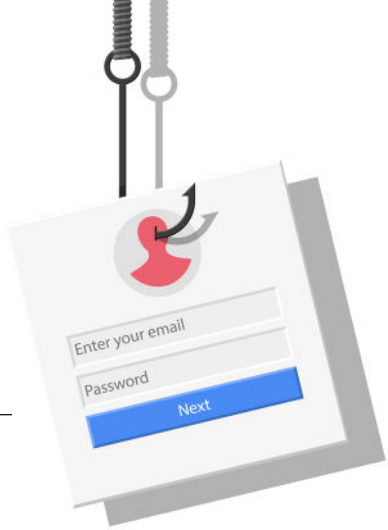
censornet.

HOW TO PREVENT PHISHING ATTACKS.

Your guide to fighting back against phishing attacks



What is a phishing attack?

Phishing attacks are constantly on the rise. They have rapidly become the most popular type of cyber-attack, with over 3.4 billion phishing emails sent out every single day worldwide.

A phishing attack – most commonly delivered via email – is a type of social engineering attack. The attack occurs when the cybercriminal sends a fraudulent message designed to trick the receiver into revealing sensitive information about themselves, or click on a malicious link.

This can be done in several ways, with phishing emails now so sophisticated, that they're often hard to differentiate from the real thing.

Common phishing attacks

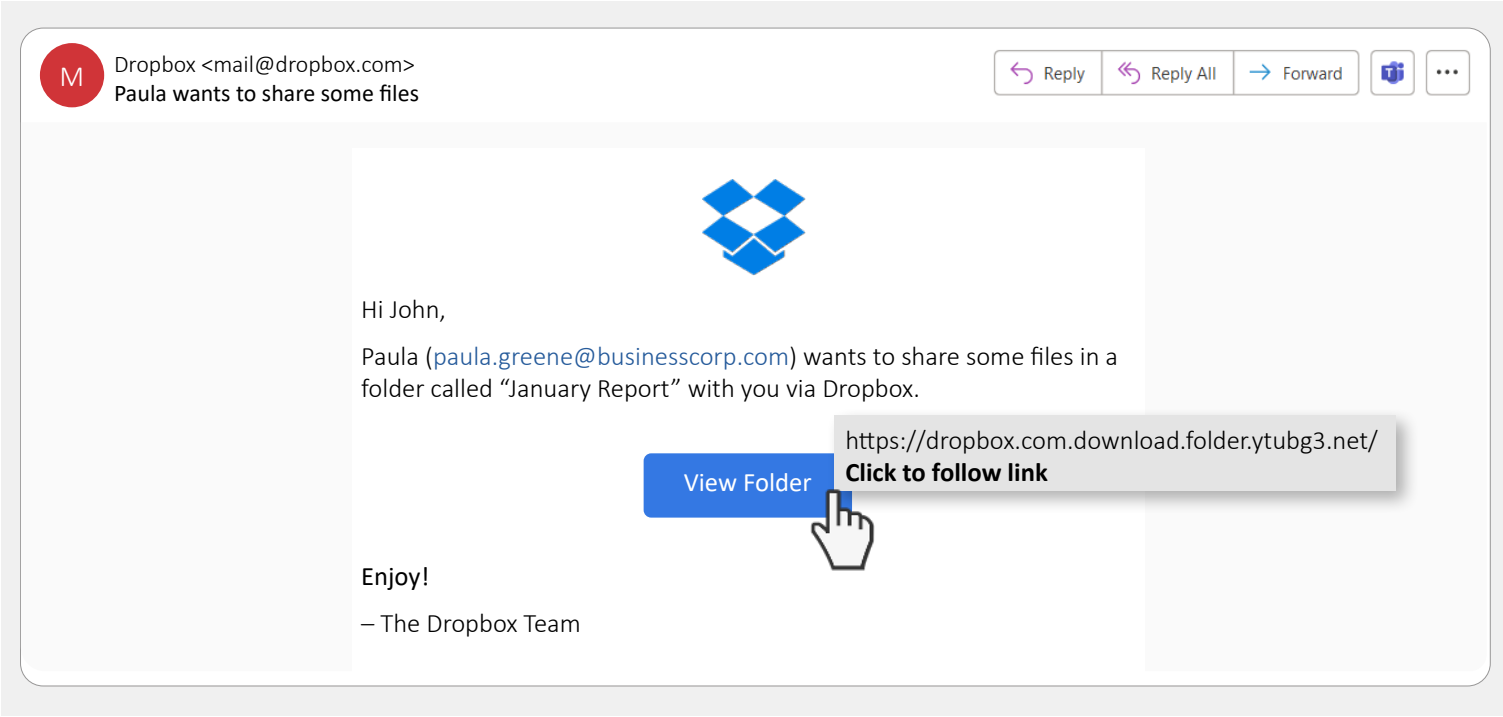
Although phishing emails can be delivered in countless different ways, they are almost always trying to get you to reveal one of two things: your password or your bank details.

Cyber criminals will attempt to contact you from an account or company you are familiar with, playing on an already established trusting relationship. It's important to remember that a phishing attack can come from any source, and there are no names or organisations which can't be spoofed.

The most common email topics include:

- Bank details expired, please confirm card number
- Password needs resetting, please enter details
- Suspicious login on your account, please confirm password
- We've had to reschedule your appointment, please click this link...

Phishing Example #1



At first glance, this Dropbox email looks like it could be legitimate. The email addresses shown are both valid and there aren't any spelling mistakes in the content. However, **whenever you see a link included in an email, you should always act with caution.**

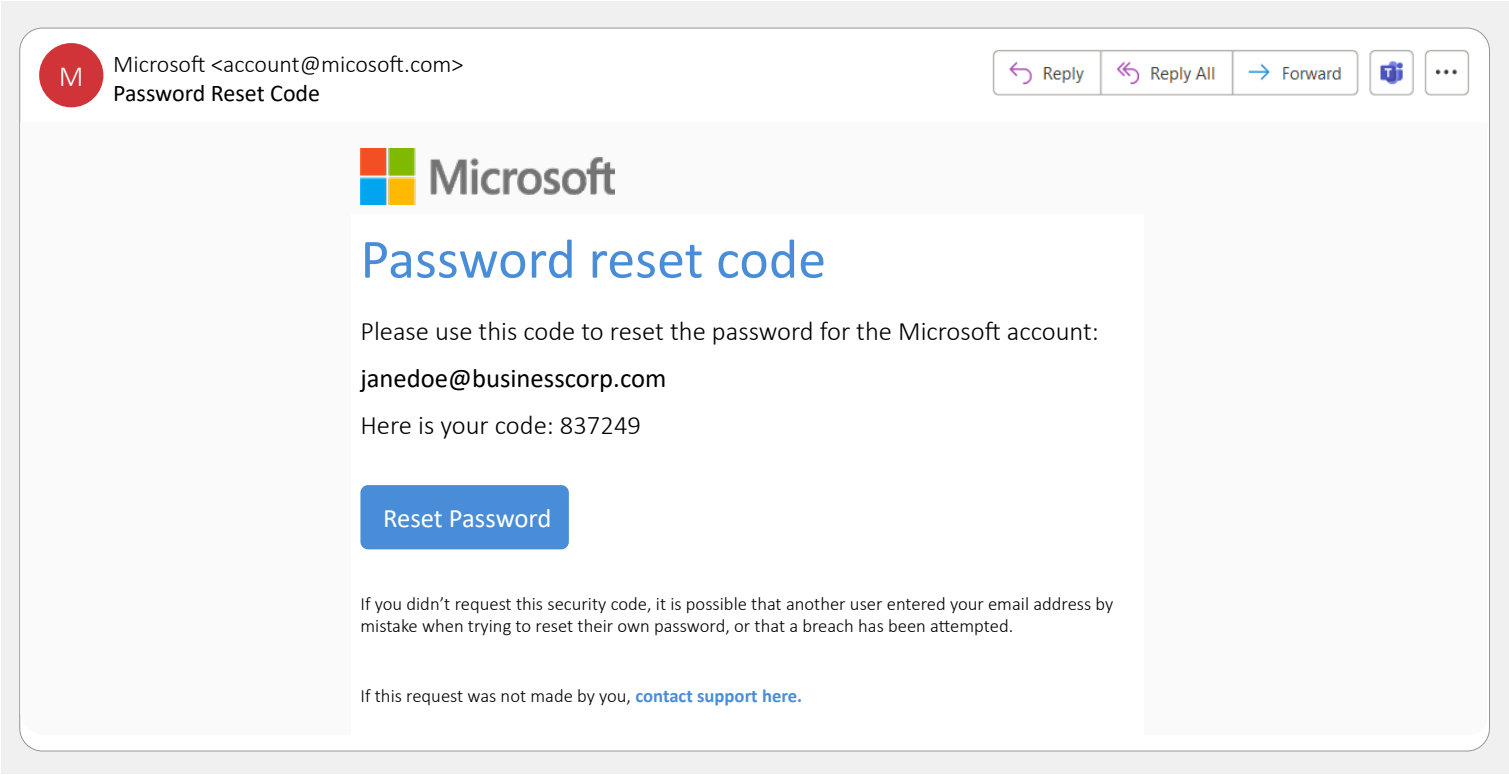
In this case, hovering over the link reveals that the actual URL is hosted on ytubg3.net, NOT on Dropbox. This makes it a phishing attack.

You should **always hover over a link to check it is legitimate** before clicking on it. If you're unable to do this on your mobile device or tablet, wait until you can use a desktop to review the link. If you don't have access to a desktop device, copy the link and paste it into an incognito browser window to ensure none of your details are captured.

If you're unable to do either of these options, then act with caution and ignore the email. Reach out to the supposed sender on a separate chain or through a new medium to try and verify if the email is a phishing attack or not.

> **96% of phishing attacks are delivered via email, 3% via malicious websites and 1% via mobile phones.**

Phishing Example #2



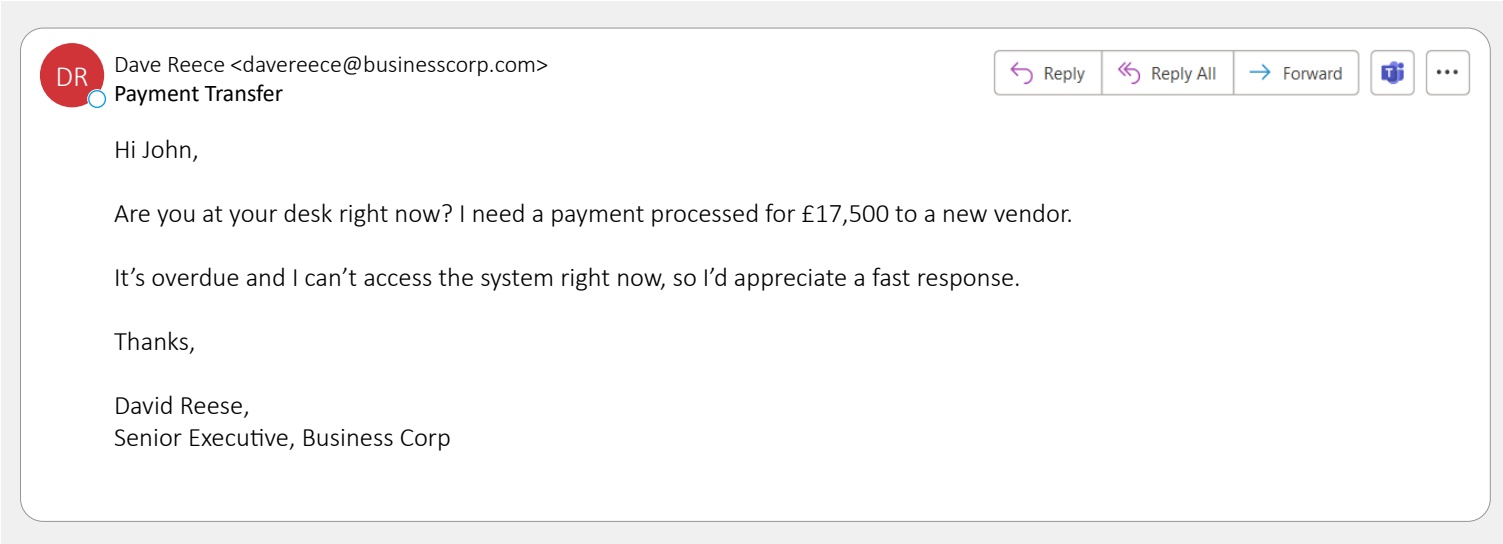
One of the more tried and tested methods used in phishing emails is through a **misspelling or spoofed site name or email address (nearby or cousin domains).**

In this case, the body of the email itself all looks legitimate, with no spelling mistakes or obvious errors – however if you look closely at the sender's email address, you'll spot a missing 'r' in the spelling of Microsoft, meaning this is not a legitimate email.

In cases like this, never click on the link and immediately report and delete the email. You should then access the account in question independently, and ideally from a different device. This can help you to verify if the account is compromised and allow you to change your passwords if necessary, or to provide further peace of mind.

> **71% of targeting attacks involve the use of spear phishing – where a particular individual or organisation is targeted.**

Phishing Example #3



This email is very difficult to identify as phishing or not. The email address is valid for the company and there aren't any spelling mistakes or links in the content.

The tell-tale sign that this is a phishing email is in the language used. There are several instances of urgent language through the phrases 'right now', 'overdue' and 'fast response'. These prompts coupled with the request for a large sum of money flag this email as suspicious and lead us to identify it as a phishing email.

You should **always act with caution when you see urgent language in an email**, as it can be used very effectively as a scaremongering tactic – aimed at getting recipients to act impulsively without thinking.

You also need to consider who the request is coming from and whether it's part of the correct procedure to make a request for a large sum of money over email.

In cases like this, you should report the email to your IT department and then delete it from your mailbox.

> **30% of phishing emails are opened, up 7% from 2020 – showing how relevant the attack method remains**

4 steps to staying safe

Take your time

No matter who the email appears to be from or what it is about, take the time to read it properly before acting.

Check it twice

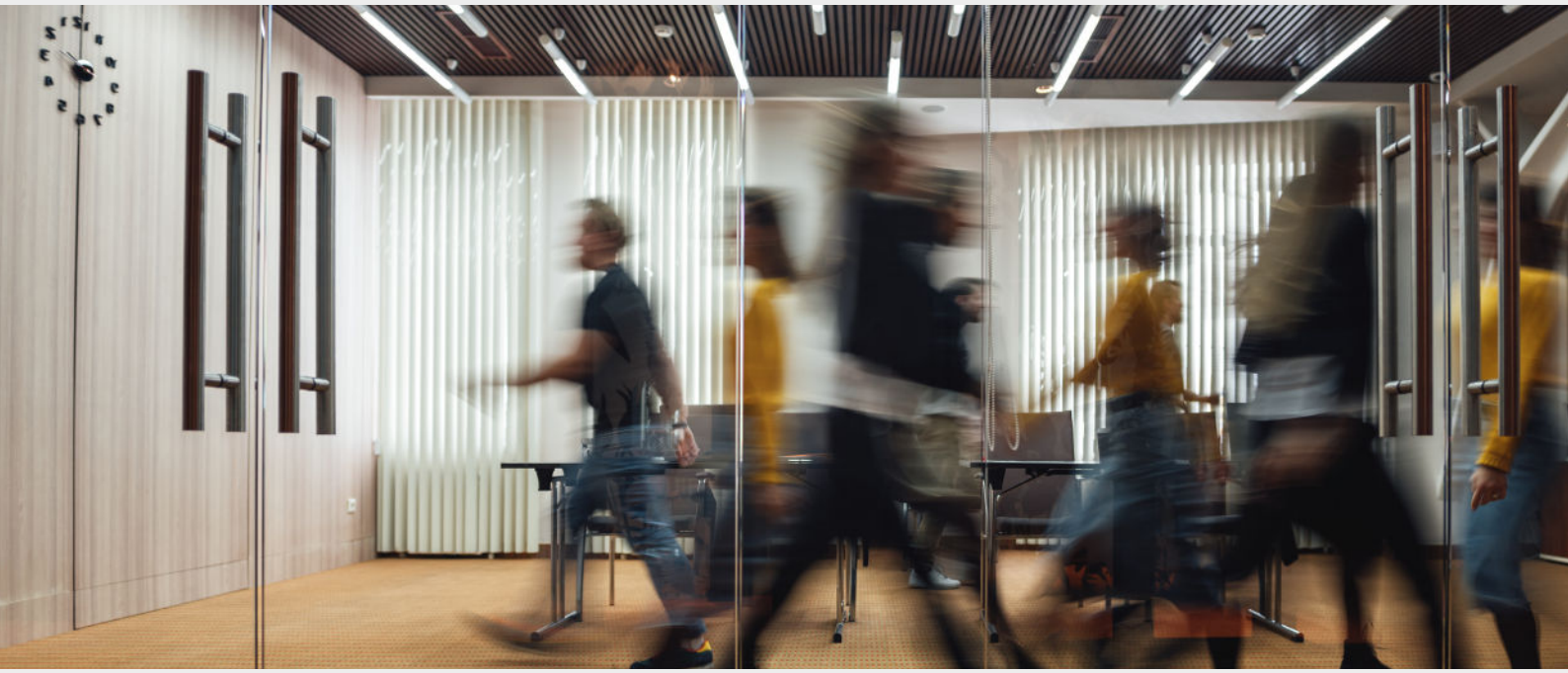
Verify the validity on another device/ browser, through a separate app or by browsing in incognito.

Seek advice

If the email has come from someone you work with, ask them about it directly for confirmation via phone or text.

Just say no

If you are in any doubt, report the email to your IT department and delete it from your inbox.



Key identifiers

As you'll have seen in the examples above, phishing emails often only have very minor errors in them, designed to be missed unless properly inspected. A few key things to look out for are:

- Urgent language
- Time sensitive requests
- Spelling mistakes
- Use of nearby or cousin domains
- Unfamiliar email addresses
- Requests for large sums of money
- Suspicious links or click buttons
- Attachments

It's likely that you won't encounter all these identifiers in one single email, so you need to be constantly aware of them and constantly checking for them.

Unfortunately, cybercriminals are now very advanced, so phishing emails tend to only include one very tiny error – remember though that if you are ever in doubt, be cautious and avoid interacting with the email.

Just half (51%) of the UK mid-market said they were able to prevent dangerous attachments from reaching users' inboxes, and only 35% had the ability to quarantine suspicious or malicious emails.

How to protect your organisation

Typically, phishing defences simply rely on users to 'spot the phish'. But as phishing attacks and the cybercriminals behind them continue to evolve, we need to be more prepared.

A multi-layered approach is the most powerful phishing protection you can get.

Step 1: Cloud Email Security

Users can't click what they don't see, so the first line of defence should be trying to prevent phishing attacks from ever reaching the recipient.

In the current threat landscape, traditional pattern matching or recurrent pattern matching technology just isn't going to cut it. Instead, a cloud-based email security solution that utilises AI to capture even sophisticated attacks is your best bet.

Directly embedded into your email network, Cloud Email Security will monitor all communications for malicious content. It will use powerful machine-intelligence to capture sophisticated attacks automatically - before you even know there is a threat.

Step 2: Identity and Access Management

Identity and Access Management (IAM) provides a layer of protection that means no matter if your logins are compromised, your assets are safe.

Intelligent IAM removes the risk of weak or compromised passwords, replacing them with secure tokens and assertions for total control over user access and zero-trust principles. Using the richest set of contextual data, access automatically blocked when suspicious behaviour is detected through the Security Decision Manager.

James doesn't normally log in at night, and certainly not from Russia. Access is blocked, and a 'successful' phishing attempt is thwarted. We might recommend James check out the next step though.

Email Security Checklist

Ensure your email security gives you these critical features:

- ☐ Pre-defined rules to give you out-of-the-box protection straight away
- ☐ Time-of-click protection from malicious domains that may appear benign at time of receipt but get weaponised at a later date
- ☐ Multiple traditional signature and behaviour based AV engines including sandboxing of file attachments
- ☐ Full analysis of Inbound email with optional Outbound email analysis using unlimited keyword lists
- ☐ Ability to quarantine suspicious or malicious emails to be previewed, released or blocked

How to protect your organisation

Step 3:
Security Awareness Training

Strengthening your human firewall is crucial to defend your organisation against phishing attacks. To do that, you need to invest in a reliable security awareness training platform.

When security awareness training is done successfully, your employees become another layer of your defence. This, alongside phishing simulations, provides users with the tools needed to identify and avoid cyber-attacks before they take hold.

Emails can be delivered via a platform directly to the recipients' inbox, just as a real phishing attack would be. The best providers then enable you to use reporting to identify where the biggest threat to your organisation is – right down from department to individual email addresses.

Take phishing to the next level

Did you know Censornet can impersonate real-world attacks?

Expose employees to phishing attacks, just like they would see in the wild. Everything from Microsoft and Google logins, to Netflix & social media account verification. You can even tailor simulations specifically to your organisation.

We also offer wider cyber security awareness training, providing interactive content and bite-sized quizzes across a range of relevant topics. Our learning journeys are specific to each organisations' needs, covering topics including phishing, malicious software, physical and mobile device safety, GDPR, CEO fraud and many more.

Step 4:
Tie it all together

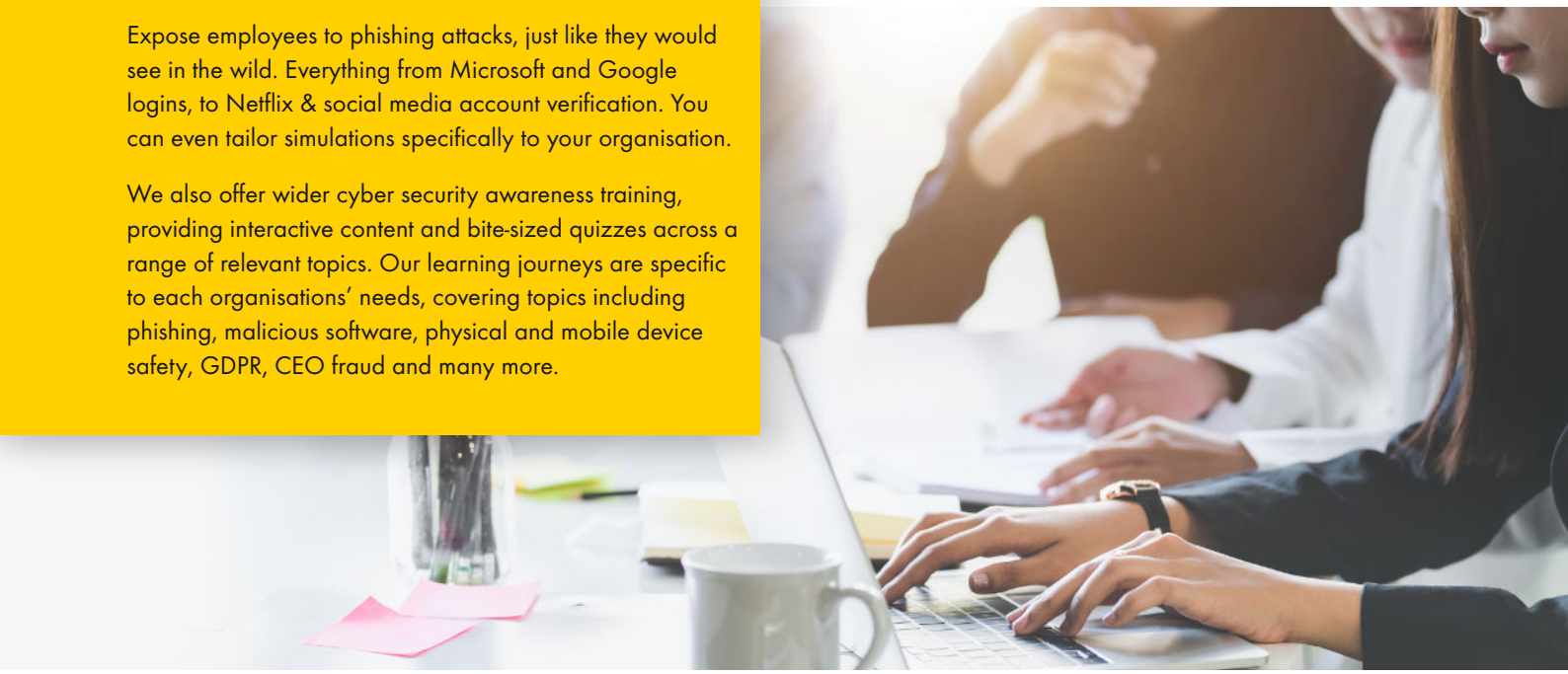
Only 37% of organisations are able to protect against cross channel attacks – for example, attacks that start via email, but continue over the web or cloud application channels.

If your endpoint solutions are siloed from each other, once an attack evades one defence – whether it's email, cloud, web, or identity – it's highly unlikely to be stopped by others.

It's no surprise then that 76% of organisations have plans to invest in a cloud-based security platform that allows their security products to autonomously share security event data to better protect their organisation.

Integrated cyber security platforms intelligently share threat data between products. If a malicious link makes it into an inbox and is clicked, your web security will catch it and make sure the same link doesn't reach a users' inbox again

Autonomous, integrated cloud security is a crucial step towards effective defence that doesn't cost the earth and can keep up with evolving multi-channel threats.



Integrated Cloud Security

You need total visibility. Seamless authentication. Powerful intelligence. Integrated email, web and cloud security with identity and context.

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 provides full spectrum threat protection for your organisation and users – no matter where they are.

Our modules provide unparalleled protection and complete integration to offer full, autonomous security and reporting in a single cloud platform.

Move beyond alert driven security and into real-time automated attack prevention.

Autonomous Security Engine

Enable traditionally silo'd products to share and react to security events and state data whilst leveraging world class threat intelligence. Prevent attacks before they enter the kill chain.

ASE provides 24x7 security so you don't need to.

Full access to threat intelligence without the cost.

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection.

Its Autonomous Integrated Cloud Security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed. For its millions of users globally, its AI-driven, autonomous solution is smarter, faster, and safer than is humanly possible.

It's supported by an award-winning team of customer support specialists. Censornet's clients include Fever Tree, Lotus Cars, Parnassia Group, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider.

It was named Technology Provider of the Year at the British Business Awards 2022. For more information, please visit https://www.censornet.com