerns, and mitigations. Since The Privacy Company was commissioned on behalf of the Dutch government and its 300,000 workers to undertake the DPIA, the findings and weight of the initial report and subsequent mitigations are significant.
- It is unclear whether any changes made in concession to the DPIA for the SLM Rijk will apply only to Dutch government agencies, or if such changes will be released worldwide for all organisations.
- Concern 7 in the original analysis was regarding the transfer of diagnostic data outside of Europe, to be stored on servers in the United States. It is unclear whether the coming changes will introduce a European solution.

About

- Date - February 8, 2019
- Impact Assessment Shows Privacy Risks in Microsoft Office ProPlus Enterprise (The Privacy Company, November 13, 2018).
- Microsoft to update Office Pro Plus after Dutch ministry questions privacy (Politico, February 8, 2019).
- Implications for - Office 365 and GDPR
- Tagged as - Security

Weekly News Drop - February 22, 2019

Roundup of recent Office 365 news:

- **Teams Outage on February 18**. Microsoft Teams was inaccessible for over 4 hours to some users on Monday February 18. Microsoft said it was due to a "connectivity issue," and mitigated the problem by rerouting traffic within the Office 365 infrastructure. See Microsoft Teams Is Down and Users Aren't Happy (Thurrott, February 18).
- **Multiple Plans per Office 365 Group**. When initially released, there was a one-to-one relationship between an Office 365 Group and a Plan in Planner; one group equaled one plan and only one plan. The Planner team recently added the ability to create multiple plans per group using the Planner web app, a capability they have called Multiplan. The ability to create multiple plans per group via the web app complements the existing ability to add multiple plans using Microsoft Teams and SharePoint. See Planner Has a New Way to Create Multiple Plans Per Group - Multiplan (Planner Blog, January 28).
- **Enhancements to Azure AD Identity Protection**. Microsoft released several enhancements to its Azure AD Identity Protection service into public preview, including a revamped user interface, APIs for integrating identity protection data into other systems, improved risk analysis methods, and a renewed focus on risky users and risky sign-ins. See Four Major Azure AD Identity Protection Enhancements are now in Public Preview (Azure AD Identity Blog, January 29).

Microsoft HoloLens 2

Description

At MWC in Barcelona (MWC being previously called Mobile World Congress), Microsoft introduced its second-generation mixed reality headset - the HoloLens 2. In comparison to the first generation headset, HoloLens 2 has:

- Doubled the field of view available to the user, enabling a more immersive experience.
- Simplified the manipulation of objects by supporting direct manipulation, gesture tracking, and eye-tracking.
- Less weight and a more streamlined experience for the wearer, including a dial-in sizing option, and support for iris recognition with Windows Hello for logging in. The visor can flip up when not required, enabling a simpler transition between mixed reality and normality.
- Out-of-the-box integrations with several other Microsoft services to speed time-to-value. For example, HoloLens 2 works with Dynamics 365 Remote Assist (enabling a first line worker to share their view with a remote expert, and the remote expert to provide mixed reality directions on how to solve a problem or troubleshoot an issue) and Dynamics 365 Layout (a mixed reality application for laying out objects in a particular space, such as machines on a factory floor). HoloLens 2 also supports an ecosystem of partners.

Microsoft announced several complementary services for HoloLens 2 at the same event:

- **Dynamics 365 Guides**. An application for creating training guides that uses HoloLens (1 and 2) to overlay step-by-step training instructions and directed guidance on physical objects (which Microsoft calls "holographic training materials"). Aimed at first line workers who are learning to follow a new process or undertake a new job. Dynamics 365 Guides is available in preview.
- **Azure Spatial Anchors**. An application for creating holograms that are anchored to a particular place in physical space. If authorized, other people can view and interact with the hologram using HoloLens and iOS and Android devices.

Microsoft also announced a customization program, where third-parties can incorporate the HoloLens 2 into their own headwear and related products. Trimble is an early partcipant in the program, and has announced a hard hat that includes HoloLens 2.

No specific shipping date was mentioned, apart from being available in 2019. HoloLens 2 is available for pre-order, at US$3500 per unit. Several monthly pricing options are also available, where HoloLens is bundled with other Microsoft mixed reality services.

Microsoft has a contract to supply over 100,000 HoloLens headsets to the US Army, valued at $480 million as part of the Integrated Visual Augmentation System program. The intent of the program is to improve the lethality of soldiers in combat situations, through capabilities such as night vision, real-time metrics on the soldier, and low-light and thermal detection of other people. Over 250 employees at Microsoft petitioned Microsoft to cancel the contract, because they did not want Microsoft technology to be used in warfare situations. CEO Satya Nadella said the contract would remain in place, and noted that Microsoft will supply HoloLens type

equipment to institutions in elected democracies.

Analysis

- Microsoft has invested significant resources in building HoloLens 2, plus significant interaction with customers to understand leading-edge use cases that could drive demand.
- At US$3500 per unit, HoloLens 2 is still very much a business and commercial play, not a consumer one. There is pent up demand for a consumer version, especially for gaming.
- Aside from the high cost (albeit it significantly cheaper than the first generation of HoloLens), HoloLens 2 has several weaknesses including no support for cellular networks, and a battery life of only 2-3 hours.

About

- Date - February 24, 2019
- Microsoft at MWC Barcelona: Introducing Microsoft HoloLens 2 (Microsoft's Official Blog, February 24)
- Microsoft at MWC 19 Barcelona (Microsoft Stories, February 24)
- New HoloLens 2 gives Microsoft the Edge in the Next Generation of Computing (Microsoft News, February 24)
- PACCAR is Exploring Dynamics 365 Guides and HoloLens 2 to Improve Employee Onboarding (YouTube, February 24)
- Announcing Azure Spatial Anchors for Collaborative, Cross-Platform Mixed Reality Apps (Microsoft Azure Blog, February 25)
- Microsoft CEO Nadella: HoloLens for War is Fine If It's Used by a Democracy (ZDNet Microsoft, February 26)
- HoloLens 2 - Going Hands-On with Holograms (ZDNet Microsoft, March 8)
- Implications for -
- Tagged as -

Worldwide Microsoft Teams Outage

Description

Microsoft Teams suffered a worldwide outage on February 18, with users in multiple Office 365 datacenter regions unable to log in. The outage affected users attempting to access Teams via the desktop and browser clients only, with the mobile client continuing to function. The difference was in how the two types of clients refreshed their authentication token, with the mobile client using a different method to the desktop and browser clients (which are based on the same code and are therefore essentially the same thing).

After investigating the root cause of the problem, engineers found that the design parameters around Azure Key Vault was to blame, and implemented an undefined change to restore service health. The outage lasted for over 5 hours during core business time in Europe and the United States.

Analysis

- Unplanned outages of core Office 365 workloads do not help the positioning of cloud services as having less downtime than on-premises solutions. Unplanned outages that affect multiple geographical regions for several hours are particularly damaging, both for the Office 365 service overall, and for the specific tools in the toolkit such as Microsoft Teams.
- Single points of failure are not good - in any service design. Microsoft had several outages in 2018 due to single points of failure in its approach to multi-factor authentication. Outages such as this one with Microsoft Teams and Azure Key Vault quickly highlight where design problems persist, and provide due cause for Microsoft to introduce greater resiliency into the core design of such components.
- With Teams becoming an important daily tool in the workflow of millions of users at hundreds of thousands of organizations, the lack of an offline capability will need to be addressed by Microsoft.

About

- Date - February 26, 2019
- Analyzing the Teams Outage of 18 February 2019 (Office 365 IT Pros, February 21)
- Microsoft Teams Went Down, But It's Not Out (Petri, February 19)
- Microsoft Teams Is Down and Users Aren't Happy (Thurrott, February 18)
- Implications for - Azure Key Vault
- Tagged as - Authentication

Office 365 Cloud App Security Expands Conditional Access

Description

Microsoft released to public preview additional app support in Office 365 for conditional access, covering both access and session policies. Conditional access was previously only available for SharePoint Online, but the newly supported apps are:

- Exchange Online
- OneDrive for Business
- Power BI
- Microsoft Teams
- Yammer

Depending on the who (user / group), what (cloud app) and where (locations, networks) of the user session, policies can block access entirely, block downloads, enforce encryption of downloaded documents, increasing monitoring, and more. Using conditional access policies does not require anything to be installed on an endpoint device, thus supporting both managed and unmanaged devices.

Conditional Access App Control in Office 365 Cloud App Security relies on Azure AD Conditional Access, and requires at least Azure AD Premium P1 licensing.

The new capabilities are in public preview, and not yet at general availability.

Analysis

- Conditional access enables the nuance of complex situations to be taken into consideration when deciding whether or not to provide access to data in Office 365. Without conditional access policies, access is either yes or no (binary), based on whether someone can authenticate correctly (and pass an MFA challenge if issued / enabled). With conditional access, the ability to see additional factors in the authentication equation are enabled - such as the type of device, where the user is connecting from, and what specific app capabilities they are requesting.
- Conditional Access App Control was previously only available for SharePoint Online, which given the wide number of apps offered in Office 365, was far too restrictive. Supporting additional apps is a good forward move by Microsoft.
- Security administrators need to ensure they create conditional access policies appropriate to the risks of their environment, and don't inadvertently create policy gaps that allow major risks to go unmanaged.

About

- Date - February 27, 2019
- Office 365 Cloud App Security Release 142 (Microsoft Docs, February 17)
- Protect Apps with Office 365 Cloud App Security Conditional Access App Control (Microsoft Docs, February 27)
- Implications for - Office 365 Cloud App Security
- Tagged as - Security

Standalone Upgrades for Microsoft 365 E3

Description

Microsoft 365 is a superset of Office 365, adding licensing for Windows 10 as well as the portfolio of device management and enhanced security capabilities in Enterprise Mobility + Security. Microsoft 365 is available for two markets - business and enterprise - and has multiple tiers available to each market segment. Microsoft 365 E5 is the top tier, offering all of the best that's available from Microsoft across Office 365, Windows 10, and Enterprise Mobility + Security. Microsoft 365 E3 is the second tier, offering a significant upgrade to Office 365 E3 or E5 standalone, but not as much as the combined bundle of Microsoft 365 E5.

Microsoft introduced two new standalone bundles that can be added to Microsoft 365 E3, which provide incremental capability and value that's already on offer in Microsoft 365 E5 without stepping up to the full Microsoft 365 E5 price point per user.

- **Identity & Threat Protection ($12/month)**. A bundle of Microsoft Threat Protection, Microsoft Cloud App Security, and Azure Active Directory. Microsoft Threat Protection includes Azure Advanced Threat Protection, Windows Defender Advanced Threat Protection, Office 365 Advanced Threat Protection, and Office 365 Threat Intelligence. A Microsoft 365 E3 customer has Office 365 E3 capabilities, so the added Office 365 capabilities noted above are from Office 365 E5.
- **Information Protection & Compliance ($10/month)**. A bundle of Office 365 Advanced Compliance (from Office 365 E5) and Azure Information Protection (for automatically classifying and protecting sensitive data).

These two new bundles were announced in early January, and will be available for purchase at the beginning of February 2019. Pricing is per user per month, and is the standard list price (therefore may be less after volume or other denominated discounts).

Analysis

With such a monumental user base (over 155 million active monthly users of Office 365 at October 2018), it is in Microsoft's financial interest to upsell its current user base to ever more expensive monthly plans. Customers on Office 365 E3, for example, have a natural upgrade path to Office 365 E5, which adds telephony services and enhanced security and compliance capabilities. Office 365 E5 delivers over 50% more revenue per user to Microsoft compared to Office 365 E3. With Microsoft 365 E3 and E5, Microsoft offers even more enhanced services with premium pricing, offering the potential of another significant uplift in its monthly revenue figures - and thus market valuation - as current customers migrate upwards. Microsoft has a valid value proposition to customers in the need for better security, information protection, and compliance capabilities; the world is an increasingly scary place, with malicious external actors, new data protection regulations, and more that demand an uplift in security and compliance maturity on the behalf of organizations.

Microsoft already offers a complex of pricing levels across its many services, and several tiers of capability within each individual product (e.g., Azure Active Directory has 4 pricing levels). While these two new service bundles provide two step-wise upgrade paths for Microsoft 365 E3 customers, it doesn't do anything to simplify the in-between pricing steps. In other words, these new plans provide Microsoft's sales force with the motivation to go back to E3 customers to talk about two optional upgrades, but most customers that have Microsoft 365 E3 could put the capabilities on offer in both upgrades to good use. How does a customer choose between the two, and at what point is it better to just upgrade to E5 completely?

It remains to be seen how many Microsoft 365 E5 customers will downgrade to Microsoft 365 E3 with one or the other of the two bundles, rather than paying the full E5 price. This will be misaligned with Microsoft's intent in introducing the two bundles, but for E5 customers not utilizing the full capabilities of E5, these intermediate steps may offer a cheaper way of proceeding.

While both bundles bring the best of what Microsoft has to offer to its customers, each service is subject to weaknesses as documented in this knowledge base. Customers would be well advised to carefully consider their options in embracing higher priced plans with capability-challenged services that offer less capability than best-of-breed options on the market.

About

- Date - January 2, 2019
- Announced via - Microsoft 365 Blog
- Implications for -
- Tagged as - Data Loss Protection, Security

Autodiscover Optimizes for Office 365 - Implications

Description

Microsoft changed the default behavior for Autodiscover starting with version 16.0.6741.2017 of the Click 2 Run version of Outlook for Windows. Autodiscover now prioritizes Office 365 over the other Autodiscover methods. If a user has a valid Exchange Online mailbox in Office 365, the new prioritization will streamline and simplify the setup process.

However, there are implications of this design, which affects customers using Exchange on-premises, Exchange in hybrid mode, other Hosted Exchange services, and more. The new prioritization approach fails when:

- A user has their mailbox on Exchange on-premises, but also has an Exchange Online license assigned to them.
- A user with an Exchange mailbox with a Hosted Exchange service provider cannot connect Outlook using Windows Phone and iOS. The presence of a Microsoft account that uses the same email address confuses autodiscover.
- A user with a personal Office 365 subscription that is tied to their business email address. It fails because the address attempts to resolve against a business tenant in Office 365.

Microsoft released a workaround to prevent the new default behavior, but it requires editing the system registry on affected Windows PCs to create a new setting. This must be done on each affected endpoint, and must be removed when/if the user does get an Exchange Online mailbox later on.

On UserVoice, customers have complained about wasting time and resources due to having to re-create Outlook profiles, re-install Office, and change passwords on various services.

Analysis

Optimizing for Office 365 is a fair call by Microsoft, given the growing dominance of Exchange Online among its customer base. However, Microsoft should execute its optimization in a way that honours other preferred architectures involving Exchange and Outlook. While a growing proportion of end users are served by Office 365, many are not.

About

- Date - November 20, 2018
- See - Outlook on UserVoice
- Implications for -
- Tagged as -

Searching Encrypted Documents and Emails

Description

Search indexing processes in Office 365 are inconsistent in how they work with encrypted documents and emails, which has implications for whether documents and email messages can be discovered using Content Search for compliance and/or eDiscovery purposes.

- In Exchange Online, encrypted messages can be decrypted by the indexing process and therefore included in the search index.
- In SharePoint Online and OneDrive for Business the opposite is true: the indexing process is unable to decrypt documents that have been encrypted, and therefore the contents of a document is hidden from the search index. Note that the indexing process is able to view and utilize any metadata attached to an encrypted document - that exists outside of what is encrypted - but any content inside the encrypted document is invisible to the indexing process.
- If an encrypted document is located using Content Search because the document's metadata included the search term, there is no option to decrypt the document during an export. The document can only be exported with its original encryption in place. This is different to encrypted messages in Exchange Online, which can be decrypted during the export process.

Analysis

Encrypted documents in SharePoint Online and OneDrive for Business are invisible to Content Search and eDiscovery Content Search, because the search indexing process is unable to look inside encrypted documents. This is different to the experience in Exchange Online, where the search indexing process can decrypt encrypted email messages to assess content inside.

Implications include:

- Encrypted documents containing information that would be responsive to an eDiscovery request will not be located, raising concerns about not producing a full set of responsive data.
- Encrypted documents containing information about a data subject will not be located under a GDPR right of access request.

About

- Date - January 4, 2019
- Announced via -
- Implications for - Content Search
- Tagged as - eDiscovery

Session ID Added to Exchange Online Audit Logs

Description

Microsoft extended the data collected for and displayed within Exchange Online Audit Logs, adding a Session ID field. This is a unique field value tied to an authentication against Azure Active Directory, and allows both manual and automated processes to differentiate actions within a mailbox by different users. For example, when the primary owner of a mailbox authenticates against Azure AD and works inside their mailbox, the Session ID value from their authentication is stamped on all audit log entries. If their account credentials had been compromised, however, and the attacker also authenticated correctly against Azure AD and gained access to the mailbox, the Session ID value from their Azure AD authentication will also be stamped on all the audit log entries they generate, but it will be a different Session ID value compared to the primary owner's Session ID. The different Session ID values provide a record of what each authenticated user did within the mailbox.

Session ID values can be manually reviewed by a security defender, but the real power is automated analysis and handling to generate early warnings of a potentially compromised mailbox. For organizations with Microsoft Cloud App Security or a SIEM (Security Information and Event Management) tool, the different Session IDs could be leveraged in policy settings for alerts and/or automated remediation actions.

The change applies to both mailbox audit logs and admin audit logs.

Note that the Session ID value changes every time a user re-enters their credentials to authenticate against Azure AD, so the mere presence of different Session ID values is not necessarily an indication of malicious activity within the mailbox.

The collection of Session ID has three requirements:

- Logon is through modern authentication, because Session ID is generated by Azure AD. Legacy authentication methods will not generate the Session ID.
- Exchange Audit Logging is turned on. From mid-to-late 2017 this happens default for tenants, but organizations who created their Office 365 tenant before it was turned on default should double-check.
- Unified audit logging in Office 365 is enabled. This enables the ingestion of Exchange Audit Log entries into the Office 365 Audit Log, accessible through the Security & Compliance Center.

Session ID offers a unique value to tie together a chain of actions by a given authentication session. Since it is generated by Azure AD, it is a more reliable unique identifier than IP address, because the latter can be obfuscated through VPNs and the use of TOR.

Analysis

- A fully unique identifier for each audit log entry is a good addition to the Exchange Audit Log.
- Microsoft notes that if an attacker is able to steal the authentication token itself, their Session ID will be the same as the attacked user's Session ID. This requires, however, control of the endpoint device, and points to the fundamental principle in security of the power of layered defenses.
- Expect to see Microsoft making use of Session ID in new default policies in Office 365 Cloud App Security and Microsoft Cloud App Security. For example, the detection of multiple Session IDs being recorded to the Exchange Audit Log at the same time could point to a current attack-in-motion. Disabling the user account or forcing a multi-factor authentication request could be used to automatically check for potential malicious behavior.
- The capture of Session ID is limited to Exchange Online currently. There is no indication from Microsoft when it will be applied more broadly to other workloads across Office 365.

About

- Date - January 4, 2019
- Announced via - Security, Privacy and Compliance Blog
- Implications for - Office 365 Cloud App Security, Microsoft Cloud App Security
- Tagged as - Security

Weekly News Drop - January 11, 2019

[Editor's note: I have been thinking about how to cover more of the Office 365 news each week. This new feature - the Weekly News Drop - is designed to capture the wider changes that don't require their own Update post. I hope you find it useful. As always, feedback is welcomed.]

Roundup of recent Office 365 news:

- **SharePoint and SMTP Authentication**. SharePoint 2019 (on-premises) now supports SMTP authentication with an SMTP email server directly, and unlike previous versions of SharePoint, no longer requires the configuration of a standalone SMTP relay in order for SharePoint to send outgoing email. The connection also works with Exchange Online using **smtp.office365.com** in the settings pane, and if Port 587 is entered, authentication via Kerberos will be preferred and anonymous authentication will be rejected. There are a few requirements on users and licensing in order for this to work with Exchange Online. See Finally - SMTP Authentication included with SharePoint 2019 (SharePoint Support Blog, January 1, 2019).
- **MyAnalytics More Broadly Available**. Microsoft announced broader availability of MyAnalytics, what it is now calling the "fitness tracker for work." When initially released, MyAnalytics required Office 365 Enterprise E5, or an additional monthly fee per user on E1 and E3 plans. In a change that will roll out over the next couple of months, MyAnalytics will become available to users licensed for Exchange Online with an Office 365 or Microsoft 365 plan (e.g., Business Essentials, Business Premium, E1, E3 and E5). In addition to broader availability to licensed users, MyAnalytics will also consume and ruminate on a wider set of data points beyond just Outlook and Exchange. Signals from Microsoft Teams, OneDrive and SharePoint will be analyzed starting from January 2019. See MyAnalytics, the fitness tracker for work, is now more broadly available (Microsoft 365 Blog, January 2, 2019).
- **Automatic Encryption with Office 365 Message Encryption?** Microsoft announced a plan to introduce a new mail flow rule for Exchange Online, so that outbound email messages containing sensitive information are automatically encrypted using the Encrypt-Only encryption template in Office 365 Message Encryption. The plan is to enable the new mail flow rule automatically - make it opt-out with notification - rather than opt-in with notification. At least one Office 365 customer has already seen the new mail flow rule added to their tenant. See Microsoft Plans to Launch Automatic Email Encryption for Office 365 Tenants (Petri, January 8, 2019).
- **Categories as Favorites in Outlook Web Access**. Microsoft's forthcoming refresh of Outlook Web Access - which is available in preview mode currently - supports marking categories as favorites. Doing so shows the category alongside other folders, groups and people in the mailbox. See New OWA Makes Categories into Favorites (Petri, January 10, 2019).
- **Office ProPlus and Office 2019 Default to 64-bit**. Beginning mid-January 2019, the default setting when installing Office ProPlus and Office 2019 will change from 32-bit to 64-bit. Customers running legacy 32-bit add-ins with Office applications will need to beware. See We're Making Some Changes to Default Installation Settings (Message Center Update MC171479, December 2018)

Control Over PST Output Size in eDiscovery

Description

Microsoft doesn't offer many options for exporting eDiscovery results from Office 365, but it does offer the ability to export messages and mailbox content to PST files. The default size of the export is set to a maximum of 10 GB, in order to balance customer demands for as much data as possible in a single export file without running into file corruption issues. While this is the default, Microsoft also offers the ability for a user to set a registry key on their computer to decrease the maximum size of the PST file export. There is nothing stopping a user from increasing the maximum size as well, but Microsoft recommends against doing this due to the potential for file corruption.

This does not seem to be a new change as much as a re-statement of what is already available, because the ability to make a registry edit to change the file size was already available in February 2017 (and the UserVoice request below was submitted in January 2017).

Analysis

- While the PST output size can be specified using a registry key on each computer running the eDiscovery Export tool, there is no ability to specify the output size as a policy setting for the organization using the Security & Compliance Center. The setting must be altered on a computer-by-computer basis, not globally for all eDiscovery users.
- Exports from Office 365 are not protected and so are at risk of alteration and spoliation. The output is a raw native export and not in a preservation format, such as forensic image format, which many eDiscovery collection tools offer. Moreover, there are no additional encryption options provided by Microsoft to encrypt the export.

About

- Date - January 14, 2019
- Announced via - Office 365 on UserVoice
- See Also - Change the size of PST files when exporting eDiscovery search results (Microsoft Docs)
- Implications for - eDiscovery Workflow
- Tagged as - eDiscovery

Mail Reads to be Audited for Exchange Online

Description

For Exchange Online audit logging, Microsoft will update the default configuration starting February 2019 to audit mail read and mail access events for owners, delegates and admins. Audit entries will be available using a new action - MailItemsAccessed - and will replace the current MessageBind action (which is less functional).

The change to the default settings will not impact customers who have created custom configuration settings for mailbox auditing. MailItemsAccessed will be available for implementation by customers with custom configurations, but will not be enforced automatically.

The default configuration will be updated beginning early February 2019.

Analysis

- Microsoft is introducing multiple changes to elevate the quality of audit reports in Office 365. The expanded scope for mail read and mail access events is illustrative of this direction, even though it initially only populates the Mailbox Audit Log for Exchange Online, not the Unified Audit Log for Office 365.
- Mail Read events will not initially flow into the Office 365 Unified Audit Log. They will only be available through the Mailbox Audit Log for Exchange Online.

About

- Date - January 4, 2019
- Announced via - Office 365 Message Center
- Implications for -
- Tagged as -

ATP Splitting Into Two Plans

Description

In item 45522 on the Microsoft 365 Roadmap, Microsoft has signalled its intent to split the Office 365 Advanced Threat Protection product into two plans and add the previously excluded Threat Intelligence into ATP: one plan will offer Advanced Threat Protection and Threat Intelligence (Plan 2), and one will only offer the current Advanced Threat Protection (Plan 1). It is worded as such:

Additional ATP Plan 1 capabilities for existing Office Threat Intelligence (ATP Plan 2) customers

We're consolidating the capabilities in current Office 365 Advanced Threat Protection(ATP) and Office 365 Threat Intelligence products to help customers with detection, protection, investigation and remediation of threats. We're offering this through two SKUs: 1. Current Office 365 ATP SKU becomes Office 365 ATP Plan 1 2. Current Office 365 Threat Intelligence SKU becomes Office 365 ATP Plan 2 Office 365 ATP Plan 2 includes Office 365 ATP Plan 2. So, we'll be backfilling Office 365 ATP P1 capabilities to existing Office 365 Threat Intelligence customers.

Note that the line *"Office 365 ATP Plan 2 includes Office 365 ATP Plan 2"* doesn't make sense. It should conclude with " ... *includes Office 365 ATP Plan **1***."

Microsoft is targeting February 2019 for release.

Analysis

- Both of these products are fully available in the Office 365 Enterprise E5 subscription bundle, so the two tiers will apply to customers with Enterprise E3 who want to step up with more security capabilities but don't want to jump all the way to E5.
- The splitting of the Advanced Threat Protection add-on for Office 365 is similar to the introduction of the two security-focused add-on plans for Microsoft 365 Enterprise E3. The full Microsoft 365 Enterprise E5 plan offers everything, but not all customers want to step up all the way to E5.
- The addition of Threat Intelligence into the ATP service description changes the feature comparison table of ATP versus Exchange Online Protection as such:

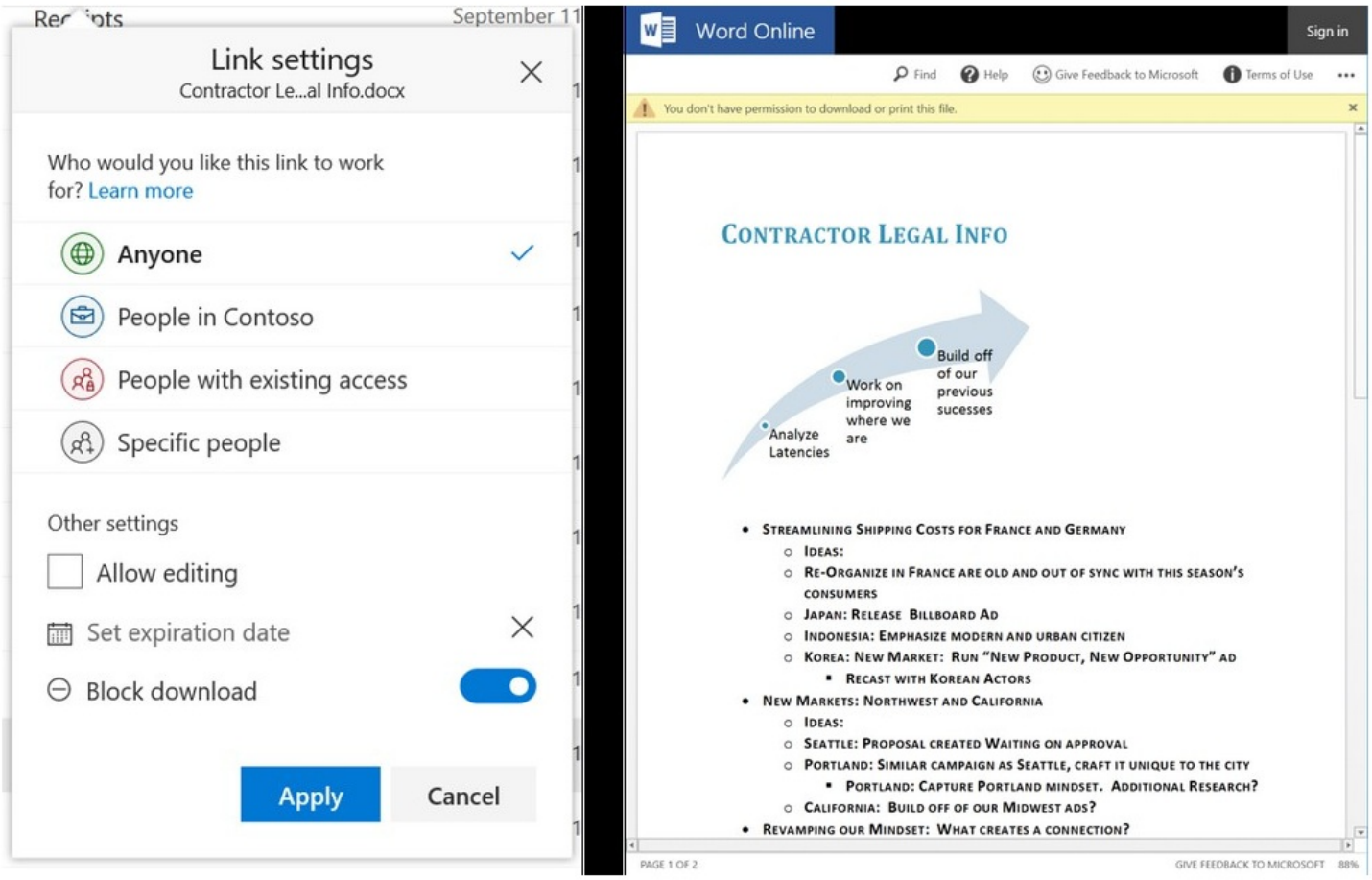
Feature	Exchange Online Protection	ATP Plan 1	ATP Plan 2
Safe Links	No	Yes	Yes
Safe Attachments	No	Yes	Yes
Spoof Intelligence	No	Yes	Yes
Quarantine	Yes	Yes	Yes
Advanced Phishing Capabilities	No	Yes	Yes
Threat Intelligence	No	No	**Yes**

About

- Date - January 11, 2019
- Announced via - Microsoft 365 Roadmap - 45522
- Implications for - Advanced Threat Protection
- See Also - Get Started with Office 365 Threat Intelligence (Microsoft Docs)
- Tagged as - Security

Sharing Links That Block Downloads

Description



Create sharing links in OneDrive and SharePoint in Office 365 that enabling viewing of content, but block the ability for users to download.

Microsoft is adding another tier of sharing link in OneDrive and SharePoint Online: the ability to create a sharing link that grants view-only access and prevents downloading the document. Such a link will force the document to open in Office Online (e.g., Word Online, PowerPoint Online, Excel Online), and will not provide the option to open in the native Office apps or to download the file.

The associated Microsoft 365 roadmap item says this capability is coming in Q1 2019.

Analysis

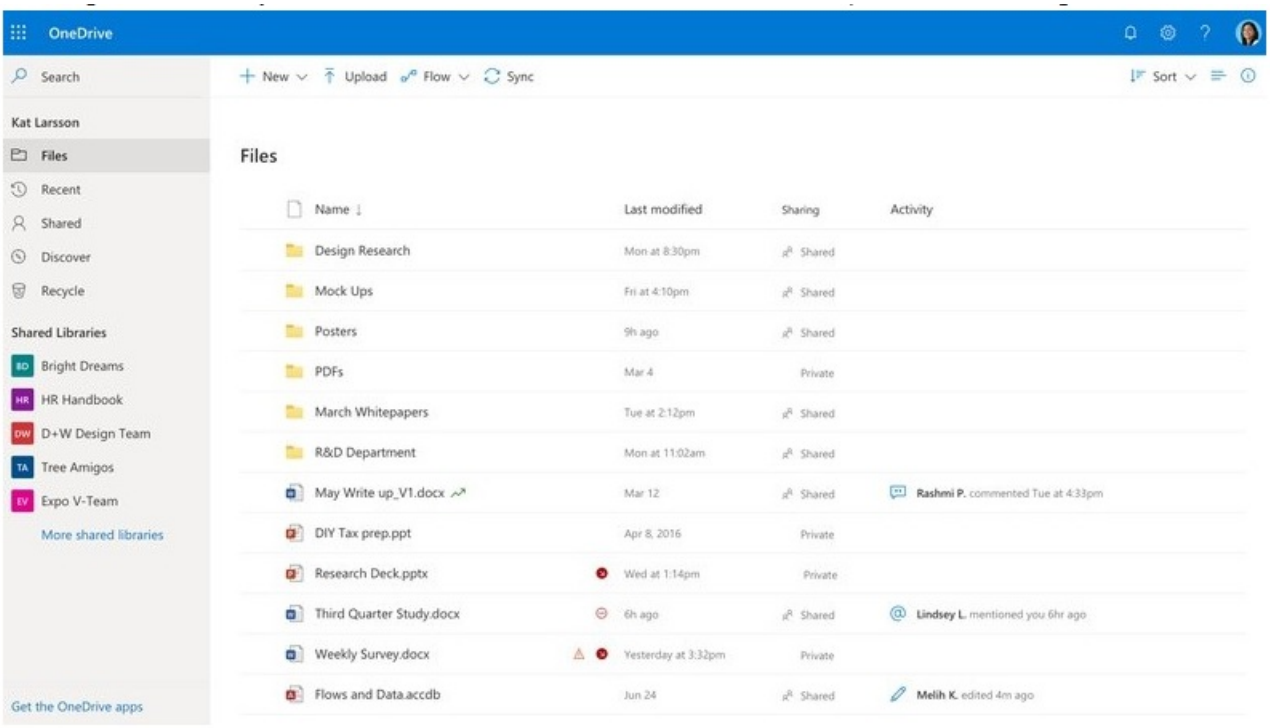
- Both OneDrive and SharePoint Online were originally positioned as places for storing files and collaborating, but clearly there are additional use cases that demand more flexibility in how specific content is shared. Not everyone is a collaborator - that is, requires edit access - and in situations where a user wants to provide the ability for a recipient to read the content while retaining ongoing access control, this new type of sharing link is a good addition to the service.

About

- Date - January 1, 2019
- Announced via - Microsoft SharePoint Community Blog
- See Also - Microsoft 365 Roadmap - 27019
- Implications for - File Sharing - Overview
- Tagged as - File Sharing

OneDrive Gains Fluent Update

Description



The OnDrive user interface updated with Fluent UI brings both an updated look and feel. plus new capabilities.

OneDrive on the web is being updated with the Fluent UI design language, which Microsoft is rolling out across Office 365 apps to provide a more consistent look-and-feel across the platform. Changes to OneDrive on the web that result from the Fluent update include:

- Recommended files - files that may be of interest to the user based on their activity and interests.
- File cards - offer a thumbnail view of a file and access to metadata. Similar to Properties in the Office apps.
- Activity and lifecycle feedback on documents - comments, edits and @mentions within files
- Shared libraries - libraries shared from SharePoint sites

Analysis

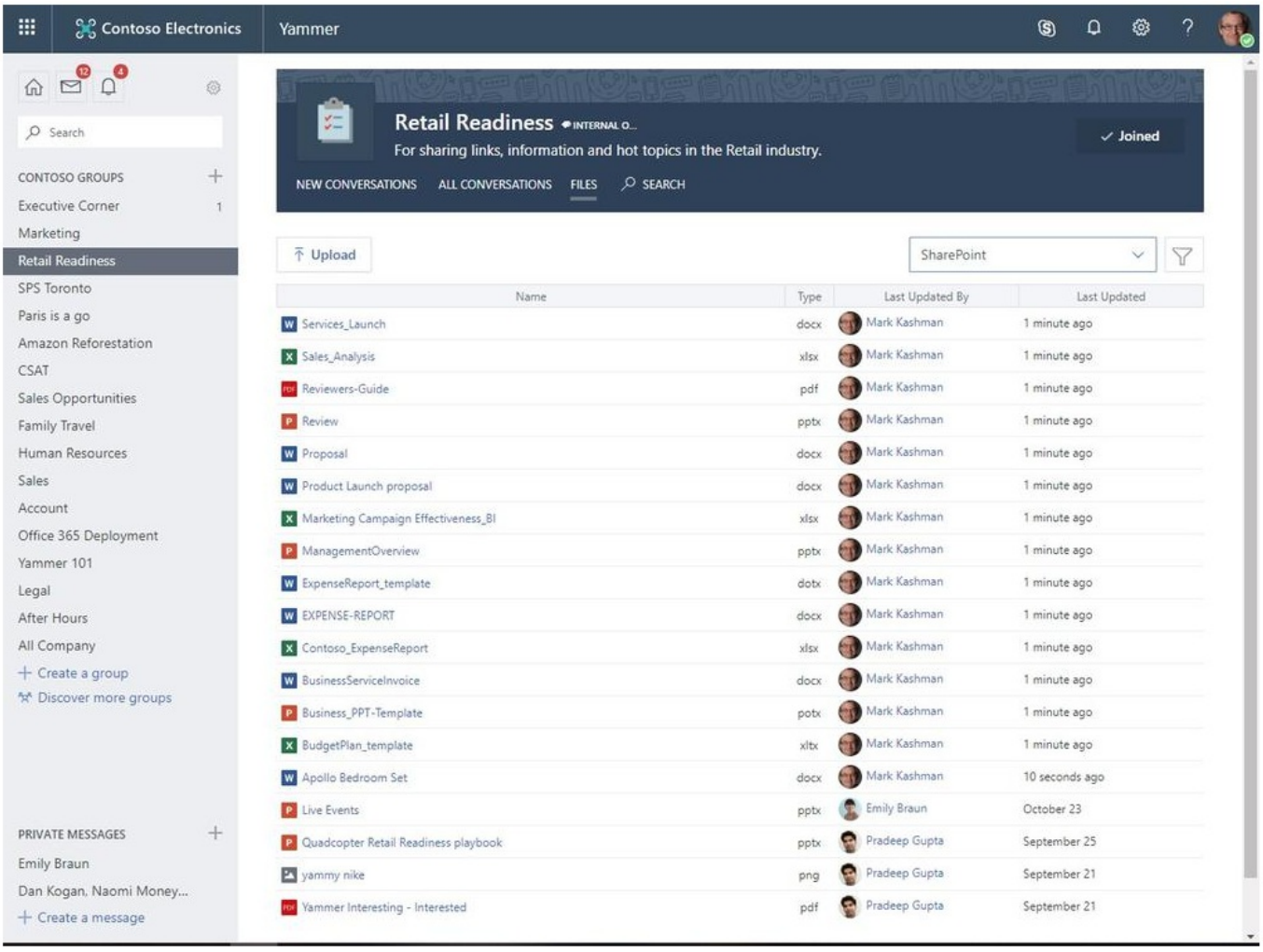
- Each of the changes associated with the Fluent UI offer reasonable and stepwise improvements. They all make sense in making OneDrive a more effective work place.
- Surfacing activity and lifecycle feedback is one of the more significant changes, because it displays the momentum and cadence happening within a document without having to open and check what's going on. Users gain a better sense of current action within a document, and can decide whether to engage directly or not. The broader explanation of what happened within the document adds more contextual cues than just the last modified date and time.

About

- Date - January 1, 2019
- Announced via - Microsoft SharePoint Community Blog
- Implications for -
- Tagged as - File Sharing

New Files in Yammer Stored in SharePoint

Description



Files uploaded to Yammer groups and conversations will be stored in the connected SharePoint document libraries.

Microsoft announced that new files uploaded to a Yammer group will now be stored in SharePoint Online, as long as the Yammer group is connected to an Office 365 Group. Until now, files uploaded to Yammer have been stored in the Yammer service.

Yammer groups with existing files have some work ahead, because existing files stored in the Yammer service will be marked as read only, and there is no automated migration service available from Microsoft to re-house existing files in SharePoint Online. For any file that requires ongoing editing, a group member is expected to download the file and then re-upload it into the Yammer group so that it is stored in SharePoint Online.

Analysis

- It has taken Microsoft far too long to integrate Yammer with the rest of the Office 365 service stack, and the housing of files in SharePoint Online is but one example. This is long overdue, and is a welcomed change.
- Microsoft's slow pace of innovation with Yammer made many people question whether Microsoft was serious about the service. There has been a revival of interest in Yammer within Microsoft over the past 12-18 months.
- Storing files in SharePoint Online enables the organization to meet its security and compliance obligations, since Office 365 capabilities like Data Loss Prevention, Sensitive Information Types, Azure Information Protection, and more will be able to be used against SharePoint Online housed files.
- Yammer is only included in an Office 365 Group if the new group is created from Yammer. Creating a new Office 365 group from Outlook, for example, will not include Yammer in the stack. This disparity seems shortsighted and wrongfooted.

About

- Date - January 1, 2019
- Announced via - Microsoft SharePoint Community Blog
- See Also - Yammer and Office 365 Groups
- Implications for -
- Tagged as - File Sharing

No More Tenant-Level Opt-Out of Modern SharePoint

Description

Microsoft announced that from April 1, 2019 (and it's not an April Fools joke), the ability to opt-out via a tenant-level setting of the modern design experience for SharePoint Online lists and libraries will be deprecated. The modern design was introduced in 2016, with customers having the ability to opt-out entirely at a tenant-level, thereby retaining the "classic mode" of SharePoint for lists and libraries. In an effort to "*make it easier for users to get to our latest features*," this change will prevent an Office 365 administrator from holding back the modern design with a single switch.

While the ability to opt-out entirely at a tenant-level is being removed, several (harder) options remain:

- Using PowerShell, an administrator can opt-out a single site collection or site, or a collection of these.
- Using List Settings within a SharePoint site, a list owner can opt-out of the modern design.
- Using a toggle switch within a modern view, the end user can switch back to the classic mode.

Lists and libraries that have customizations not supported by the modern design experience will be automatically set to classic mode.

Microsoft offers the SharePoint Modernization scanner to help customers assess the impact of the switch between modern and classic experiences.

Analysis

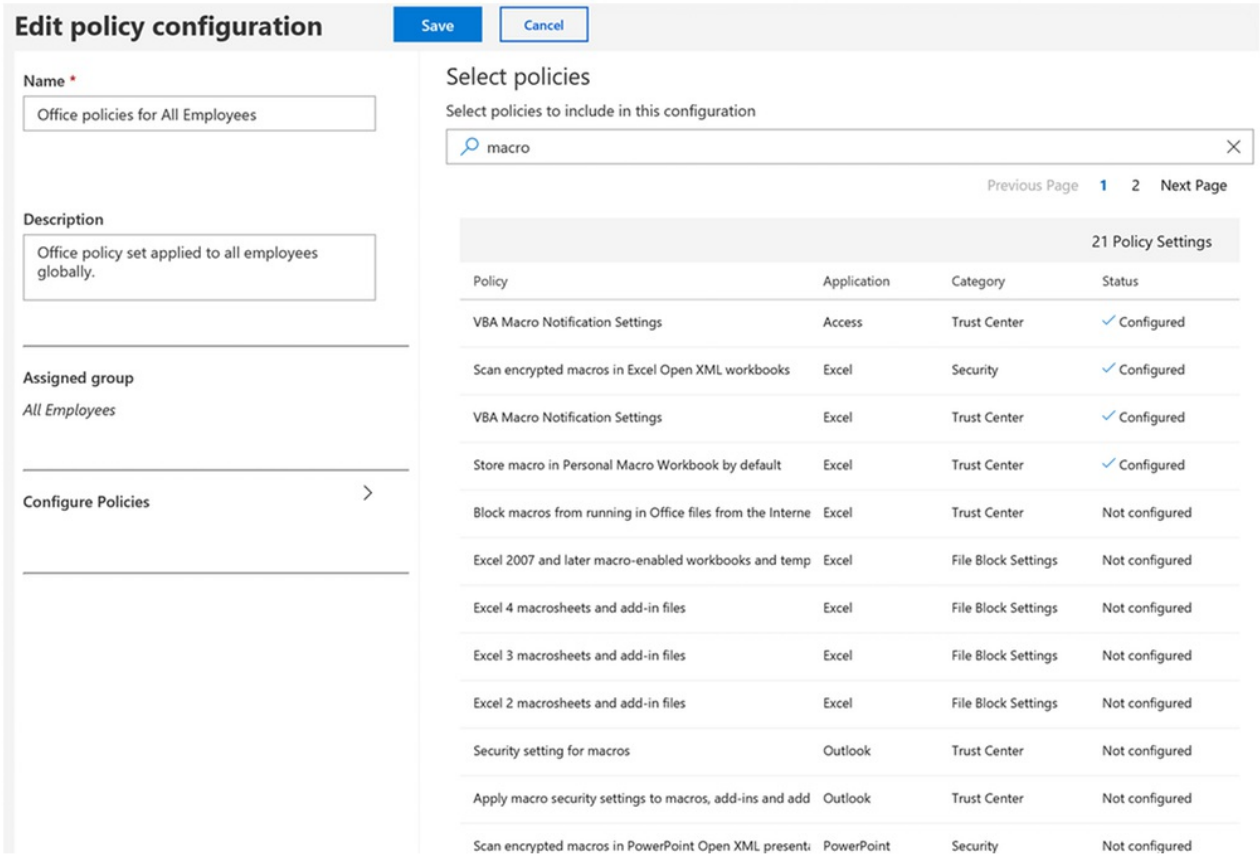
- Microsoft continues dancing around the core issue of the identify of their customer. Is their customer the Office 365 administrator who manages the Office 365 tenant, or does Microsoft have a direct relationship with each end user within a tenant and can therefore specify what they can and cannot see (and use)? If the customer is the Office 365 administrator, Microsoft's role is to make improvements available for opt-in, but forcing improvements through to the end user is overstepping their rights. Adding complexity to this issue is that the answer may be different by workload - Office apps are frequently updated with forced capabilities that impact the end user directly.
- Perhaps foreseeing a firestorm of complaint from its customer base, Microsoft issued the news through a blog post on TechCommunity that is closed to comments.

About

- Date - January 15, 2019
- Announced via - The SharePoint Community Blog
- See Also - Getting Started with the SharePoint Modernization Scanner
- Implications for -
- Tagged as - File Sharing

Policy Service for Office 365 ProPlus

Description



Microsoft released a new policy configuration service for Office 365 ProPlus, the version of the installed Office apps that is included with the Enterprise E3 and E5 Office 365 plans. The service enables an administrator to define policies on over 1600 policy options, and have these enforced when a user logs in using an Azure AD account. The service does not require the use of Microsoft Intune or mobile-device management services.

The specifics are:

- The service only works with Office 365 ProPlus. It does not work with other versions, such as Office 2019 and Office 365 Business.
- A policy is assigned to a security group in Azure AD. This group can be synced from on-premises Active Directory.
- New policies items are automatically added to the pool of available policy settings, although new policy items are added as "Not configured."
- Policy settings are enforced on Office 365 ProPlus. This is a step beyond setting initial configurations and preferences that the user can change, which is what the Office Customization Tool provides.
- Only requires Office 365 ProPlus, or in other words, does not require that the machine is joined to a domain. The service works with both managed and unmanaged devices - it is on Office 365 ProPlus that the policies are enforced.
- Creating and viewing policy configurations is available to an Office 365 Global Admin, Security Admin, or Desktop Analytics Admin.

[**April 2019**] Office Cloud Policy Service was released to General Availability on April 23, 2019. See Weekly News Drop.

Analysis

- Configuring security related policy items provides another line of defense against security threats in the organization, reducing the possible attack surface at a policy level.
- Currently only works with Office 365 ProPlus, and is thus limited to Windows PCs. As long as an organization only has Office 365 ProPlus in deployment this is not an issue. It becomes more of an issue if there are different versions of Office in use

across a heterogeonous device footprint.
- It is not possible to exclude a group from a policy; this is, you can't create a policy that is applied to All Employees except for members of the Security Team.

About

- Date - January 9, 2019
- Announced via - Office 365 Blog
- See Also - Overview of the Office client policy service (Preview) for Office 365 ProPlus
- Implications for -
- Tagged as - Security

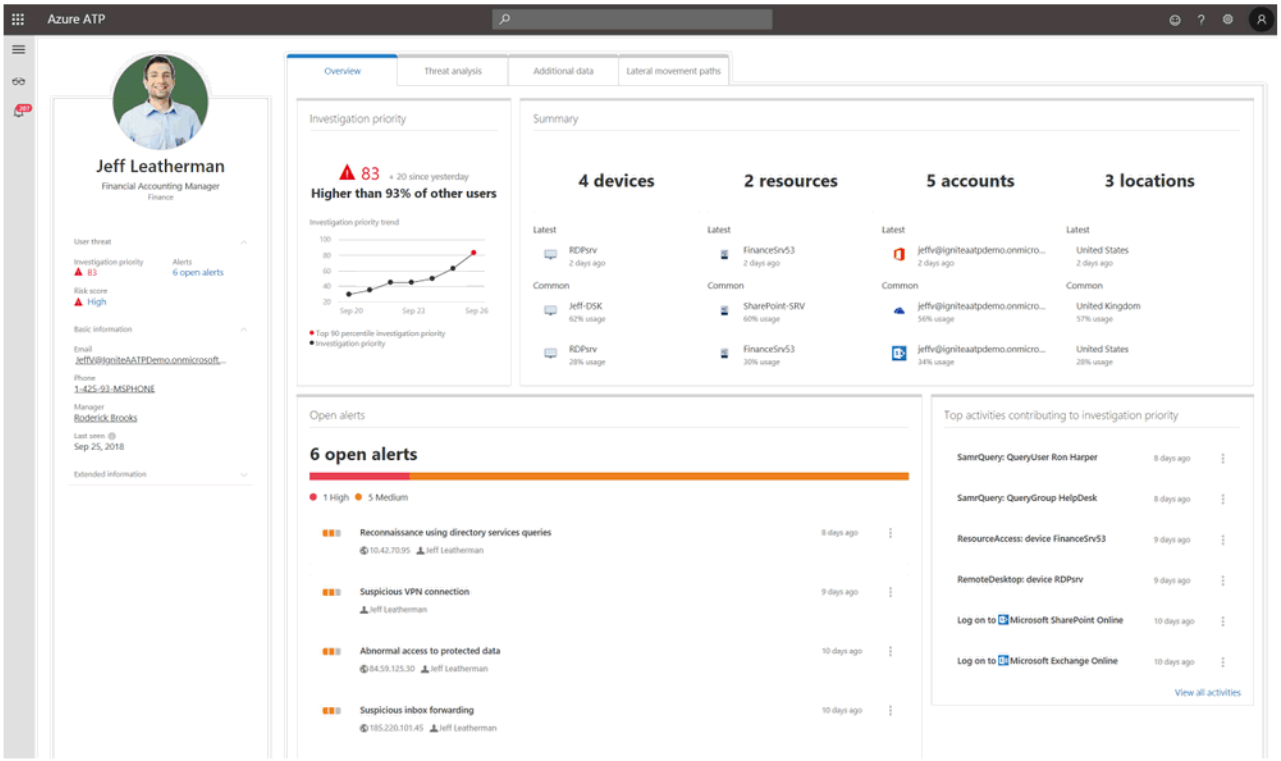
Weekly News Drop - January 18, 2019

[Editor's note: I have been thinking about how to cover more of the Office 365 news each week. This new feature - the Weekly News Drop - is designed to capture the wider changes that don't require their own Update post. I hope you find it useful. As always, feedback is welcomed.]

Roundup of recent Office 365 news:

- **Threat Playbooks for Automated Investigations**. Microsoft is developing an extension for Threat Explorer, due for release in Q2 2019 (April-June 2019). The new extension will introduce threat playbooks that can be triggered automatically when a threat is detected. A playbook provides step-by-step guidance on how to respond to and mitigate a new threat, some of which will require a security analyst and some of which will be triggered automatically (for investigation and gathering insight). See Auto-Investigation with Threat Playbooks (Microsoft 365 Roadmap, January 2019).
- **Windows 7 End of Support**. Support for Windows 7 ends on January 14, 2020, with support for Office 2010 not far behind. Microsoft is encouraging businesses to upgrade to Windows 10 and Office 365 ProPlus. See 2019 is the year to make the shift to a modern desktop (Microsoft 365 Blog, January 2019).
- **Cloud Access Security Broker (CASB) Status and Market Share**. Microsoft said that two analyst firms continue to be impressed with its full CASB - Microsoft Cloud App Security - and that according to Microsoft's internal analysis, Microsoft has 30% of the CASB market currently. Gartner moved Microsoft from the Niche Players quadrant to the Challengers quadrant in its latest Magic Quadrant for Cloud Access Security Brokers, and KuppingerCole ranks Microsoft as a market leader (behind Symantec). See Microsoft gains strong customer and analyst momentum in the Cloud Access Security Brokers (CASB) market (Microsoft Secure, January 2019).
- **No Data Centers in Africa in 2018**. In mid-2017 Microsoft announced that it would open two data centers in South Africa before the end of 2018. It missed its deadline, due to the complexity of doing so, but is apparently still committed to the location and is now saying that 2019 is the year. See Microsoft Misses Deadline for African Data Centers (Petri, January 2019).
- **Windows 10 Mobile End of Life**. Support for Windows 10 Mobile ends on December 10, 2019. Microsoft will not release any further hotfixes or security updates after this date. Microsoft recommends that Windows Mobile users shift to iOS or Android. See Windows Phone users: Your reminder that support ends in December 2019 (ZDNet, January 2019).

Azure Advanced Threat Protection



Description

- A cloud service in Azure for detecting and investigating advanced attacks and insider threats across users, servers and endpoints - in the cloud and on-premises. Azure ATP provides protections in the cloud and for on-premises servers, endpoints and user accounts in Active Directory.
- Aggregates and correlates activity and security signals to create a behavioral profile for each user. Relies on multiple data sources, including group members and permissions, network traffic, event logs, VPN data, IP address (for location signals), and more. Uses multiple methods for identifying suspicious user and device behavior, including known-technique detection and behavioral analytics. For example, if a user account is used to log in using a previously unseen device from a previously unvisited location, the risk of a compromised user account is quite high.
- Receives signals from Windows Defender ATP with data on specific actions taken on an endpoint. A SecOps analyst can pivot from Azure ATP to Windows Defender ATP to investigate a specific device.
- Provides proactive recommendations on identity configurations and security settings to reduce the potential attack surface.
- [**September 2018**] Integrates with Azure AD Identity Protection, which adds activity and security signals from Azure AD. The combined service - Azure ATP with Azure AD IP - enables the calculation of an overall risk score on a user-by-user basis, which in turn can be leveraged by SecOps analysts in prioritizing mitigations for users and risk situations. For example, in the screenshot above, Jeff has a risk score that is 93% higher than all other users in the firm.
- [**September 2018**] Microsoft claims that Azure ATP is protecting "millions of users" at organizations worldwide.

Analysis

- The concept of a risk-based user profile across multiple signals is an idea that shows up in the capabilities of Cloud Access Security Brokers (CASB) of third-party vendors. It is not something that is available in Office 365 Cloud App Security or Microsoft Cloud App Security, the two CASBs on offer from Microsoft. Azure ATP offers this complementary view of user risk, albeit in a separate service.

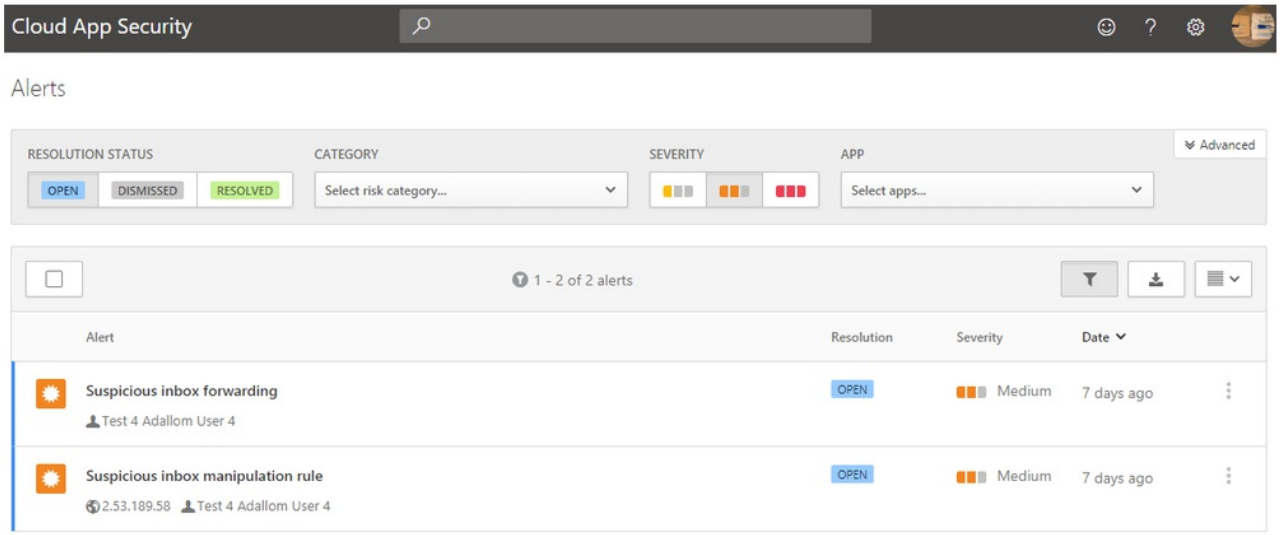
About

- Date - September 26, 2018

- Source - Enterprise Mobility + Security Blog
- See Also - What is Azure Advanced Threat Protection?
- Implications for - Azure Advanced Threat Protection
- Tagged as - Azure, Security

New Rules in Microsoft Cloud App Security

Description



Microsoft added two new detection rules to Microsoft Cloud App Security to detect malicious activities within a user's inbox. The two rules alert on suspicious behavior due to inbox forwarding and inbox manipulation rules that could indicate that the user's account has been compromised. The two policies are:

- **Suspicious inbox forwarding**. Examines rules set in Exchange Online mailboxes, and triggers an alert when an inbox forwarding rule is set on a user's inbox. Such rules can be used to exfiltrate information to an external mailbox, providing an attacker with both valuable data (a data breach situation) and insight into further access and compromise opportunities (for example, how to access another system or device).
- **Suspicious inbox manipulation rule**. Looks for rules that automatically move certain messages out of a user's inbox and hide them in infrequently used folders. Such rules look for keywords that could alert the actual mailbox owner that their mailbox has been compromised, thereby hiding the malicious activities being undertaken through the mailbox.

The two rules are also available in Office 365 Cloud App Security, the cut-down version of Microsoft Cloud App Security that is available in Office 365 Enterprise E5 or as an add-on to other plans.

Analysis

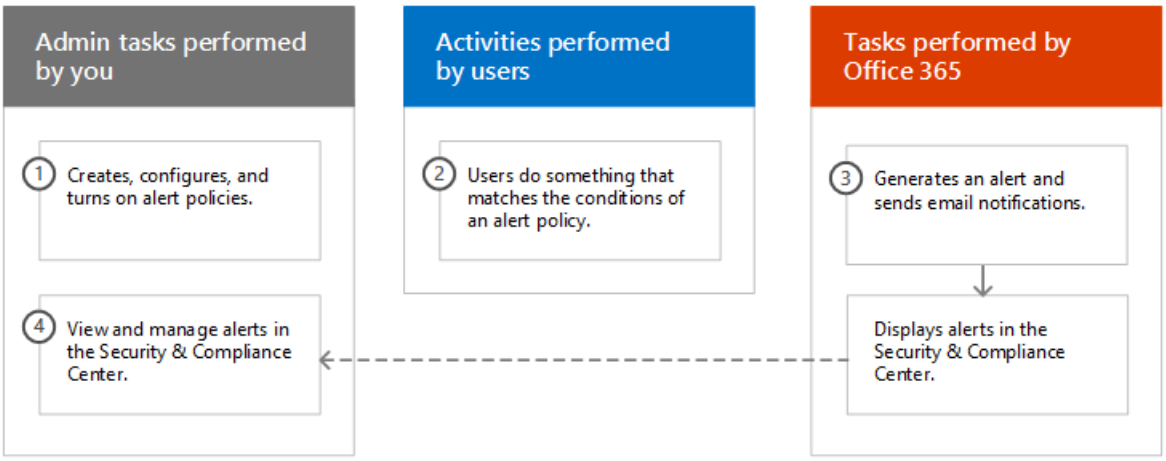
- Since inbox rules can be created and hidden from the user, having a separate line of defense that pays attention to what is happening - visible and invisible - is essential. Both of these rules are important and valuable, and represent a good addition to the baseline detection policies created in both versions of Cloud App Security.

About

- Date - December 13, 2018
- Announced via - Enterprise Mobility + Security
- Implications for - Microsoft Cloud App Security, Office 365 Cloud App Security
- Tagged as - Security

Role-Based Access Control to Alerts in Office 365 Security & Compliance Center

Description



Microsoft is adding a level of nuance to the role-based access control model for accessing alerts in the Office 365 Security & Compliance Center. Currently any user with the ManageAlerts or ViewOnlyManageAlerts roles can see all alerts generated from all of the security and compliance capabilities in Office 365. This means that users see many more alerts than they need for their job role, which only creates confusion, noise and distraction.

After the change, the role held by a user will flow through to the category of alerts they have access to. Only alerts relevant to their role will be displayed. In the new design, the role assigned to a user defines the category of alerts they can view. For example (these are Microsoft examples):

- Members of the Records Management role group can view only the alerts that are generated by alert policies that are assigned the **Data governance** category.
- Members of the Compliance Administrator role group can't view alerts that are generated by alert policies that are assigned the **Threat management** category.
- Members of the eDiscovery Manager role group can't view any alerts because none of the assigned roles provide permission to view alerts from any alert category.

Analysis

- Reducing noise and distraction from role-irrelevant notifications is a good refinement to introduce to the Office 365 Security & Compliance Center. It also plays to the need of organizations to strengthen their approach to data protection, part of which is not providing too wide an access remit to data.
- Restricting the ability to create alert policies to someone knowledgeable in the specific security or compliance area prevents an well-intentioned but uninformed administrator from setting up the wrong policies. It is unclear whether the role-based access control change for viewing alerts by role also extends to creating alert policies by role.

About

- Date - January 17, 2019
- Announced via - Office 365 Message Center MC172220
- See Also - Alert Policies in the Office 365 Security & Compliance Center
- Implications for -
- Tagged as - Security

DLP and Windows Defender ATP

Description

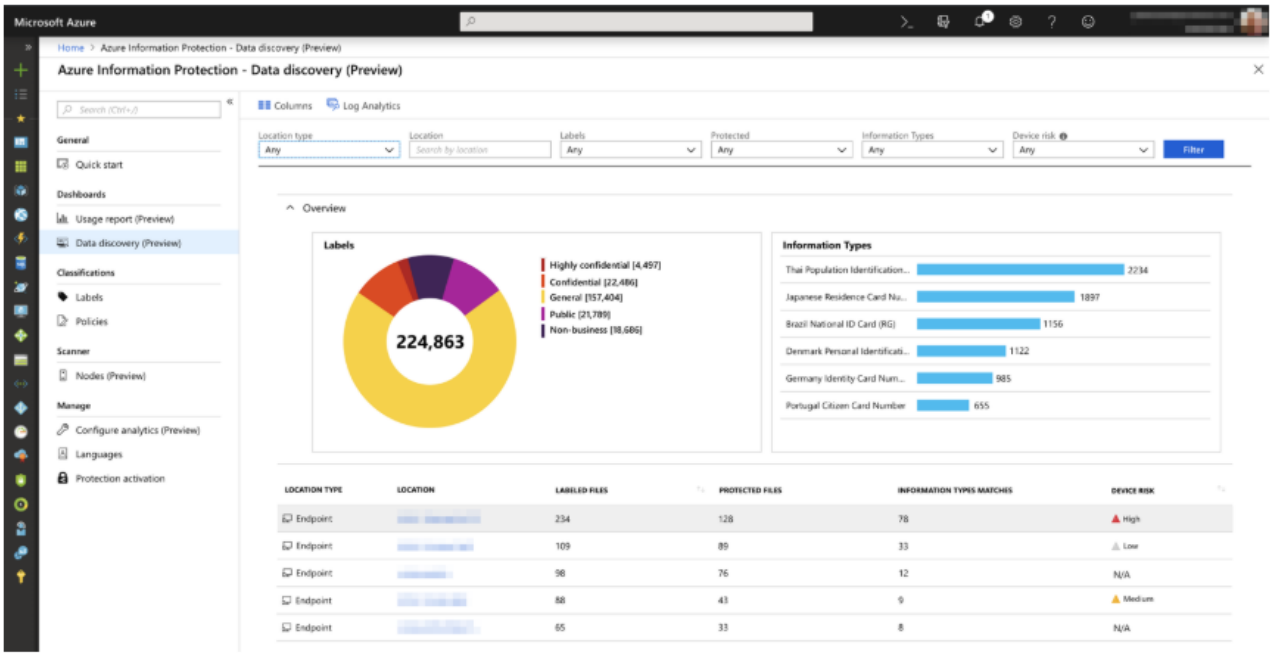


Figure 1. Azure Information Protection – Data discovery dashboard shows data discovered by both Windows Defender ATP and Azure Information Protection

Microsoft talked about the integration between Windows Defender ATP - its endpoint protection platform for Windows - and services in Office 365 and Microsoft 365. Integrations include:

- Sensitivity labels configured in the Security & Compliance Center (or Azure Information Protection) are understood by Windows Defender ATP. When sensitive content - such as a labeled document - is identified by Windows Defender ATP, the presence of the document is signaled to Azure Information Protection for aggregated reporting.
- Additionally, the presence of sensitive content is signaled to the Windows Defender Security Center, which in turns calculates a composite data sensitivity ranking for each device. This can be used by a SecOps analyst in prioritizing mitigations across the fleet of endpoints after a security incident or data breach.
- Sensitivity labels can be configured with endpoint DLP protection, meaning that a Windows Defender ATP-enabled endpoint will enforce the protections defined for the content. Specifically, this means protected files can't be opened by unauthorized client apps, stored in unauthorized cloud apps, or stored in unauthorized network locations. Protections are enforced by Windows Information Protection.

Analysis

Microsoft is lining up its capabilities to deliver an end-to-end security and data loss protection / prevention chain.

- Endpoints receive policy settings from cloud services, and in turn feed policy matches back to the cloud service.
- Cloud services consume updates from endpoints, and use these update signals for prioritization in decision making.
- Microsoft's chain works only within an end-to-end Windows ecosystem. While sensitivity labels can be applied on macOS, Android and iOS devices, Windows Defender ATP and Windows Information Protection are not available on those platforms.

About

- Date - January 17, 2019
- Announced via - Microsoft Secure
- Implications for - Sensitivity Labels, Azure Information Protection
- Tagged as - Data Loss Protection

Weekly News Drop - January 25, 2019

[Editor's note: I have been thinking about how to cover more of the Office 365 news each week. This new feature - the Weekly News Drop - is designed to capture the wider changes that don't require their own Update post. I hope you find it useful. As always, feedback is welcomed.]

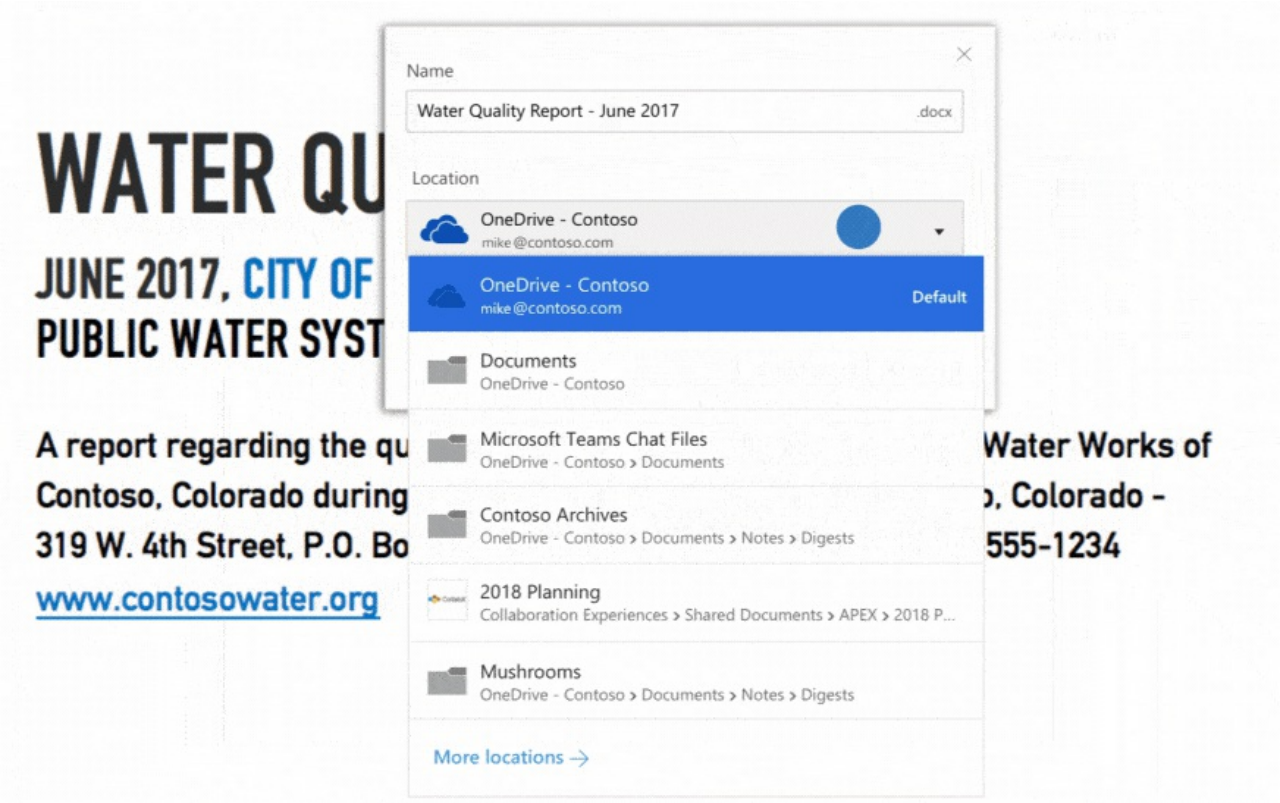
Roundup of recent Office 365 news:

- **Power Platform in 2019**. Power BI (analytics), Flow (workflow automation) and PowerApps (application development) are three apps included in some Office 365 plans. But they have a wider contribution too. Together they are known as the "Power Platform." The three apps are increasingly important across Microsoft for extending and leveraging capabilities in Dynamics 365 and Microsoft 365, in response to the explosion of sensors that deliver data which can be used to proactively address customer requirements. See Why Microsoft's 'Power Platform' is one of the biggest bets for 2019 and beyond (ZDNet, January 2019).
- **Personal Account Sign-In Options**. For users logging into Office 365 with a personal Microsoft account, additional login options will be available from mid-February 2019; does not apply to work- or school-issued Office 365 credentials. GitHub will be the first alternative account to be supported, followed by LinkedIn and other undefined sign-in options in the coming months. See Microsoft 365 Roadmap 45516 and Message Center Update (January 2019).
- **Outlook Web App Updates**. Microsoft is continuing to gradually release new features to the "it's coming soon" version of Outlook Web App. New features include the ability to schedule a Microsoft Teams meeting from a meeting invite, dark mode, and a changed default when composing a new email so that encrypting a message applies the Encrypt Only template rather than the Do Not Forward one. This third change is not noted in the article. See New OWA Maturing in Different Ways (January 2019).
- **Lululemon and Azure AD**. Case study write-up of lululemon's adoption of Azure AD over the past 5+ years. Single sign-on has been welcomed by the user population (since it delivers a much improved user experience than without it), over 200 apps are now linked to Azure AD for identity and authentication, and the adoption of risk-based multi-factor authentication for lululemon's 18,000 employees was easier than expected. There is no mention of lululemon using Microsoft Cloud App Security as well, but [1] they probably are since they have Enterprise Mobility + Security, and [2] the visibility of security events across multiple cloud services is becoming essential. See Azure AD helps lululemon enable productivity and security all at once for its employees (Microsoft Secure, January 2019).
- **Exchange Online Outage in Europe on January 24**. Users in parts of Europe were unable to access Exchange Online on Thursday January 24, due to some domain controllers in Azure AD becoming unresponsive. Some affected users said they were without access to Office 365 for at least 7 hours during their business day. See Office 365 Outage is Blocking Access to Mailboxes (Petri, January 2019).

- **Office 365 Available re App Store for Apple Mac**. Microsoft added Office 365 for Mac to the Mac App Store, enabling Mac customers to download Office 365 directly from Apple rather than separately from Microsoft. The download covers Word, Excel, PowerPoint, Outlook, OneNote, and OneDrive. New users can activate an Office 365 subscription within the Office for Mac apps. Office 365 apps have previously been available in the iOS App Store, but not the Mac edition. See Office 365 for Mac is available on the Mac App Store (Microsoft 365 Blog, January 24, 2019) and The Mac App Store welcomes Office 365 (Apple Newsroom, January 24, 2019).

Streamlining Files to the Cloud

Description



Microsoft announced that a new default file save experience is coming in February 2019, so that Office 365 documents will default to saving in OneDrive or SharePoint Online, rather than a user's device. The default behavior applies to Word, Excel and PowerPoint documents on Windows and Mac.

The new default file save experience is another example of Microsoft trying to get as much content stored in Office 365 as possible. Other examples are:

- **Known Folder Move**. Key end user folders on a device are moved from device-local storage to storage in OneDrive. Known Folders include Desktop, Documents and Photos.
- **OneDrive Files on Demand**. Offers a way of actively managing which files are downloaded and stored on a device. While all folders and files in OneDrive are displayed when looking at the OneDrive folder on a device, only requested files and folders are synchronized. This means users can have a very large OneDrive folder in Office 365 (e.g., 1 TB of documents), and while all files and folders are displayed as being present, only ome files and folders are actually synced to the user's device. This protects data from loss, reduces network bandwidth requirements, and allows users to work with devices that have small local storage options (e.g., 128 GB or 256 GB).

Analysis

- Content stored in Office 365 can be more easily shared with co-authors, collaborators, and clients. Real-time co-authoring, sharing links, and more do not work with documents stored on endpoints.
- Content stored in Office 365 is available for Files Restore, eDiscovery searches, DLP scans, and more. The security and compliance capabilities in Office 365 don't work with content beyond Office 365, so getting as much as possible into the service aligns with Microsoft's wider investments in information governance for customers.
- It is unclear whether the default location for saving new files is configurable by the tenant administrator, either on a global tenant basis or group-by-group.

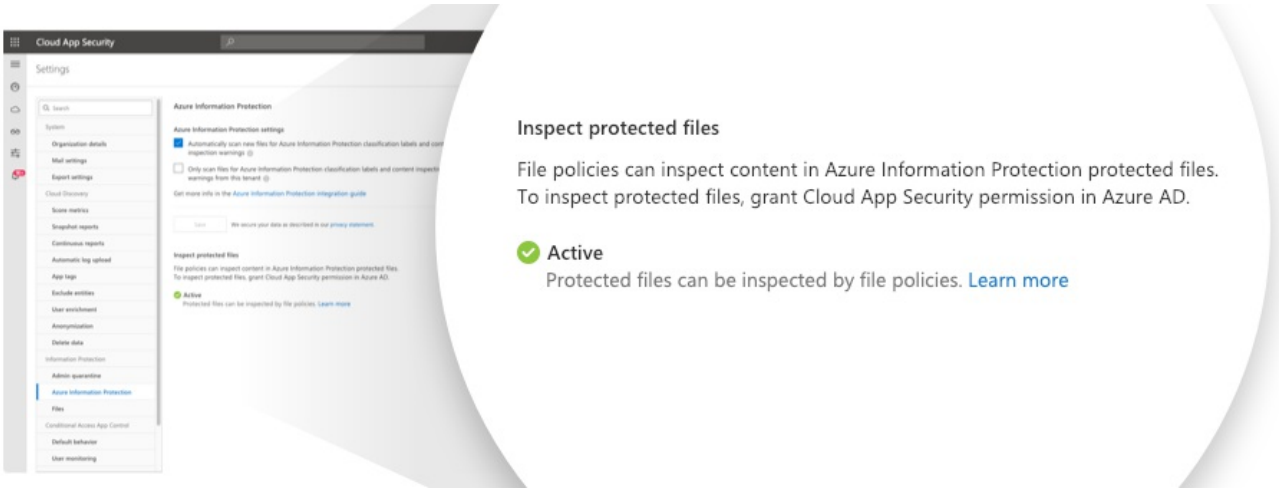
About

- Date - January 25, 2019

- Announced via - Office 365 Blog
- Implications for - File Sharing - Overview
- Tagged as - File Sharing

Inspecting Encrypted Files with Microsoft Cloud App Security

Description



Microsoft released a new capability in Microsoft Cloud App Security, which enables the inspection of protected (encrypted) files for sensitive content. The new capability works with files protected by Azure Information Protection, and offers an additional check for data loss irrespective of how the end user has labeled the file using Azure Information Protection. For example, if a user has unintentionally labeled a file as being non-sensitive but the file actually contains sensitive data, Microsoft Cloud App Security can identify that sensitive content is being sent and generate an alert or take action to mitigate the situation.

Analysis

- With the growing ease of applying protection settings and encryption to content in Office 365, there is a corresponding need to ensure encryption isn't used to hide malicious data exfiltration activity and to prevent mistakes in labeling from being identified. The heightened demand for data protection is driving the need to do as much as possible to protect the organization and its members.
- Office 365 Cloud App Security is not covered with this update, because it is not used for DLP and file scanning.

About

- Date - January 29, 2019
- Announced via - Enterprise Mobility + Security Blog
- Implications for - Azure Information Protection, Microsoft Cloud App Security
- Tagged as - Data Loss Protection, Encryption, Security

Updates to Advanced eDiscovery

Description

Microsoft announced the rollout of new capabilities to its Advanced Discovery service, including a new user interface, hold notifications and acknowledgement tracking, working sets, and integrated review and redaction. These new capabilities are intended to empower customers to do more of their eDiscovery workflow tasks directly in Advanced eDiscovery, without having to revert to parallel systems or third-party products.

New capabilities include:

- **Custodian Management**. Notify custodians about legal holds, track which custodians have been notified, and use personalized mail-merge style emails for the initial notification and further escalations and reminders. Actions taken by custodians within data sources can also be viewed and tracked.
- **Case Management**. Setting out a schedule of jobs and sub jobs within a given case, and tracking of progress at both the job and sub job levels. It is unclear whether jobs and sub jobs can be assigned to someone within the case, or are just defined as outstanding tasks to be done.
- **Working Sets**. Search results in an eDiscovery search can change as newly responsive information is located. This is not always helpful, so a working set locks the content in a search result at a particular point in time. An eDiscovery analyst can add more content if desired, but new search results do not automatically update the set.
- **Review and Redact**. Integrates review and redaction capabilities directly into the Advanced eDiscovery interface. eDiscovery analysts can view a variety of file types, and annotate, mark-up, and redact content.
- **Data Investigations**. In limited preview, with limited information available. Offers IT and SecOps teams the ability to search for and take action on specific data, such as confidential information that has been leaked, or an investigation into a data breach. Some remediation capabilities are apparently on offer too.

The new Advanced eDiscovery capabilities are apparently available immediately, and are being actively rolled out to customers.

Analysis

- These updates and new additions reflect a significant upgrade of the capabilities in Advanced eDiscovery. While they are not available in the base eDiscovery capabilities, the addition to Advanced eDiscovery gives Microsoft bragging rights with customers that with the right plan (E5 or an add-on), it is offering the functionality required.
- The additions to Advanced eDiscovery address several of the weaknesses and limitations we have pointed out regarding Microsoft's eDiscovery portfolio. They do not, however, address all of the weaknesses and limitations.

About

- Date - January 29, 2019
- Announced via - Security, Privacy and Compliance Blog
- See Also - Now Do More with Advanced eDiscovery in Microsoft 365 (YouTube)
- Implications for - eDiscovery Workflow
- Tagged as - eDiscovery

New Supervision ("Supervision 2019")

Description

Microsoft released a new Supervision offering in Office 365, for compliance with communications monitoring regulations such as FINRA. Microsoft's announcement has broadened the role of Supervision to support two additional use cases and now includes chat and conversation data from Microsoft Teams.

The new Supervision:

- Is positioned to address three use cases: compliance with communications monitoring regulations, internal communications policy monitoring, and identifying risks in communications. For internal communications policy monitoring, the service is being positioned to help with monitoring acceptable use, ethical standards, and the presence of offensive language. For identifying risks, Microsoft suggests that the service can look for unauthorized communications about confidential projects.
- Extends beyond support for just Exchange Online, adding chats and channels in Microsoft Teams (matching chats are processed into Exchange once every 24 hours; it is not real-time), and third-party communications. Support for third-party data requires that the data is imported into Exchange mailboxes using the standard third-party import service for Office 365.
- Adds a browser-based interface within the Security & Compliance Center for reviewing, tagging, commenting and resolving communications items flagged for review. The add-in for Microsoft Outlook is still available, and Outlook on the web can also be used.
- Works with Microsoft's standard sensitive information types and any custom information types defined by the client.
- All review activities are fully audited.

Analysis

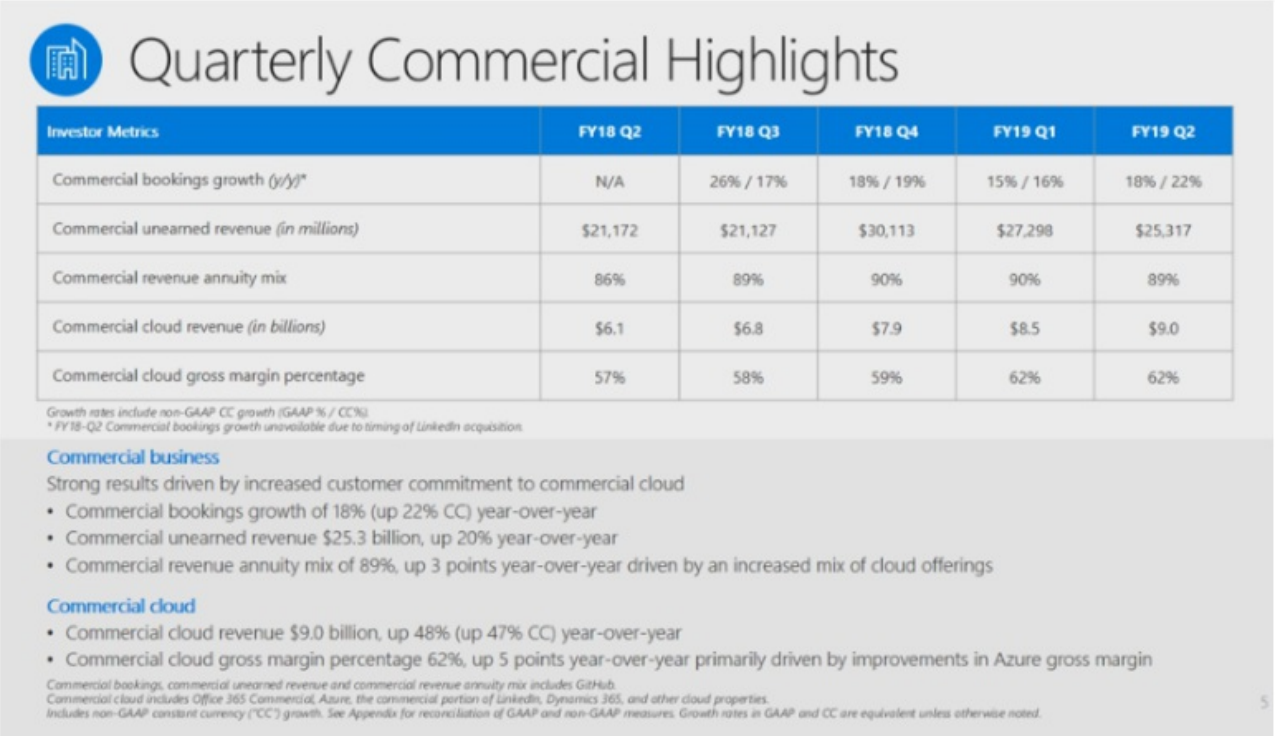
- The previous supervision offering, introduced in May 2017, suffered from some significant weaknesses. Microsoft released no updates to this earlier version of Supervision from May 2017 to late January 2019, indicating a lack of interest and priority in the offering. See Supervisory Review for FINRA.
- Each of the updates in Supervision 2019 are a significant improvement compared to the earlier Supervision offering from 2017.
- The applicability and resonance with customers for the two new use cases for Supervision 2019 remains to be seen. The need for monitoring communications under FINRA is a regulatory requirement, and while the other two suggested use cases are valuable, whether Supervision is used to achieve these remains untested. For example, is supervising the sending of email messages that contain confidential project information the best approach to take, or should this be dealt with using DLP where offending messages can be blocked?

About

- Date - January 29, 2019
- Announced via - Security, Privacy and Compliance Blog
- See Also - Supervision Policies in Office 365 (Microsoft Docs)
- Implications for - Supervisory Review for FINRA
- Tagged as - eDiscovery

Office 365 Market Snapshot - Microsoft's Q2 2019

Description



Quarterly Commercial Highlights

Investor Metrics	FY18 Q2	FY18 Q3	FY18 Q4	FY19 Q1	FY19 Q2
Commercial bookings growth *(y/y)**	N/A	26% / 17%	18% / 19%	15% / 16%	18% / 22%
Commercial unearned revenue *(in millions)*	$21,172	$21,127	$30,113	$27,298	$25,317
Commercial revenue annuity mix	86%	89%	90%	90%	89%
Commercial cloud revenue *(in billions)*	$6.1	$6.8	$7.9	$8.5	$9.0
Commercial cloud gross margin percentage	57%	58%	59%	62%	62%

Growth rates include non-GAAP CC growth (GAAP % / CC%).
** FY18-Q2 Commercial bookings growth unavailable due to timing of LinkedIn acquisition.*

Commercial business

Strong results driven by increased customer commitment to commercial cloud

- Commercial bookings growth of 18% (up 22% CC) year-over-year
- Commercial unearned revenue $25.3 billion, up 20% year-over-year
- Commercial revenue annuity mix of 89%, up 3 points year-over-year driven by an increased mix of cloud offerings

Commercial cloud

- Commercial cloud revenue $9.0 billion, up 48% (up 47% CC) year-over-year
- Commercial cloud gross margin percentage 62%, up 5 points year-over-year primarily driven by improvements in Azure gross margin

Commercial bookings, commercial unearned revenue and commercial revenue annuity mix includes GitHub.
Commercial cloud includes Office 365 Commercial, Azure, the commercial portion of LinkedIn, Dynamics 365, and other cloud properties.
Includes non-GAAP constant currency ("CC") growth. See Appendix for reconciliation of GAAP and non-GAAP measures. Growth rates in GAAP and CC are equivalent unless otherwise noted.

5

Microsoft announced its market performance numbers for Q2 of the 2019 fiscal year. As with last quarter, strong results were posted for Office 365 commercial, Dynamics 365, Surface, and more. Specifically:

- Revenue for the quarter was $32.5 billion, with a net income of $10.3 billion. This was an increase of 18% compared to a year ago.
- Microsoft did not release a revised number of monthly active users for Office 365 commercial, but did say that revenue for the segment was up 34% compared to a year ago. The last official number is 155 million from October 2018. Based on some Excel magic using the numbers Microsoft supplied in its earnings announcement, we believe the number has increased to 162 million.
- Consumer users of Office 365 grew to 33.3 million, only slightly higher than 32.5 million in the first quarter.

Analysis

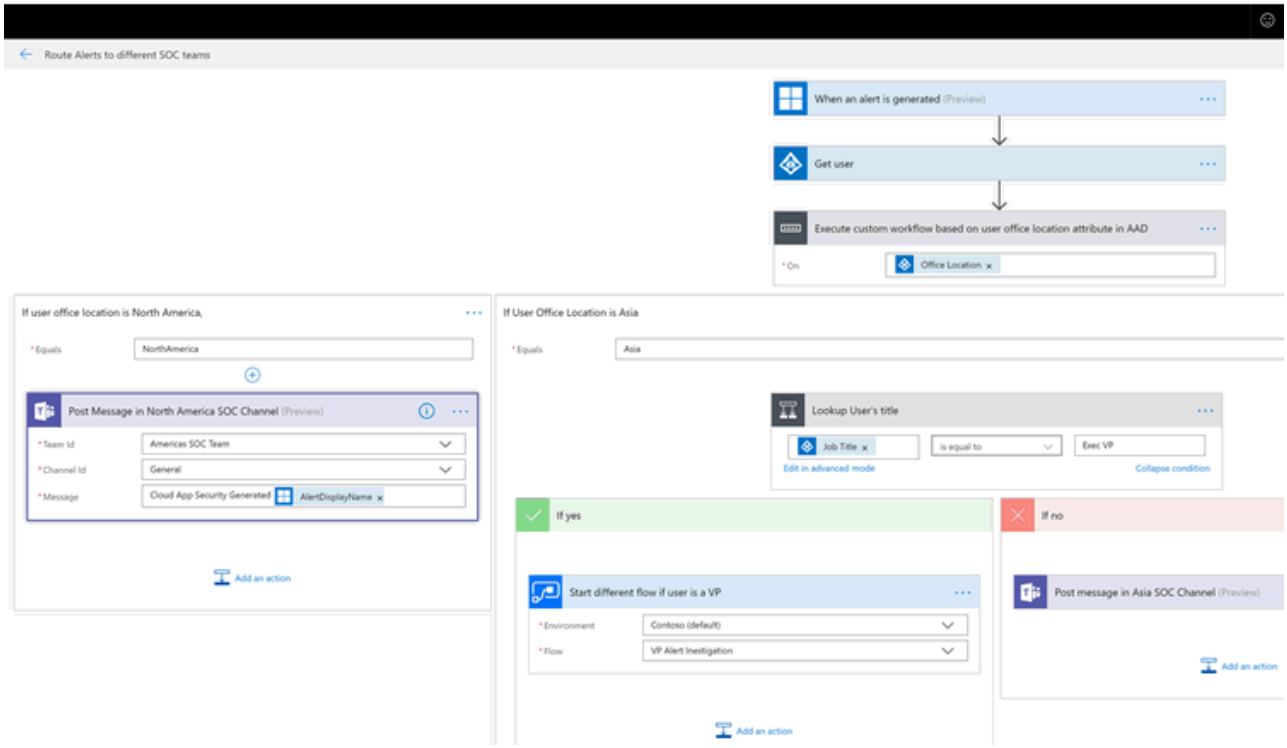
- Microsoft is still returning strong growth numbers for Office 365. It claimed that revenue growth was 34% year-on-year, which is partly due to net new Office 365 subscribers, and partly due to selling more expensive plans.
- There was no breakdown of Office 365 subscribers versus Microsoft 365 subscribers. With Microsoft including key capabilities in its cloud offerings beyond Office 365 that are included in Microsoft 365, it is fair to expect that Microsoft's revenue for commercial cloud offerings still has a good growth opportunity. In other words, while the growth in actual subscriber numbers will slow down, Microsoft's push to Microsoft 365 is an attempt to increase the per user revenue rate.

About

- Date - January 30, 2019
- See - Microsoft Investor Relations
- See - Microsoft Q2 Strong Amid Commercial Cloud Revenue Surge to $36 Billion Annual Run Rate (ZDNet)
- Implications for - Office 365 - Overview

Security Workflows with Microsoft Flow

Description



Microsoft added an option to Office 365 Cloud App Security and Microsoft Cloud App Security to instantiate a security workflow in Microsoft Flow when an event matches a policy and an alert is required. Options were previously limited to an email and/or text message alert. The integration with Microsoft Flow creates many new possibilities for intelligent routing, approvals for action, and automated enforcement. Microsoft outlined five security workflow ideas:

- **Differential Routing of Alerts**. Allocate alerts to different SecOps teams ased on attributes of the alert, such as the office location of the affected user. The office location can be returned using a lookup of the employee's name against Azure AD, and the alert allocated to a work queue in Microsoft Teams or something similar. Nested logic in alternative workflow paths can result in different workflows being used based on the identity, role, or other attribute of the user.
- **Requesting Approval for Actions**. While a SecOps analyst can view an alert in Microsoft Cloud App Security, they will generally know nothing about the affected employee, their travel schedule, and any special deviations from their normal baseline of activity (for example, rushing to another country to attend a family funeral). Integration with Microsoft Flow means that an alert on "Activity from infrequent country," for example, can be routed to the employee's manager to request input on what action to take.
- **Ticket Generation**. Route alerts to a service management system like ServiceNow or Jira, thereby integrating Cloud App Security alerts with other tickets and incidents.
- **Confirm User Activity**. Send a text message or email message to an employee when an alert is raised, requesting confirmation of their activity. This workflow will need to be designed with care, because [1] if the employee's account has been compromised, the attacker could confirm the invalid activity and thus keep it hidden, or [2] it could tip off an employee with malicious intent that their activity is being monitored, and give them a way of keeping it hidden by rejecting the alert.
- **Create Firewall Rules**. When an unsanctioned app is identified through discovery analysis, request approval from a SecOps analyst or manager to create a rule on the organization's firewall to block the unsanctioned app in the future.

The integration with Microsoft Cloud App Security is currently available. The integration with Office 365 Cloud App Security is scheduled for the end of March 2019.

Analysis

- Alert options of a text and/or email message are limited and less than what's needed. Microsoft's integration with its Flow offering is a strong move to [1] leverage capabilities already included in Office 365 / Microsoft 365, and [2] create new

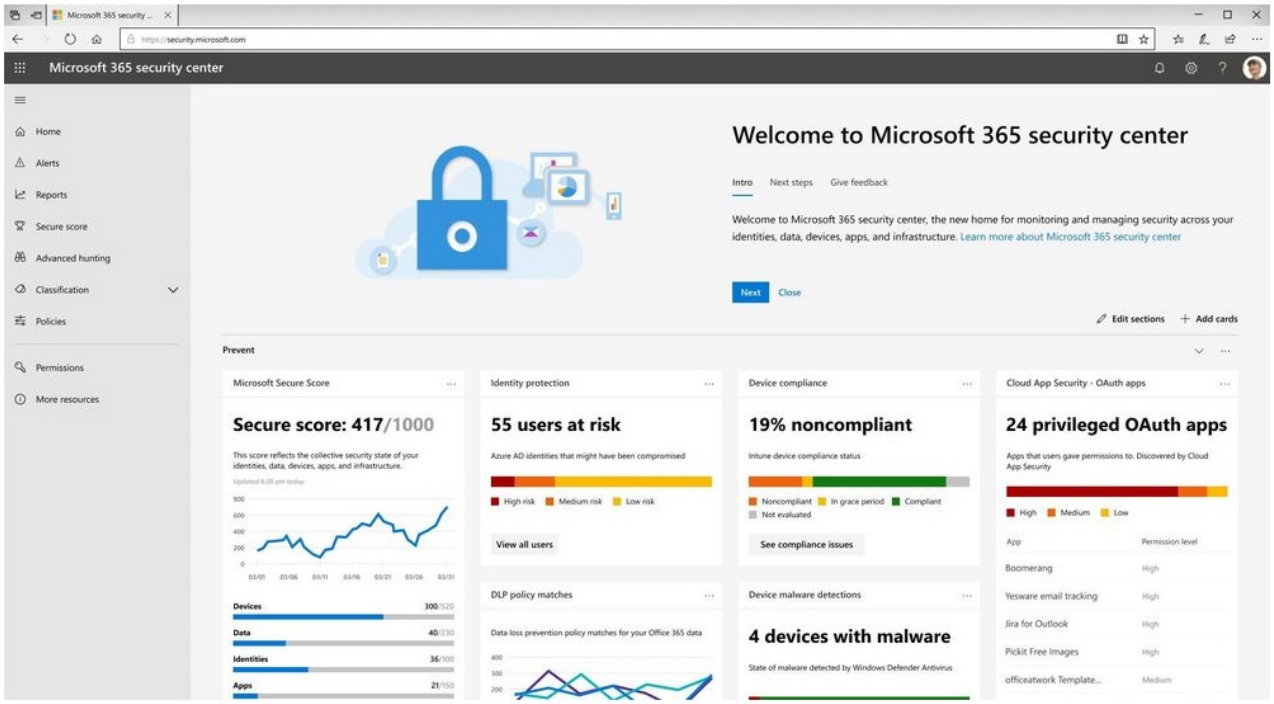
possibilities for much more advanced alerting and policy-based automated actions depending on the nature of an alert and any additional insight gathered through the workflow design.
- SecOps analysts either need to learn how to use Microsoft Flow for creating security workflow playbooks or collaborate across the organization with someone who understands best practices around Flow design.

About

- Date - January 9, 2019
- Announced via - Enterprise Mobility + Security Blog
- Implications for - Microsoft Cloud App Security, Office 365 Cloud App Security
- Tagged as - Security

Microsoft 365 Security Center and Compliance Center

Description



For Microsoft 365 subscribers only, Microsoft announced two new dedicated platforms for security and compliance teams. Rather than offering a single platform that covered both security and compliance, the new Microsoft 365 Security Center for security teams and the new Microsoft 365 Compliance Center for compliance teams offer a focused platform for each team.

Regarding the two new platforms, Microsoft says:

- A dedicated platform is required in (larger) organizations, because the security and compliance teams are different. Providing scoped access to a dedicated platform for each team is easier than providing scoped access for each team to a shared platform. Access to either requires having the appropriate role in Azure AD.
- The **Microsoft 365 Security Center** provides access to identity and access management, threat protection, information protection, and security management. The Center is designed around identity, endpoints, user data, cloud app, and infrastructure, and provides dashboards and insights into historical and current security posture (e.g., using Microsoft Secure Score).
- The **Microsoft 365 Compliance Center** provides access to Compliance Manager, data governance (for example, classifications and label analytics on the use of retention and sensitivity labels), data subject requests, and more. The Center offers steps, checklists and suggested action points to improve compliance.
- Once the two new platforms are available, the former combined Microsoft 365 Security & Compliance Center will be removed from service.
- The two platforms will be progressively rolled out to applicable tenants before the end of March 2019.

Analysis

- Microsoft 365 was originally positioned as an aggregated license for capabilities in Office 365, Enterprise Mobility + Security, and Windows 10. Microsoft 365 was a licensing construct that aggregated capabilities in these three streams, and did not in itself deliver any new capabilities. These two new centers are different, in that they should be available in the Office 365 stream but are not. They represent new capabilities that are above-and-beyond what the underlying streams have to offer.
- It is unknown at this point whether the new services are just Microsoft 365 plays initially in order to throttle demand so Microsoft can stress test them before rolling them out more widely to just Office 365 subscribers, or if Microsoft will hold the line that they are only Microsoft 365 plays in order to drive upgrade / upsell opportunities from "just" Office 365 to the full Microsoft 365 offering. It's a cleaner and clearer separation, and that can be viewed as a value-added offer for larger organizations who have

more data protection, compliance and security complexities to deal with, but by the same token and on the other hand, since most of the fundamental services are Office 365 ones, the new portals could just as easily be for just Office 365 customers too.

About

- Date - January 29, 2019
- Announced via - Security, Privacy and Compliance Blog
- Implications for - Security & Compliance Center Splitting in 2019
- Tagged as -

Records Management Updates

Description

Microsoft announced several updates to the records management capabilities in Office 365:

- Compliance requirements that mandate WORM and non-WORM storage for immutability of records can be met with Exchange Online as long as Preservation Lock is turned on for a Retention Policy. Since Exchange Online is also used to store Skype for Business chats and Microsoft Teams chats and channels, these too are covered. This analysis is documented in an independent assessment by a third-party, although it notes that certain capabilities are not currently supported. Microsoft has indicated an intent to address these areas of lack by July 2019.
- File Plan Manager is generally available. File Plan Manager enables a record manager to create a hierarchical file plan for their Office 365 tenant, and to import current schedules from on-premises and other records systems into Office 365.
- The Disposition Workflow - for Retention Labels but not Retention Policies - can produce a certificate of destruction as part of the workflow to defensibly delete content.
- Event-based retention, one of the retention types available in Data Governance, starts the retention period when something happens - such as an employee leaving or a vendor contract expiring. Event-based retention requires careful labeling of individual documents so discrete documents can be related directly to a specific employee or a specific vendor contract, for example. The new change is that an event-based retention policy can now be triggered by an event in another system, which is signaled through an API to Office 365.
- For customers with access to the new Microsoft 365 Compliance Center, Label Analytics for Office 365 and Azure Information Protection labels is now available in preview.

Analysis

- Records management, retention schedules, different types of retention approaches, file plans and more are specialized topics that carry significant weight in organizations. In Office 365, the details matter greatly - what does specifically work and under what conditions, and what does not specifically work and under what conditions.
- With the many changes to end-user productivity applications and toolsets, the flow-on effects for records management, retention and more are often dealt with later. This can slow down the willingness of a regulated organization to release new but unsupported Office 365 capabilities to their employees.

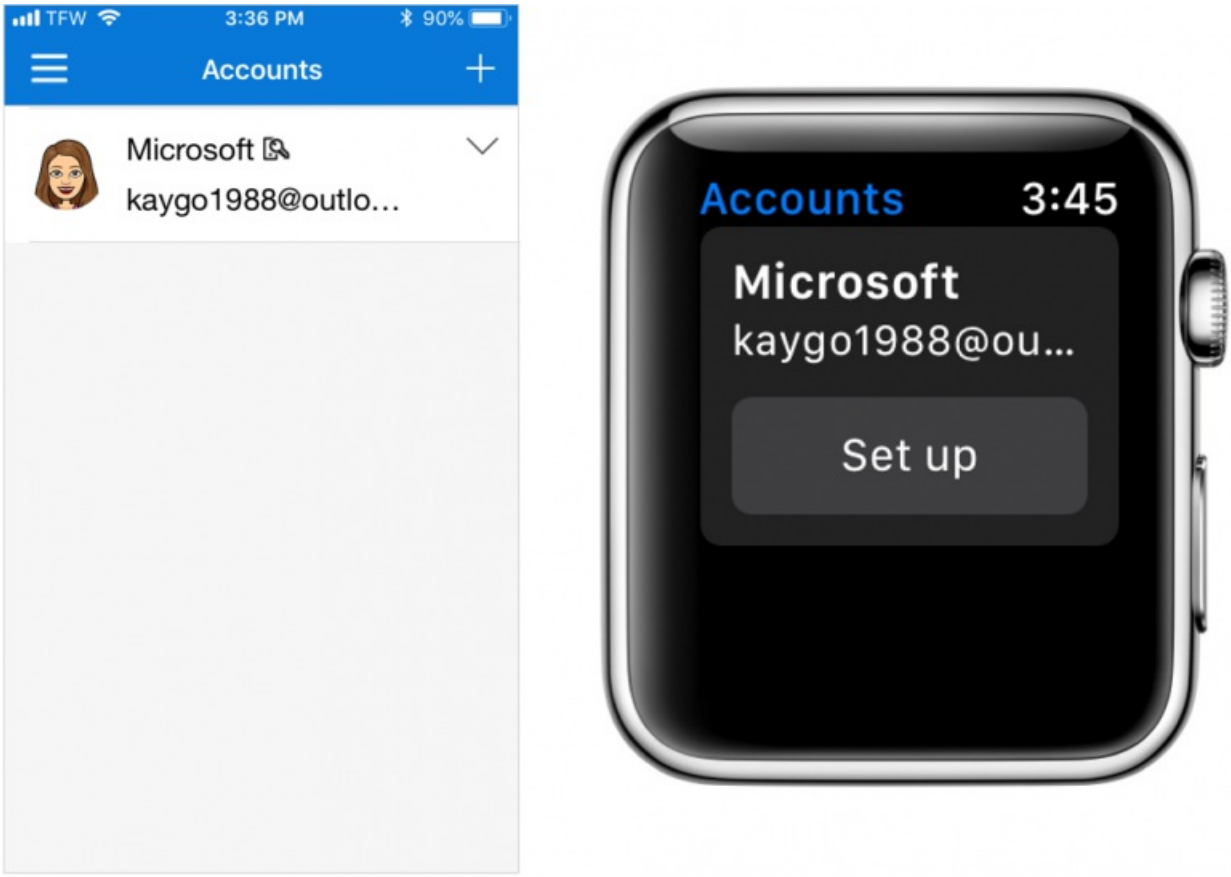
About

- Date - January 29, 2019
- Announced via - Security, Privacy and Compliance Blog
- Implications for -
- Tagged as - Archiving

Apple Watch App for Microsoft Authenticator

Updated on August 29, 2018

Description



Microsoft announced the public preview of the Apple Watch companion app for Microsoft Authenticator. It enables a user to use their Apple Watch to approve push authentication requests that require a second factor - a PIN or biometric signal - without needing to use their Apple iPhone for the second factor. The companion app works with Microsoft personal accounts and Work and School accounts that are set up with push notifications. This support requires the use of version 6.0 of the Authenticator app, which will be released to General Availability in September 2018.

The new companion app for the Apple Watch is a step beyond what is currently available:

- Current capability - a push notification that **does not** require a PIN or biometric second factor can be approved on the Apple Watch by touching the Approve button.
- New capability - a push notification that **does** require a PIN or biometric second factor can now be approved on the Apple Watch by touching the Approve button. The second factor is assumed based on the user wearing the Apple Watch, and having unlocked it via the Watch PIN when putting it on their wrist. The other condition is that the Watch "stays within range of your phone" - but precisely how that will be enforced remains to be seen. The full way to enforce this would be that if the Watch went out of range of the phone, the Authenticator app would enforce a phone-based second factor for the PIN or biometric signal.

Using the Apple Watch to approve requests that require a PIN or biometric second factor must be set up on the Apple Watch for each account.

Analysis

Releasing a companion app for the Apple Watch is a natural stepwise improvement, and streamlines the authentication process for accounts that require a second factor of authentication. Users will have the same approval process for Microsoft accounts, regardless of whether a second factor is required or not.

The interesting question is whether the indirect usage of the PIN on the Apple Watch that was supplied at a generic point in time is sufficient security for an account that requires a PIN or biometric signal for a second factor of authentication at a specific point in

time. That you have put the Watch on your wrist and that you have entered a PIN number at that point to unlock the Watch provides a direct signal for unlocking the Watch, but to assume the applicability of this for a subsequent and unrelated / uncorrelated authentication request is a significant assumption. Clearly the user must set up the app on their Watch to support this behavior, but administrators may want to option to disable this functionality to enforce a higher authentication proof that is specifically supplied.

The second interesting question is whether multi-factor authentication should demand independent factors or can support tightly-linked ones. The concept of knowing one and having the other has traditionally been about independent or mutually-exclusive factors: you know the password, and have a security token (e.g., the RSA SecurID or something similar). Or you know the password, and have the phone that's been linked to the account so you can retrieve the code that's sent by SMS. Or the phone has an authenticator app that displays a changing unique code. In those cases the two are independent and mutually exclusive. With approach Microsoft is taking with the Apple Watch, the two factors are intricately linked: you have the Watch and you know the PIN number for the Watch, and therefore these two factors are enough to provide access.

About

- Date - August 27, 2018
- Announced via - Enterprise Mobility + Security
- Implications for - Authentication - Overview
- Tagged as - Authentication

Data Center Outage in US South Central

Description

A severe weather event in Texas during the night of September 3-4, 2018, which included lightning strikes, compromised the cooling systems at the San Antonio TX data center - called US South Central. The data center responded automatically to shut down affected systems, thereby preventing further damage in the data center. In terms of Office 365, this affected multiple services such as Exchange Online, Power BI, SharePoint Online, Microsoft Teams, Intune and more.

The official Office 365 service health status page at 1.46pm Pacific time on Tuesday September 4 stated:

Office 365 service health status

Title: Unable to access Office365 services

User Impact: Users may be unable to access or use some features within the Office 365 service.

More info: Users may be intermittently unable to access the Office 365 portal. Additionally, users who are able to access the service may experience the following behaviors:

Exchange – Some users were unable to access Outlook on the web, though service is now restored. Email access through other protocols was unaffected.
Power BI – A subset of users may receive a 'Server unavailable' error or may be unable to log in, though our monitoring indicates that availability has recovered. Further details on Power BI can be found under service incident PB147603.
SharePoint – Most impact has been mitigated, but a small subset of users may be unable to make or save changes to SharePoint sites and content. Further details on SharePoint mitigation can be found under service incidents SP147560 and SP147618.
Microsoft Teams – Users may be unable to authenticate or access Office documents within Teams. We're working to verify that this issue is now resolved. Further details on Microsoft Teams can be found under service incident TM147626.
Intune – Affected users may be intermittently unable to access the Intune portal or other functionality. Further details on Microsoft Intune can be found under service incident IT147609.
Education - Affected users may be seeing issues with services including School Data Sync and Assignments within Teams. Further details on School Data Sync can be found under service incident OE147685.

Current status: We're continuing to apply mitigations and our telemetry indicates that availability for the remaining impacted services is improving.

Scope of impact: This issue could potentially affect any of your users who are hosted out of the San Antonio data center. Impact is specific to a subset of users who are served through the affected infrastructure.

Start time: Tuesday, September 4, 2018, at 9:09 AM UTC

Preliminary root cause: Extreme weather in the San Antonio area caused a data center issue, which has affected multiple Office 365 services.

Next update by: Wednesday, September 5, 2018, at 1:00 AM UTC

View your Office 365 service health dashboard.

The most significant impact beyond Office 365 seems to have been Azure AD, which affected both regional and non-regional customers. Users were unable to log in during the day, with some being continuously prompted for login credentials.

Microsoft claimed that customers / tenants beyond the region were not affected, but numerous customers used Twitter to share details of service degradation beyond US South Central. Customers also experienced problems that went beyond the outage

behaviors noted in Microsoft's service advisory, citing problems with outbound email, access to the Admin Center, OneNote notebook access, and an inability to use Content Search or eDiscovery Search, among others.

Analysis

- Outages in cloud services cause major disruption around the world, whether it is a Microsoft cloud service or from Google, Amazon or another player. Given the millions of organizations that rely on cloud services daily, outages swiftly become visible, impactful, and a global problem.
- The latest outage at Microsoft demonstrates that it has not yet mastered the architecture of a fail safe, resilient and reliable cloud service. Outages happen, which affects local customers hosted off the directly affected infrastructure, as well as non-local customers who may experience cascading effects. Outages that affect pivot services like Azure AD can have far reaching effects. Despite having a global network of regional and in-country data centers, neither Office 365 or Azure can fail over seamlessly in the event of an outage.
- Microsoft still has some tidying up to do around where data is located, because having data in one data center location is a recipe for problems. In this case, Visual Studio Team Services stored account metadata for early tenants in San Antonio - even tenants created in Europe - and the disruption to San Antonio therefore had effects for any customer with data stored there. By rights, this data should be have been moved already. Two other Azure services were similarly affected far beyond the US South Central region: Azure Databricks and Scheduler.

About

- Date - September 4, 2018 (US time)
- News Coverage - ZDNet
- Implications for - Tenant Architecture, Authentication - Overview
- Tagged as - Authentication, Security

Lifecycle Management of Guest Accounts in Office 365

Description

Office 365 is increasingly supporting access from guest users - those outside a given tenant - but offers no tools for managing the lifecycle of guest accounts once created. A guest can remove their own account from a tenant, but if they don't do this, the account stays in place until an administrator disables or deletes it. This results in a proliferation of outdated guest accounts, which could potentially be used to introduce vulnerabilities into the environment.

- Guest access is now supported in Microsoft Teams, Office 365 Groups, SharePoint Online, Planner, and OneDrive for Business.
- Administrators can use PowerShell to manage guest accounts, but lack any specific lifecycle management tools. Microsoft doesn't supply anything specific for managing these accounts in Office 365. For example, there is no ability to tie the deletion of a guest account with a time-based signal nor the archiving of the final artifact that was shared with him or her.

Analysis

- The mere proliferation of guest accounts doesn't create an immediate problem for an Office 365 administrator, but over time can result in a lack of clarity on which accounts remain valid and which can be deleted. Since guest accounts attract no licensing requirements, there is no direct financial cost from retaining unnecessary guest accounts.
- What is unknown at this point is the potential for a guest account to be hijacked by a malicious attacker, and then used to introduce threat bearing documents or files into a shared place such as Microsoft Teams, SharePoint Online, or OneDrive for Business. Guest accounts don't have wide access to resources, but could having some access be leveraged against the organization?
- Multi-factor authentication can not be enabled for Guest accounts, because these do not attract a license. Therefore, the potential exists for guest accounts to be easier to compromise than standard accounts, and once compromised through credential harvesting, could be used to enable lateral movement through a tenant.

About

- Date - October 18, 2018
- Announced via - Petri
- Implications for - Authentication - Overview
- Tagged as - Authentication

Office 365 DLP Updates

Description

Microsoft announced three upcoming changes for Office 365 DLP - one to be released in October 2018, and two due for release before the end of March 2019. Specifically:

- [**Roadmap 34252**] Customers will be able to create a custom sensitive information type using the user interface of the Security & Compliance Center. Previously this could only be done through a specially-crafted XML file. The ability to create via the UI will be available in October 2018.
- [**Roadmap 34246**] Office 365 DLP rules will be able to block chat messages in Microsoft Teams if sensitive information is detected. It is unclear what performance lag this will introduce into the real-time chat engine in Microsoft Teams. This enhancement is due before the end of March 2019.
- [**Roadmap 34247**] Files in SharePoint Online and OneDrive for Business are currently cleared for external sharing by default (if external sharing is allowed in the tenant), unless they scan as containing sensitive data. Starting before the end of March 2019, files will be treated as sensitive by default, until the scanning for sensitive information types has completed. Once declared as being free of sensitive data, the file will be available for external access.

Analysis

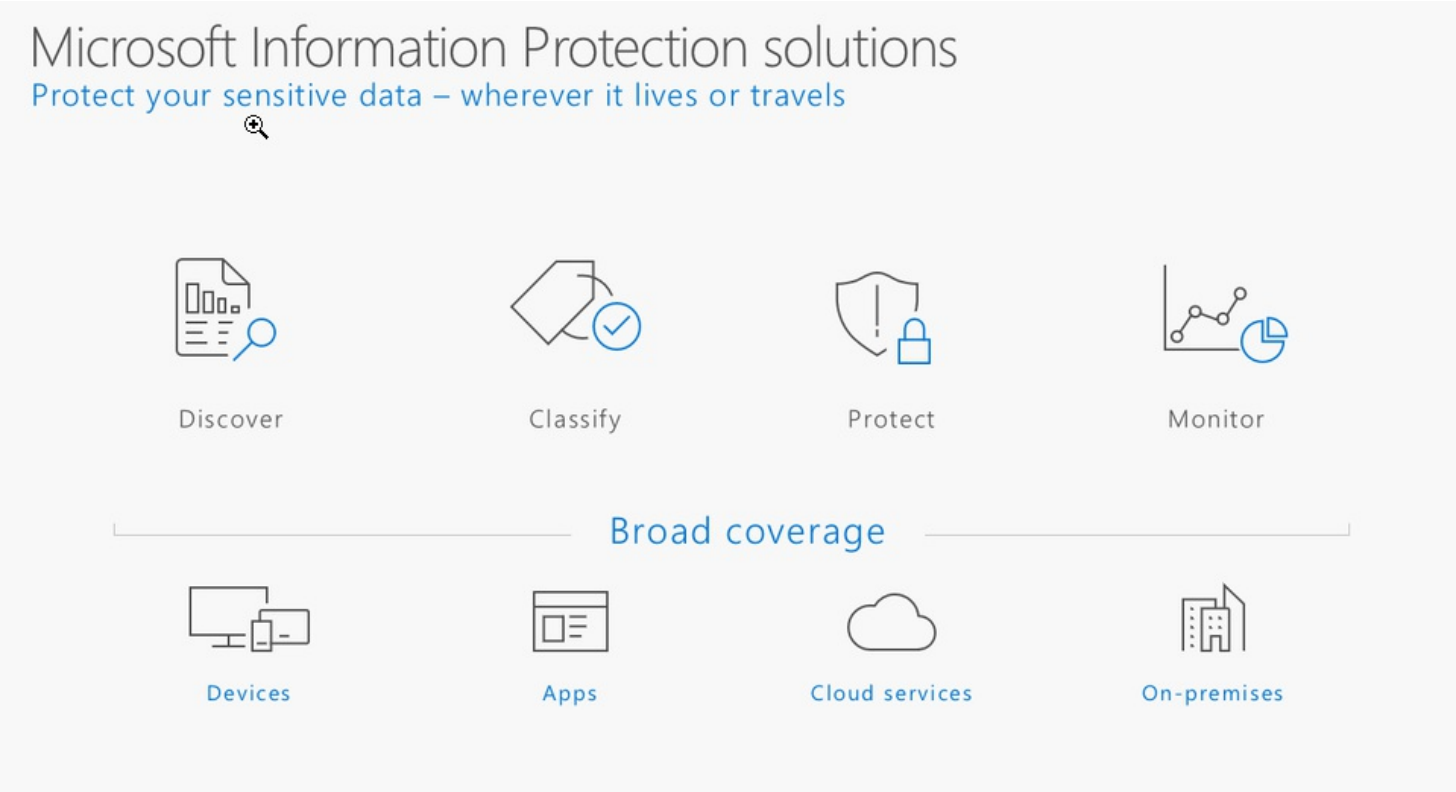
- The additions signalled above are good step-wise improvements for Office 365 DLP.
- Microsoft already offers some real-time scanning for sensitive information in files in SharePoint Online and OneDrive for Business, but the default status of the file is not set to sensitive.
- Setting files status in SharePoint Online and OneDrive for Business to sensitive by default will increase the level of protection for files from the moment of creation or addition to a document library in SharePoint Online or to a shared folder in OneDrive for Business.
- In order for sensitive data to be identified, the rules must first have been set up by an administrator for the tenant. There is no protection of sensitive information by default. If there is no Office 365 DLP policy, nothing will be identified.
- Office 365 DLP rules currently rely on the notion of thresholds, that is, an explicitly declared minimum number of offending data elements that match a sensitive information type in order to reduce the false positive rate. For example, only block an outgoing email message if it or an attachment contains more than 10 credit card numbers (or social security numbers, etc.). It is unclear how these thresholds will be interpreted in the context of a Microsoft Teams chat exchange, if for instance, only one credit card number is exchanged, or if ten credit card numbers are sent through 10 individual messages. Will the Office 365 DLP engine be able to see the potential exfiltration or exchange of sensitive data across multiple discrete messages?
- All three improvements rely on the use of sensitive information types which can be easily circumvented so that a match is not generated. See Identification of Sensitive Data.

About

- Date - October 8, 2018
- Announced via - Microsoft 365 Roadmap (items 34252, 34246 and 34247)
- Implications for - DLP in Security & Compliance Center, Identification of Sensitive Data
- Tagged as - Data Loss Protection

Updates to Information Protection

Description



Microsoft announced and released multiple capabilities for its Information Protection services at Ignite 2018. Specifically:

- The configuration of labels and protection policies for both Azure Information Protection and Office 365 is now centrally managed in the Office 365 Security & Compliance Center. Labels are synchronized from the Security & Compliance Center to Azure for advanced configurations. Protection policies include encryption and access restrictions, visual marking, and controlling external access to labeled sites and groups. This was released to General Availability.
- A software development kit (SDK) for Information Protection was released to enable third-parties to build integrations between their offerings and Microsoft Information Protection. The SDK for Windows, Mac and Linux was released to General Availability, and the SDK for iOS and Android to public preview. Where Microsoft is focused on enabling its applications (Word, Excel, PowerPoint, Outlook) to apply labels, the SDK enables third-party app developers to extend their offerings to leverage the labels and protection settings as defined in Information Protection policies.
- A new version of the Azure Information Protection client for Windows was released to public preview, with support for Word, Excel, PowerPoint and Outlook on Windows. The new client supports default labeling, mandatory labeling, and visual marking. Once released to general availability in Q1 2019 (January-March 2019), the client should also support automatic classification and more.
- Native integration of labeling within Word, PowerPoint, Excel and Outlook on the Mac. For Office for Windows, the Azure Information Client is required for labeling, but Microsoft is moving in the direction of native integration rather than requiring an add-on client. For Mac users, this was released to preview for Office Insiders. Similar native integration was announced (for release in early October) for Word and PowerPoint on iOS and Android, again available only to Office Insiders at this point.
- In response to a question on the blog post, Microsoft said that support for Excel and Outlook on iOS and Android would be available "in the next 3-4 months," so something in the January-February 2019 timeframe.
- For users with the new Windows 10 October 2018 update (which has had its share of early release troubles and is so far delayed), documents and emails with sensitivity labels will be accessible to Windows Information Protection, and the policy actions as defined respected. For example, if a sensitivity label on a document states that it should not be distributed outside the organization, Windows will not allow the document to be copied or shared beyond the work boundary.
- Adobe Acrobat Reader was announced as Microsoft's "preferred" PDF reader, and from October 2018, Acrobat Reader will natively enforce protections on labeled PDFs (effective October 12, 2018). This will require a plug-in in the first instance, and

work only Windows. Support for Acrobat DC and other platforms is expected later in 2018.

- A dashboard with analytics on the use of labeled and protected documents and emails. This is in preview. Note that this is not accessible from the Security & Compliance Center, but requires a subscription to Azure Information Protection.

Analysis

- The whole area of information protection (Microsoft's term) and how it works (and doesn't) is hugely important for any organization wanting to improve its data protection standards in light of data regulations such as GDPR and CCPA. Microsoft actions to improve how sensitive data is identified, protected, and retained or deleted is vitally important. But it needs to get it right as soon as possible, because data protection regulations are already in place (and more is coming). These updates help the onwards journey, but there's still not enough in market yet (too many private and public previews, "still comings," etc.).

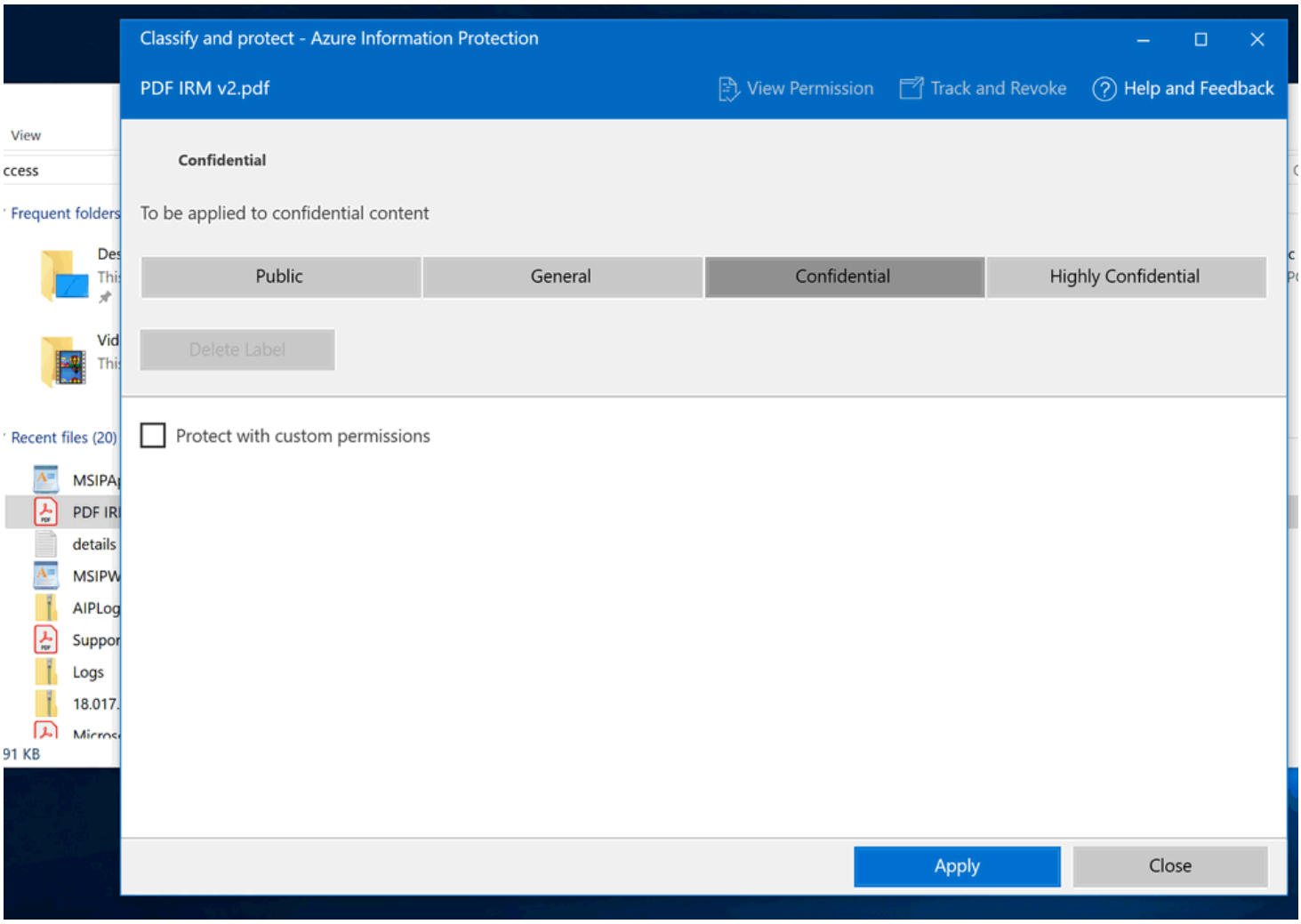
- Users of Office Online (Word Online, Excel Online, PowerPoint Online, etc.) do not yet have the ability to add labels. Microsoft has not yet disclosed a data for release, although acknowledges it is working on this.

About

- Date - September 26, 2018
- Announced via - Enterprise Mobility + Security Blog
- See also - Public Preview for Adobe Reader Released (October 12, 2018)
- Implications for - Azure Information Protection
- Tagged as - Security

Adobe Acrobat Reader and Azure Information Protection

Description



Following its announcement at Microsoft Ignite 2018, Microsoft and Adobe released the public preview of PDF support in Azure Information Protection (AIP). This means that customers licensed for Azure Information Protection can use the new AIP client for Windows to classify and protect a PDF document, and anyone with the Adobe Acrobat Reader (and new plug-in with AIP support) can open a classified and protected PDF document to read.

The details are:

- Classifying a PDF document requires the new AIP client for Windows, which is in Public Preview. A subscription is required for this.
- Reading a classified PDF document requires Adobe Reader with the new AIP plug-in. This is available to anyone, and does not require a subscription to Azure Information Protection.
- Classifying a document means selecting one of the labels set up in the Office 365 Security & Compliance Center, or in Azure Information Protection (although both of these provide a unified set of labels, effective September 2018).
- A classified PDF document retains the standard .pdf extention.
- Opening a classified PDF document in a PDF reader other than Adobe Reader will result in an error page of sorts being displayed. This cover page points the individual to download links for WIndows, Apple and Android.

Analysis

- Azure Information Protection provides classification and protection (encryption) capabilities for individual files and documents. Protection to date has centered on core Microsoft Office document types - such as Word, Excel and PowerPoint. Adding PDF

support is a good first step beyond Office to the wider files used in the market, and with the frequency of its use, PDF is the perfect place to start.

- A PDF file must be classified and protected from Windows File Explorer, using the right-click option to Classify and Protect. There is no option in Adobe Reader to assign a classification, nor in the full Adobe Acrobat client. Support for Adobe Acrobat DC is apparently due before the end of 2018.
- Classifying PDF documents is currently a Windows-only play. No options are available for other platforms at this time, although apparently this is due before the end of 2018.
- PDF documents must be classified and protected using the new AIP client. Existing PDF documents that have been protected by earlier approaches in Office 365 - such as Information Rights Management - are not supported.
- While Azure Information Protection and Office 365 share the same set of classification labels, using the AIP client requires a subscription to Azure Information Protection. This is not included in Office 365 plans.
- Microsoft released the integration to General Availability in December 2018. See Adobe Acrobat Reader and Azure Information Protection (December 2018).

About

- Date - October 12, 2018
- Announced via - Azure Information Protection Blog
- Implications for - Azure Information Protection
- Tagged as - Data Loss Protection

Adobe Acrobat Reader and Azure Information Protection

Description

Following its release to public preview in October, Microsoft announced the general availability of the integration between Adobe Acrobat Reader and the Azure Information Protection client for Windows. The integration means that customers licensed for Azure Information Protection can use the new AIP client for Windows to classify and protect a PDF document, and anyone with the Adobe Acrobat Reader (and new plug-in with AIP support) can open a classified and protected PDF document to read.

Analysis

See the October 2018 update for further analysis and implications.

About

- Date - December 11, 2018
- Announced via - Azure Information Protection Blog
- Implications for - Azure Information Protection
- Tagged as - Data Loss Protection

Manual Sensitivity Labels

Description

Microsoft signaled three tranches of updates to allow a user to manually select a sensitivity label to apply to documents and/or email messages. The three updates will be released during 2019, as follows:

- **January 2019** - Mac and Android support, for Word, PowerPoint and Excel. Not for Outlook.
- **2Q 2019** - Windows support for Word, PowerPoint, Excel and Outlook. Removes the need for the Azure Information Protection client.
- **3Q 2019** - Web support, covering Outlook on the web and Office Online (Word, PowerPoint and Excel).

Analysis

Sensitivity labels can currently be applied using the Azure Information Protection client, which was only ever released for Windows only. Microsoft has previously signaled its intent to add these capabilities directly into its core end user productivity applications on Windows, Mac, iOS and Android platforms. Mac and Android are first in the above update because sensitivity labels can already be manually added in Office for Windows through the Azure Information Protection client, although this is now a stop gap measure not a long-term direction.

There is no mention of iOS support.

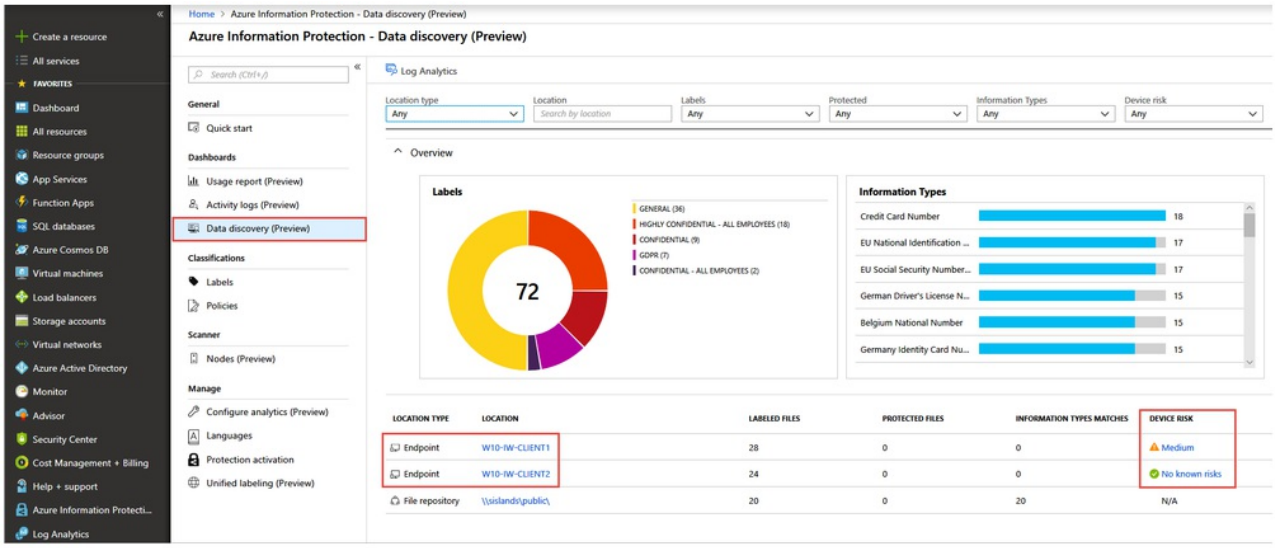
The manual addition of a sensitivity label to a document or email is only one way of labeling. Two other options include automatic labeling in real-time on a current document or email, and after-the-fact labeling of content at rest using the Azure Information Protection Scanner.

About

- Date - December 19, 2018
- Announced via - Microsoft 365 Roadmap
- Implications for - Azure Information Protection
- Tagged as - Data Loss Protection

Azure Information Protection and Windows Defender ATP

Description



Data from Windows Defender ATP is marked with Location Type - Endpoint

Microsoft introduced an integration between Windows Defender ATP and Azure Information Protection into public preview. The integration - if turned on - means that when a file with a sensitivity label is created or modified on a Windows 10 device, Windows Defender ATP will automatically report this to Azure Information Protection Analytics. The implication is that organizations gain a consolidated view of where sensitive data is being stored across network devices and endpoint devices.

The Analytics dashboard reports the device risk status, which is fed from Windows Defender ATP and is based on the presence of any active security threats. Endpoints with active risks that contain sensitive data are prime candidates for actions to mitigate a data breach and reduce further compromise.

Analysis

- This is a sensible and valuable integration between two separate but related product offerings by Microsoft.
- Being able to proactively track the status of endpoints is a critical component of knowing the current security and compliance status of the organization. Getting an organization to install the endpoint monitoring client on all devices can be a challenge, however, and thus Microsoft 's ability to leverage its ownership of Windows 10 gives it at a systemic advantage.

About

- Date - December 8, 2018
- Announced via - Azure Information Protection Blog
- Implications for - Azure Information Protection
- Tagged as - Data Loss Protection

Real-Time Microsoft Cloud App Security Controls for On-Premises Web Apps

Description

Azure AD Application Proxy is a capability of Azure AD that can be used for enabling single sign-on and secure remote access to web apps that are hosted on-premises, for example, a SharePoint site in SharePoint Server. These on-premises web apps are integrated with Azure AD, so that an Azure AD account can be used to provide authentication. Azure AD Application Proxy provides remote access without requiring Virtual Private Networks (VPNs) or the use of a demilitarized zone (DMZ).

Microsoft announced an integration between Microsoft Cloud App Security and Azure AD Application Proxy, so that the real-time conditional access controls in Microsoft Cloud App Security can be evaluated as part of the authentication decision for on-premises web apps. For example, if the user's session is considered risky due to the use of an unmanaged device, real-time controls can be enforced to prevent the download of files from an on-premises web app. The integration provides consistency of policy across cloud and on-premises web apps.

Analysis

- Consistency in policy definition and enforcement across all web apps provides an ideal future destination, enabling define-it-once and enforce-it-everywhere security. The capabilities on offer from Microsoft provide solid support for this journey.
- Single sign-on and secure remote access for on-premises web apps requires Azure AD Application Proxy. This is not available in the edition of Azure AD that comes with Office 365; it requires either Basic, Premium P1 or Premium P2 licensing of Azure AD. In a similar way, Microsoft Cloud App Security is not included in any Office 365 license; it require separate licensing, or licensing as part of Microsoft 365.

About

- Date - November 19, 2018
- Announced via - Enterprise Mobility + Security Blog
- References - How to Provide Secure Remote Access to On-Premises Applications (about Azure AD Application Proxy)
- Implications for - Microsoft Cloud App Security
- Tagged as - Authentication, Security

Multi-Hour MFA Outage in the United States

Description

On Tuesday November 27, 2018, Microsoft's multi-factor authentication service in Azure AD had a multi-hour outage, beginning at 9.15am PT and ending sometime after midday. The outage supposedly only affected customers in the United States, but customers in other regions were affected too (e.g., United Kingdom).

Microsoft engineers said the problem was due to a domain name system (DNS) issue, and that the mitigation involved restarting the authentication infrastructure.

Analysis

- Two times in 10 weeks is bad. Two times in two weeks is terrible.
- Having to recycle / restart the authentication infrastructure doesn't sound like a very resilient system design. Surely there are more appropriate, cloud-scale approaches to mitigating issues than "turning it off and on again." That might fly for a solitary Windows PC here and there, but the entire infrastructure?

About

- Date - November 27, 2018
- Sources - ZDNet Microsoft, The Register, ArsTechnica
- Implications for - Multi-Factor Authentication
- Tagged as - Authentication

Password-Less Sign-On Coming for Azure AD

Description

Microsoft announced that users will be able to log into Azure AD work and school accounts from early 2019 without entering their username and password. Biometric support is being added to Azure AD accounts, based on the use of a FIDO2-compliant security key or Windows Hello by the end user.

The above roadmap announcement was made as part of the release of password-less sign-on to a Microsoft account using Windows 10 (Version 1809) and Microsoft Edge on November 20, 2018. For users with the latest release of Windows, either Windows Hello (face scan or fingerprint scan) or a FIDO2-compliant device can be connected to Microsoft Edge for signing into sites that work with a Microsoft account, such as Outlook.com, Skype, OneDrive, Office 365, and more.

Microsoft said that it is initially supporting two FIDO2-compliant devices: the YubiKey 5 range from Yubico, and the Fetian Biopass.

Analysis

- Password-less sign-on embraces a different form of multi-factor authentication. The usual pattern is knowing something and having something; for example, knowing the password and having a security key that displays a code (or having a pre-registered phone to receive a code). The new pattern eliminates the thing to know and requires having two things - a device that can accept biometric input (a camera on a laptop, or a security key) and the connected biometric input (a face or a fingerprint).
- Multi-factor authentication offers much more security over an online account than relying on a username and password alone. Phishing for account credentials works so well because if multi-factor authentication is not enabled on the account, the username and password are enough to get full access to it.
- While a separate second factor - such as a security key - offers an enhanced level of protection, misplacing, losing, or having the security key stolen will create difficulties logging in. This is not a Microsoft issue. Yubico, for example, recommends that users have a spare YubiKey available for this scenario. And Microsoft has also addressed the problem by enabling users to register multiple MFA devices.

About

- Date - November 20, 2018
- Announced via - Microsoft 365 Blog
- See also - Yubico Blog, Fetian Press Release
- Implications for - Multi-Factor Authentication
- Tagged as - Authentication

Global MFA Outage - November 19, 2018

Description

Office 365 service health status

Title: Unable to sign in to Microsoft 365 services

User impact: Affected users may be unable to sign in using Multi-Factor Authentication (MFA).

More info: Users may also be unable to carry out self-service password resets.

Current status: We're continuing to investigate the underlying cause of the issue while monitoring the continued success of MFA requests.

Scope of impact: Impact may be experienced by users accessing Office 365 services via Multi-Factor Authentication.

Start time: Monday, November 19, 2018, at 4:39 AM UTC

Next update by: Tuesday, November 20, 2018, at 6:00 AM UTC

View your Office 365 service health dashboard.

Users of Azure and Office 365 with multi-factor authentication turned on were unable to log in to their accounts on Monday November 19, due to a global MFA outage. Users across the world were affected; Microsoft claimed the outage only affected a "subset of users," but the impact was felt by users worldwide.

- The outage started at 4.39am UTC on Monday November 19.
- During the outage, Microsoft said that users located in Europe, Middle East and Africa, and Asia Pacific were affected / impacted.
- Most of the issues were apparently resolved by 9.30pm UTC on Monday November 19, however Microsoft engineers continued to track the issue for many hours after this.
- The outage affected the different approaches for receiving the second factor, including the Microsoft Authenticator app, text message, and calls.
- On November 26, Microsoft disclosed the results of its root cause analysis. Two root causes were caused by a bug in the code update from November 13-16; these resulted in the MFA servers being unable to cope with the load of MFA requests on Monday morning. The inability to cope initially manifested as latency, but escalated to non-performance (the third root cause). Microsoft also said that its monitoring and telemetry tools did not work properly; they incorrectly reported the MFA system was operating in a healthy state. Microsoft has promised at least four improvement actions.

Analysis

- Multi-factor authentication, in general, adds a strong layer of protection to user accounts. As a general policy, almost everyone should have MFA turned on.
- The cost of lost productivity for the one day outage for affected organizations is significant.
- Microsoft proved again that its approach to MFA in Azure and Office 365 is poorly architectured and delivers a single point of failure. If Microsoft's MFA services are down, affected users can't get to work.
- Perhaps Microsoft's mission of "helping everyone achieve more" should be modified to address the MFA outage on November 19: "But not today."

- Some customers using third-party MFA services with Office 365 claimed to be unaffected by the outage, such as Duo and Okta. See Global outage of Office 365 MFA, considering Duo (Spiceworks).

About

- Date - November 19, 2018
- Sources - ZDNet Microsoft, Computer Business Review, ZDNet Microsoft (root cause analysis, November 26)
- Implications for - Multi-Factor Authentication
- Tagged as - Authentication

Support for Multiple MFA Devices Per User

Description

Microsoft released support for multiple MFA devices per user for all Azure MFA users (including Office 365), with a maximum of five current devices per user. This allows users to have more than one MFA device accessible. Microsoft says this enables users to have different devices for different environments, or to be less affected if they happen to leave their single MFA device at home one day.

The five devices can include the Microsoft Authenticator app, software OATH tokens, and hardware OATH tokens.

Support for multiple devices is generally available, at October 23, 2018.

Analysis

- Having support for multiple MFA devices could result in people becoming negligent in protecting their MFA devices. When each person has only a single MFA device, it is essential that they know where it is, that they have it available, and that they note when it goes missing. With having multiple devices available, including potentially one or more that are primed for action but kept as backup, loss or theft may go unnoticed for weeks or months. This opens the potential for account compromise, even for those accounts protected with MFA.

About

- Date - October 23, 2018
- Announced via - Azure Active Directory Blog
- Implications for - Multi-Factor Authentication
- Tagged as - Authentication

Support for Hardware OATH Tokens in Azure MFA

Description

Microsoft released the public preview of hardware OATH token support in Azure Multi-Factor Authentication, although hardware token support requires the full Azure MFA service that comes with an Azure AD Premium P1 or P2 license. Hardware OATH token support is not available in the bundled Azure MFA for Office 365 service.

- Hardware OATH token support is available for any OATH token with a 30- or 60-second refresh, that has a secret key of 128 characters or less.
- The implementation supports the use of the Time-Based One-Time Password (TOTP) algorithm.
- Initial support is available for tokens from DeepNet Security, Token2, and Yukico (although this requires an accessory app to work).
- Microsoft offers a file upload option for associating hardware tokens with user accounts. This has to be in a specially formatted CSV file.
- Initial support appears to exclude FIDO2 keys and Universal Two Factor (U2F), although what was announced was only the public preview, not the general availability. There is no mention in the Microsoft Roadmap for FIDO2 and U2F as they relate to Azure MFA.

Analysis

- Lack of support for hardware OATH tokens has been a long-running shortcoming in Microsoft's multi-factor authentication offer. Adding this support is a good improvement for the service.
- Support for hardware OATH tokens requires an Azure AD Premium P1 or P2 license, which can be added to an Office 365 license or acquired as part of a Microsoft 365 license. This means hardware OATH token support is not available for Office 365 subscribers in general, providing a further example of Microsoft 365 being the bigger picture.

About

- Date - October 23, 2018
- Announced via - Azure Active Directory Blog
- Implications for - Multi-Factor Authentication
- Tagged as - Authentication

Windows 10 and OneDrive Sync Settings

Description

The next release of Windows 10 (Version 1809, or Redstone 5) introduces an integration between Storage Sense and OneDrive. Storage Sense is a Windows 10 feature that monitors the local drive and tidies up unnecessary files so as to optimize the storage consumed. The forthcoming integration means that the user can specify a number of days after which unused files that the user has synced from OneDrive will be removed from their device. The file will be changed to online-only and removed from the device, but will still remain accessible if needed in the user's OneDrive.

Note that the default value is Never, meaning that the removal of files from the local device is an opt-in feature.

Analysis

Every vendor struggles with the balance between releasing tools that enable productivity through information availability and protecting information from too much disclosure / availability. What should this person have access to based on their job role and their tasks is a governance question for organisations, that's enabled by technical capabilities offered by vendors. Data loss prevention stops people from flowing information to other people when it's sensitive or confidential and the other party doesn't have access rights. Access control lists on collaborative workspaces, shared folders, and systems of all kinds provide another form of information protection – it lets those who need the content in, and keeps those who don't have the right to the content out. Role-based access control goes a step further and adds the nuance of who can and cannot take specific actions within a system.

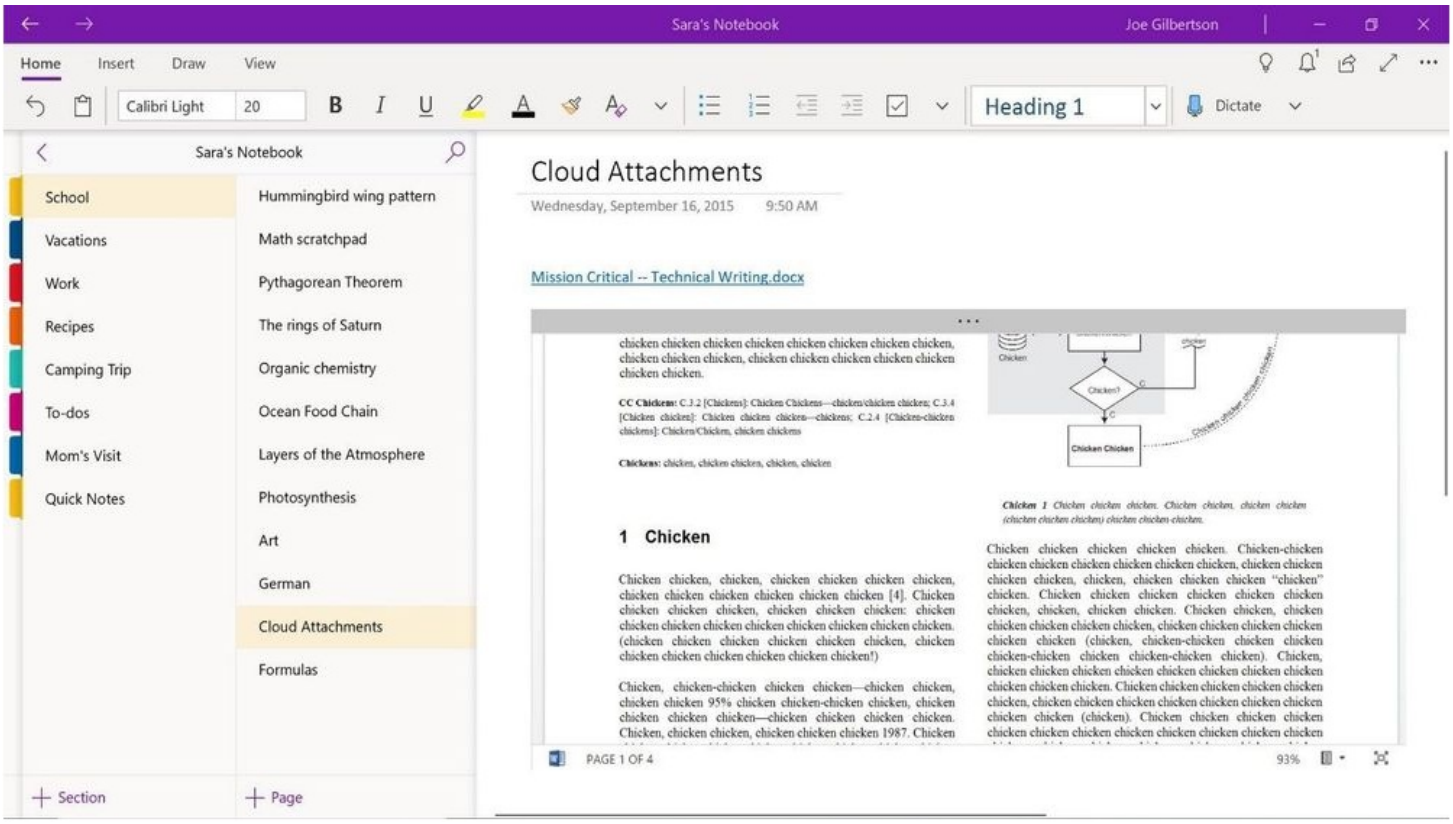
Choosing to sync your OneDrive contents to a local machine is great for productivity – everything is immediately available whether you are connected to the network or not. But the risk is that unauthorised access to your machine – directly by a person or indirectly by a security threat executing and exfiltrating the data on your disk – will enable access to content by people who do not have authorisation. To information that is sensitive, confidential, or in need of special protections. The above forthcoming integration with Storage Sense in Windows 10 will mean that content from OneDrive that is not used often can be removed from local storage, reducing the potential information protection disclosure surface. If it's not there directly, it can't be accessed directly … and thus there's another action required to gain access, which can be evaluated against up-to-the-second security policies.

About

- Date - August 12, 2018
- Announced via - Thurrott
- Implications for - File Sharing - Overview
- Tagged as - File Sharing, Data Loss Prevention

OneDrive Files in OneNote

Description



Microsoft announced a soon-to-be-released integration between Microsoft OneNote (for Windows 10 and Mac) and Microsoft OneDrive. The integration means that a document attached to a page in a OneNote notebook will be stored in OneDrive, not directly on the OneNote page. The document will sync via OneDrive, and if changes are made to the document by a co-author, these changes will flow via OneDrive into the OneNote page. The document, therefore, will not be a point-in-time snapshot that gets out of date, but will be always up-to-date.

Microsoft Office documents attached to a OneNote page will be display a live preview (for example - see above for); other types of documents will be displayed as a link.

The announcement on October 17 said the integration is "coming in the next few weeks," so perhaps in the first week of November 2018.

Analysis

- Supporting sync of files attached to a OneNote page is a step beyond what has been offered to date via the OneDrive sync client. The sync client takes a standard file folder structure and keeps the documents in sync. That's the standard approach for keeping files in sync - it's just a delta change between files stored in a folder. The OneNote integration is an innovative extension that's not available elsewhere.
- Files attached to a OneNote page that are not already stored in OneDrive will be synced through to OneDrive. It is unclear where these files will end up. They could all sync to a folder called something like "OneNote Attachments" though, which would be consistent with how the integration between OneDrive and Outlook works (using a folder called "Email Attachments").
- The file can only be stored in OneDrive, not in another cloud repository such as Box or Dropbox. This plays nicely to Microsoft's strategy of building integrations between its own products that aren't available for others.
- Once the file is in OneDrive, the user can share the document with other people. This allows another avenue of sharing specific content - for example, just the document - rather than giving access to an entire OneNote notebook. While a collaborator could be invited to a OneNote page, it could potentially result in the disclosure of information beyond what they should be privy to. Sharing the document only via OneDrive reduces the sharing surface.

About

- Date - October 17, 2018
- Announced via - Office 365 Blog
- Implications for - File Sharing - Overview
- Tagged as - File Sharing

Files Restore for SharePoint Document Libraries

Description

Microsoft announced that its Files Restore capability that's available with OneDrive is coming to SharePoint document libraries starting in December 2018. Files Restore for SharePoint works directly in SharePoint and across Office 365 where a SharePoint document library is surfaced, such as in Microsoft Teams, Outlook groups, and Yammer groups connected to an Office 365 Group.

The restoration of a document library to a previous state - at any point during the previous 30 days - can be initiated by a site administrator.

Analysis

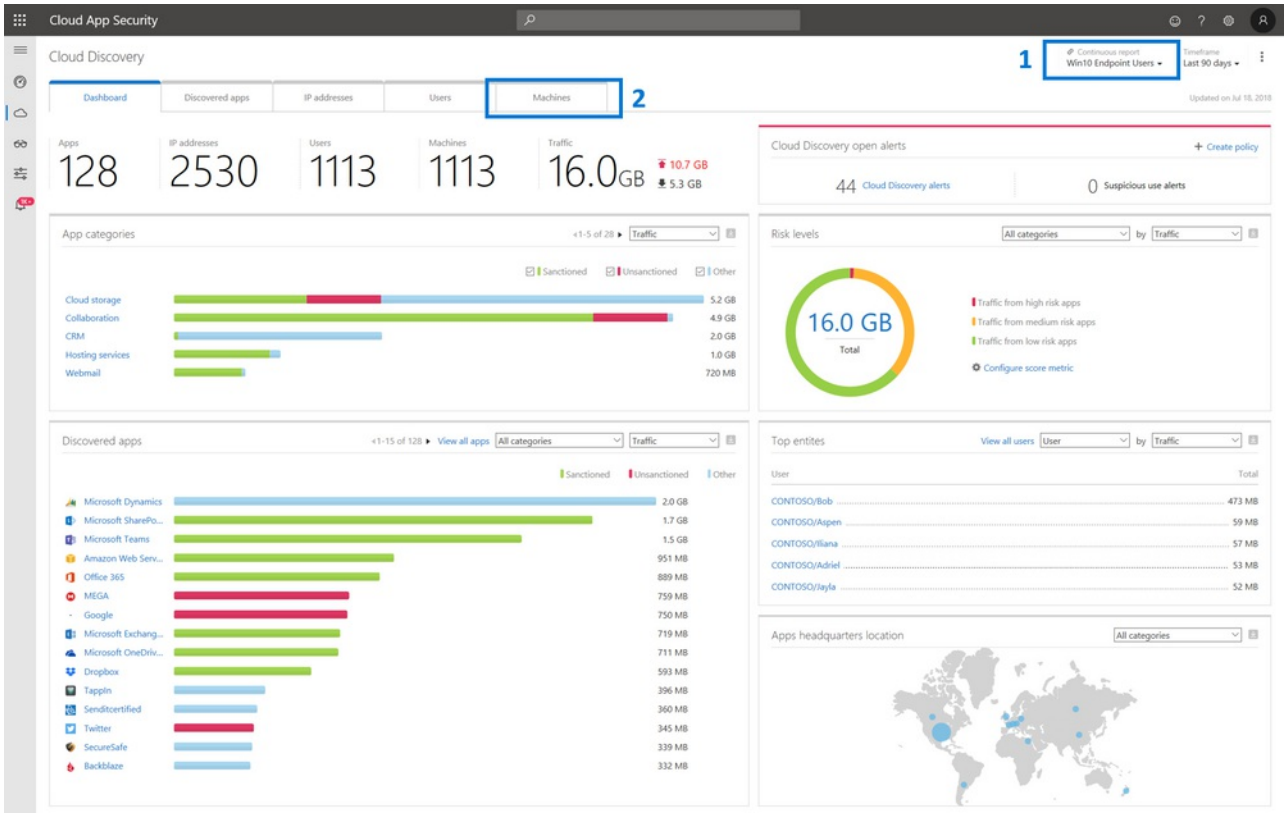
- OneDrive Files Restore was the proof of concept. Office 365 subscribers were quick to request support for SharePoint document libraries as well.
- OneDrive Files Restore has two issues, and it is likely that these will also apply to the SharePoint experience. Specifically:
  - [1] Only basic file and folder activities are restored - e.g., create, delete, rename, update, move and copy. Sharing and permissions settings are not restored or reverted. These must be applied again.
  - [2] Files Restore relies on the Recycle Bin as its source of recoverable files and folders. Any files or folders that have been removed from the Recycle Bin - for example, by the user permanently deleting these items - are unrecoverable.
- Files Restore applies to document libraries only, not to list items. Since OneDrive doesn't support lists, this capability has not been tested there before bringing it across to SharePoint.

About

- Date - October 17, 2018
- Announced via - Microsoft SharePoint Community Blog
- Implications for - File Sharing - Overview
- See also - OneDrive Files Restore
- Tagged as - File Sharing

Microsoft Cloud App Security and Windows Defender ATP for Discovery

Description



Microsoft released an integration option between Windows Defender ATP and Microsoft Cloud App Security. If enabled by the admin for their entire organization (and the fleet of enrolled Windows 10 devices), Windows 10 Defender ATP will continuously log resource usage on local machines to Microsoft Cloud App Security. This data will be used to discover which cloud apps and services are being used via the device, irrespective of which network the device is connected to. Without this integration, Microsoft Cloud App Security is only able to see cloud app usage that flows through firewalls and other network devices that supply it with traffic log information.

When looking at the discovery dashboard in Microsoft Cloud App Security, an administrator will be able to open Windows Defender ATP for deeper investigation of a specific device.

This integration is not available in Office 365 Cloud App Security, the version that is included in Office 365 Enterprise E5. Microsoft Cloud App Security is part of Enterprise Mobility + Security E5, and can be acquired standalone or as part of an E5 plan for Microsoft 365.

Windows Defender ATP is available with Windows 10 Enterprise E5. This is also part of Microsoft 365 Enterprise E5.

The integration was released to preview in September 2018, and to general availability in March 2019. See Microsoft Cloud App Security Updates (March 2019).

Analysis

- Integrating the two services is a natural enhancement for Microsoft to deliver. Microsoft Cloud App Security can only see the usage data it is fed, and without this integration, that means firewalls and other network devices that log usage data. With this integration, all enrolled Windows 10 endpoints will also supply usage data for a more complete picture.
- How a Cloud App Security Broker (CASB) acquires its insight into actual usage is a point of competitive differentiation between CASB vendors. While having an agent installed on endpoints provides deep data insight, no CASB vendor wants to rely only on this, because of the deployment and maintenance challenges of distributing agents to all endpoints. Microsoft is leveraging what it already collects directly on endpoints to feed endpoint data to Microsoft Cloud App Security - a good leveraging of its capabilities without incurring additional deployment cost on an organization.

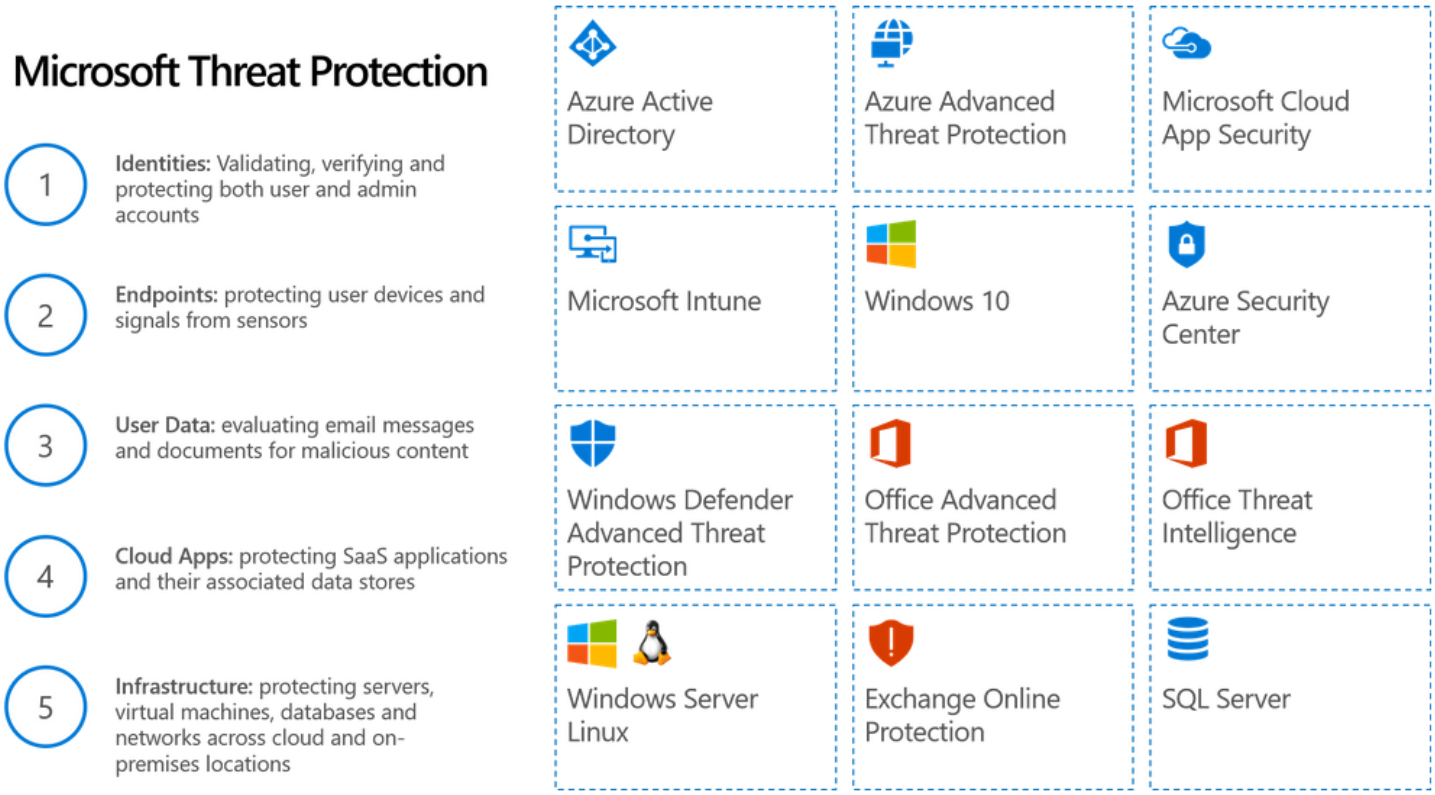
- Microsoft's Intelligent Security Graph is involved as the middle data broker between Windows Defender ATP and Microsoft Cloud App Security. The data sharing is not direct between the two services for an organization. This means that all resource usage on Windows 10 devices are shared with the Intelligent Security Graph, and in addition to its usage by Microsoft Cloud App Security, Microsoft leverages the telemetry for enhancing its security posture and approach. Since identifiable data is fed from Windows 10 devices to Microsoft Cloud App Security, this same information must also exist in the Intelligent Security Graph. Microsoft will need to be very careful in how it handles this information in light of an increasing regulatory focus around the world on protecting personal data.

About

- **Date** - September 27, 2018
- Announced via - Enterprise Mobility + Security Blog
- Implications for - Microsoft Cloud App Security
- **Tag** - Security

Microsoft Threat Protection

Description



At Ignite 2018, Microsoft announced Microsoft Threat Protection, a Microsoft 365 offering that creates a single bundle of different Microsoft security and threat protection products. Microsoft Threat Protection:

- Relies on the 6.5 trillion daily signals in the Microsoft Intelligent Security Graph.
- Focuses on protecting five categories of threats - identities, endpoints, user data, cloud apps, and infrastructure. Some individual products have a role to play across categories, including Office 365 ATP and Microsoft Cloud App Security.
- Microsoft says that its Threat Protection portfolio includes its own security services, along with specific capabilities from partners. It is not clear which partner offerings are included in Microsoft Threat Protection.
- The customer who spoke at the Ignite session on Microsoft Threat Protection commented on the power of unifying their security services with Microsoft. This was a shift from best-of-breed vendors or no-vendor in each of the respective security categories in the portfolio of offerings that makes up Microsoft Threat Protection.
- Will require security professionals who understand the intricate interlinkages between and across the different products and services in Microsoft Threat Protection.

Analysis

- Bundling different tools into a single offering is a long-running Microsoft strategy. Microsoft Office - a bundle of Word, Excel and PowerPoint - was an early example in the 1990s that helped tilt the office productivity software market in Microsoft's favour.
- Microsoft has previously delivered security and threat protection products as add-ons, extensions or advanced options for its different tools. These separate security and threat protection products have come out of product-aligned groups, rather than cross-product or supra-product aligned groups. Microsoft Threat Protection is a good step in the right direction of reducing the count of separate offerings, and emphasizing higher-level capability areas.
- Microsoft asserts - rightly so - that the modern organization faces a wide and diverse attack surface, and also asserts - probably rightly so as well - that no single product or service can secure the entire modern workplace. However, Microsoft has contributed to this problem, by creating such a plethora of product-aligned security services that it can confuse and undermine the ability for customers to ensure protection across the attack surface. The introduction of a unified offering is directionally right for both Microsoft and customers, but it will have to be much more than a bundling of disparate services into a single pane of

glass.

- While unification is a good direction for Microsoft, the respective individual services still suffer from various weaknesses, as noted in the pages in this Analysis Services. Unification will not address these weaknesses and drawbacks.
- Third-party vendors will face an elevation of the playing field, away from point products to an overall portfolio offering. Even the ability to demonstrate excellence in one category against mediocrity or a "good enough" offering by Microsoft in the same category may be offset against the much larger overall set of offerings.
- Microsoft Threat Protection is a Microsoft 365 play, not an Office 365 play.

About

- Date - September 27, 2018
- Announced via - Security, Privacy and Compliance Blog
- Implications for - Office 365 Advanced Threat Protection, Exchange Online Protection, and Microsoft Cloud App Security.
- Tagged as - Security

OAuth Threat Monitoring in Microsoft Cloud App Security

Description

Microsoft says that it is seeing increased usage of web applications using OAuth for requesting access to Office 365, Salesforce, and G Suite data and account capabilities. When a user approves an OAuth request, their account credentials for the target service are shared with the requesting service in a secured obfuscated manner, and an access token is created that provides ongoing access until revoked. This means that changing the password on the account will not revoke the access token, nor will introducing a multi-factor authentication prompt.

However, attackers are leveraging OAuth to seek approval for malicious applications that masquerade as a valid service.

Microsoft says that across its customer base, there is an average of 81 OAuth apps that have been approved by employees in each organization, but some organizations have a combined approval count of over 250.

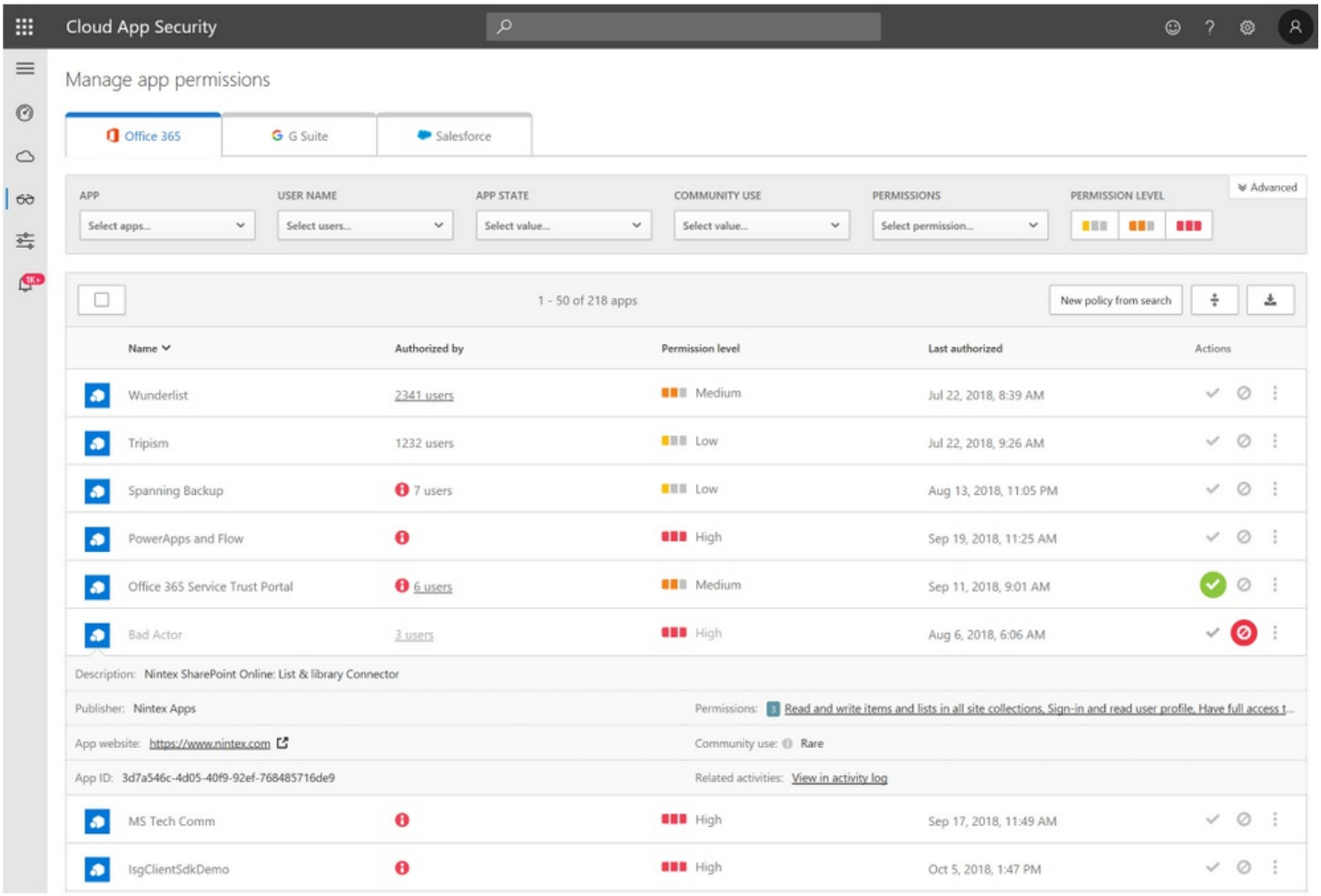


Image 2: App permission overview dashboard in Microsoft Cloud App Security

Microsoft Cloud App Security, the cloud access security broker (CASB) that ships in Enterprise Mobility and Security and/or Microsoft 365, can report on OAuth applications in use and provide certain controls. Specifically:

- Microsoft Cloud App Security can report on OAuth applications that employees have approved to connect to Office 365, Salesforce, and G Suite. Details include the number of users who have authorized the app, and a brief description of how commonly used the app is across all of Microsoft's customers.
- Connected apps can be marked as approved (which provides a green tick for visual notification; it doesn't do anything beyond that) or non-approved. The latter can also be used to revoke whatever permissions are currently in place for the newly non-approved or banned app.
- Admins can create app permissions policies for OAuth applications, using triggers such as permission level, user coverage, and user type (normal or privileged). For example, policies can automatically revoke OAuth permissions for specific trigger conditions, such as the app requested full access to the user's data.

- An app permissions policy can be created that provides a blacklist for apps that meet specified conditions. For example, block all apps that require Full Data Access.

Note that Microsoft Cloud App Security is different to Office 365 Cloud App Security. The former has these capabilities; the latter does not.

Analysis

- Every organization should have a cloud access security broker (CASB) as part of their security arsenal. Microsoft offers one in Microsoft 365 and Enterprise Mobility and Security, and there are many other vendors that offer CASBs with similar and better capabilities.
- Marking an OAuth app as banned in Microsoft Cloud App Security functions as a black list, albeit not in real-time. Users can re-approve OAuth requests for the app, but once Microsoft Cloud App Security detects the re-approval, it will be deactivated again.

About

- Date - October 25, 2018
- Announced via - Enterprise Mobility and Security Blog
- See Microsoft Docs - Manage App Permissions in Microsoft Cloud App Security
- Implications for - Microsoft Cloud App Security
- Tagged as - Security

Microsoft Cloud App Security - Roadmap Updates

Description

Microsoft released (or announced) new capabilities for Microsoft Cloud App Security at Ignite 2018. It also offered some signals on what is coming with the offering.

The new capabilities were:

- Public preview for real-time session controls in Microsoft Office 365 (e.g., SharePoint Online) using Conditional Access App Control.
- Support for on-premises apps, via an integration with Azure AD Application Proxy. This extends Microsoft Cloud App Security beyond cloud apps.
- Integration with Windows Defender ATP for gathering signals on cloud app usage beyond the corporate network. See analysis at Microsoft Cloud App Security and Windows Defender ATP for Discovery (September 2018).
- Automatic detection and revocation of risky OAuth App permissions. See analysis at OAuth Threat Monitoring in Microsoft Cloud App Security (October 2018).
- Integration with Microsoft Flow as an alert option when creating policies in Microsoft Cloud App Security. This significantly extends the alert options beyond sending an email or text message, providing integration with workflow definition tools in Microsoft Flow. For example, a specific policy could route an alert into ServiceNow, or alternatively to the manager of the person who triggered the policy for determining the correct remediation.
- Integration with the iboss Secure Cloud Gateway Platform, for two main purposes: firstly, the discovery of cloud apps, and secondly, for real-time enforcement of policies.

The roadmap announcements - which are vaguely specified - were:

- Real-time session controls will be available later in 2018 for additional Microsoft cloud services, such as Microsoft Teams, the Azure portal, and Dynamics 365.
- The intent to provide even more advanced DLP capabilities.
- The intent to do more with the integration with Windows Defender ATP.
- The intent to broaden the ability of Microsoft Cloud App Security to monitor and control apps in real-time. This was noted as "for any app," "with even more granular app controls," and for non-browser-based apps too.
- The intent to extend the ability to assess the security posture for a cloud service to other PaaS and IaaS providers. Microsoft already offers security posture assessment capabilities for Azure.
- The intent to offer better SecOps capabilities.
- The intent to provide additional built-in threat detection capabilities.

Analysis

- The announced or released updates are all solid next steps for Microsoft Cloud App Security. Broadening beyond cloud apps is particularly interesting, because it represents a coming-full-circle moment for the offering (meaning that cloud app security brokers - CASBs - were introduced because on-premises security tools were blind to cloud apps, and now CASBs are also able to provide visibility into and control for on-premises applications).
- The integration with Microsoft Flow removes the limitations around what can be done with an alert (which was previously to generate an email or text message, which are both blunt options). Flow integration provides many options to embrace the nuances of the context around the alert.

About

- Date - September 26, 2018
- Announced via - Enterprise Mobility and Security Blog
- Implications for - Microsoft Cloud App Security

- Tagged as - Security

Microsoft Cloud App Security Alerts

Description

On its Microsoft 365 Roadmap site, Microsoft disclosed that alerts related to Office 365 apps and services that are created in Office 365 Cloud App Security and Microsoft Cloud App Security will be unified into the Alerts view in the Office 365 Security & Compliance Center. This change will be introduced in December 2018.

Currently there are two places for an administrator to check for alerts:

- The Alerts section in the Security & Compliance Center, and
- The Alerts view in Office 365 Cloud App Security and Microsoft Cloud App Security.

Analysis

Separating alerts for the same services across two different control planes is not great design. The two Cloud App Security offerings from Microsoft do more than just alert on Office 365, but it is good to see the integration of alerts on Office 365 into a single alerts screen in the Security & Compliance Center.

It remains to be seen if the rich alerting data and analytics available in Office 365 Cloud App Security and Microsoft Cloud App Security will also be ported to the Security & Compliance Center.

About

- Date - November 21, 2018
- Sources - Microsoft 365 Roadmap #44243
- Implications for - Office 365 Cloud App Security, Microsoft Cloud App Security
- Tagged as - Security

Office 365 Cloud App Security Updates

Description

Microsoft enhanced Office 365 Cloud App Security with several updates during September to December 2018. Microsoft's standard approach is to release capabilities to Microsoft Cloud App Security first, and then retrofit the applicable changes into Office 365 Cloud App Security. Microsoft Cloud App Security provides cloud security capabilities to more than 16,000 cloud apps, while Office 365 Cloud App Security is a scoped version focusing on Office 365 and related services.

Recent updates to Office 365 Cloud App Security include:

- App permission policies can be set to automatically revoke access to an OAuth application that is considered risky. To make the intent of these policies clearer, Microsoft changed the name of App permission policies to OAuth Apps.
- Cloud Discovery can accept log files from Forcepoint Web Security Cloud, has enhanced support for the i-Filter parser, and features an enhanced custom log parser.
- Docker on Windows can be used to automatically upload log files; supports Windows 10 (Fall Creators Update and newer) and Windows Server 1709 and later.
- OAuth app policies can be scoped to groups, to enable greater nuance in how policies are applied.
- Support for Microsoft Dynamics activities that are supported in the Office 365 audit log.
- Several new anomaly detection policies, such as data exfiltration, deletion of multiple virtual machines in a single session, and suspicious inbox manipulation rules. These policies provide warning and early detection for data breaches, account compromise, malicious internal actors, and more.
- Integration with Microsoft Flow, so administrators can create more advanced alert and action pathways.

Analysis

- Enabling automated remediation in policies is a good direction for Microsoft (and all CASB vendors). Alerting to an administrator is important, but proactively taking action to prevent or minimize harm is even better.
- Microsoft now offers a solid selection of anomaly detection policies in Office 365 Cloud App Security. It is using generalized insights gained from Office 365 Cloud App Security deployments in the wild to identify the type of problems facing its customers, and doing something about it.
- Both Office 365 Cloud App Security and Microsoft Cloud App Security give administrators the super-power of insight and visibility into what is happening across the service. It enables the early detection of bad actions, compromised accounts, and malicious internal actors.

About

- Date - December 26, 2018
- Announced via - Microsoft Docs
- Implications for - Office 365 Cloud App Security
- Tagged as - Security

Multi-Geo Available in India

Description

Microsoft announced that from December 2018, India will become available as a satellite geo-location for its Multi-Geo customers. This means that Multi-Geo customers can select India as a satellite geo for specific users, and their Exchange Online mailbox and OneDrive for Business contents will be homed in India.

Microsoft also said that once Multi-Geo is available for SharePoint Online that it will be possible to home SharePoint sites in India as well.

Analysis

India's new Personal Data Protection Bill of 2018 mandates local in-country data residency. All data must be stored in country, although while some data can also be stored out-of-country, "critical" personal data - a term that is not defined in the bill - must be stored exclusively within India.

About

- Date - December 7, 2018
- Announced via - Office 365 Blog
- Implications for - Tenant Architecture
- Tagged as - Security

Hosted Apps Obfuscated to Microsoft Cloud App Security

Description

Cloud apps running on cloud hosting platforms are reported in aggregate in Microsoft Cloud App Security under the banner of the cloud hosting platform, and not broken down into data on usage for the cloud app directly. For example, cloud apps running on Fastly and in some cases Amazon Web Services (AWS), are reported as part of aggregated data for Fastly and AWS, not the actual cloud app that is being used.

Microsoft acknowledges that Microsoft Cloud App Security is lacking in this regards, and is actively investigating how to address the shortcoming.

Analysis

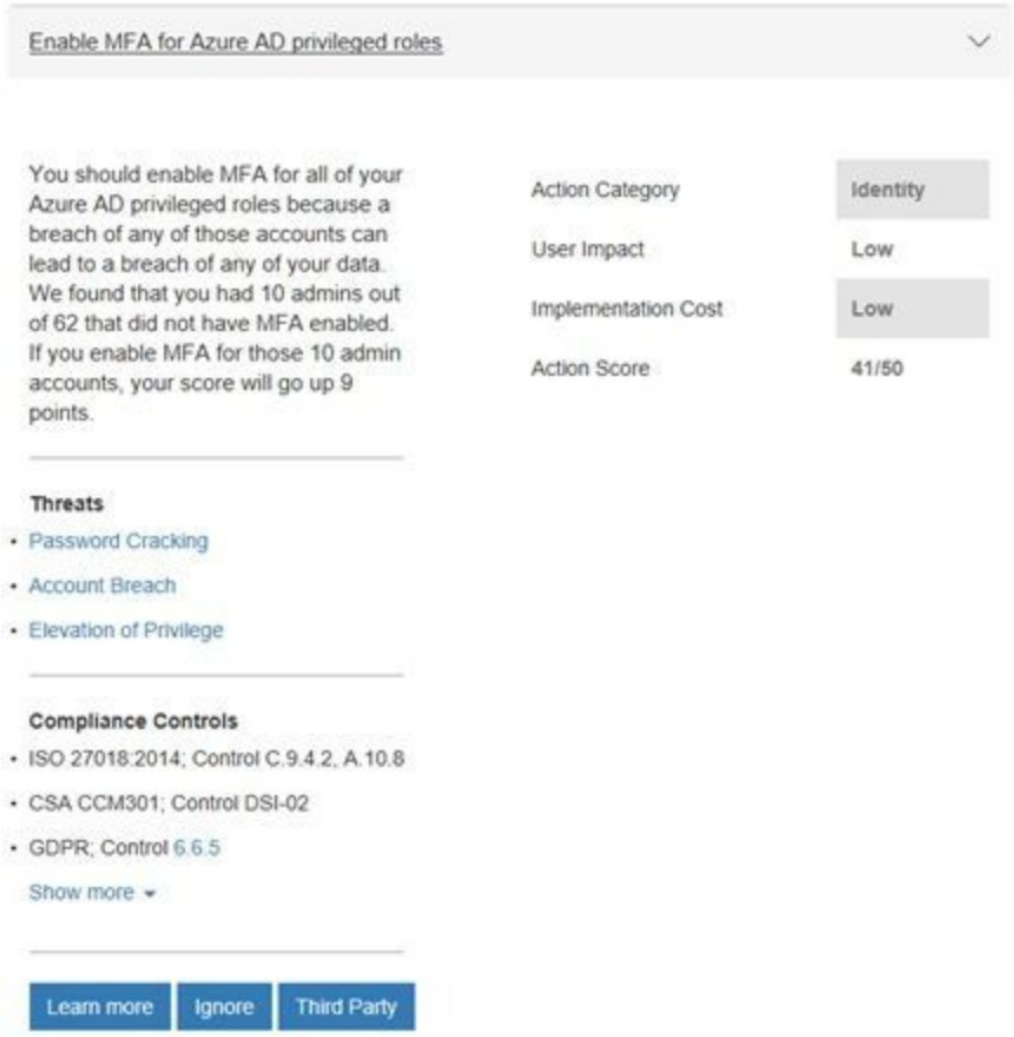
- The lack of app-level insight means security professionals are blind to the potential threats in cloud services. Employees may be using malicious apps or apps with security vulnerabilities that are aggregated under an overall cloud services platform that presents as being fit-for-purpose.

About

- Date - October 11, 2018
- Announced via - Microsoft Cloud App Security Community
- Implications for - Microsoft Cloud App Security
- Tagged as - Security

Microsoft Secure Score Updates

Description



Microsoft released two minor enhancements to Microsoft Secure Score:

- Added a link to the compliance standards, regulations and controls from Compliance Manager, showing the connection between an item in Secure Score and the underlying compliance rationale. Microsoft intends to add more hyperlinks to these compliance controls, and has added them to give Compliance Professionals a better sense of how their work impacts their organization's Secure Score standing.
- Added a status icon to the Secure Score dashboard to highlight if the data is not up-to-date. The icon does not display if everything is working as it should, but is shown if there is a problem. Any remediation steps that need to be taken are noted in a hover-over to the icon.

Analysis

- Secure Score is a simple but clever way of quantifying the security and risk posture of an organization's use of Office 365 (and other Microsoft 365 services), along with specific guidance on how to improve the score on an item-by-item basis.
- The above two changes are minor enhancements, but good small improvement steps to introduce nonetheless.

About

- Date - November 2, 2018
- Announced via - Security, Privacy and Compliance Blog

- Implications for -
- Tagged as - Security

Office 365 Cloud App Security Updates (July - September 2018)

Description

Microsoft introduced several changes to Office 365 Cloud App Security - the trimmed version of Microsoft Cloud App Security for Office 365 - over July-September. Changes were:

- [July 2018] Anomaly detection policies can automatically enforce a remediation, such as suspending the user.
- [July 2018] App permission policies can be used to automatically detect risky OAuth applications and approvals.
- [July 2018] Managed Security Service Providers (MSSPs) can work more easily with Office 365 Cloud App Security. New capabilities allow admin access for external users, and the ability for an administrator with admin rights in multiple tenants to move more seamlessly between each tenant.
- [August 2018] App permission policies can be scoped to work across multiple apps, rather than just one. Apps can be approved or banned, and banning an app revokes all consent previously granted, and does not allow users to grant access in the future.
- [August 2018] A new query that highlights which apps in the discovery tab are GDPR ready.
- [September 2018] The menu bar moved from across the top to the left hand side. This was to introduce similarity with other Microsoft security portals, such as the Admin Center and the Security & Compliance Center.
- [September 2018] Admins can notify Microsoft of OAuth apps that seem malicious.
- [September 2018] New support for the IBoss Secure Cloud Gateway and Sophos XG for log parsing to identify cloud apps in use on the network.

Analysis

- The increased availability of automated remediation actions is good to see, as is the ability for MSSPs to use the offering with clients.
- Many of the changes of small and incremental, which is the rule of the game now.

About

- Date - September 5, 2018
- Announced via - Microsoft Docs
- Implications for - Office 365 Cloud App Security
- Tagged as - Security

Microsoft's Phish Miss Rate - From Highest to Lowest?

Description

Microsoft talked up its journey during 2018 of enhancing anti-phishing capabilities in Office 365. The diagram below shows Microsoft's internal analysis on phishing miss rates, with the orange bar the Microsoft one. Of the seven vendors in the chart, Office 365 - with both Exchange Online Protection and Advanced Threat Protection - **was the worst performer each month**, except for December against the unnamed Vendor 7. Clearly, Microsoft's EOP and ATP were not working over this initial timeframe.

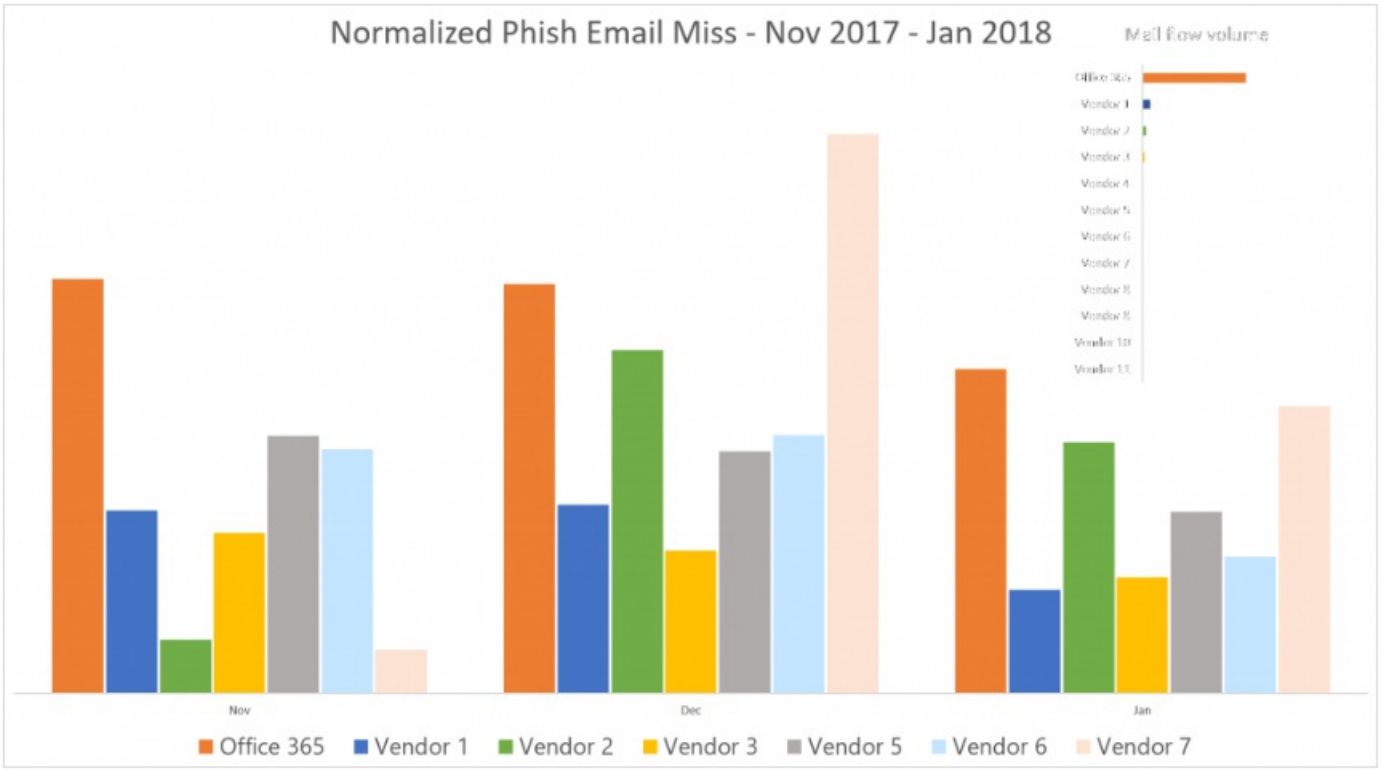
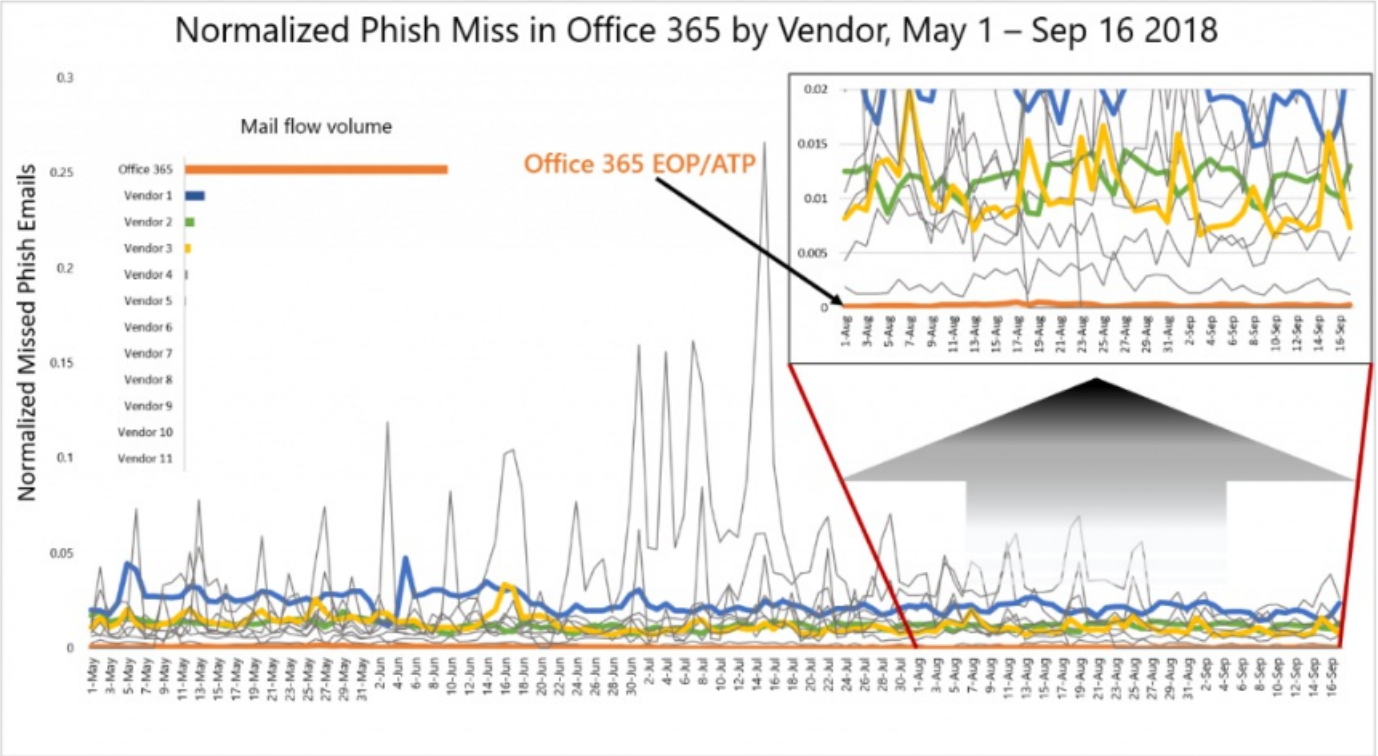


Figure 4. Normalized phish email miss from November 2017 to January 2018 in Office 365 email traffic. Inset shows actual mail flow volume.

It's second diagram - albeit laid out differently and therefore not comparable with the first - now claims that it has the lowest phish miss rate due to its substantial phishing investments during 2018 in four separate categories of phishing attacks. As a result of these investments, Microsoft claims that during 2018 it has so far:

- Blocked 5 billion phishing emails.
- Protected 7 billion URL clicks using Safe Links.
- Detonated 11 billion unique items in Advanced Threat Protection sandboxing.



Analysis

- The effectiveness rate depicted is a combination of EOP and ATP. Every Office 365 subscriber gets EOP, thus making it a basic service element. Only Office 365 E5 subscribers - or those getting ATP through an add-on - have access to ATP. Thus Microsoft's phishing capabilities are inexplicably linked to Advanced Threat Protection. Without ATP the efficacy rate would be much worse.
- All reported figures are internally generated by Microsoft and not via a third-party testing service. It is impossible to know whether the two diagrams reflect a true transformation in the efficacy of Microsoft's phishing prowess, or merely tell its latest "marketing story."
- At Ignite 2017 (last year), the highlighted marketing story was that Office 365 ATP secured three times more users than its closest competitor (who was unnamed). In light of the above research - if you at least accept Microsoft's own admission that it was fairly useless over the November 2017-January 2018 timeframe - the true story was that while it secured three times more users (in quantity), it offered less effective protection for all of them. Every single organization would have seen more effective protection using a third-party service for threat protection.
    - See Microsoft Ignite 2017 blog post with the 3x number

About

- Date - October 17, 2018
- Announced via - Microsoft Secure Blog
- Implications for - Advanced Threat Protection
- Tagged as - Security

Safe Links in Microsoft Teams

Description

Microsoft announced that Safe Links from Advanced Threat Protection will protect links received in Microsoft Teams, starting in Quarter 2 of CY 2019 (April-June). This means that the safety of the destination link is evaluated at time-of-click, but only by looking for the link in a blacklist. The actual site is not checked dynamically by Safe Links.

Analysis

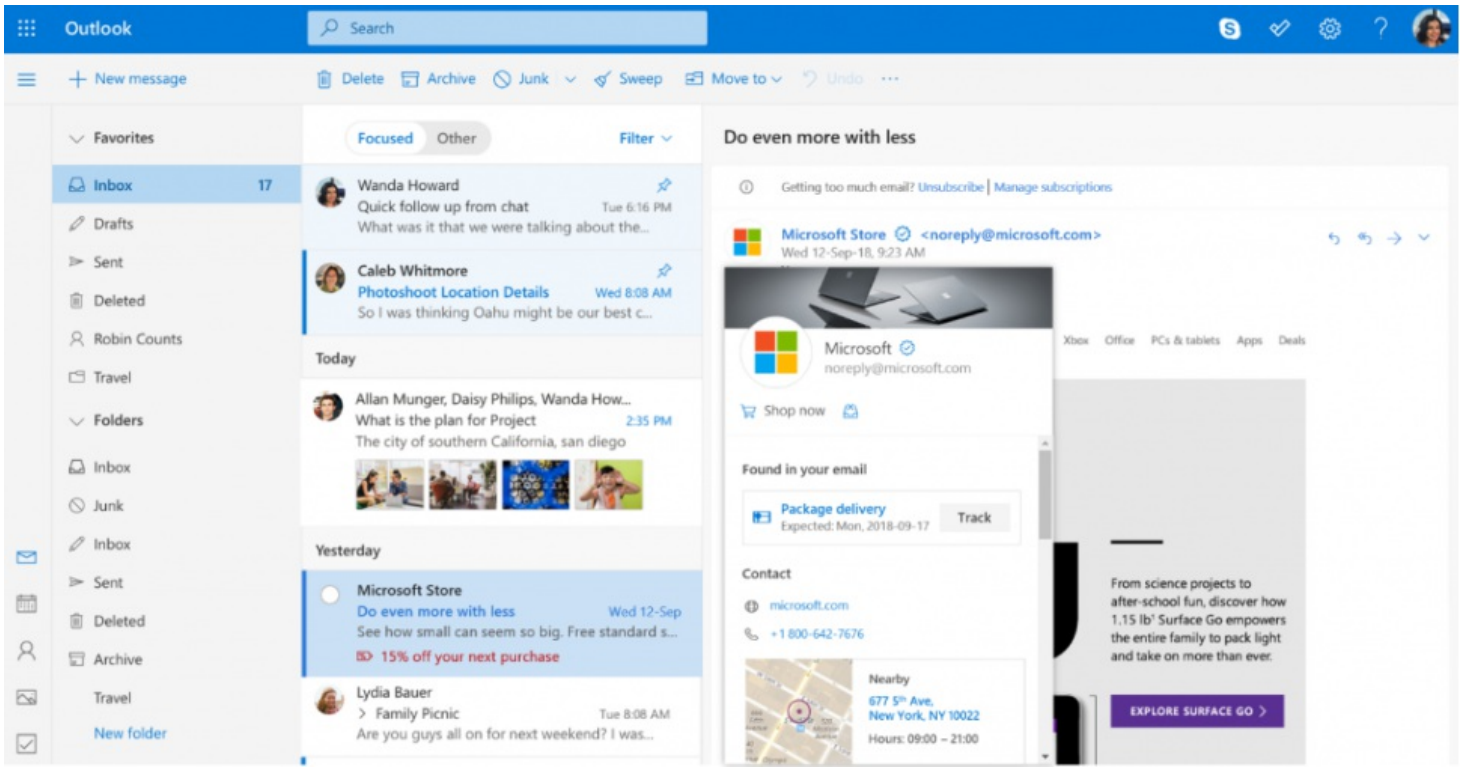
- In principle, extending Safe Links to every place a link can be clicked is the right direction for Microsoft. Users should have global protection against malicious sites from anywhere in Office 365. Partial protection that's enabled in some applications and disabled in others is not good enough.
- Safe Links is part of Advanced Threat Protection, which requires an E5 license or to be licensed as a separate add-on.
- Safe Links will check a URL at time-of-click against known blacklists of malicious sites. It does not actually evaluate for the presence of threats at the destination URL at time-of-click. Safe Links will pass a user through to a malicious web site if that site is not on a blacklist of known malicious sites. Some third party solutions offer dynamic URL scanning to check suspicious URLs before the time-of-click.

About

- Date - October 10, 2018
- Announced via - Microsoft 365 Roadmap 34298
- Implications for - Advanced Threat Protection
- Tagged as - Security

Verified Businesses in Outlook.com

Description



Microsoft introduced a new programme where businesses (brands) can register their details with Microsoft, and once registered, when an email from the business (brand) is received by an Outlook.com user, a verified icon will be displayed. This is intended to enable end users to more easily identify legitimate messages from legitimate businesses in Outlook.com, which is a problem due to the increase in phishing and spam. While some messages are easily spotted as fake, an increasing proportion are so close to looking real that it is becoming difficult to discern the real from the fake. A verified business icon associated with an email message will give the user high comfort that the message is valid, and therefore they will be more likely to read it rather than delete it unread as a safeguard.

Analysis

- This does not affect messages received in Outlook (Office 365). This is an Outlook.com feature, but if the capabilities are also used as a signal to reduce phishing and spam, the capability could be applied more broadly across Microsoft's email properties (including Exchange Online and Outlook in Office 365). This is an interesting additional test for message validity; it essentially adds a proprietary extension for checking for impersonation.
- Dropbox and Office 365 phishing messages that attempt to do account compromise are commonly let through by the filters in Office 365. What's weird, however, is that the vast majority (all?) have internal links that point to a non-Dropbox or non-Office 365 destination. While this is pure speculation, if the process of registering a business could include the pre-declaration of valid click-through destinations, then additional signals would be available for reducing phishing attempts from common brands, including Microsoft.
- If a validly registered business is subject to account credential compromise, and the hacker distributes email messages with a malicious payload that reaches Outlook.com users, the supposed higher trust of a verified business may lead recipients to trust the contents of the message more than they should.

About

- Date - October 2, 2018
- Announced via - Windows Blogs
- Implications for -
- Tagged as - Security

Multi-Geo for SharePoint and Office 365 Groups

Description

Microsoft announced that Multi-Geo for SharePoint Online and Office 365 Groups (specifically the SharePoint Site and the associated mailbox) will be added to Multi-Geo in quarter 1 of 2019. Multi-Geo for these two workloads will go into private preview in late 2018. This expands the workloads in Office 365 that are multi-geo enabled from two user-centered services (Exchange Online and OneDrive for Business) to services that could have multiple owners.

Details for Multi-Geo for SharePoint Online and Office 365 Groups are:

- Each Multi-Geo user should have their preferred data location stored in Azure AD. This setting is used to determine where new SharePoint sites and Office 365 Groups are created. It does not appear possible for a given user to create a site in a different data location, however.
- SharePoint Hub Sites can aggregate sites from the main tenant or any of the satellite geos. It does not matter where the site is located for inclusion in a Hub site, although clearly site access permissions will come into play when a given user attempts to view or work with the sites in a Hub site.
- SharePoint Home will show news updates curated from relevant sites for each user. This is powered by the Office Graph, and access rights will ensure that what a person cannot see is not shown.
- When first introduced at Ignite 2017, Multi-Geo was limited to Office 365 tenants with at least 10,000 seats. In April 2018, this was reduced to 5,000 seats. In October 2018, this was reduced to 2,500 seats, with the specifics being that at least 5% of these seats must be enabled for Multi-Geo (that is, 125 seats).

Analysis

- Microsoft explicitly states that Multi-Geo does not deliver GDPR compliance, on the basis that GDPR does not mandate where data is stored. Organizations can, however, use Multi-Geo to enable data residency in specific geographies, thereby simplifying their own internal data residency requirements and satisfying the demands of regulators.
    - Note that India's new Personal Data Protection Bill of 2018 does mandate local in-country data residency. All data must be stored in country, although while some data can also be stored out-of-country, "critical" personal data - a term that is not defined in the bill - must be stored exclusively within India.
    - Microsoft may also be stating the GDPR compliance exclusion because it can not guarantee that all data is stored within a given region, country or data center. That is, Office 365 is architectured to work across a global network of data centers, and some services - such as Azure AD (which contain personal data on individuals) - is a non-regional service. Stating the exclusion in a blanket way removes the need for Microsoft to re-architect Office 365 for in-country and in-region data residency, a strategy which it attempted with the German data center in 2015, but is subsequently deprecating. See Microsoft Announces New Data Centers for Germany (August 2018).
- The reduction in seat count minimum in one year - from 10,000 when announced at Ignite 2017 to 2,500 in October 2018 - takes the service in the right direction. Many customers have voiced a desire for Multi-Geo capabilities, but have been prevented from using the service due to having fewer than 10,000 or 5,000 seats. Microsoft notes that it wants to reduce the minimum even further. Overall, the minimum seat threshold has been used to give Microsoft time to get the service and its associated support processes right before opening it to the masses.
- Microsoft has no way to prevent cyber-squatting for geo domain names. For example, if the Office 365 tenant name is tenantname, the URL for the main tenant on SharePoint Online would be tenantname.sharepoint.com. A geo domain name would then be, for example, tenantnameeur.sharepoint.com for Europe, and tenantnameaus.sharepoint.com for Australia. But these are full domain names that could be preempted by anyone creating a demo tenant with that name. Microsoft's guidance is to have a number of options available for each geo domain name. Microsoft may have to introduce a naming policy to prevent this in the future, or switching to a sub-sub-domain name approach, where something like eur.tenantname.sharepoint.com or aus.tenantname.sharepoint.com is used instead.

About

- Date - September 27, 2018
- Announced via - Office 365 Blog
- Implications for - Tenant Architecture

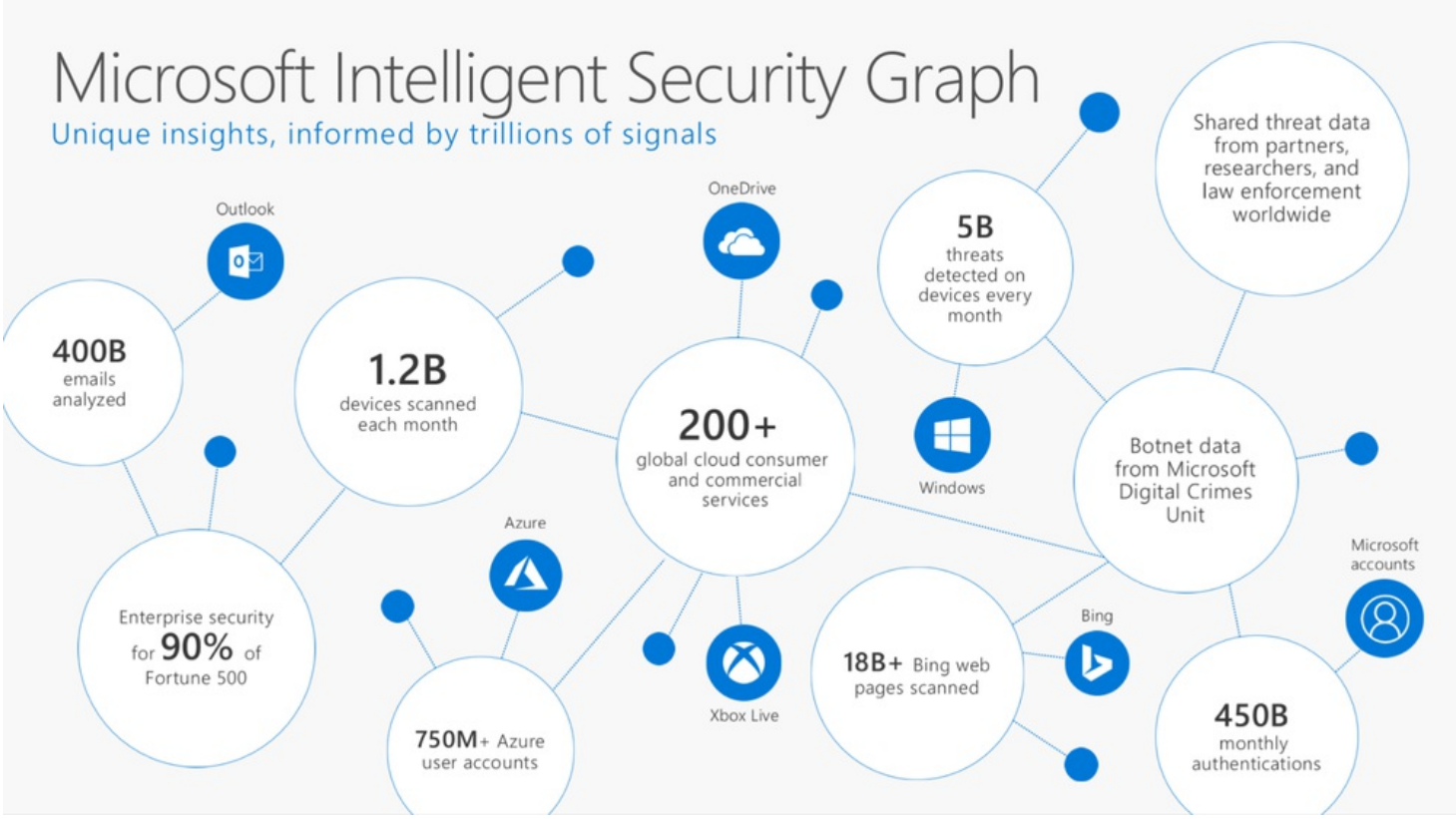
- Tagged as - Security

Threat Protection Review and Assertions

Description

In the weeks leading up to Microsoft Ignite 2018, the Office 365 Security, Privacy and Compliance team delivered a couple of blog posts reviewing recent progress in Office 365 Advanced Threat Protection. Recent additions include:

- Safety tips in Outlook can be turned on or off by an admin.
- Admins have the ability to set a policy on what action should be taken when malicious spoof is detected.
- Admins have greater control over the strength of spoof filters.
- Safe Links is now applied to internal email, to help address account compromise situations through credential theft / compromise.
- New reports available for Office 365 admins regarding malware, phish and user-generated messages.
- Anti-impersonation protections enforced in real-time for spoofing (both domain spoofing and user impersonation spoofing).



Microsoft claims that:

- Phishing was the number one threat vector for Office 365 customers in its 2017 security research.
- The Microsoft Intelligent Security Graph provides 6.5 trillion signals per day, some of which are used by Office 365 ATP for distinguishing threats from non-threats.
- Microsoft's malware catch rate is greater than 99.9%.
- Microsoft analyzes 400 billion emails each month, and of these, only detects 600 million as being malicious. That translates to a malicious identification rate of only 0.0015%. This rate is Microsoft's own assertion as to the malware catch rate of ATP and EOP together.

Analysis

- There are few opportunities to gauge the truth of Microsoft's claims about its malware catch rate ("greater than 99.9%"). The claim is self-proclaimed, and is not subject to a review by an independent third-party.

- If Office 365 ATP and EOP together only identify 0.0015% of all email as malicious, then its services are fundamentally broken and ineffective. This would explain why end users still receive many malicious emails every day; ATP and EOP just can't see the malicious intent. The services don't work, because 99.9985% of the email stream is flagged as non-malicious.
    - In user terms, assuming 150 million active users of Office 365, that's roughly 2700 emails per person per month, or around 120 per business day (sent and received). Microsoft's catch rate of 0.0015% stops four (4) messages per month per user from getting delivered. Undoubtedly these four messages per month per user are serious threats and should be stopped, but many other threats still get delivered.
    - [**Comparison**] One vendor of anti-spam and anti-malware tools analyzed the email stream for one of its large enterprise customers. Using its email security tools, of the 1.2 million emails delivered over the month, 7300 were identified as malware or phishing. This represents a malicious identification rate of 0.6%, or 400 times greater than Microsoft's rate. Where this vendor identified 7300 messages, Microsoft would have only identified 18.
    - [**Comparison**] Symantec's recent Internet Security Threat Report (March 2018) found that users received an average of 16 malicious emails per month, or 4x as many as Microsoft is able to identify.

- Microsoft is over-playing the value of the volume of threat signals it analyzes. If the above catch rate of 0.0015% is accurate, then it lacks the ability to identify the bad from the good. It has too many general-purpose signals to process, and is therefore ineffective at distinguishing those that carry threat. The 6.5 trillion daily signals blind ATP and EOP instead of giving sight.

- Some customers and business partners have been vocal in pointing out that ATP is ineffective as a total email security solution, and that many threats are still getting delivered to user inboxes. For example, that ATP does not stop emails with malicious links from getting through to user's inboxes (which is true, given protection is analyzed at click time), and that some malicious links are noted as being safe but actually link to a malicious payload. If ATP declares a link safe, less security-conscious end users will become the victim of a successful attack.

About

- Part 1 on Staying Ahead of Modern-Day Attacks: Recent Updates to Office 365 ATP and its Real-World Impact (September 13, 2018)
- Part 2 on Staying Ahead of Modern-Day Attacks: Defense-at-Scale Approach with Office 365 ATP (September 21, 2018)
- UserVoice discussion on Phishing Attacks Using Office 365 Compromised Accounts
- Implications for - Advanced Threat Protection
- Tagged as - Security

Windows Virtual Desktop

Description

Microsoft announced Windows Virtual Desktop, as part of Microsoft 365. Hosted on Microsoft Azure, Windows Virtual Desktop combines Windows 10 (or Windows 7 with Extended Security Updates), Office 365 ProPlus, and the security and compliance capabilities from Office 365, Azure AD, and Enterprise Mobility + Security. It is touted as a multi-user Windows 10 offering, and Microsoft highlights opportunities including:

- Tight control for compliance and security purposes over the desktop experience, for firms in regulated industries.
- The ability to easily provision desktops that offer only specific apps to certain employees.
- Alternatives for providing mobile workers and firstline workers with a desktop experience that's available on multiple devices and device form factors.

Microsoft said it also has an ecosystem story for Windows Virtual Desktop, although specific details for this won't be released until later.

Windows Virtual Desktop was announced, with a public preview due before the end of 2018.

Analysis

- Server virtualization changed the face of IT, enabling a more agile and rapid deployment approach that maximized the use of physical resources.
- Microsoft is extending this approach to end users, bundling up many of its resources and assets to deliver a ready-to-run desktop experience for people that don't need a dedicated device.
- Windows Virtual Desktop is complementary to the new Microsoft Managed Desktop, which additionally includes a physical device supplied by and managed by Microsoft (although not necessarily a Microsoft device).
- Microsoft is increasingly becoming the IT department for organizations, rather than just supplying the tools of the trade for the organization to equip its own IT department. Office 365 delivers productivity apps, Dynamics 365 delivers business apps (with greater maturity needed in this offering, but it's improving), Enterprise Mobility + Security and Azure Active Directory deliver security and identity capabilities, and there are now two ways to also get endpoint capabilities (one physical, one virtual). Once you add the richness and breadth of Microsoft Azure to the mix, Microsoft is positioning itself to do everything.

About

- Date - September 24, 2018
- Announced via - Microsoft 365 Blog
- Implications for -
- Tagged as - Security

Specific Admin Roles for Microsoft Teams

Description

Office 365 Global Administrators have full administrative rights to Microsoft Teams. In order to decrease the scope of administrative control offered to an admin making changes or troubleshooting in Microsoft Teams, Microsoft introduced four Teams-specific admin roles. One scopes full control over Teams only, and three provide control over subsets of the communications capabilities in Microsoft Teams that have come across from Skype for Business Online.

The four new roles are:

- Teams Service Administrator - complete control over Teams admin.
- Teams Communications Administrator - manage calling and meetings features in Microsoft Teams
- Teams Communications Support Engineer - troubleshoot communications issues with advanced tools.
- Teams Communications Support Specialist - troubleshoot communications issues with basic tools.

Admin Roles in Microsoft Teams	Teams Service Administrator	Teams Communications Administrator	Teams Communications Support Engineer	Teams Communications Support Specialist	Specifics include
Manage meetings	■	■			Meeting policies, configurations, conference bridges
Manage voice	■	■			Calling policies, phone number inventory and assignment
Manage messaging	■				Messaging policies
Manage all org-wide settings	■				Federation, Teams upgrade, Teams client settings
Manage teams and associated settings	■				Manage membership (from October 2018)
View user profile page	■	■	■	■	
Troubleshoot user call quality problems	■	■			Advanced troubleshooting toolset
View all call record information	■	■	■		Troubleshooting calls in Call Analytics
View user information for one specific user	■	■		■	Troubleshooting calls in Call Analytics

These roles can be assigned in Azure AD, but not yet in Office 365.

Analysis

- This is a solid addition to the administration options for Microsoft Teams. An Office 365 Global Administrator has complete control over everything in Office 365, and needing to use that role for administering Microsoft Teams was a poor design choice. The addition of scoped roles illustrates the ongoing maturity of Microsoft Teams.
- Managing telephony capabilities has long required a specialized skillset, often not held by general-purpose IT administrators. The Teams Service Administrator and Communications Administrator roles will enable IT administrators with specialized telephony capabilities to have suitably scoped control over the calling and communications infrastructure behind Microsoft Teams.
- As with many scoped roles, the applicability of these new roles apply more to larger Office 365 tenants, where the scope of complexity requires division of duties and specialized training in specific Office 365 services and workloads. Smaller Office 365 tenants can use more general-purpose roles, and generally have much less complexity to deal with.

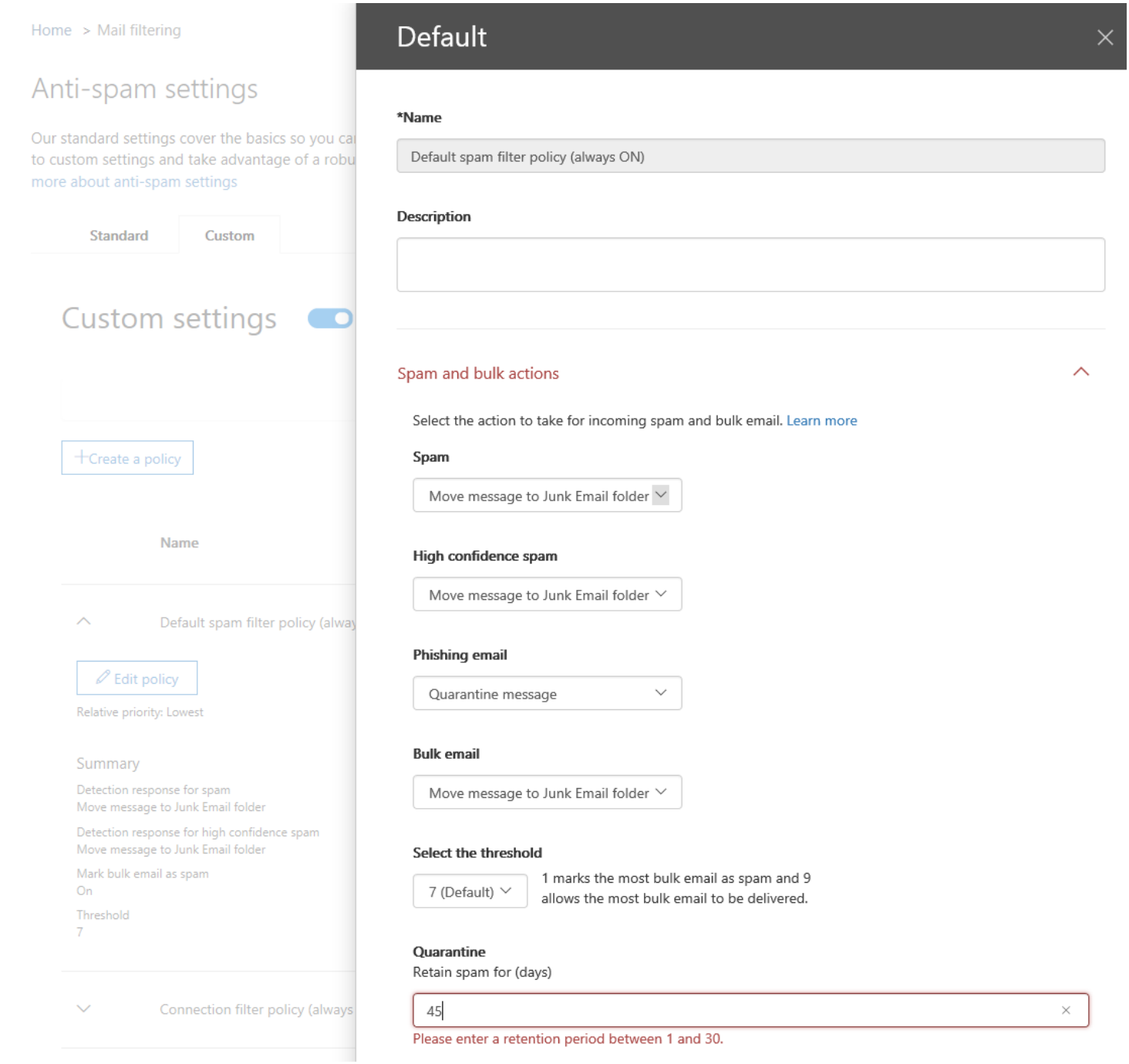
About

- Date - September 19, 2018
- Announced via - Microsoft Docs
- Implications for -
- Tagged as - Security

Maximum Quarantine Period Increased to 30 Days

Description

Using custom anti-spam settings, it is now possible to set the maximum quarantine period to 30 days. Microsoft says that the default is also 30 days, but a check of a couple of existing tenants has the number still set at 15 days.



Previously this setting was subject to a default and maximum of 15 days.

Analysis

- Osterman Research has previously decried 15 days as being too short as the maximum retention period. Doubling this is a good start, and will enable users on regular vacations to not miss important messages that are inadvertently moved to the quarantine. Those on extended vacation may still be impacted, but that may come down to delegation to another person while away for more than 30 days.

About

- Date - September 5, 2018
- Announced via - Microsoft Docs
- Implications for - Spam Quarantine
- Tagged as - Security

Microsoft Announced New Data Centers for Germany

Description

Microsoft signalled its intent in March 2018 to elevate its data center approach in Germany to be consistent with the rest of the world. The current approach - called Microsoft Cloud Germany and introduced in 2015 - provides an isolated Office 365 experience that enables German companies to comply with Germany's data residency regulations. This included Microsoft appointing a local German company to act as the data trustee, thus avoiding the situation of a US company having access to Germany customer data. The creation of a separate approach for Germany, however, meant that customers would not have access to the new Office 365 services, and more fundamentally, that the Office 365 data center strategy for the rest of the world would diverge from the approach in Germany.

On August 31, Microsoft announced that its two new data centers will be ready for new customers starting in the fourth quarter of 2019. These are located in Berlin and Frankfurt, and will be first-class data centers and part of a consistent approach to the delivery of services through Microsoft Azure and Office 365.

- Microsoft Azure will be available from 4Q 2019, with Office 365 to follow in 1Q 2020. Microsoft said that Dynamics 365 will be available sometime during 2020.
- Effective immediately, Microsoft is not accepting new customers for the current Microsoft Cloud Germany. New customers for Office 365 will need to choose one of the existing European data center locations, or wait until the new Germany data centers are available. Current customers can continue using Microsoft Cloud Germany, migrate to an existing European data center location, or migrate when the Germany data centers are available.
- The new approach will deliver recent Office 365 services to German customers, who have been denied access due to the Microsoft Cloud Germany approach. These include Azure Information Protection, Microsoft Teams, Microsoft Planner, MyAnalytics and more.

Analysis

- Embracing a globally consistent approach to data center deployment and operation is a good move by Microsoft, and will enable it to deliver access to recent and new Office 365 services. Not having these available in the German market was diminishing the overall value proposition of Office 365 in Germany, in comparison to other countries. The release of the new data centers will eliminate the need for separate and specific Office 365 plan variants for the German market.
- There is no mention of how Microsoft has addressed the issue of a US company having access to German customer data, a situation it avoided with the earlier approach through a German company acting as the data trustee. Perhaps Microsoft's investments in regulatory compliance and operational proof/evidence in other markets during 2015-2018 have eliminated this specific requirement.
- China is also a non-consistent Office 365 location, and is different again from the Germany approach of 2015. In China, Microsoft has licensed certain Office 365 technologies to 21Vianet. It remains to be seen if Microsoft will change its China strategy to be in line with its consistent global approach for Office 365.

About

- Date - August 31, 2018
- Announced via - Microsoft News Centre Europe
- Implications for - Tenant Architecture
- Tagged as - Security

Teams Data Residency in Australia and Japan

Description

Microsoft announced that customers creating a new tenant in Australia and Japan will be able to store their conversation and chat data from Microsoft Teams in country. This change is effective August 27, 2018 for all new customers.

The specifics are the same as for the recent Canada announcement:

- This only applies to new customers creating a new tenant in Australia or Japan, and only to conversation and chat data in Microsoft Teams. SharePoint Online, OneDrive for Business, and Exchange Online are already homed in Australia or Japan, if that's where the tenant is created.
- Current customers will be able to migrate their conversation and chat data in Microsoft Teams to Australia or Japan during 2019 sometime. Microsoft has promised a migration service to facilitate this process.
- Other data in Microsoft Teams is unaffected, which primarily means the files shared during conversations, meetings and chats. Where these are stored depends on where the SharePoint site for the team is located, and where the user sharing a file into a private chat or meeting has their OneDrive for Business located. If these are in Australia or Japan, those files will be stored in the appropriate country.
- Customers using third-party storage services or partner apps that store data are dependent on where those third-parties are geo-located. If they are not in Australia or Japan, then the data will not be resident within Australia or Japan.

Analysis

For all practical purposes right now, this announcement is just a signaling device at this time that a change is coming. It may make a difference for Australian and Japanese organizations evaluating Office 365 right now, but everyone already using Office 365 is stuck with the current state for a while yet.

Microsoft Teams Data	Stored In	Current Customers	New Customers
Conversation Data	Azure Chat Service	Hong Kong, Singapore, or South Korea	Australia or Japan
Chat Data	Azure Chat Service	Hong Kong, Singapore, or South Korea	Australia or Japan
Images	Azure Media Services	Hong Kong, Singapore, or South Korea	Australia or Japan
Media	Azure Media Services	Hong Kong, Singapore, or South Korea	Australia or Japan
Files			
Files Shared in a Channel	SharePoint Site	Depends on where the team's SharePoint site was created	Depends on where the team's SharePoint site was created
Files Shared in a Private Chat	OneDrive for Business account of the user who shared the file	Depends on where the user's OneDrive is stored	Depends on where the user's OneDrive is stored
Files Shared in a Chat During a Meeting/Call	OneDrive for Business account of the user who shared the file	Depends on where the user's OneDrive is stored	Depends on where the user's OneDrive is stored
Files Stored in a Third Party Service	Third Party File Storage Service	Depends on where the third-party file storage service stores their files	Depends on where the third-party file storage service stores their files
Tabs	Stores no data; just a link	NA	NA
Other Partner App	Partner App Data Location	Depends on where the partner app stores its data	Depends on where the partner app stores its data

In the table above, I try to pick out the specifics on where your data is located. Data location depends on how / why / who / what / where. In looking at the above:

- Brand New Customer in Australia or Japan – yes, you could have all your Microsoft Teams data stored in Australia or Japan.
- Existing Customer in Australia or Japan – your SharePoint and OneDrive storage and Exchange mailboxes will be stored in country, but your Teams data is currently stored in Hong Kong, Singapore and/or South Korea. From 2019, you will have the option of migrating it to Australia or Japan.
- Existing Customer with Multi-Geo – *if* the SharePoint site for the Team was created in Australia or Japan, and *if* the user sharing a file has their OneDrive also located in Australia or Japan, then your files will be stored in region, but until you migrate in 2019, your conversation and chat data in Teams will be stored out of country in the associated geo datacenter (Hong Kong,

Singapore, or South Korea - or other).

About

- Date - August 27, 2018
- Announced via - Microsoft Teams Blog
- Implications for - Tenant Architecture
- Tagged as - Security

Threat Defense on Mobile Devices with Intune and BETTER

Description

Customers using BETTER Mobile can use the BETTER ActiveShield service to notify Microsoft Intune of security or content vulnerabilities on iOS and Android devices. The additional threat signals from BETTER ActiveShield work in conjunction with the signals that Intune already pays attention to, and if required, a conditional access policy will be enforced on the mobile device. For example, if an app is exhibiting malicious style behaviors, Intune and Azure AD will enforce a conditional access policy or mitigation, such as requiring a second authentication, blocking data flow to corporate apps, or preventing access on the device to corporate apps. If the device can be remediated, access will be restored.

Microsoft already supports integration with several mobile threat defense vendors; BETTER Mobile is the latest to join this group. To encourage exploration of its capabilities, BETTER Mobile is offering up to 50 licenses at no charge for 18 months to any Microsoft Intune customer.

Analysis

Integration with third-party specialist mobile threat defense vendors enables the capturing of signals that would otherwise be invisible to Microsoft Intune. While Intune already captures many signals, the partnering strategy allows Microsoft to focus on enhancing its core capabilities in Intune while enabling third-parties to supplement these for organizations that require greater and better coverage.

BETTER Mobile is one of the options available for integration with Microsoft Intune. Microsoft supports integration with several mobile threat defense vendors (albeit only one per tenant), providing options to customers but also signaling those third-party vendors that have approved integrations.

About

- Date - August 24, 2018
- Announced via - Enterprise Mobility + Security Blog
- Implications for - Mobile Threat Defense
- Tagged as - Security

Anti-Spoofing Added to All Exchange Online Protection Plans

Description

Microsoft offers enhanced anti-spoofing capabilities in the Office 365 Enterprise E5 plan (these are also available in the Advanced Threat Protection add-on). One of these capabilities enables an administrator to specify what do to with messages that fail implicit email authentication checks, with the options being to move the offending message to the recipients' Junk Email folder (the default option) or to move such messages to quarantine. E5/ATP customers have had the ability to specify a behavior different to the default in Office 365.

Starting mid-September and taking until early October to roll out, Microsoft announced that this capability will transition to being general-purpose in Office 365, available to all customers as a feature of Exchange Online Protection. The change, therefore, is that messages which fail implicit authentication will be routed by default to junk mail, rather than being delivered to the recipient's inbox.

Analysis

It is unclear what specifically will and will not be made generally available out of the anti-spoofing capabilities to Exchange Online Protection customers. It seems like the above gives non-E5/ATP customers the ability to use the newly available default anti-spoofing policy, and to modify the default one as required. What is unclear is how much of the spoof intelligence capabilities - also in E5/ATP only - will also be released for generalized consumption. The Message Center announcement makes reference to spoof intelligence both directly and indirectly; directly by name, and indirectly by referring to its capability for blocking or allowing domains allowed to send spoofed mails.

It doesn't seem like it costs Microsoft much to offer this and make enhanced anti-spoofing protection available to all customers. And by reverse, if an increased number of invalid messages are pushed to junk or quarantine instead of to the user's inbox, the perception of service quality will rise.

About

- Date - August 16, 2018
- Announced via - Office 365 Message Center
- Implications for - Exchange Online Protection and Advanced Threat Protection
- Tagged as - Security

Teams Data Residency in Canada with Others to Come

Description

Microsoft announced that customers creating a new tenant in the Canadian geo will be able to store their conversation and chat data from Microsoft Teams in country. For a tenant already created in the Canadian geo, the conversation and chat data has been stored in the United States region. Effective August 10, new Canada-based tenants will have Microsoft Teams data stored in Canada.

Note that the specifics are important:

- This only applies to new customers creating a new tenant in Canada, and only to conversation and chat data in Microsoft Teams. SharePoint Online, OneDrive for Business, and Exchange Online are already homed in Canada, if that's where the tenant is created.
- Current customers will be able to migrate their conversation and chat data in Microsoft Teams to Canada during 2019 sometime. Microsoft has promised a migration service to facilitate this process.
- Other data in Microsoft Teams is unaffected, which primarily means the files shared during conversations, meetings and chats. Where these are stored depends on where the SharePoint site for the team is located, and where the user sharing a file into a private chat or meeting has their OneDrive for Business located. If these are in Canada, those files will be stored there.
- Customers using third-party storage services or partner apps that store data are dependent on where those third-parties are geo-located. If they are not in Canada, then the data will not be resident within Canada.
- The same treatment will be available for Australia and Japan before the end of August 2018.

Analysis

For all practical purposes right now, this announcement is just a signaling device at this time that a change is coming. It may make a difference for Canadian organizations evaluating Office 365 right now, but everyone already using Office 365 is stuck with the current state for a while yet.

Microsoft Teams Data	Stored In	Current Customers	New Customers
Conversation Data	Azure Chat Service	United States	Canada
Chat Data	Azure Chat Service	United States	Canada
Images	Azure Media Services	United States	Canada
Media	Azure Media Services	United States	Canada
Files			
Files Shared in a Channel	SharePoint Site	Depends on where the team's SharePoint site was created	Depends on where the team's SharePoint site was created
Files Shared in a Private Chat	OneDrive for Business account of the user who shared the file	Depends on where the user's OneDrive is stored	Depends on where the user's OneDrive is stored
Files Shared in a Chat During a Meeting/Call	OneDrive for Business account of the user who shared the file	Depends on where the user's OneDrive is stored	Depends on where the user's OneDrive is stored
Files Stored in a Third Party Service	Third Party File Storage Service	Depends on where the third-party file storage service stores their files	Depends on where the third-party file storage service stores their files
Tabs	Stores no data; just a link	NA	NA
Other Partner App	Partner App Data Location	Depends on where the partner app stores its data	Depends on where the partner app stores its data

In the table above, I try to pick out the specifics on where your data is located. Data location depends on how / why / who / what / where. In looking at the above:

- Brand New Customer in Canada geo – yes, you could have all your Microsoft Teams data stored in Canada.
- Existing Customer in Canada geo – your SharePoint and OneDrive storage and Exchange mailboxes will be stored in Canada, but your Teams data is stored in the United States currently. From 2019, you will have the option of migrating it to Canada.
- Existing Customer with Multi-Geo – *if* the SharePoint site for the Team was created in the Canadian geo, and *if* the user sharing a file has their OneDrive also located in the Canadian geo, then your files will be stored in region, but until you migrate in 2019, your conversation and chat data in Teams will be stored out of geo (United States or other).

About

- Date - August 10, 2018
- Announced via - Microsoft Teams Blog

- Implications for - Tenant Architecture
- Tagged as - Security

Microsoft Cloud App Security and AWS S3

Description

Microsoft discussed the ability for Microsoft Cloud App Security (MCAS) to provide insight into usage of Amazon Web Services S3 buckets, including mis-configurations and login activities. This insight is achieved through the use of the AWS App Connector. MCAS can be configured to alert on or take action on:

- When an S3 bucket has public read access settings, in case the S3 bucket should be kept private but is instead publicly accessible. MCAS can also be set to automatically apply a governance action if public read access settings are identified.
- Login activities from countries that are considered abnormal places to login from, such as where the organization does not have a presence, or is known for malicious activity. The activity could be valid - such as when an employee is visiting that country for business or on holiday - but the alert provides the opportunity for an administrator to check authenticity.
- Block downloads of confidential files.
- Protect the download of unclassified files.

Microsoft made reference to numerous recent data breaches at organizations using AWS S3 buckets with the wrong access permissions in place.

Analysis

An AWS S3 bucket provides a storage service for data of all types, and thus can be used for many purposes, including hosting private data or publishing a web site. The former requires tight access control, while the latter requires open or public access. When an S3 bucket is mis-configured, this means that the data access privileges are not set correctly, so that people who are not authorized to access the data are able to. This generally happens when public read access is mistakenly turned on for an S3 bucket. Some organizations use S3 buckets as a backup location for personal and sensitive data, and if this is accessible to non-authorized individuals, several negative consequences can result.

The AWS App Connector works by integrating Microsoft Cloud App Security with Amazon's CloudTrail service for governance, compliance and auditing. Events and activities that are captured by CloudTrail are surfaced in Microsoft Cloud App Security. This integration means that Microsoft decreases the need for an administrator to spend time using AWS CloudTrail, since the events and activities flow through to a single, centralized location in Microsoft Cloud App Security. The insertion of Cloud App Security in the monitoring chain can help decrease the reliance on AWS as a branded service, and also the familiarity of administrators with the AWS toolkit - and thus perhaps decrease the loyalty to AWS over time.

This was not an announcement of new functionality, but rather a reminder of current capabilities available in the full Microsoft Cloud App Security offering. Microsoft promised an update on how MCAS supports Azure as well, but that has not so far been released.

About

- Date - August 3, 2018
- Announced via - Security, Privacy & Compliance Blog
- Implications for - Microsoft Cloud App Security
- Tagged as - Security

Customer Lockbox Access Approver Role

Description

Released - Microsoft released a new role for approving Customer Lockbox requests by Microsoft support engineers. Previously only a Global Administrator could approve these requests. Now anyone can be explicitly named to the Customer Lockbox Access Approver role.

Customer Lockbox is available through:

- Office 365 Enterprise E5 plan
- Office 365 Enterprise E3 plan with the Advanced Compliance add-on

Analysis

The new Customer Lockbox Approval role is a good addition to the service, because weighing down global admins with every small detail on running the service isn't a good design principle nor operational reality. Just because someone is the global admin of a tenant does not equate with them having the right mix of business knowledge to be able to judge between valid and invalid requests by Microsoft engineers during support incidents. Someone else might be better placed to do that, and without giving them global admin access rights, this specific role provide a better chain of authority and approval. Hence the new role is a good nuance to add, and is in line with the general proliferation of feature-specific roles in Office 365.

We observe several weaknesses:

- [**Weakness**] Customer Lockbox requests are not used for all Office 365 workloads. Full coverage is enforced for Exchange Online, SharePoint Online, and OneDrive for Business. Partial coverage is available for Skype for Business. The other Office 365 workloads are excluded.
- [**Weakness**] Global Administrators retain the ability to approve Customer Lockbox requests. It does not appear to be possible to explicitly remove this approval right from a Global Administrator, in order to fully home the role outside of the IT group / department.
- [**Weakness**] Any approver has the full ability to approve a Customer Lockbox request without reference to a second approver. It does not appear possible to require two approvers for Customer Lockbox requests.

About

- Date - August 2, 2018
- Announced via - Security, Privacy & Compliance Blog
- Tagged as - Security

Audit Log Retention Increased to One Year - for Some Users

Description

In a summary post from Microsoft Ignite 2018 about achieving compliance with Microsoft 365, Microsoft disclosed a change to the retention duration for audit log entries. Organizations with Microsoft 365 or Office 365 E5 now have access to one year of audit logs, up from the previous limit of 90 days. This was released to public preview in September 2018.

Organizations with lesser plans than Office 365 E5 still only get 90 days, except when the Advanced Compliance add-on is added to Office 365 E3 or Exchange Online Plan 1.

Analysis

- Increasing the audit log retention duration only for Office 365 E5 and Microsoft 365 subscribers is an interesting twist. Perhaps these are the organizations that have the greatest need for long retention durations, or perhaps it's just yet another push to migrate organizations to the more expensive plans.
- The limited retention duration of audit log entries has been problematic for some time. The ability for an administrator to track through the predicates of an event that was only discovered months after occurring is difficult when the retention timeframe was so short. This left many administrators completely blind to what actually happened.
- The longer retention timeframe for audit log entries only applies to new audit log records created after the longer retention period is released. It does not apply retrospectively to pre-existing audit log entries. For instance, entries that are already 89 days old when the longer retention period is released will be deleted the next day; they will not have their life extended by another 275 days.
- The duration of retention depends on the license of the individual generating the audit log records, rather than an organization-level compliance license. Organizations with mixed license types across its employees will therefore experience differential retention timeframes per user, which could prove to be frustrating. Clearly Microsoft's answer will be to license everyone for E5, Microsoft 365 or the Advanced Compliance add-on.

About

- Date - September 25, 2018
- Announced via - Microsoft 365 Blog
- Implications for - Audit Reports - Office 365
- Tagged as - Archiving

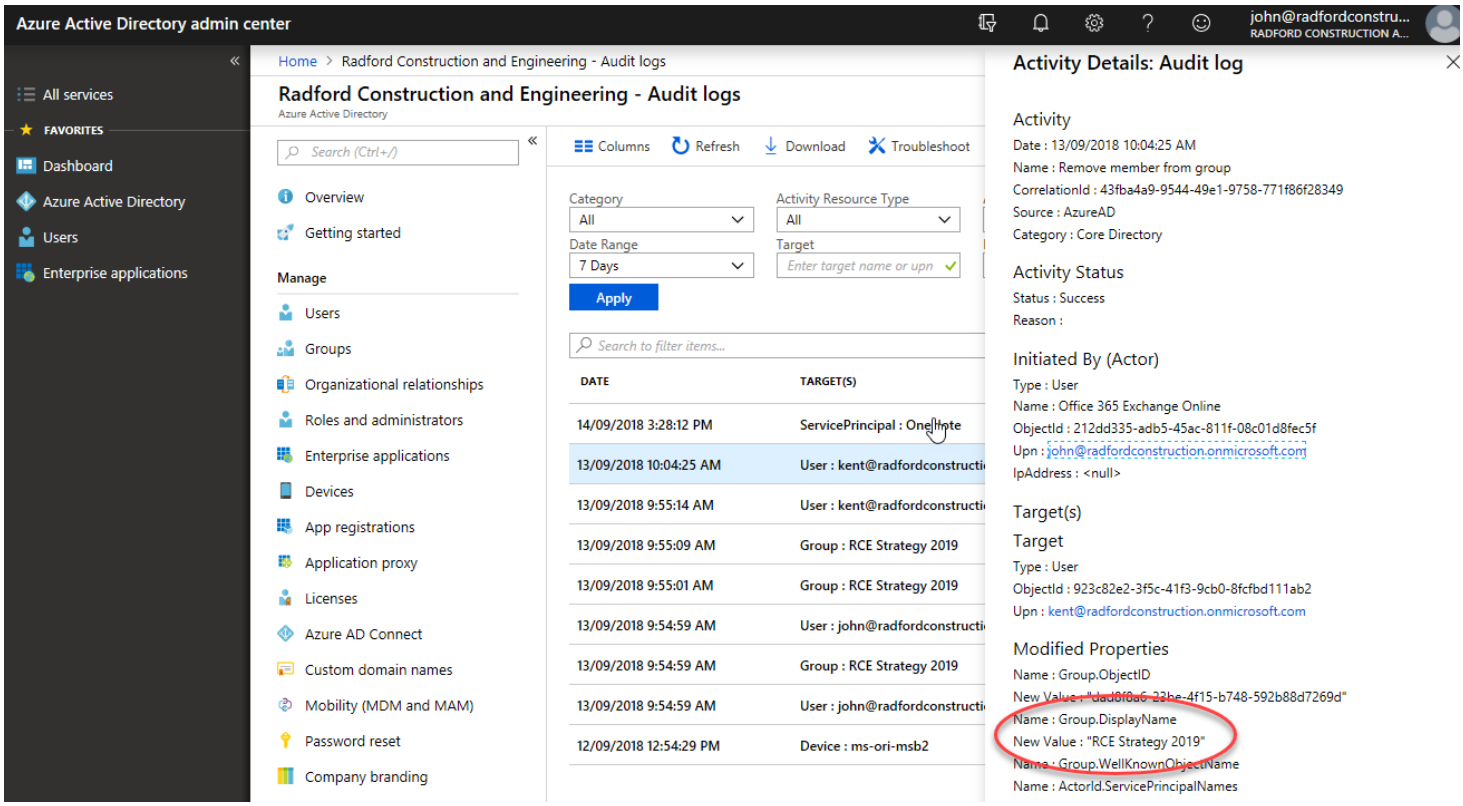
Audit Log Truncating Azure AD Records

Description

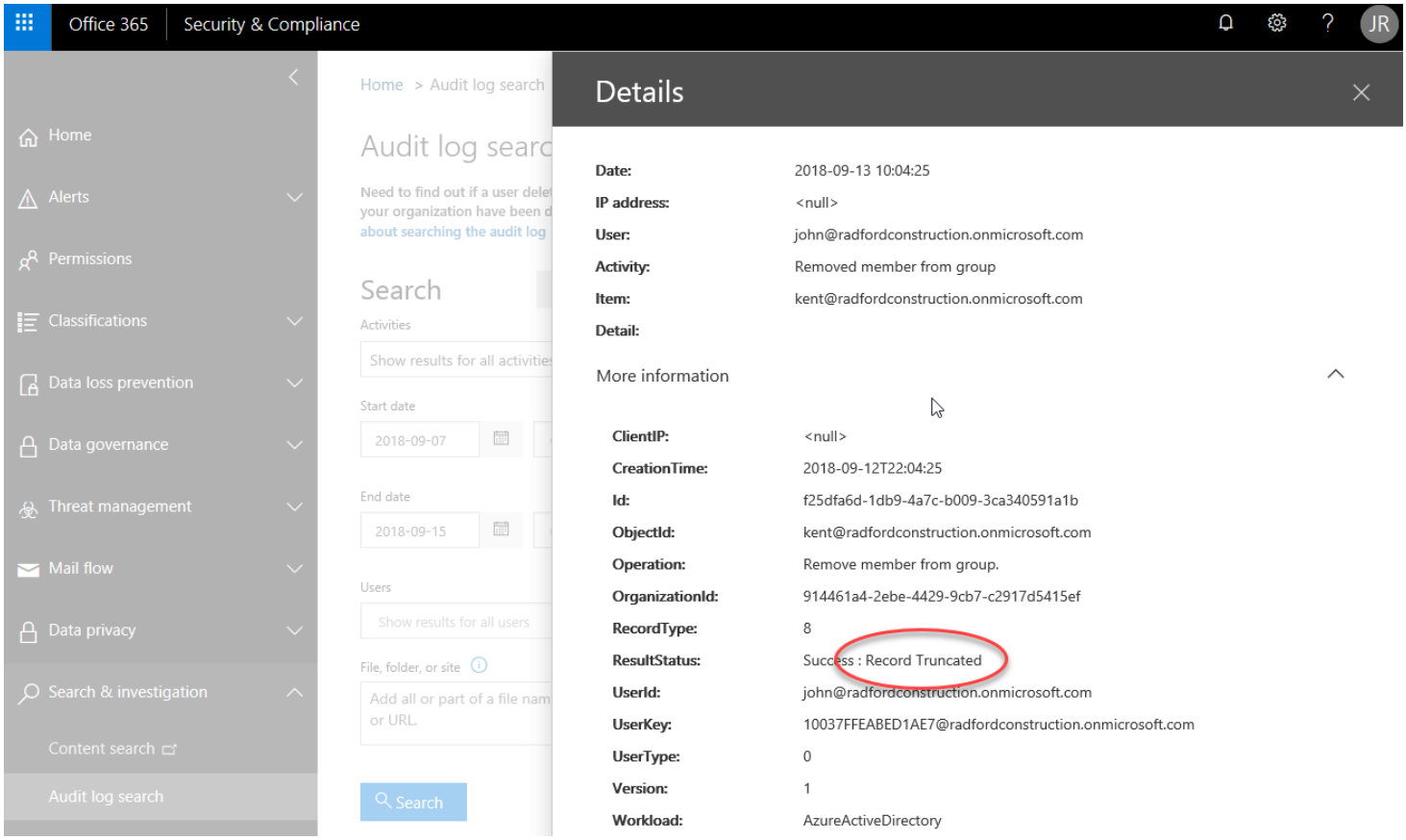
Azure AD Activity records provide a log of changes to directory objects in Azure AD. Tracked activities include adding an owner to a group, adding an owner to a policy, adding and removing users, and many others. A subset of these activity records from Azure AD are copied across to the Office 365 Audit Log, thereby creating a single stream of audit records relevant to Office 365 for access by authorized Office 365 administrators via the Security & Compliance Center.

Sometime during June 2018 and July 2018, certain record types created in Azure AD related to group operations started to be truncated when copied across to the Office 365 Audit Log. Specifically, activity records for adding members to a group and removing members from a group are excluding the name of the group from the audit log record created in Office 365. The correct information is shown in the associated activity record in Azure AD, but is no longer being correctly copied across to the Office 365 Audit Log.

For example, the user John has removed the user Kent from the group called RCE Strategy 2019. This is the activity record in Azure AD, which correctly identifies these facts:



The associated Audit Log entry in Office 365 omits the name of the group:



It is unclear whether this change is by deliberate design at Microsoft, or represents a coding error or bug that has gone undetected.

Analysis

- Using the Office 365 Audit Log record no longer provides the full details required for understanding which group a user has been added to or removed from.
- If this change is due to a coding error or bug on the behalf of Microsoft, it calls into question the quality assurance processes used at Microsoft for Office 365 in general, and security and compliance capabilities specifically. Truncating records of important information for security and compliance purposes does nothing to engender confidence that other record types are not being compromised either.
- [**May 2019**] Microsoft fixed the record truncation problem in early May 2019, eight months after being alerted to the problem. For compliance related records, this is unacceptable.

About

- Date - September 12, 2018
- Announced via - Office 365 for IT Pros Blog
- Implications for - Audit Reports - Office 365
- Tagged as - Archiving

New Guided Workflow for Deleting Microsoft 365 Users

Description

Microsoft introduced a guided workflow for deleting a user from Office 365, which includes the option of re-assigning access to the user's OneDrive documents and Outlook mailbox. The guided workflow is designed ensure a repeatable process. Access to the user's OneDrive documents could previously only be assigned to their manager (as defined in Azure AD), but this change enables access to be assigned to anyone in the tenant. Note that Office 365 offers no ability to manage user ownership rights in other Office 365 services, such as SharePoint Online or Microsoft Teams. For example, a user cannot be automatically removed from an Office 365 Group, or ownership of a Microsoft Teams workspace cannot be automatically re-assigned.

By default, once a user is deleted, his or her OneDrive is retained for 30 days and then deleted. This can be changed to a maximum of 3650 days (essentially 10 years). Note that this workflow does not interfere with this deletion process; it merely enables re-assigning the OneDrive for the specified retention timeframe to the user's manager or anyone else in the tenant.

Analysis

When skilled IT architects and administrators were needed for deploying on-premises solutions, a certain baseline of IT administrative competence was essential (and developed / refined in process). In the new world of cloud services where is it simple to sign-up to Office 365 and get started, these more behind-the-scenes administrative competencies can be easily overlooked and under-developed. Less frequent tasks become more difficult to do properly because there are many steps with inter-linked implications and consequences. Deleting a user from Office 365 without unintentionally causing an information management crisis is a good example, and while Microsoft's written guidance is clear on what to do, this guided workflow takes it a step further into the realm of automation.

By August 27, there were over 80 comments on the announcement post, indicating a high-degree of interest in the idea of guided workflows for admins. Apart from the "thanks for doing this" comments, the majority complained about the inability of this workflow to support hybrid setups, because Azure AD is populated and controlled by Active Directory on-premises. Various admins shared their manual workflow processes for deleting a user in a hybrid situation, but a common refrain was for greater capabilities from Microsoft to address the non-basic situations where only Office 365 is being used. Given the wide divergence that exists in how Office 365 is used in conjunction with on-premises Microsoft solutions, and the equal divergence in how organizations specifically need to address offboarding and compliance requirements, it will be almost impossible for Microsoft to deliver a single guided workflow that addresses the needs of organizations with a hybrid setup.

About

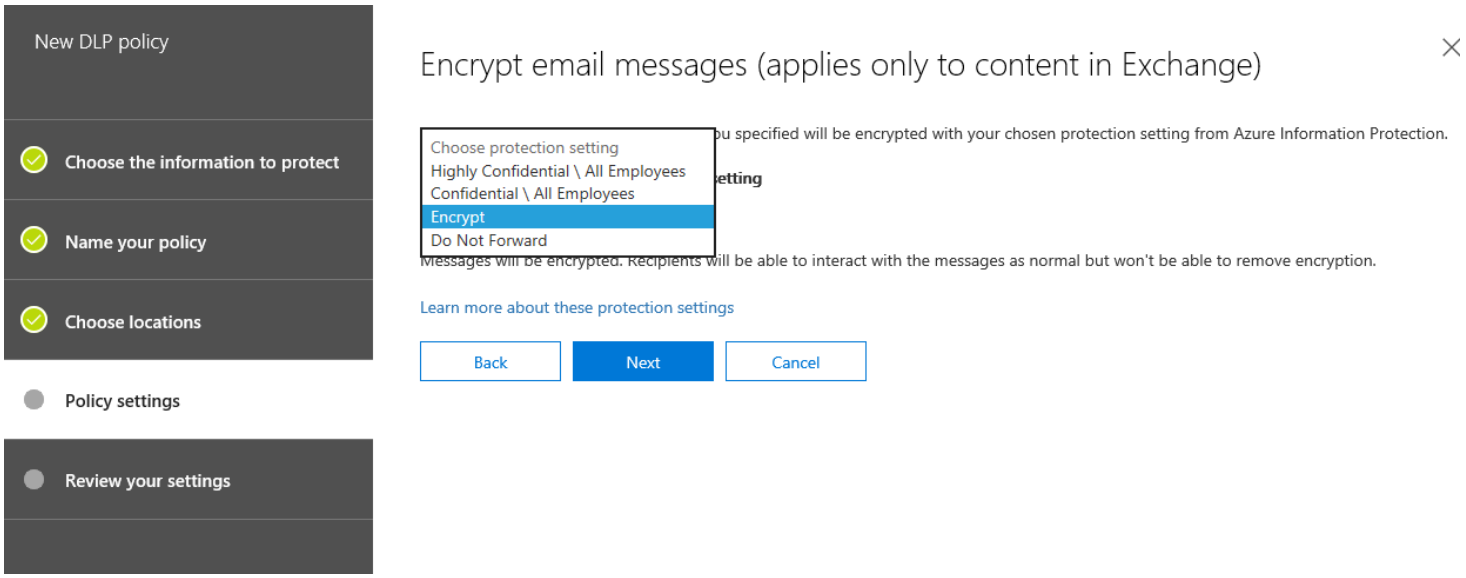
- Date - August 2, 2018
- Announced via - Microsoft 365 Blog
- Tagged as - Archiving

Apply Encrypt Only with a DLP Rule in the Office 365 Security & Compliance Center

Description

Encrypt Only is the latest encryption template released by Microsoft for Office 365 Message Encryption Version 2. It is offered in addition to the original Do Not Forward policy template, which many users found too restrictive. The Encrypt Only template encrypts the message and attachments in transit and at rest within the user's mailbox, but does not prevent forwarding of the message to other people in order to share its contents as appropriate. Applying the Encrypt Only template is currently a manual-only option in Outlook, where a user who wants to encrypt using the template must select the Encrypt Only option for every message.

Via the Office 365 Roadmap (item 31524), Microsoft in early September 2018 signaled that an automatic option is coming, whereby it will soon be possible to use a DLP rule to enforce the Encrypt Only template on messages. A check of the Security & Compliance Center on September 11, 2018 - with an Enterprise E5 plan - shows that this capability is already available.



Analysis

- The Office 365 Security & Compliance Center supports creating DLP rules that protect content based on sensitive information types or labels. The ability to look for a label in email is not supported, so only a match based on sensitive information types is possible.
- The encryption of email messages only applies to Exchange as a location; it does not support OneDrive for Business or SharePoint Online.
- It is unclear why Microsoft has included this ability on the Office 365 Roadmap when it is already available.

About

- Date - September 8, 2018
- Announced via - Office 365 Roadmap 31524
- Implications for - Office 365 Message Encryption - Version 2
- Tagged as - Data Loss Protection, Encryption

Updates to Office 365 Message Encryption

Description

Microsoft announced a bevy of updates to Office 365 Message Encryption v2 at Ignite 2018. These were:

- The ability for an admin to turn off encrypted attachments when using the Encrypt-Only template is now generally available. This setting must be applied using PowerShell, and appears to be a blanket on or off setting for the entire Office 365 tenant.
- The ability to use DLP rules in the Security & Compliance Center for encrypting messages is now available. Usually this will be on the basis of sensitive information being identified within the message or an attachment.
- By the end of 2018, PDF documents attached to messages will also be encrypted. Previously OMEv2 only supported Office documents, which limited its applicability. PDF document support is a good single step in the right direction of broader support, but OMEv2 is still very much a Microsoft (plus PDF) play, not anything wider.
- There are new options for applying branded templates to encrypted emails (using an Exchange Mail Flow rule), although this is noted for business-to-consumer emails only. It is unclear what happens for business-to-business emails.
    - Once released in Q1 of CY2019, branded templates will be possible based on department, product, or geographical region or country.
    - See ID 34924 on the Microsoft 365 Roadmap for details.
- A limited scope ability to revoke messages was introduced in public preview. If the message was sent to a consumer email account, and if the message requires logging into the viewing portal, and if the message was branded, then an administrator can use PowerShell to revoke the message based on message ID. Revocation does not apply in other situations. Apparently it will be possible at some point to force all messages to use a link-based approach that requires the use of the viewing portal, rather than being able to work in-line in Outlook with the encrypted message.
- A new report on Encrypted messages was added to the Security & Compliance Center; this is in public review rather than general availability. The reports show encrypted message volume by encryption method, by volume and encryption template, and total encrypted message volume by top recipient domains. Reports show details about each message (e.g., sender, recipient, encryption template), and the delivery of reports to an admin by email can be scheduled.

Analysis

- The updates released at Ignite 2018 provide new functionality that has been missing in action. The updates are directionally appropriate, e.g., broader control through Unified DLP in the Security & Compliance Center, new support for encrypting PDF documents, and message revocation (under stingent conditions).
- Use of DLP in the Security & Compliance Center for automatic message encryption suffers from the design limitations in Unified DLP (for example, no ability to sort order the rules) and sensitive information types (for example, the inability to match slightly altered numbers). See DLP in Security & Compliance Center.
- Microsoft claims that messages received natively in-line to Outlook can not be revoked, while link-based versions can. But this doesn't make theoretical sense, unless OMEv2 suffers from a fundamental design flaw. Since the rights of the user who received an encrypted message in Outlook must be checked when it is opened, theoretically the message could still be revoked by revoking the encryption key. On the other hand, Microsoft may just be releasing revocation capabilities slowly, and will add native in-line Outlook revocation later.
- An end user cannot revoke their own message from their list of Sent messages in Outlook. An administrator must do this using PowerShell.

About

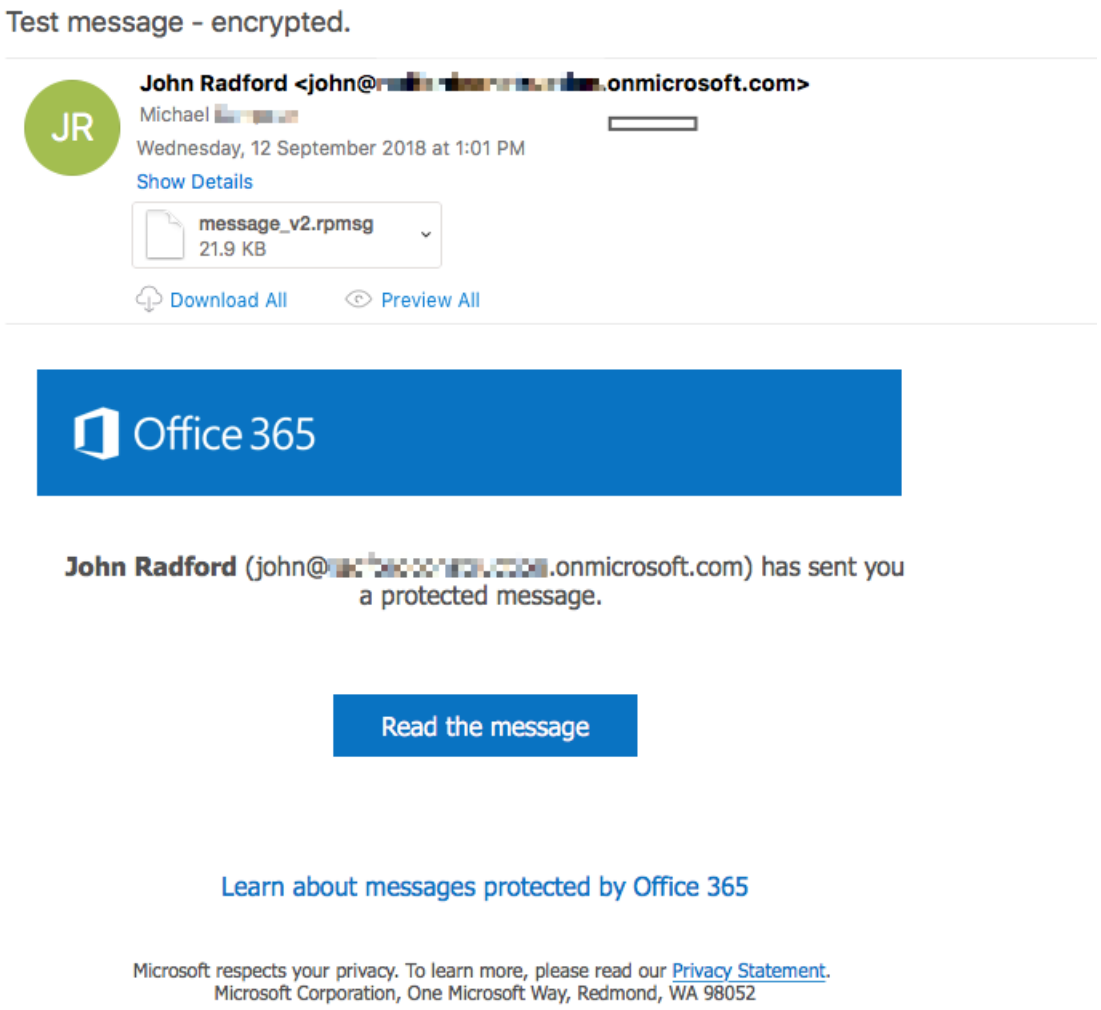
- Date - September 25, 2018
- Announced via - Security, Privacy and Compliance Blog
- Implications for - Office 365 Message Encryption - Version 2
- Tagged as - Encryption

Outlook for Mac to Support Office 365 Message Encryption in 2019

Description

Outlook for Mac users have been unable to use Office 365 Message Encryption, since the capabilities for doing so were not available in Outlook for Mac. Via its Office 365 Roadmap site, Microsoft announced that the ability to protect email content with Office 365 Message Encryption will be available in the first quarter of 2019. Note this is the estimated release date, as at September 2018.

If an Outlook for Mac user is sent a message encrypted with Office 365 Message Encryption, a link to view the message and respond to it via a web browser is provided. Clicking the "Read the Message" button opens the message in a web browser using the viewing portal for Office 365 Message Encryption.



Analysis

- In-line access to OMEv2 messages has recently been added to Outlook for Windows, but no timeframe was offered for Outlook for Mac. The above clarifies when this support is coming.
- Within the OMEv2 offering, having a consistent experience regardless of which platform Outlook is running on is the right direction for Microsoft. Outlook for Mac will lag the availability of in-line OMEv2 capabilities in Outlook for Windows by 6-9 months, depending on when it is actually released.

About

- Date - September 6, 2018
- Announced via - Office 365 Roadmap 32646

- Implications for - Office 365 Message Encryption - Version 2
- Tagged as - Encryption

Azure DC Virtual Machines at Public Preview

Description

Microsoft released the public preview of the DC-series of virtual machines, which enable data protection for data while in use. The release is part of Microsoft's vision around confidentiality and data protection in cloud services. The DC VMs are available in two data center locations - US East (which was also available in private preview) and Europe West - with more locations on the roadmap.

The DC-series is run on specialty hardware with Trusted Execution Environments. In public preview, this is based on the new Intel Xeon processors with Intel SGX technology. The Open Enclave SDK is also used, for creating a confidential space for developing applications.

Early customers include financial institutions (for Blockchain applications) and data analytics firms (to enable big data analytics without compromising data protection).

Analysis

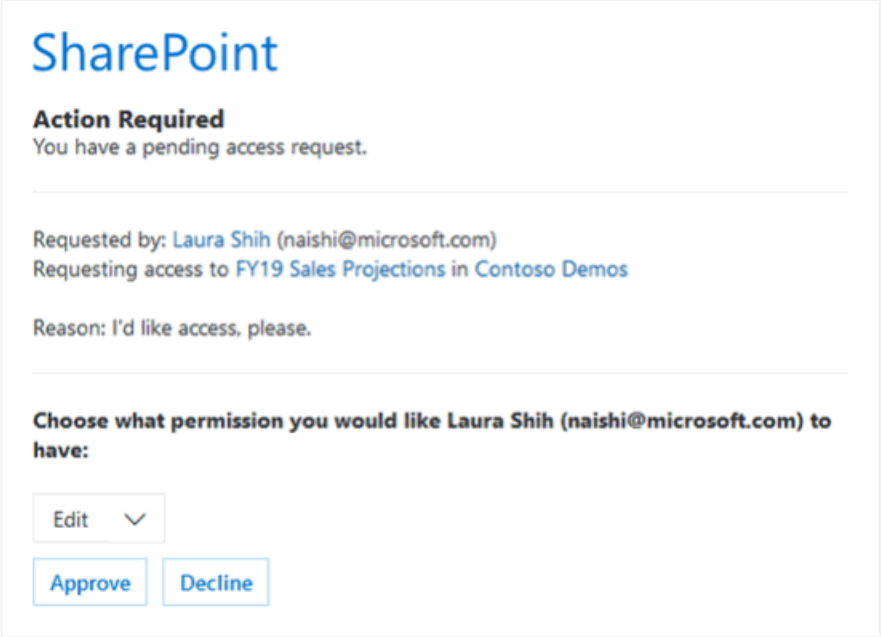
- Azure DC virtual machines are an Azure offering, not an Office 365 one. However, it is interesting to take note of wider developments at Microsoft in terms of data protection.
- Data protection is an all encompassing mandate. Organizations subject to data protection regulations (in particular) need to assess how data protection and data privacy are built in by design. Microsoft offers varying approaches to data protection, including data-in-transit (for example, Office 365 Message Encryption), data-at-rest (for example, service encryption in Office 365), and now also options for protecting data-in-use (assuming Azure DC VMs are used).

About

- Date - October 10, 2018
- Announced via - Azure Blog
- Implications for -
- Tagged as - Encryption

Access Requests from SharePoint Online

Description



Microsoft announced two forthcoming changes for the Outlook integration of the Access Requests feature in SharePoint Online:

- If the request has already been approved or declined by a site owner, the message card will advise the current site owner that the request has already been actioned by another. This prevents a duplicate action being taken, as well as preventing a different action (where the second site owner, for example, declines the request after the first site owner has already approved it).
- The option to choose which permissions level to grant to the requestor. While Edit remains the default, the approver will be able to select the View permission instead.

The Outlook integration - called Access Request Actionable Message - enables a single click Approve or Decline response directly within an email notification to a site owner, rather than having to open SharePoint Online and deal with requests there.

Analysis

- Basic, step-wise feature improvement in usability.
- Microsoft adds the approved user directly to the permissions list for the SharePoint site or document, instead of adding them to the default Site Members (Edit permission) or Site Visitors (View / Read permission) groups. This has resulted in pushback from some customers who would prefer the groups to be updated, rather than permissions to be granted directly, because it has flow-on implications over time for managing group and user access to SharePoint resources. See SharePoint Access Request Ignoring Default Group.

About

- Date - November 7, 2018
- Announced via - Microsoft OneDrive Blog
- Implications for -
- Tagged as - File Sharing

OneDrive for Business Updates

Description

The OneDrive Team outlined numerous updates for OneDrive for Business starting November 2018. These include:

- The iOS and Android apps can be used to scan documents, whiteboards, images from the field, a site visit, and more.
- The iOS and Android apps will prompt for custom metadata when a scan is started from a Library with custom metadata. This capability is part of the Mobile Capture feature.
- When taking a scan of meeting notes, the OneDrive apps for iOS and Android will prompt the user to share the scanned image with the other people who attended the meeting. The OneDrive team says this is powered by the Microsoft Graph. This feature is called Meeting Note Sharing.
- Making use of the commonly used sharing dialog screen in Word, Excel and PowerPoint on iOS and Android. This reduces the possibility of confusion by having a specific version for iOS and Android.
- A redesigned Recent view of files in OneDrive for Business via a web browser, providing a more intuitive grouping based on recency bands (for example, "Yesterday" "This Week" and "Last Week").
- A redesigned Manage Access list, which shows who has access to a given file, and at what level (view only, edit).
- The announced deprecation of support for the OneDrive sync client on Mac OS Yosemite 10.10 and El Capitan 10.11 from February 1, 2019. Since both versions of Mac OS are no longer in mainline support by Apple, Microsoft has removed its intent to keep supporting them. Users are encouraged to upgrade to one of the later versions of Mac OS.

Analysis

- It is unclear what limits and restrictions are in place for Meeting Note Sharing. For example, if the meeting is held in a specific meeting room and the user takes a photo of the meeting notes while still in the meeting room and during the time period of the meeting, it would make sense that the Microsoft Graph could associate the location, the scan, and the timeframe with a calendar entry and thus a list of invitees. If the meeting notes are scanned outside of the meeting room and at a different time, will the same linkage be able to be created?

About

- Date - November 7, 2018
- Announced via - Microsoft OneDrive Blog
- Implications for -
- Tagged as - File Sharing

MC183701

We're Making Some Changes to Anti-Spoofing Enforcement Actions

Date - June 28, 2019

We're making some changes to the enforcement actions for intra-org spoof and Domain-based Message Authentication, Reporting, and Conformance (DMARC) failures. Towards the end of July, we're simplifying the way that you manage anti-spoofing protection within Office 365 by consolidating all spoof-related actions under a single policy.

This message is associated with Office 365 Roadmap ID 46841.

How does this affect me?

We are simplifying the way that you manage anti-spoofing by consolidating all spoof actions and management under the Anti-Phishing policy. This means that we will no longer take the Spam action, as dictated in the Anti-Spam policy, for intra-org spoof and DMARC failures. Cross-org spoof will continue to be managed by the Anti-Phishing policy without changes. Additionally, we have further simplified anti-spoofing protection management by stamping all mails, including intra-org spoof, with a Composite Authentication result in the Authentication-results headers. The Composite Authentication results always include our verdict, and the reason code corresponding with our verdict: compauth= pass, fail, none reason=XYZ. This makes it much easier to quickly decipher our verdict on the authentication of the mail and whether we deemed the mail spoof, and why.

This change may result in some messages that would previously have been marked as spam now being marked as phishing attempts (CAT:SPOOF). In other cases, if you were moving all spam to the junk folder and phish to quarantine, you will now see all messages in quarantine.

We'll be gradually rolling these changes out starting in late July, and we expect the rollout to be complete by end of August.

What do I need to do to prepare for this change?

As a result of this change, you may begin to see more mail take the spoof action, as dictated by the Anti-Phishing policy. If legitimate messages are being impacted due to the sender domains authentication, the following actions may be taken to receive these messages in the users' inboxes:

- Tenant admins can add the domain pair to the PhishFilterPolicy as being allowed to spoof.
- Users can add safe senders individually using their email client.

Microsoft 365 is the Bigger Picture

Description

Microsoft made Microsoft 365 a big deal at its annual Ignite conference in 2017, and has continued to push Microsoft 365 versus Office 365 only during the opening half of 2018. Microsoft 365 is a combined license for Office 365, Enterprise Mobility + Security, and Windows 10. In terms of enabling productivity and safeguarding information for the modern knowledge and information worker, it's an almost all-encompassing offer.

Microsoft is putting its messaging and focus behind Microsoft 365, de-emphasizing Office 365 alone as the dream destination. For example:

- The Office 365 Admin Center has been replaced with the Microsoft 365 Admin Center.
- The blog for Office 365 news (blogs.office.com) has been replaced with the blog for Microsoft 365 news. This uses a microsoft.com address, not an office.com one. See the Microsoft 365 Blog.
- The Office 365 Public Roadmap will be replaced in mid-September - just in time for Ignite 2018 - with a combined roadmap for Microsoft 365. This will encompass Office 365, Windows 10, Enterprise Mobility + Security, and Microsoft Azure. See Message Center Major Change Notification - August 17, 2018.
- Various new and enhanced capabilities are not available to "only" Office 365 subscribers, even those with the top-of-the-line Enterprise E5 license. Newer capabilities often require add-on licensing to an Office 365 plan, or moving to a full Microsoft 365 license.
    - [**Example**] Hardware OATH token support requires the full Azure MFA, available as part of Azure AD Premium P1 or P2, or a Microsoft 365 plan. See Support for Hardware OATH Tokens in Azure MFA.

About

- **Date** - August 17, 2018

MC176246

We're Making Some Changes to How You Manage Restricted Users

Message from Office 365 Message Center - Reference

Date - **March 21, 2019**

Restricted Users is a new Office 365 feature. We'll begin rolling this feature out soon. It is a replacement for the Exchange Action Center.

This message is associated with Microsoft 365 Roadmap ID: 31546.

How does this affect me?

The Action Center has been moved to the Security and Compliance Center (SCC) as a new feature called the Restricted Users portal. Administrators can now use SCC to remove restrictions from user accounts that have been blocked from sending mail to external users due to suspicious activity. We plan on expanding this feature to automate remediation actions that check for things like compromise, but also prevention tips like password change and enabling MFA.

We began gradually rolling this out in early March, and we anticipate roll out completion worldwide by the end of March 2019.

What do I need to do to prepare for this change?

There is nothing you need to do to prepare for this change.

See also:

- Removing a User from the Restricted Users Portal After Sending Spam Email (Microsoft Docs)

MC177651

We're Making an Update to Office 365 Enterprise Plan Names

Date - April 12, 2019

We’re updating Office 365 Enterprise plan names. This change will be made in late April, 2019.

How does this affect me?

The license display names of the Office 365 Enterprise plans will be updated to remove the word "Enterprise" (e.g. "Office 365 Enterprise E3" will be updated to "Office 365 E3").

This name change will go into effect on April 30, 2019.

What do I need to do to prepare for this change?

You don't need to do anything, but may consider updating your user training, and notifying your helpdesk.

MC177501

We're Changing Your Default SharePoint Admin Center Experience

Message from Office 365 Message Center - Reference

Date - **April 10, 2019**

The new SharePoint admin center will be the default experience for organizations. We have completed rolling out to Office 365 organizations of 50 or fewer licenses, as communicated in MC173771, and are now rolling out more broadly.

This message is associated with Microsoft 365 Roadmap ID 46375.

How does this affect me?

The SharePoint admin center experience will default to the new admin center experience. You can switch back to the classic experience as necessary.

We'll be gradually rolling this out in early May and will be complete by the end of May.

What do I need to do to prepare for this change?

You don't need to do anything, but may consider updating your user training, and notifying your helpdesk.

To switch to the classic experience temporarily, select “Classic SharePoint admin center” in the left pane of the new SharePoint admin center.

To control the default experience for all global and SharePoint admins in your organization: In the new SharePoint admin center, select Settings in the left pane, and then select Default admin center experience. Turning the setting to Off will set the classic admin center as default and On will set the new admin center as default. This control is available now.

This change will be skipped for customers that have modified the setting of their default admin center experience.

MC173614

Information Protection updates to the existing Office 365 E3, E5, Advanced Compliance and Information Protection

Message from Office 365 Message Center - Reference

Date - **February 20, 2019**

We're updating the existing Office 365 E3, E5, Advanced Compliance and Information Protection & Compliance SKUs to include:

- Information Protection for Office 365 – Standard, or
- Information Protection for Office 365 – Premium

We'll be gradually rolling this out to customers in March, and the roll out will be completed worldwide by the end of March.

How does this affect me?

As this rollout is completed you may see a new Service Plan, there is no immediate impact, but it is being added in support of upcoming features.

What do I need to do to prepare for this change?

There is nothing you need to do to prepare for this change. Please refer to the Additional Information to configure and use sensitivity labels.

MC176396

Giving Your Organization More Transparency and Control Over Microsoft 365 Cloud Connected Experiences for Office

Message from Office 365 Message Center - Reference

Date - **March 25, 2019**

Microsoft protects and respects the privacy of your Office data, whether that data is an email, a Word document stored in OneDrive, or similar user content. This protection of your Office data also extends to the data that Microsoft uses to ensure your Office apps are up to date, secure, and performing as expected; and to the rich productivity and collaboration experiences enabled by connecting the apps to Microsoft's cloud. To increase the transparency and control of this data for our customers, beginning with **Version 1904 of Office 365 ProPlus in Monthly Channel and Monthly Channel (Targeted) for Windows**, we're launching new capabilities to enable organizations to determine the level of diagnostic and related data that Office is sending to Microsoft, as well as a tool to view the data being sent. Work is underway to enable these controls for Office on other platforms; we'll send additional Message Center posts when those updates are ready.

This change is related to the Microsoft 365 Roadmap ID: 49779.

How does this affect me?

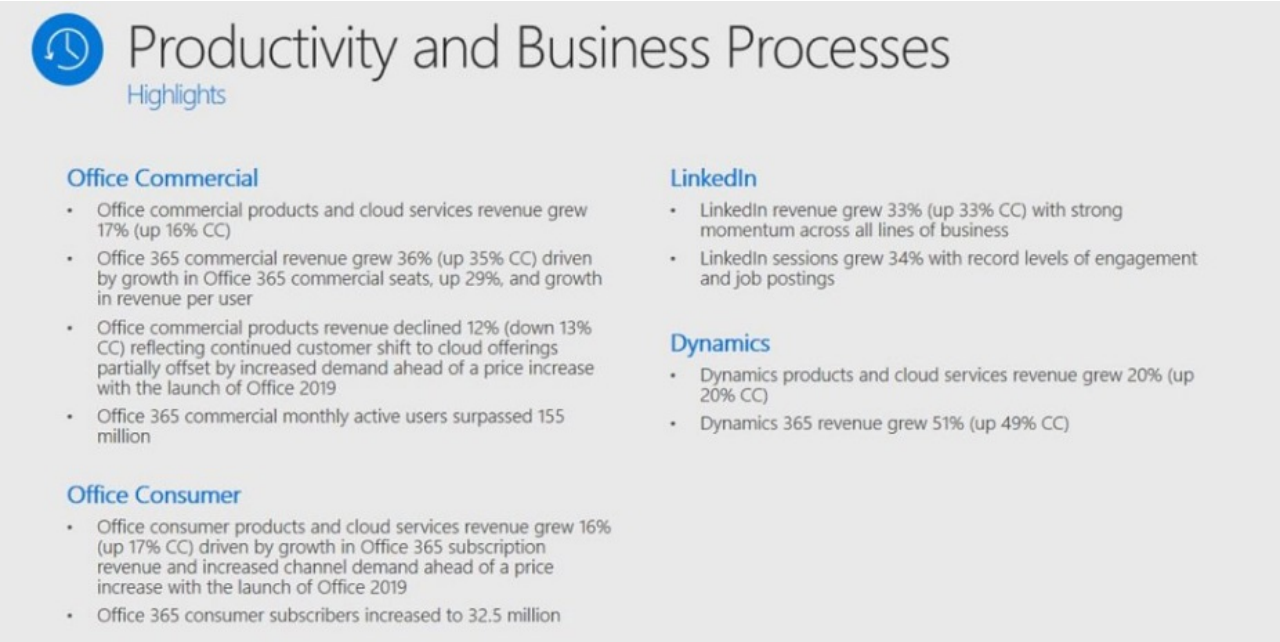
These controls allow organizations on behalf of their users, to determine the capabilities provided by connecting Office to the Microsoft 365 cloud, as well as the amount of diagnostic and related data that is sent to Microsoft. If no changes are made by the organization, all such data will continue to be sent. Note that limiting the data sent may reduce the capabilities of the Office apps and services and may make troubleshooting issues more difficult and time consuming. And remember, we take our responsibility to protect this data seriously.

What do I need to do to prepare for this change?

We encourage you to read the information posted at the link below, in order to understand the types of data being discussed, the choices that organizations have to view and control this data, and the protections in place to safeguard your privacy. Those organizations that want to manage the data sent to Microsoft will be able to use the Office Client Policy Service, which is in public preview, or Group Policy to set these controls for their users.

Office 365 Market Snapshot - Microsoft's 1Q2019

Description



Microsoft announced its market performance numbers for Q1 of the 2019 fiscal year. Strong results were posted for Office 365, Dynamics 365, Surface, and more. Specifically:

- Revenue for the quarter was $29.1 billion, with a net income of $8.8 billion. This was an increase of 19% compared to a year ago.
- The number of monthly active users for commercial customers of Office 365 increased to 155 million. This is up from 135 million at April 2018.
- Consumer users of Office 365 grew to 32.5 million. Two years ago - at September 2016 - Microsoft had 24 million monthly active users on consumer plans.

Analysis

- Microsoft is still returning strong growth numbers for Office 365 - it added 20 million users in the past quarter. As the base number keeps increasing, it will become harder for Microsoft to keep up its current rate of growth.
- There was no breakdown of Office 365 subscribers versus Microsoft 365 subscribers. With Microsoft including key capabilities in its cloud offerings beyond Office 365 that are included in Microsoft 365, it is fair to expect that Microsoft's revenue for commercial cloud offerings still has a good growth opportunity. In other words, while the growth in actual subscriber numbers will slow down, Microsoft's push to Microsoft 365 is an attempt to increase the per user revenue rate.

About

- Date - October 24, 2018
- Announced via - Microsoft Investor Relations
- Implications for - Office 365 - Overview

We're Making Some Changes to Default Installation Settings

Message from Office 365 Message Center - MC171479

Date - **December 22, 2018**

Office ProPlus and Office 2019 will now be installed with 64-bit as the default setting. Previously, the default setting was 32-bit at installation. This change will begin rolling out in mid-January, 2019.

How does this affect me?

After this change takes place, the 64-bit version of Office will automatically be installed unless you explicitly select the 32-bit version before beginning the installation process.

If you install the 64-bit version, but wanted the 32-bit version instead, you must first uninstall the 64-bit version before installing the 32-bit version. The same is true if you installed the 32-bit version but want to install the 64-bit version.

This change will begin rolling out in mid-January, 2019.

What do I need to do to prepare for this change?

There’s nothing you need to do to prepare for this change. Please click Additional Information below to learn more.

Additional Information

See Choose between the 64-bit or 32-bit version of Office

Exchange Online Mailbox Audit to Add Mail Reads by Default

Message from Office 365 Message Center - MC171679

Date - **January 4, 2019**

To ensure that you have access to critical audit data to investigate security incidents in your organization, we're making some updates to Exchange mailbox auditing. After this change takes place, Exchange Online will audit mail reads/accesses by default for owners, admins and delegates under the MailItemsAccessed action.

This message is associated with Microsoft 365 Roadmap ID: 32224

How does this affect me?

The MailItemsAccessed action offers comprehensive forensic coverage of mailbox accesses, including sync operations. In February 2019, audit logs will start generating MailItemsAccessed audit records to log user access of mail items. If you are on the default configuration, the MailItemsAccessed action will be added to Get-mailbox configurations, under the fields AuditAdmin, AuditDelegate and AuditOwner. Once the feature is rolled out to you, you will see the MailItemsAccessed action added and start to audit reads.

This new MailItemsAccessed action is going to replace the MessageBind action; MessageBind will no longer be a valid action to configure, instead an error message will suggest turning on the MailItemsAccessed action. This change will not remove the MessageBind action from mailboxes which have already have added it to their configurations.

Initially, these audit records will not flow into the Unified Audit Log and will only be available from the Mailbox Audit Log.

We'll begin rolling this change out in early February, 2019. If you are on the default audit configuration, you will see the MailItemsAccessed action added once the feature is rolled out to you and you start to audit reads.

What do I need to do to prepare for this change?

There is no action you need to take to derive the security benefits of having mail read audit data. The MailItemsAccessed action will be updated in your Get-Mailbox action audit configurations automatically under AuditAdmin, AuditDelegate and AuditOwner.

If you have set these configurations before, you will need to update them now to audit the two new mailbox actions. Please click Additional Information for details on how to do this.

If you do not want to audit these new actions in your mailboxes and you do not want your mailbox action audit configurations to change in the future as we continue to update the defaults, you can set AuditAdmin, AuditDelegate and AuditOwner to your desired configuration. Even if your desired configuration is exactly the same as the current default configuration, so long as you set the AuditAdmin, AuditDelegate and AuditOwner configurations on your mailbox, you will preclude yourself from further updates to these audit configurations. Please click Additional Information for details on how to do this.

If your organization has turned off mailbox auditing, then you will not audit mail read actions.

Additional Information

See Enable Mailbox Auditing in Office 365 (Microsoft Docs)

Role-Based Access to Alerts in Office 365 Security

Message from Office 365 Message Center - Reference

MC172220

Date - **January 17, 2019**

We're updating alert policies in the Office 365 Security & Compliance Center with more granular role-based access control. With this feature, admins will have more granular control over which alerts can be viewed by whom in the Office 365 Security & Compliance Center. After the release, roles a user has will determine what category of alerts they have access to. For example, a Compliance admin will no longer have access to Threat management or Mail flow alerts, which helps them better focus on triaging and investigating compliance related alerts, like Data governance, Data loss prevention, etc.

This message is associated with Microsoft 365 Roadmap ID 44245.

We'll be gradually rolling this out to customers starting February 19, 2019 and the roll out will be completed worldwide by the end of March.

How does this affect me?

Today, when admins go to the View alerts page in the Office 365 Security & Compliance Center, they can see all alerts regardless of the category of alerts if they have the "ManageAlerts" or "ViewOnlyManageAlerts" role.
With this change, they will need more specific roles in addition to "ManageAlerts" or "ViewOnlyManageAlerts" in order to see specific categories of alerts.

What do I have to do to prepare for this change?

For users or admins who need to access alerts, make sure they have the correct roles assigned in the Office 365 Security & Compliance Center before the change rolls out.

To see the complete role and category mapping, please click Additional Information.

Additional Information

Alert Policies in the Office 365 Security & Compliance Center (Microsoft Docs)

Sign-In Options to Office 365 for Personal Accounts

Message from Office 365 Message Center - Reference

Date - **January 12, 2019**

We're updating the Office 365 login page with new sign-in options that will enable user access to their personal accounts. We'll begin rolling this feature update out in mid-February, 2019.

This message is associated with Microsoft 365 Roadmap ID 45516

How does this affect me?

After this change takes place, when signing into Office, your users will see a new link that says "Sign-in options" on the Office 365 login page. Clicking on this link will bring the user to a new screen that will show additional login options that only work for personal Microsoft account users. Moreover, users will be warned that signing in via additional options will only enable personal account access. These options will not be enabled for users in Office 365 tenants and will not change how Office 365 users sign-in to their work or school resources.

Initially, users will be able to use their GitHub account credentials to sign-in. If you have not granted your users access to GitHub, they will not be able to sign-in using their GitHub credentials. Over the coming months, LinkedIn and other sign-in options will be added.

We'll begin gradually rolling this out in mid-February, and we anticipate roll out completion worldwide by the end of February 2019.

What do I need to do to prepare for this change?

You don't need to do anything, but may consider updating your user training, and notifying your helpdesk. Please click Additional Information to learn more.

Security & Compliance Center Splitting in 2019

Description

In Microsoft 365 Roadmap #44767, Microsoft disclosed that it will be introducing two new centers in Microsoft 365 (and Office 365) in 2019: the Security Center and the Compliance Center. Each will become a centralized workspace for security or compliance, and each will offer the ability to manage the security or compliance posture for the organization. This directional statement appears to result in the splitting of the current unified Security & Compliance Center into two separate and more focused control centers.

The new Microsoft 365 Security Center will be accessed through security.microsoft.com.

The new Microsoft 365 Compliance Center will be accessed through compliance.microsoft.com.

Analysis

- [**January 2019**] Microsoft released the two new centers, but they are only for Microsoft 365 subscribers, not Office 365. The changes affects the Microsoft 365 Security & Compliance Center, but not the Office 365 Security & Compliance Center. See Microsoft 365 Security Center and Compliance Center.
- The current unified Security & Compliance Center is accessed via protection.office.com. Role-based access control can be used to reduce the security and compliance tools that individuals users have access to. However, Microsoft has mixed two quite different capabilities in a single unified control center. Except in very small organizations, an individual user with role responsibilities for the security settings and tasks of Office 365 will not also have role responsibilities for the compliance settings and tasks of Office 365.
- Creating focused control centers will allow the simplification of the user interface and appropriate navigational elements for each.
- From the current Security & Compliance Center, the new **Security Center** is likely to include:
  - Alerts on security, e.g., malware threats
  - Permissions
  - Threat Management
  - Reports on security, e.g., Office 365 ATP file types, malware detected in email.
- From the current Security & Compliance Center, the new **Compliance Center** is likely to include:
  - Alerts on compliance, e.g., data loss
  - Classifications
  - Data Loss Prevention
  - Data Governance
  - Data Privacy
  - Search & Investigation
  - Service Assurance
  - Reports of a compliance nature, e.g., labels, supervision, DLP incidents, etc.
- It is unclear where the current Mail Flow control capabilities will go. The new Security Center would be the more obvious place out of Security or Compliance, or they could be put into the general Admin Center.

About

- Date - December 6, 2018
- Announced via - Microsoft 365 Roadmap

Office 365 Numbers by Workload

Description

	Number active users (paid seats)	Number cloud users (including free seats)
Exchange Online	135 – 150 million	180 million
SharePoint Online	110 – 130 million	140 million
Teams	25 – 30 million	35 million
Yammer	5 – 8 million	9 million
Planner	3 million	3 million

Table 2: Summarizing User Numbers for Office 365 workloads

Tony Redmond attempts to reconcile many statements from Microsoft in order to ascertain the breakdown of usage across the workloads in Office 365. In Tony's analysis:

- Exchange Online and SharePoint Online are the two mega-workloads in Office 365, with very high usage across the overall number of Office 365 users.
- Microsoft Teams is a distant third, but with a rapidly growing base of active users. The service was only launched to general availability in March 2017, so growth to 25-30 million in less than two years is a significant achievement for Microsoft.
- Other services, such as Yammer and Planner, are used by a much smaller percentage of the Office 365 active user base. This does, however, still equate to a high number in the scheme of things in comparison to competitor offerings.

Analysis

- As Tony says in his article, while the numbers are probably wrong in their specifics, the overall trend lines are about right.
- Another workload that will have a high active user count is Office ProPlus. It is likely to be somewhere between the Exchange Online and SharePoint Online numbers.

About

- Date - December 6, 2018
- Announced via - Petri IT Knowledgebase
- Implications for - Office 365 - Overview

Anti-Spoofing Added to All Exchange Online Protection Plans

Message from Office 365 Message Center - Reference

Date - **August 16, 2018**

We're extending coverage of enhanced anti-spoofing protection to all Exchange Online organizations

Major update: General Availability rollout started

Applied to: All customers

We're excited to announce that we're extending enhanced anti-spoofing capabilities to all Exchange Online Protection (EOP) organizations. Previously, this feature was only available to E5 and Advanced Threat Protection (ATP) add-on organizations.

If you are an existing E5/ATP customer, then this feature was previously enabled for you. We continue to add additional updates to improve this filter, including a new spoof intelligence insight that is being rolled out to provide better visibility and review experience.

If you have previously disabled enhanced anti-spoofing in your anti-phishing policy or via customer support, you will not be impacted.

This message is associated with Office 365 Roadmap ID: 32820.

How does this affect me?

After this change takes place, your organization will have access to enhanced anti-spoofing functionality that utilizes cloud intelligence, sender reputation and patterns to identify potentially malicious domain spoofing attempts. The new functionality works in conjunction with existing standards based email authentication checks (DMARC/DKIM/SPF). Once this feature is enabled, messages that fail our extended implicit authentication checks will be automatically sent to the junk mail folder. You can use policies to customize these actions and turn this functionality on and off.

We are also updating the Get/Set-PhishFilterPolicy cmdlet to allow you to block/allow domains that are allowed to send spoofed mails, as well as the Get/Set-AntiphishPolicy cmdlet to let you modify the policies applied to spoofed messages. After the cmdlet changes, we will also roll out policy options in Security and Compliance center

If you have domain 'allow' or 'safe' sender policies or transport rules in place, they will not be impacted.

Policy options for these changes will be available after September 1. We'll begin rolling this out and will be enforcing changes after September 21, 2018. We anticipate rollout completion in the following weeks.

What do I need to do to prepare for this change?

If you wish to disable enhanced anti-spoofing functionality, you will need to set polices before September 21, 2018. After September 21, we will begin rolling this feature out worldwide, and will enforce the available settings.

To access settings and make changes you'll need to use Get/set-Antiphishpolicy PowerShell cmdlets (after September 1). The same will also be possible via the Security and Compliance Center (under Threat Management->Policy->Anti-Phishing) once those changes are rolled out for EOP.

Please click Additional Information to learn more about how anti-spoofing functionality can benefit your organization and to learn how to access settings to enable and disable this feature.

Microsoft 365 Public Roadmap

Message from Office 365 Message Center - Reference

Date - **August 17, 2018**

New feature: The Microsoft 365 Public Roadmap

Major update: General Availability rollout started

Applied to: All customers

We're excited to announce that we are releasing a new version of the Office 365 Roadmap in mid-September.

This message is associated with Office 365 Roadmap ID: 25177.

How does this affect me?

In mid-September, the Office 365 Roadmap will become the Microsoft 365 Roadmap and will move to a new web location. In addition to retaining all the current information and functionality of the existing Office 365 Roadmap, the new site will include Microsoft 365 product features from Windows 10, Enterprise Mobility Suite, and Azure.

We will have redirects in place so that the deep links in any existing Message Center posts will continue to function, and any bookmarks you have set to the Roadmap will continue to work.

With the new Microsoft 365 Roadmap, you'll be able to:

- Utilize multiple new search filters such as "product," "cloud instance," and "platform".
- View additional information for the features on the Roadmap, including whether the feature is deploying in Targeted Release, preview, specialized cloud instances or worldwide. This information will be located on the feature card, or available via search in the Roadmap.
- Leverage new RSS capabilities through a custom link on the Roadmap web page. Using the RSS features feed you can subscribe to be notified of real-time feature updates, and view the notification in Outlook, supported browsers or mobile readers. Power users can use various tools to automate the handling of RSS updates to integrate them into their own 3rd party services.

Other changes that will occur are:

- The existing Office 365 URL (https://products.office.com/business/office-365-roadmap) will be replaced with a new Microsoft 365 Roadmap URL. Please note that the existing Office 365 Roadmap URL will automatically redirect to the new page.
- The "previously released" category will become the "launched" category. Launched features will remain in the "launched" category for six months after going live.

What do I need to do to prepare for this change?

You don't need to do anything to prepare for this change. Please click Additional Information to learn more.

Index

Supervision 2017

Audit Reports

20190104 Session ID Added to Exchange Online Audit Logs

August 2019

20190808 Exact Data Match in DLP

20190809 Weekly News Drop

20190815 Netherlands on Data Privacy Risks

20190816 Weekly News Drop

20190819 Microsoft Cloud App Security Updates

20190823 Weekly News Drop

20190830 Weekly News Drop

Authentication

20190207 Support of Email OTP in Azure AD

20190715 Authentication Methods Reporting

Authentication - Overview

Password Hash Synchronization

Azure AD

20190207 Support of Email OTP in Azure AD

20190514 Azure Durability

20190520 Azure AD Entitlement Management

20190523 Identity Data in Europe

20190524 Identity Secure Score Released

20190528 Azure AD Provisioning Updates

20190607 Weekly News Drop

20190705 Automatic Guest Account Creation in Azure AD

20190710 Passwordless with Azure AD

20190715 Authentication Methods Reporting

Activity Logs - Azure AD

Azure AD B2B Collaboration

Azure AD Identity Protection

Federation with Azure AD

Mobile Threat Defense

Multi-Factor Authentication

Password Hash Synchronization

Passwordless Authentication with Azure AD

Self-Service Password Reset

Update Log - Authentication

Azure AD Activity Logs

Activity Logs - Azure AD

Azure AD Identity Protection

20190802 Azure AD Identity Protection Updates

Azure Advanced Threat Protection

20190121 Azure Advanced Threat Protection

Azure Advanced Threat Protection

Azure ATP

20190121 Azure Advanced Threat Protection

Azure Advanced Threat Protection

Azure Information Protection

20190129 Inspecting Encrypted Files with Microsoft Cloud App Security

20190305 Credential Detection Using Azure Information Protection

Azure Information Protection

Azure Rights Management Service

Identification of Sensitive Data

Microsoft Information Protection

Office 365 Message Encryption - Version 2

Azure Key Vault

Azure Key Vault

Customer Key

Azure Rights Management

Azure Rights Management Service

Encrypt

Office 365 Message Encryption - Version 1

Office 365 Message Encryption - Version 2

Azure Sentinel

20190311 Azure Sentinel and Microsoft Threat Experts

20190313 Microsoft Cloud App Security Updates

20190318 Update on Microsoft Threat Protection

Baseline Protection

Multi-Factor Authentication

BETTER Mobile

Mobile Threat Defense

BlackBerry

No Archiving for Some Content Types

BlueTalon

20190730 BlueTalon Acquired

Bounty Program

Authentication - Overview

Update Log - Authentication

Business Email Compromise

20190725 Symantec on BEC Numbers

Compliance Boundaries

20190812 Compliance Boundaries

Compliance Manager

20190529 Compliance Manager 2019

Conditional Access

20190227 Office 365 Cloud App Security Expands Conditional Access

Mobile Threat Defense

Conditional Access App Control

20190902 Expanded Conditional Access in Microsoft Cloud App Security

Content Search

Content Search

Litigation Hold Capabilities

Credential Compromise

20190604 Barracuda on Account Takeover

Credential Phishing

Credential Phishing and Email Fraud

Customer Key

Azure Key Vault

Customer Key

Encryption - Overview

Data Centers

20190618 Data Centers in Middle East

Data Investigations

20190430 Data Investigations

Data Loss Protection

20190124 DLP and Windows Defender ATP

Azure Information Protection

Data Loss Protection - Overview

DLP in Exchange Online

DLP in Security & Compliance Center

Identification of Sensitive Data

Microsoft Information Protection

Office 365 Sensitivity Labels

Data Protection

20190218 Microsoft Response to Dutch DPIA

Data Residency

20190318 Data Residency in France for Microsoft Teams

20190422 Yammer in Europe and eDiscovery

Data-at-Rest

Customer Key

Encryption - Overview

Delete a User

Federation with Azure AD

DLP

20190808 Exact Data Match in DLP

DMARC

20190603 Free DMARC Discovery for Office 365

Do Not Forward

Do Not Forward

Office 365 Message Encryption - Version 2

Document Fingerprinting

Data Loss Protection - Overview

eDiscovery

20190114 Control Over PST Output Size in eDiscovery

20190422 Yammer in Europe and eDiscovery

20190522 SharePoint Security and Compliance Updates

Content Search

eDiscovery - Overview

eDiscovery Workflow

Indexing File Types

Update Log - eDiscovery

eDiscovery Workflow

eDiscovery Workflow

Litigation Hold Capabilities

Email Fraud

Credential Phishing and Email Fraud

Email OTP

20190207 Support of Email OTP in Azure AD

Encrypt Only

Encrypt

Office 365 Message Encryption - Version 2

Update Log - Encryption

Encryption

20190129 Inspecting Encrypted Files with Microsoft Cloud App Security

20190212 Sensitivity Labels with S/MIME Option

Customer Key

Encryption - Overview

Office 365 Message Encryption - Version 2

Europe

20190523 Identity Data in Europe

Event-Based Retention

20190131 Records Management Updates

Exact Data Match

20190808 Exact Data Match in DLP

Exchange Online

20190104 Session ID Added to Exchange Online Audit Logs

Advanced Threat Protection

Content Search

DLP in Exchange Online

eDiscovery Workflow

License Required for Ex-Employees' Mailboxes

Litigation Hold Capabilities

Office 365 Message Encryption - Version 1

Scoped Administrative Access

Supervision 2017

Exchange Online Audit Log

20190114 Mail Reads to be Audited for Exchange Online

Exchange Online Protection

Credential Phishing and Email Fraud

Exchange Online Protection

Exchange Public Folders

eDiscovery Workflow

February 2019

20190207 Support of Email OTP in Azure AD

20190208 Weekly News Drop

20190212 Sensitivity Labels with S/MIME Option

20190215 Weekly News Drop

20190222 Weekly News Drop

20190225 Microsoft HoloLens 2

Office 365 Sensitivity Labels

File Explorer Search

20190821 File Explorer Search in Windows 10

File Plan Manager

20190131 Records Management Updates

File Sharing

20190114 OneDrive Gains Fluent Update

20190128 Streamlining Files to the Cloud

File Sharing - Overview

Files Restore

OneDrive Files Restore

SharePoint Files Restore

France

20190318 Data Residency in France for Microsoft Teams

GDPR

20190218 Microsoft Response to Dutch DPIA

20190326 Office 365 ProPlus with Privacy Controls

20190730 BlueTalon Acquired

20190815 Netherlands on Data Privacy Risks

Data Loss Protection - Overview

Office 365 and GDPR

Guest Accounts

20190520 Azure AD Entitlement Management

HoloLens

20190225 Microsoft HoloLens 2

Hybrid Security

Support for Hybrid Architectures

Identity

20190510 Identity Security at Microsoft

Identity Secure Score

20190524 Identity Secure Score Released

Inactive Mailboxes

License Required for Ex-Employees' Mailboxes

Incident Remediation Workflow

Reporting for Response to Threats

Information Barriers

20190430 Information Barriers

Information Barriers in Teams

Information Protection

20190307 Information Protection Updates

January 2019

20190102 Standalone Upgrades for Microsoft 365 E3

20190103 Autodiscover Optimizes for Office 365 - Implications

20190104 Searching Encrypted Documents and Emails

20190104 Session ID Added to Exchange Online Audit Logs

20190111 Weekly News Drop

20190114 ATP Splitting Into Two Plans

20190114 Control Over PST Output Size in eDiscovery

20190114 Mail Reads to be Audited for Exchange Online

20190114 OneDrive Gains Fluent Update

20190114 Sharing Links That Block Downloads

20190115 New Files in Yammer Stored in SharePoint

20190115 No More Tenant-Level Opt-Out of Modern SharePoint

20190116 Policy Service for Office 365 ProPlus

20190118 Weekly News Drop

20190121 Azure Advanced Threat Protection

20190122 New Rules in Microsoft Cloud App Security

20190122 Role-Based Access Control to Alerts in Office 365 Security & Compliance Center

20190124 DLP and Windows Defender ATP

20190128 Streamlining Files to the Cloud

20190129 Inspecting Encrypted Files with Microsoft Cloud App Security

20190129 Updates to Advanced eDiscovery

20190130 New Supervision

20190131 Microsoft 365 Security Center and Compliance Center

20190131 Records Management Updates

20190201 Weekly News Drop

Advanced Threat Protection

Azure Advanced Threat Protection

Azure Information Protection

Content Search

eDiscovery Workflow

File Sharing - Overview

Microsoft Cloud App Security

Office 365 Cloud App Security

Office 365 Message Encryption - Version 2

Office 365 Sensitivity Labels

Supervision 2017

July 2019

20190702 Anti-Phishing Policy Update

20190702 Synchronous URL Detonation

20190704 Threat Explorer Hunting Updates

20190705 Automatic Guest Account Creation in Azure AD

20190705 Weekly News Drop

20190710 Passwordless with Azure AD

20190712 Weekly News Drop

20190719 Weekly News Drop

June 2019

20190603 Free DMARC Discovery for Office 365

20190604 Barracuda on Account Takeover

20190606 Discovered Resources in MCAS

20190607 Weekly News Drop

20190614 Weekly News Drop

20190618 Data Centers in Middle East

20190624 FlawedAmmyy Trojan

20190625 OneDrive Personal Vault

20190625 Preservation Hold Library Update

20190627 Microsoft Cloud App Security Updates

20190628 Weekly News Drop

Labels

Azure Information Protection

Legal Hold

Audit Logs - Office 365

License Required for Ex-Employees' Mailboxes

Litigation Hold Capabilities

Limited File Types

Data Loss Protection - Overview

Indexing File Types

Manual Scan

No Manual Scan

March 2019

20190305 Credential Detection Using Azure Information Protection

20190311 Azure Sentinel and Microsoft Threat Experts

20190313 Microsoft Cloud App Security Updates

20190318 Data Residency in France for Microsoft Teams

20190318 Update on Microsoft Threat Protection

20190326 Office 365 ProPlus with Privacy Controls

Market Performance

20190131 Office 365 Market Snapshot - Microsoft's Q2 2019

20190507 Office 365 Market Snapshot - Microsoft's Q3 2019

May 2019

20190430 Data Investigations

20190430 Information Barriers

20190507 Microsoft Build 2019

20190507 Office 365 Market Snapshot - Microsoft's Q3 2019

20190508 Advanced eDiscovery Updates for Q4 2019

20190510 Identity Security at Microsoft

20190513 Microsoft Secure Score Updates

20190514 Azure Durability

20190514 Support for Longer Passwords

20190515 Avanan Global Phish Report 2019

20190515 Microsoft Threat Protection Update

20190517 Weekly News Drop

20190520 Azure AD Entitlement Management

20190521 OneDrive Updates at SharePoint Conference 2019

20190522 SharePoint Security and Compliance Updates

20190523 Identity Data in Europe

20190523 Records Management

20190524 Weekly News Drop

20190528 Azure AD Provisioning Updates

20190528 Can't Change Tenant Name

20190529 Compliance Manager 2019

20190531 Weekly News Drop

Information Barriers in Teams

Microsoft 365

20190102 Standalone Upgrades for Microsoft 365 E3

20190131 Microsoft 365 Security Center and Compliance Center

Azure Information Protection

Microsoft 365 Roadmap

20190408 Roadmap Updates

Microsoft 365 Security Center

20190513 Microsoft Secure Score Updates

Microsoft Cloud App Security

20190122 New Rules in Microsoft Cloud App Security

20190129 Inspecting Encrypted Files with Microsoft Cloud App Security

20190131 Security Workflows with Microsoft Flow

20190313 Microsoft Cloud App Security Updates

20190318 Update on Microsoft Threat Protection

20190606 Discovered Resources in MCAS

20190627 Microsoft Cloud App Security Updates

20190819 Microsoft Cloud App Security Updates

20190902 Expanded Conditional Access in Microsoft Cloud App Security

Microsoft Cloud App Security

Microsoft Information Protection

Microsoft Defender ATP

20190325 Windows Defender ATP Goes Mac

20190730 Monotonic Machine Learning Models

Microsoft Flow

20190131 Security Workflows with Microsoft Flow

Microsoft Information Protection

Microsoft Information Protection

Microsoft Intune

Mobile Threat Defense

Microsoft Office

20190415 Microsoft Office Vulnerabilities

Microsoft Teams

20190226 Worldwide Microsoft Teams Outage

20190318 Data Residency in France for Microsoft Teams

20190430 Information Barriers

Advanced Threat Protection

Content Search

Information Barriers in Teams

Update Log - eDiscovery

Microsoft Threat Experts

20190311 Azure Sentinel and Microsoft Threat Experts

Microsoft Threat Protection

20190318 Update on Microsoft Threat Protection

20190515 Microsoft Threat Protection Update

Middle East

20190618 Data Centers in Middle East

Mixed Reality

20190225 Microsoft HoloLens 2

Multi-Factor Authentication

eDiscovery Workflow

Multi-Factor Authentication

Self-Service Password Reset

Update Log - Authentication

Multi-Geo

Tenant Architecture

Netherlands

20190815 Netherlands on Data Privacy Risks

Office 365 Cloud App Security

20190131 Security Workflows with Microsoft Flow

20190227 Office 365 Cloud App Security Expands Conditional Access

Office 365 Cloud App Security

Office 365 E3

20190307 Information Protection Updates

Office 365 E5

20190307 Information Protection Updates

Office 365 Cloud App Security

Office 365 Message Encryption

20190430 Advanced Message Encryption

Do Not Forward

Encrypt

Encryption - Overview

Office 365 Message Encryption - Version 1

Office 365 Message Encryption - Version 2

Update Log - Encryption

Office 365 ProPlus

20190116 Policy Service for Office 365 ProPlus

20190326 Office 365 ProPlus with Privacy Controls

OneDrive

20190128 Streamlining Files to the Cloud

20190312 OneDrive and Granular Restore

20190521 OneDrive Updates at SharePoint Conference 2019

20190625 OneDrive Personal Vault

20190821 File Explorer Search in Windows 10

Advanced Threat Protection

Content Search

eDiscovery Workflow

File Sharing - Overview

OneDrive Files Restore

OneDrive for Business

20190114 OneDrive Gains Fluent Update

20190114 Sharing Links That Block Downloads

20190705 Automatic Guest Account Creation in Azure AD

20190903 Shared With Me in OneDrive

Outage

20190226 Worldwide Microsoft Teams Outage

Password Hash Sync

20190607 Weekly News Drop

Password Hash Synchronization

Passwordless Authentication

20190710 Passwordless with Azure AD

Passwords

20190514 Support for Longer Passwords

Phishing

20190515 Avanan Global Phish Report 2019

20190702 Anti-Phishing Policy Update

Preservation Lock

20190131 Records Management Updates

Privileged Access

Scoped Administrative Access

Privileged Accounts

Multi-Factor Authentication

Scoped Administrative Access

Update Log - Authentication

Ransomware

OneDrive Files Restore

Records Management

20190523 Records Management

Retention

Azure Information Protection

Retention Labels

20190408 Retention Labels Meltdown

Role-Based Access Control

20190122 Role-Based Access Control to Alerts in Office 365 Security & Compliance Center

S/MIME

20190212 Sensitivity Labels with S/MIME Option

Safe Attachments

Advanced Threat Protection

Safe Links

20190702 Synchronous URL Detonation

Advanced Threat Protection

Scoped Administrative Access

Scoped Administrative Access

Secure Score

20190513 Microsoft Secure Score Updates

20190524 Identity Secure Score Released

Security

20190730 Monotonic Machine Learning Models

Security - Overview

Self-Service Password Reset

Self-Service Password Reset

Update Log - Authentication

Sensitive Data

Content Search

Data Loss Protection - Overview

Identification of Sensitive Data

Supervision 2017

Sensitive Information Types

20190808 Exact Data Match in DLP

Sensitivity Labels

20190212 Sensitivity Labels with S/MIME Option

20190307 Information Protection Updates

Office 365 Sensitivity Labels

September 2019

20190902 Expanded Conditional Access in Microsoft Cloud App Security

20190903 Shared With Me in OneDrive

20190906 Weekly News Drop

SharePoint Files Restore

20190822 SharePoint Files Restore Failure

SharePoint Files Restore

SharePoint Online

20190114 Sharing Links That Block Downloads

20190115 New Files in Yammer Stored in SharePoint

20190115 No More Tenant-Level Opt-Out of Modern SharePoint

20190522 SharePoint Security and Compliance Updates

20190625 Preservation Hold Library Update

20190705 Automatic Guest Account Creation in Azure AD

Advanced Threat Protection

Content Search

eDiscovery Workflow

Litigation Hold Capabilities

SharePoint Files Restore

Storage Limitations in SharePoint Online

SIEM

Activity Logs - Azure AD

Spam

20190717 Admin Submissions for Suspicious Emails

Credential Phishing and Email Fraud

Spam Quarantine

Spam Quarantine

Spam Quarantine

Spoof Intelligence

Credential Phishing and Email Fraud

Supervision

20190130 New Supervision

Supervision 2017

Supervision 2019

Supervision 2019

20190423 Supervision 2019 Updates

Supervisory Review

Supervision 2017

Tenant

Tenant Architecture

Tenant Architecture

20190528 Can't Change Tenant Name

Third-Party Content

eDiscovery Workflow

No Archiving for Some Content Types

Third-Party Data

20190423 Archiving with Native Connectors

20190523 Records Management

Third-Party Security

Support for Parallel Third-Party Security Solutions

Threat Explorer

20190704 Threat Explorer Hunting Updates

Threat Intelligence

20190114 ATP Splitting Into Two Plans

Threat Management

Unified Visibility Across Attacks

Threat Protection

Microsoft Threat Protection

Threat Reporting

Reporting for Response to Threats

Windows 10

20190821 File Explorer Search in Windows 10

Windows Defender ATP

20190124 DLP and Windows Defender ATP

20190313 Microsoft Cloud App Security Updates

20190325 Windows Defender ATP Goes Mac

Microsoft Defender ATP

Microsoft Threat Protection

Windows Information Protection

Microsoft Information Protection

Yammer

20190115 New Files in Yammer Stored in SharePoint

20190422 Yammer in Europe and eDiscovery

Zero-Hour Purge

Spam Quarantine

Glossary