Datasheet

Identity as a Service (IDaaS)

Censornet IDaaS takes a user's enterprise identity – typically in Active Directory or Azure AD – and extends it across multiple cloud and mobile applications using federated identity standards.

IDaaS eliminates passwords, replacing them with more secure tokens or assertions and provides a Single or Zero Sign-On experience for users.

IDaaS delivers significant time savings, removes the costly overhead of password resets, and results in more trusted and secure logins.

Identity is critical at a time when the traditional perimeter is no longer relevant. Context is the new perimeter and identity is the killer context. IDaaS ensures the right people (and things) get access to the right resources (applications, data), at the right times, for the right reasons.

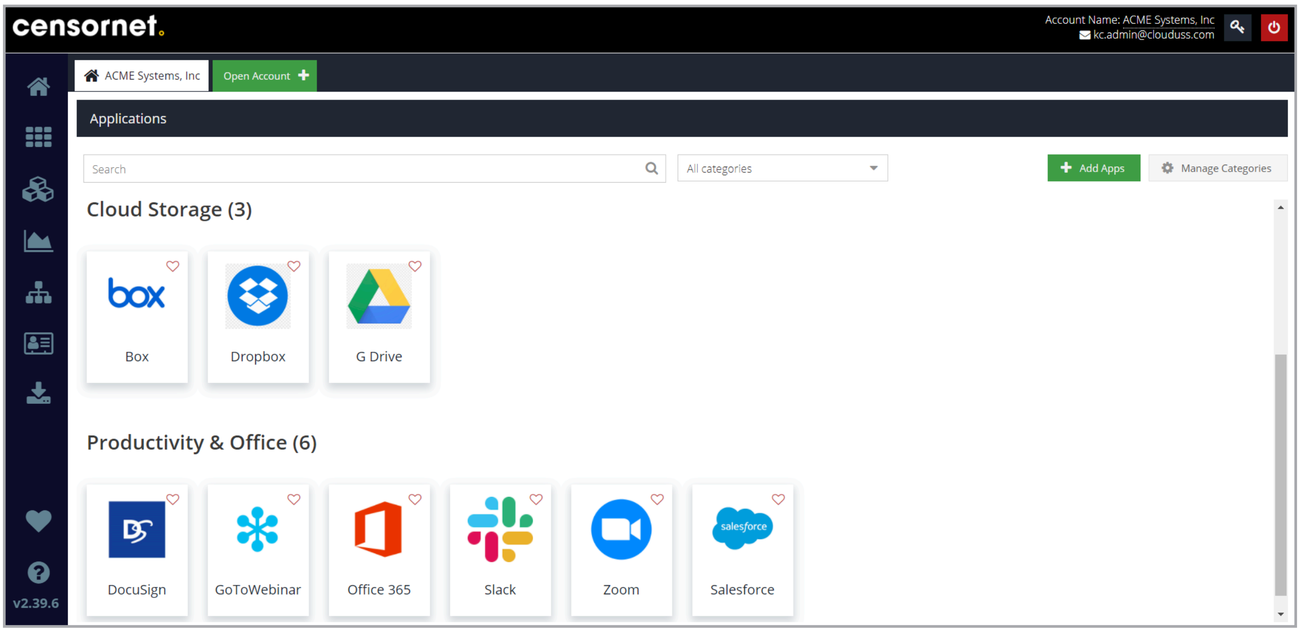
IDaaS is fully integrated with Censornet's Autonomous Security platform that also includes Email Security, Web Security, Cloud Application Security (CASB) and Multi-Factor Authentication. A single web interface provides central policy configuration and management, as well as data visualization and reporting.

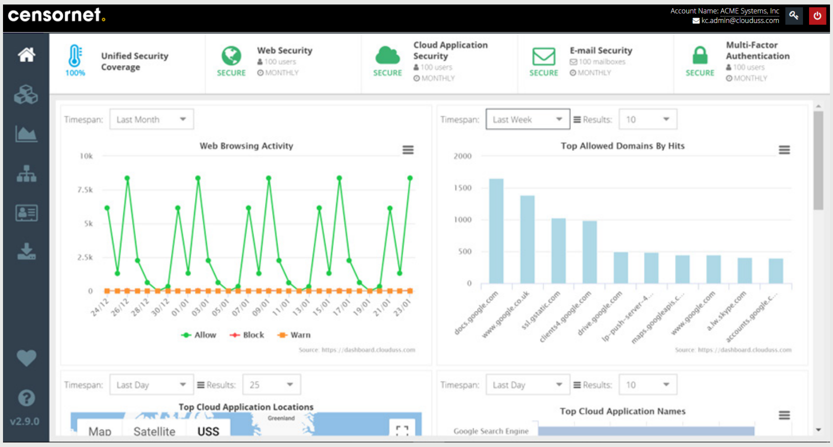
IDaaS is enabled by configuring an identity provider (or IdP) within the Censornet platform, along with one or more applications (service providers). There is no additional hardware or software to deploy. Simple step-by-step guides are available for major identity providers and common cloud apps, including salesforce, O365, Google Workspace, Dropbox and box.

IDENTITY AS A SERVICE

- Extends enterprise identity (in AD, AAD, Google Workspace directory, JumpCloud) across multiple cloud and mobile applications
- Supports SAML and other federated identity standards
- Delivers Single Sign-On (SSO) or Zero Sign-On for users (once authenticated to a trusted identity source such as a Windows domain or O365/M365)
- Replaces passwords with more secure tokens or assertions – users log in to applications without having to enter credentials
- Includes a user 'Application Launcher' page for easy access to all supported applications, or simply works with existing bookmarks/links
- Unique 'Identity Broker' offers flexible implementation in a wide range of environments alongside existing IdPs
- Supports multiple IdPs with the ability to define other 'trusted identity sources' to integrate with other existing identity stores
- Connects between Service Providers (SPs) and IdPs in any arrangement with conditional flows
- Advanced 'Security Decision Manager' assesses all contextual information available at the time of an authentication request to determine whether to allow or deny application access
- Includes full activity/audit reporting across all successful – and unsuccessful - access attempts

User Application Launcher



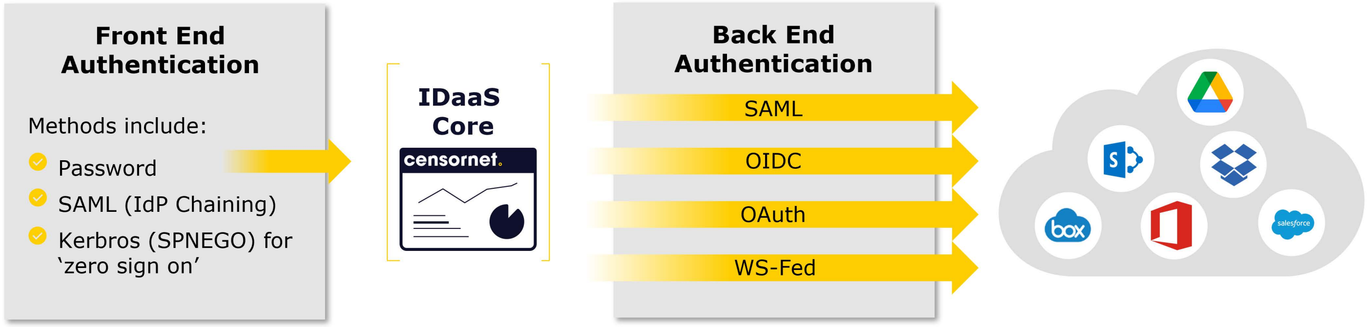


IDaaS is fully integrated with the Censornet Autonomous Integrated Cloud Security platform. The admin portal provides rich data visualization and reporting across an extensive set of attributes and criteria.

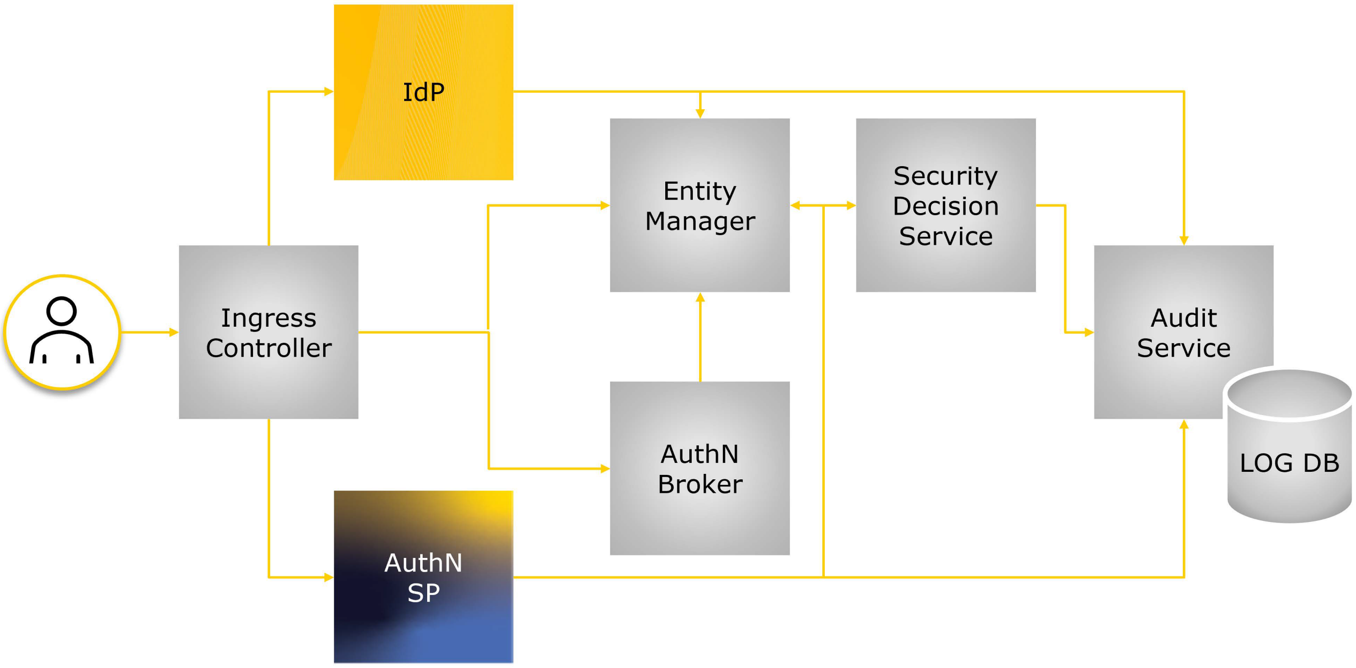
Analysis and reporting is available by time, user, IP address, identity provider, service provider (application) and outcome (allow, deny access).

Whether audit data is required purely for visibility into user application access, or for more formal attestation of compliance with internal policies or external standards, regulations and legislation, IDaaS will provide the evidence needed.

IDaaS Architecture



Identity Broker



KEY FEATURES

Federated Identity	Support for SAML and other federated identity standards. Extends enterprise identity (in AD, AAD, Google Workspace directory, JumpCloud etc) across any applications that support SAML.
IdP Support	Censornet IDaaS supports multiple IdPs – and IdP chaining – for flexible integration into existing environments / identity ecosystems.
Trusted Identity Sources	Define other external/existing identity sources with the unique Identity Broker for wider integration within complex environments.
Security Decision Manager	Assesses all contextual information available at the point of authentication (time, location, geolocation etc) to determine whether to allow or deny application access.

MANAGEMENT

Application Catalogue	Support for SAML and other federated identity standards. Extends enterprise identity (in AD, AAD, Google Workspace directory, JumpCloud etc) across any applications that support SAML.
Application Launcher	Censornet IDaaS supports multiple IdPs – and IdP chaining – for flexible integration into existing environments / identity ecosystems.
User Synchronization	Define other external/existing identity sources with the unique Identity Broker for wider integration within complex environments.
Web Interface	Assesses all contextual information available at the point of authentication (time, location, geolocation etc) to determine whether to allow or deny application access.
Delegated Administration	Allows creation of multiple administrators with different levels of access to the portal. Predefined roles and a full 'Role Builder' are provided.

REPORTING

Real-time Visibility	Query identity related activity in real-time using a range of filters/ criteria. See exactly which users are accessing, or attempting to access, which applications.
Report Builder	Administrators can define their own reports based on available field names and criteria. Reports can be saved and then exported. Audit reports can be searched using criteria including time, user, IP address, identity provider, service provider (application) and outcome (allow, deny access).
Scheduling and Alerting	Link reports to schedules and optionally only receive a report when there is content (alert mode).
Top Trend Reports	A selection of pre-defined trend reports with chart and table data. Trend reports can be exported to PDF and emailed to recipients.
Multiple Views	Analyse and report by time, user, IP address, identity provider, service provider (application) and outcome (allow, deny access).
Log Retention & Auto-archiving	IDaaS log data is archived automatically after 365 days and available to download from the portal for a period of a further 12 months.

DEPLOYMENT

Configuration of IdP(s) and SP(s)	IDaaS is enabled by configuring one of more IdPs and SPs. No additional software (or hardware) is required.

Autonomous Integrated Cloud Security

E. EMAIL

Secure your entire organization from known, unknown & emerging email security threats - including email fraud.

S. SAT

Defend your organisation against cybercriminals by strengthening your engaging and stimulating automated training.

W. WEB

Protect users from webborne malware, offensive or inappropriate content & improve productivity.

C. CASB

Discover, analyze, secure & manage user interaction with cloud applications - inline & using APIs.

M. MFA

Reduce impact of large scale data breaches by protecting user accounts with more than just passwords.

ID. IDaaS

Control user access with complete identity-threat protection. Automatically authenticate users using rich contextual data.

Our Platform

Our cloud security platform integrates email, web, and cloud application security, seamlessly with identity management and advanced data loss prevention to activate the Autonomous Security Engine (ASE).

This takes you beyond alert driven security and into real-time automated attack prevention.

Advanced DLP

Prevent sensitive data getting into the wrong hands.

Enterprise-grade DLP across email, web and cloud applications for the ultimate real-time protection.

Autonomous Security Engine

Prevent attacks before they enter the kill chain.

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence.

CENSORNET LTD

Matrix House, Basing View,
Basingstoke, RG21 4FF, UK

Phone: +44 (0) 845 230 9590

CENSORNET LTD

Park Allé 350D, 2605 Brondby,
Denmark

Phone: +45 61 80 10 13

CENSORNET LTD

700 Lavaca Street Suite 1400-
PMB#100122 Austin, TX 78701

Phone: +1 (877) 302-3323