10 TOP TIPS

FOR IMPROVING YOUR COMPANY'S EMAIL SECURITY

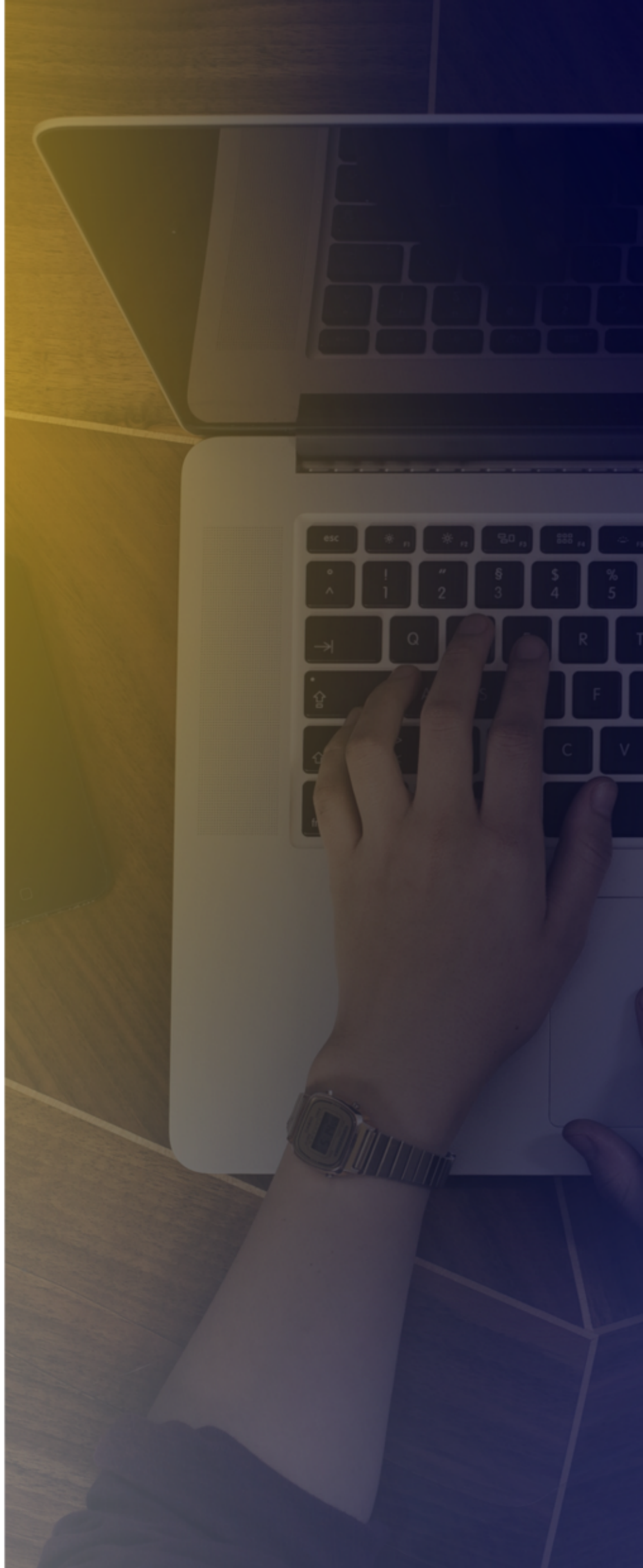
censornet.

10 TOP TIPS FOR IMPROVING YOUR COMPANY'S EMAIL SECURITY

Chances are your business relies heavily on email on a day to day basis to communicate internally, externally and just to make things happen. Email is one of the most enduring enterprise applications, something often taken for granted – but despite its longevity, it's an application that continues to cause headaches for the IT department when it comes to security.

Perhaps because of emails' long-term use, there is a sense of safety, and that users understand email security. But this can be a mistaken sense of safety, often based on outdated information. Email may be a maturing medium, but attacks using email as an entry point continue to become more technically and creatively sophisticated, the measures to defend against them must also.

Starting with the most basic measures, and working up to more sophisticated solutions, here are some things to watch our for and our top ten tips for improving your organisation's email security.



1 Employee education is the bare minimum of email security.

At the last count there were more than 3,000 security vendors in the market, offering a bewildering array of products, most of them point product solutions that address one small area of the overall threat spectrum.

All this choice can be overwhelming, but one thing is for sure: you need to be educating your employees on how to use email properly. Whether this is through regular automated training or a more hands-on approach, your employees should are a vital part of your defence.

2 Be aware of the CEO.

The chief executive is increasingly targeted by hackers, both as a potential victim for phishing but also used as bait to phish others. A phishing campaign that targets executives or important individuals is called Whaling, and is motivated by the high-value information these individuals hold.

CEO impersonation is also on the rise, where hackers create a fake CEO email account using a nearby domain (if they're smart), to trick employees into leaking sensitive information with simple plain text email messages. It's a fiendishly simple attack because if the "boss" tells an employee that they need to be sent financial information urgently, they may not think twice about doing what they're told.

Good email security solutions are multi-layered to protect against the modern email threat and for example, support email authentication standards including SPF and DKIM/DMARC to reduce impersonation or spoof emails.

3 Email link scanning.

Email link scanning tools can provide a safety net against attacks that rely on malicious links. These solutions check whether URLs in an incoming email are suspicious, which removes the risk of an employee not spotting the carefully crafted domain in the page address or clicking on a link to a perfectly legitimate site that's temporarily compromised.

Some link scanners offer the options to scan links at time of delivery of the email, as well as at time of click – to protect the user based on real-time reputation and content analysis.

4 Encryption has its place.

Many organisations don’t know that the underlying email protocol, simple mail transfer protocol (smtp), does not include any form of encryption. Many people think that because email is encrypted between the mail client (e.g. Outlook) and the email server (e.g Exchange) that email is protected in transit. In fact, email leaving the server is in clear text and can be intercepted and read as it bounces off servers, typically in multiple locations before reaching the destination email server of the recipient.

Email security solutions offer the ability to enforce encryption (using TLS) to specific domains, or to even try to use TLS opportunistically - falling back to an unencrypted session if a secure connection cannot be established. This is sometimes called policy-based encryption.

Site to client (business to consumer) email encryption is challenging as there’s no one single standard. Some email security solutions enable the user to tag an email (perhaps with SECURE) at the start of the subject line to encrypt specific messages. The recipient receives a link to an https site to view the message, rather than receiving the message itself (which would be sent in the clear). This might be referred to as user-based encryption.

5 Backup, archiving and continuity.

Almost as important as email security are services that ensure an organisation is able to comply with legislative and regulatory compliance requirements, or that in the event of an email outage, maintain operations and user productivity (email is after all a critical business application).

Simple email backup services will keep copies of all inbound messages (and optionally outbound) and store them for a defined period (usually several years). Email archiving solutions enable regulated companies achieve compliance with features such as tamper-proof storage and functionality to adhere to ediscovery requests or warrants.

Email continuity provides users with access to an 'Emergency Inbox' usually via a web portal accessed via the browser that contains access to Inbox and Sent items from the last 7-30 days. In the event that the primary email provider (or server) fails, users can still read and respond to email until service is restored. These services may not be sexy, but they provide a level of reassurance particularly when moving email off premises.

6 Outbound Email Filtering.

Whereas many of these measures stop the bad guys getting in, Outbound Email Filtering focuses on stopping the sensitive data from getting out.

By checking what is going out, as well as going in, companies can stop data from being leaked by accident or spot employees that are potentially being exploited. Moreover, if one employee email account is infected with malware, outbound filtering should prevent it from reaching and affecting other accounts.

7 Algorithms are king.

Algorithms are king when it comes to identifying and stopping threats and are one of the most effective ways of protecting from modern email threats. Traditionally, email security tools worked using pattern-based approaches, looking at messages for elements that had already been observed in a live spam run, or previous spam run. This approach is still valuable, although fairly rudimentary, but as threats have evolved email security tools have had to as well.

A CEO impersonation attack, for example, would be able to bypass a pattern-based approach because on the surface there is nothing suspicious about a plain text email from one email account to another, especially if it is customised specifically for the victim. Algorithmic analysis is, therefore, vital for catching advanced attacks. Rather than looking at email content, algorithmic analysis breaks down the email into its core characteristics and attributes and assigns each email a weighted score on how suspicious it is. Using this far more sophisticated analysis, alongside pattern analysis which still has its place, organisations can go a long way to halting incoming attacks.

8 Threat intelligence.

Threat intelligence is becoming increasingly important in many aspects of security, and email security is no different. If an attacker is sending a simple plain text email from a legitimate server/domain that hasn't just been registered, where the server matches the domain, with an IP address that isn't blacklisted, that has valid MX and SPF record, then there may be nothing to identify the email – algorithmically or otherwise – as malicious. Threat intelligence may provide a crucial additional layer of defence.

Domain-based threat intel will provide a high risk rating if the registrant has a criminal track record of registering domains and using them to launch attacks, or distribute malware.

9 Outbound Email Filtering.

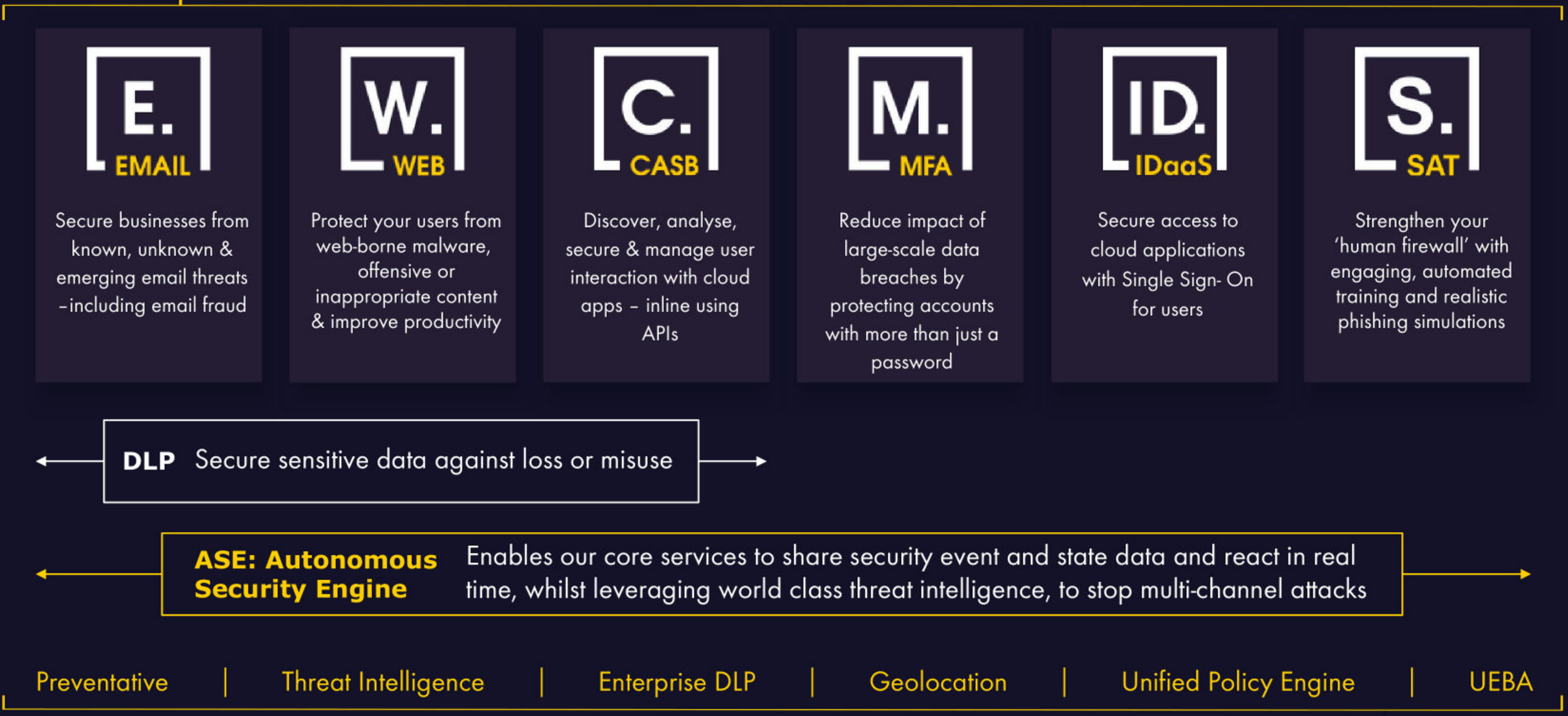
Email security is critical, but it's only one way attackers can get in. Criminals are also targeting other points of weakness in your organisation, the cloud applications you use, the websites your employees visit. It's important to use tools to protect all of these channels in unison, but often they are siloed. This means that those in charge of protecting their employees don't have proper visibility over what is happening in their digital environments. Look for a solution that is well integrated with other elements of security.

10 Automation is the future.

Automation is the future for truly breaking down those siloes. A platform, like ours, that combines all of an organisation's core security services, has the ability to feed information from one service to another. If a link in an email is dodgy it will automatically be added to web security and blocked for all employees. This is the future of email security.

Censornet Platform

We give you the confidence and control of enterprise-grade cyber protection. Our Autonomous Security platform integrates attack intel across email, web, cloud apps and identity to ensure cyber defences react at lightning speed.



E. EMAIL

Secure businesses from known, unknown & emerging email threats – including email fraud

W. WEB

Protect your users from web-borne malware, offensive or inappropriate content & improve productivity

C. CASB

Discover, analyse, secure & manage user interaction with cloud apps – inline using APIs

M. MFA

Reduce impact of large-scale data breaches by protecting accounts with more than just a password

ID. IDaaS

Secure access to cloud applications with Single Sign- On for users

S. SAT

Strengthen your 'human firewall' with engaging, automated training and realistic phishing simulations

DLP Secure sensitive data against loss or misuse

ASE: Autonomous Security Engine Enables our core services to share security event and state data and react in real time, whilst leveraging world class threat intelligence, to stop multi-channel attacks

Preventative | Threat Intelligence | Enterprise DLP | Geolocation | Unified Policy Engine | UEBA censornet.

www.censornet.com