FORTRA™

Enhancing Microsoft Security with Fortra Advanced Email Security

Table of Contents

Why Email Security Remains Top of Mind

It should come as no surprise that email remains the most popular way to communicate in business, and it's why many cyberattacks target email. Email security needs to be an essential part of an organization's cybersecurity policy.

Not only are email attacks popular, but there are many ways to achieve an email attack and gain access to organization's data. Here is a look at the most common threats to email security:

Malware

Files or links to files that if executed (clicked, downloaded, etc.) can infect a machine with a virus, ransomware, or spyware.

Spam

Unsolicited commercial email designed to encourage the recipient to purchase goods or services from potentially illegal or fake sites.

Phishing

Most commonly emails – they can also be text messages, social media, and even phone calls – that mimic a trusted person or brand to steal sensitive data or gain access to an organization's network.

Spear Phishing

Emails disguised as trusted communications from a reliable source usually within the organization. For example, it may appear to be coming from a person with authority within the recipient's organization.

Business Email Compromise (BEC)

Scams such as executive spoofing use social engineering to deceive people into believing they're interacting with a trusted sender. By gaining this trust, the cybercriminal can have money sent to their accounts, gain access to sensitive data, or other ill-intended actions.

Spyware

A type of malware where unauthorized transfer or copy of data from a device or network. This method of hacking can be very difficult to detect as it mimics normal network traffic.

Ransomware

A type of malware attackers used to hold data hostage thereby crippling an organization's operations unless a ransom is paid. Ransomware tends to get a great deal of publicity as it can bring organizations to a halt and be quite costly.

Accidental Data Loss

The loss of data due to mistakes, such as sending the wrong data to a recipient or data to the wrong recipient.

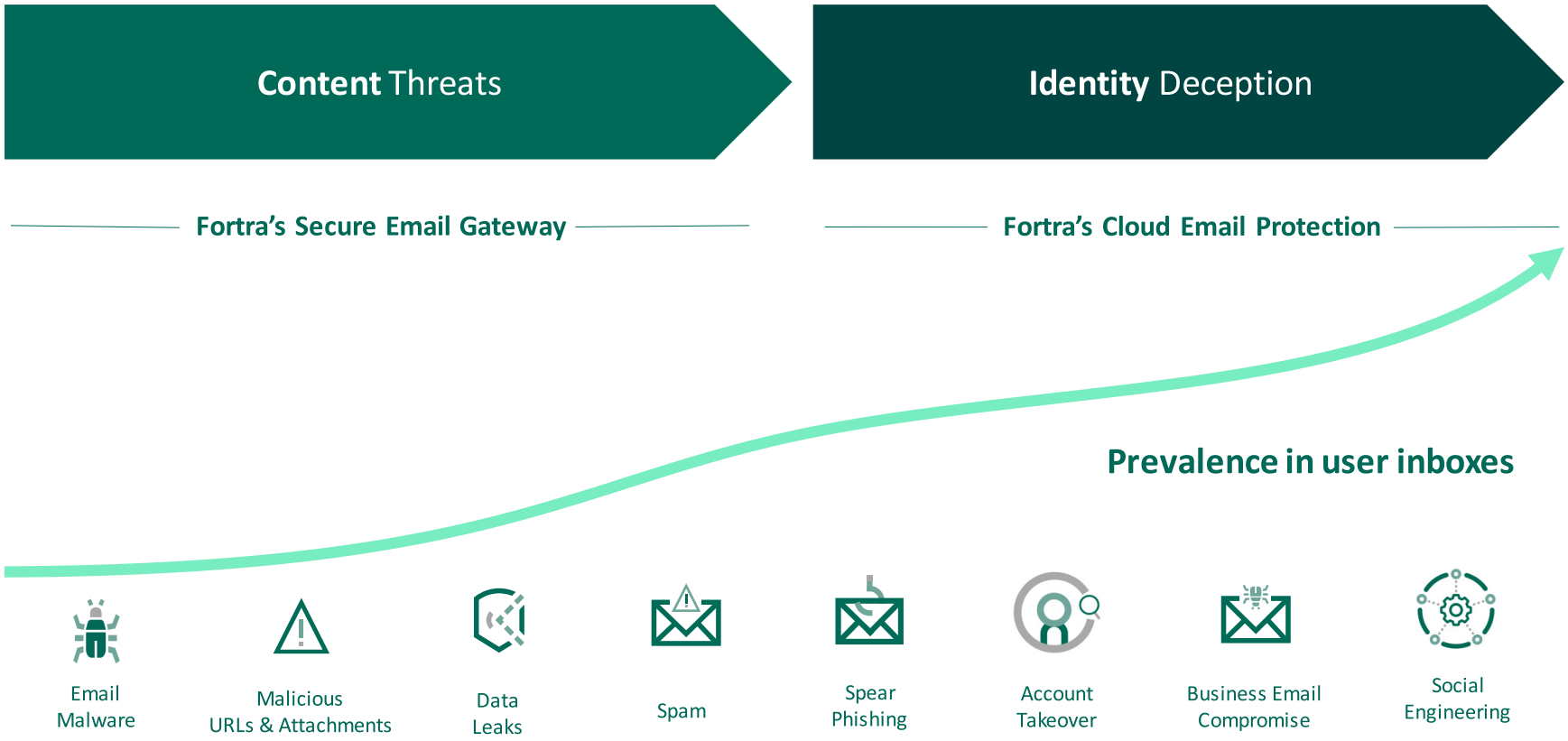
Account Takeover

Where a user's account credentials have been compromised, they then log in as the real user and send messages pretending to be them.

A Layered Approach to Your Email Security

Microsoft 365 continues to be at the top of the list for email providers for businesses worldwide. M365 reached more than 63 million subscribers according to their January 2023 Shareholders' meeting. With high volumes of email moving in and out of organizations, it is important to make sure that email security solutions can keep up with daily threats looking to try new ways to infiltrate. And while M365 offers tiers of security features, their email security capabilities are not enough on their own. In fact, evidence demonstrates that M365 can miss certain data security requirements that customers may have.

The resulting shortcomings leave businesses and organizations vulnerable. Fortra can fill the email security gaps while complementing an existing email platform, such as M365.



Keeping the Bad at Bay Across the Threat Lifecycle

Unfortunately, shortcomings abound along the spectrum of threat protection—from the staging of email-borne threats outside your organization to active threats landing in the inbox. From content-based threats to identity deception techniques, your security architecture has its work cut out for it when it comes to solving the toughest email security challenges.

While M365 has basic content protections available, such as anti-virus, anti-spam, archiving, and encryption, it does not deliver the deep content inspection (DCI) enterprises need to be fully secure. That's because content-based threats don't only exist on the surface, but can be deeply embedded in inbound messages, including files, URLs, attachments, images, etc.

Compounding the content delivery issue, identity deception techniques, such as spear phishing attacks and BEC, are specifically designed to provide threat actors easy access to user inboxes. Most Secure Email Gateways are not attuned to stopping these types of identity threats. They can be delivered in myriad ways, are increasingly difficult to identify, and user-reported threat indicators are generally not enough to stop them.

While some M365 Exchange Online Protection tiered plans come with Defender (or it can be bolted on), other third-party email security solutions in the market provide higher levels of protection against more sophisticated, targeted attacks, such as spear phishing. In fact, a research report issued by Egress in 2021 found Microsoft's traditional static Data Loss Prevention (DLP) rules to be inadequate to deal with human error—with an astonishing 100% of IT leaders reporting that they were frustrated by this.[1]

In addition, outbound data loss can lead to leaks or sensitive information leaving your organization, which can result in compliance failures and the loss of confidential proprietary data. Egress' same report substantiated this prevalence of outbound data loss when it clocked 85% of organizations using M365 having an outbound email data breach.[2]

Luckily, Fortra's Advanced Email Security solutions, including our Secure Email Gateway (SEG), Cloud Email Protection (CEP), and Suspicious Email Analysis (SEA), combat various threat scenarios where others—like M365 Enterprise tiers and other threat protection products— fall short.

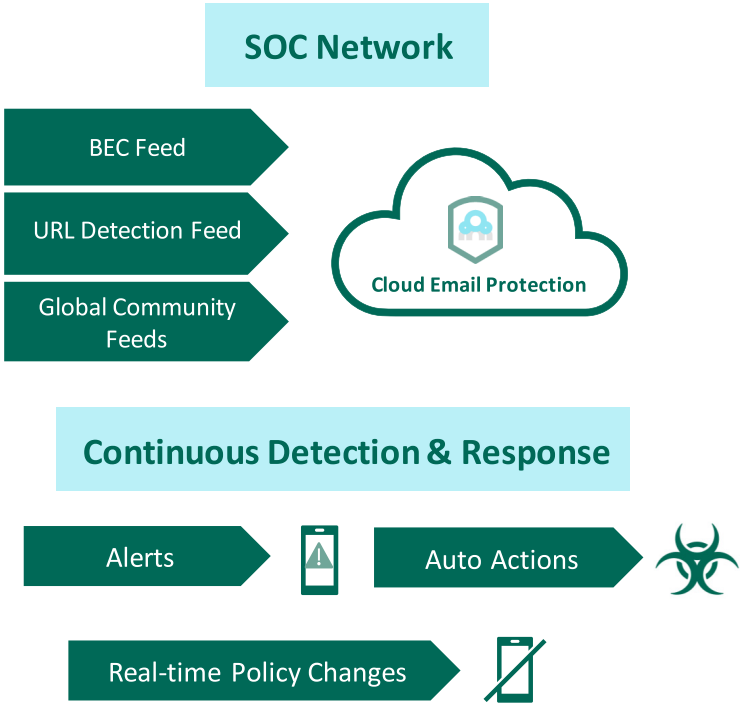
> **"BUT YOU SHOULD BEAR IN MIND THAT, STANDALONE, THE BUILT-IN EMAIL SECURITY FEATURES PROVIDED BY MICROSOFT LIKELY WON'T COVER YOUR ORGANIZATION AGAINST ALL THREATS YOU MIGHT FACE, AND TO THE LEVEL OF PROTECTION YOU MIGHT NEED."**
>
> **— EXPERT INSIGHTS BLOG**

[1]Megan Rees, "Is Microsoft 365 Secure For Business?", **Expert Insights**, Nov 24, 2022
[2]Derek Belair, "Key Practices to Close the Microsoft 365 Security Gap," **Channel Futures**, October 21, 2022

A Step Ahead of the Others in External Threats

Fortra's Advanced Email Security solutions help enterprises combat a broad range of threats from spam to spear phishing attacks with three key differentiators, including:

1. DCI that granularly identifies and stops hidden inbound threats buried deep in email content, attached images and documents, as well as outbound data loss of sensitive and regulated data
2. Identity Threat Detection that provides an AI-driven, additional layer of security behind the gateway to protect against spear phishing and other advanced email attacks that make it past frontline secu rity stacks
3. Global Inbox Threat Intelligence, including crowdsourced malicious indicators, that serves as the underlying foundation and constantly strengthens and informs your architecture against the latest or most relevant threats



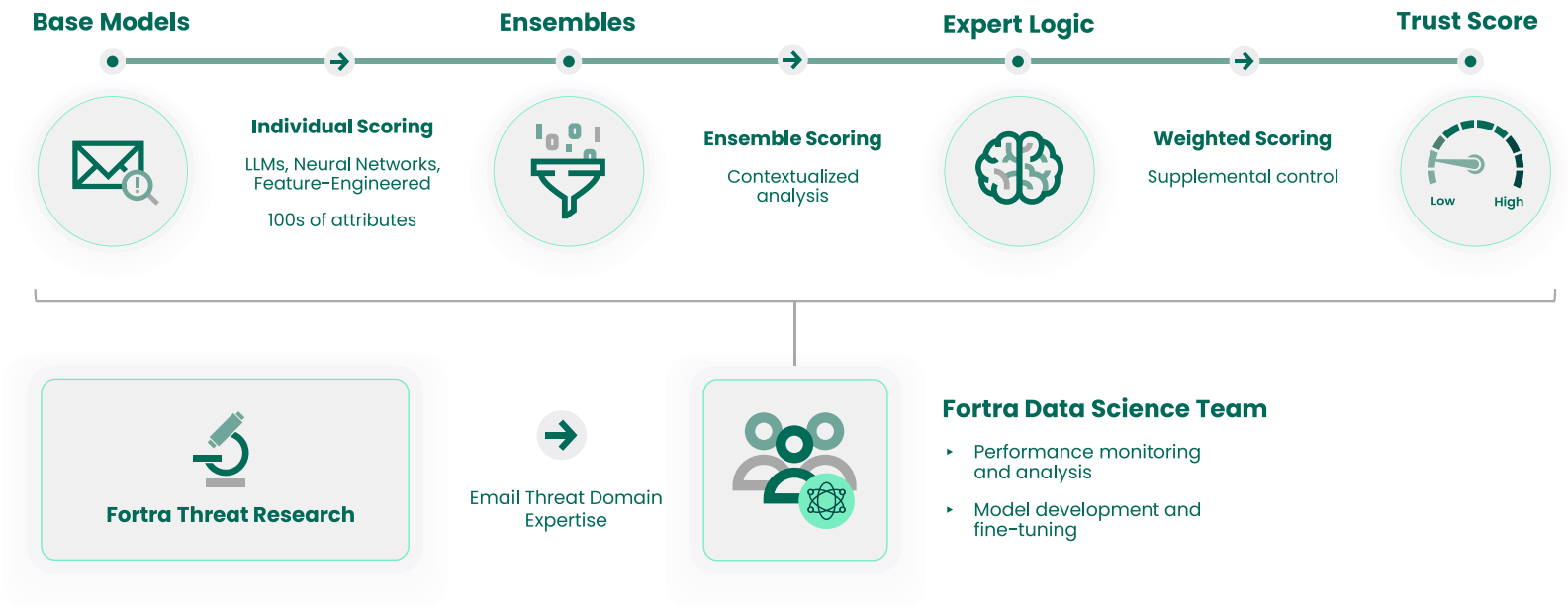
The Data Science Behind Fortra's Premier Integrated Cloud Email Security Solution (ICES)

Fortra's Data Science team employs a combination of machine learning, large language models, and neural networks to determine whether an email should be trusted. It quickly detects and stops advanced impersonation threats, like BEC, that bypass signature or pattern-based defenses, before reaching user inboxes.

In contrast, M365 is generally not able to detect malicious emails that use impersonation techniques. As such, these malicious emails continue to bypass the native controls of M365 because they look for previously recognized signatures of malicious content and thus can find nothing wrong with the emails. And any such detection requires cumbersome rule configuration and upkeep from M365.

This new approach gets more effective with every email analyzed. As a result, it effectively transitions the email security paradigm from one that was designed to address isolated events to one that continuously protects the organization against evolving email threats, as quickly as they emerge. And because this technology is always on, it becomes possible to continuously rescore messages and remove those that evaded initial detection from inboxes.

So while M365 stops the vast majority of the most common types of attacks, Cloud Email Protection and Fortra's complementary solution, Suspicious Email Analysis, provide the defense needed to stop the most dangerous and sophisticated attacks. With this combination of the Fortra Advanced Email Security solutions and M365, email attacks are stopped with 99.9% efficacy—enabling users to trust their inbox and SOC teams to quickly and efficiently identify and respond to emerging threats.

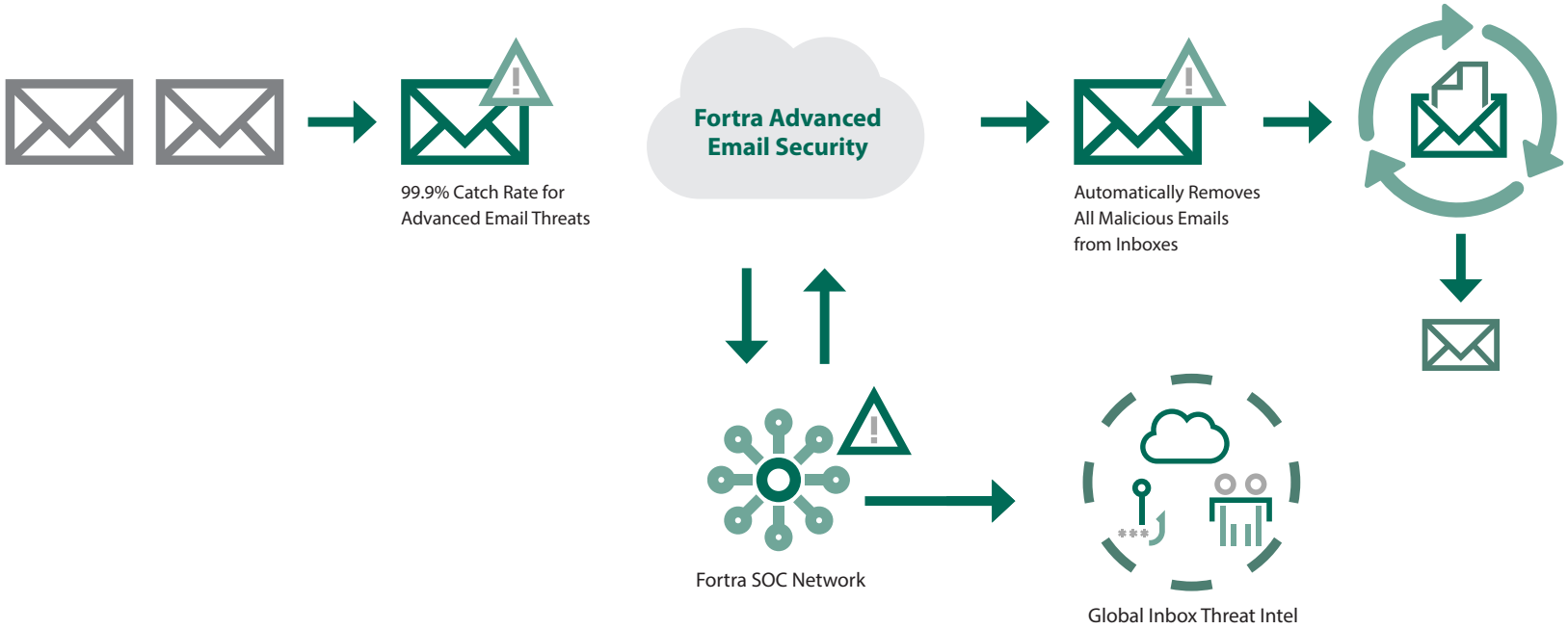


A Step Ahead of the Others in External Threats

Search and destroy is an on-demand policy that quickly and efficiently searches historical email data and implements policies to move emails to junk folders or delete them. Research also suggests that **zero-day attacks** are on the rise and while these attacks can be difficult to pinpoint, Fortra's Global Inbox Threat Intel relies on real-time intelligence from trillions of emails generated by your users, our global base, and other Fortra feeds to understand behaviors and relationships.

However, there are still ways for cybercriminals to get through, which is why Fortra developed automated continuous detection and response technology by leveraging CEP and SEA to continuously monitor for new indicators of compromise (IOCs) detected by threat intelligence, and quickly remediate using combined malicious indicators.

Traditional email security controls rely on blocking cyberattacks at a single point in time when email is delivered. But some threats weaponize post-delivery, after they've made it to the inbox. Continuous Detection and Response uses the output of world-class threat intel to continuously apply the knowledge of new IOCs to search for malicious content in historical email, while also evaluating new inbound emails and applying enforcement actions like junk, delete, or both. Finally, the comprehensive solution can detect and automate the claw-back of those emails that have made it into the inbox.



Thorough Phishing Response Without Burdens

Fortra's SOC team leverages a combination of machine-vetted analysis and expert review to ensure accurate detection. Then they prioritize the reported incidents by elevating the most suspicious to the top of the list. Then, a responsive feedback loop updates your team and quick and thorough mitigation ensures the threats are stopped. It does so by:

- Investigating employee-reported phish
- Automating phish remediation
- Providing CISO-level insights and reporting
- Using RESTful API integration with SIEM/SOAR tools

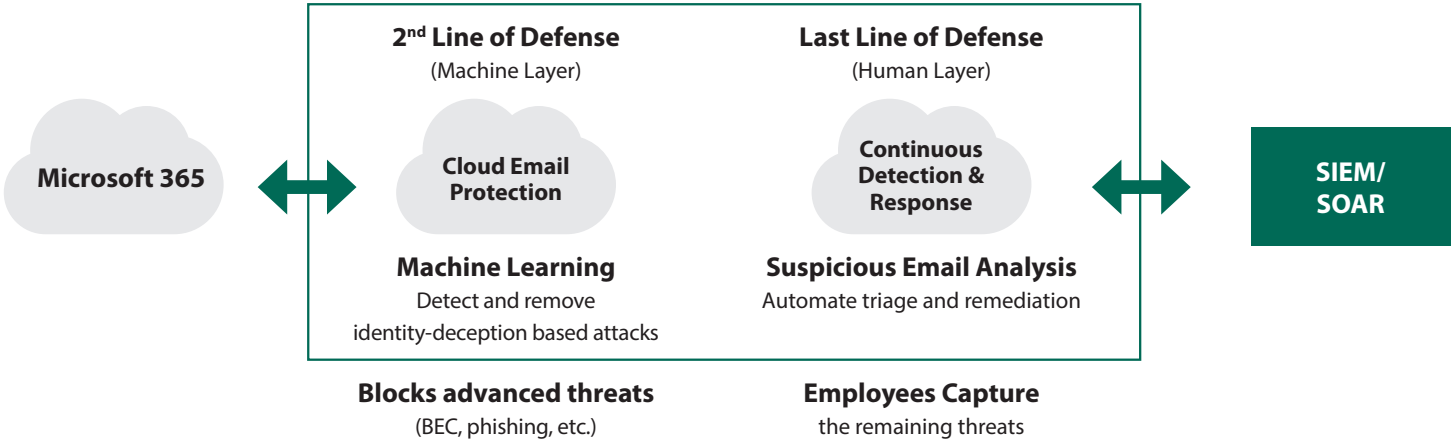
Quick Discovery and Takedown of Malicious Domains

Fortra Advanced Email Security possess strong tools for fighting against lookalike domains, which are frequently used in phishing and BEC attacks. Hundreds of thousands of look-alike domains are created every year by cybercriminals DMARC helps email administrators prevent imposters from spoofing domains by specifying whether spoofed emails should be allowed, quarantined, or rejected by recipients.

DMARC serves as a gatekeeper to a receiving email server and part of Fortra's DMARC Protection. Then analytics allow users to understand where email from their domains is coming from and who is spoofing them. DMARC Protection is the gold standard in the industry. Using DMARC as part of an email best practice allows you to:

- Authenticate all legitimate email messages and sources for email-sending domains, including internal and third-party senders.
- Publish an explicit policy that instructs mailbox providers how to deliver or dispose of messages that are determined to be inauthentic.
- Gain intelligence on all use of their domains in email messages from across the Internet.

Then Fortra's Domain Monitoring proactively mines global domain registrations and DNS data to find lookalike domains. Having an extensive network of trusted registrar partners, Fortra's customers benefit from the highest success rate and fastest takedown of malicious domains in the industry.



Closing the Gaps on Internal Threats

Identify How Data Flows Within Your Organization

When it comes to preventing data loss via email, enterprises often focus mainly on outbound email traffic, but Fortra's SEG was designed to detect content coming in and out, even scanning internal email if desired.

Organizations have a lot of data. It could be sensitive customer data, intellectual property, or even classified information. Accidentally sharing the wrong information is a real risk, even internally.

While this sharing and collaborating of information is vital for business, it can also open an organization up to accidental data loss. Sensitive data needs to be protected whether it is for regulatory purposes (HIPAA, GDPR, ITAR), personal data protection (e.g. PII, PCI), or to protect the business—such as intellectual property, trade secrets, etc. Preventing accidental data loss should be just as important as preventing external threats from reaching the organization.

Fortra Advanced Email Security solutions allow managers to provide controls to restrict certain data from being sent or viewed by specific individuals. Having a departmental manager make decisions on data authorization can strengthen email security and data loss protection policies as IT may not be equipped to know the context of data regulations. This alleviates many burdens for the organization.

Using additional perimeter protection, Fortra's SEG applies DCI on messages. There are multiple ways SEG does this, including:

- Scanning content in a multi-stage process:
  - Identifies the file type by file signature
  - Extracts content for inspection
  - Decompresses file by removing text, metadata, images and embedded files from documents using Optical Character Recognition (OCR)
- Performing message authentication checks using SPF, DKIM, and DMARC
- Carrying out anti-spam content checking using multiple engines
- Malicious URL detection and removal

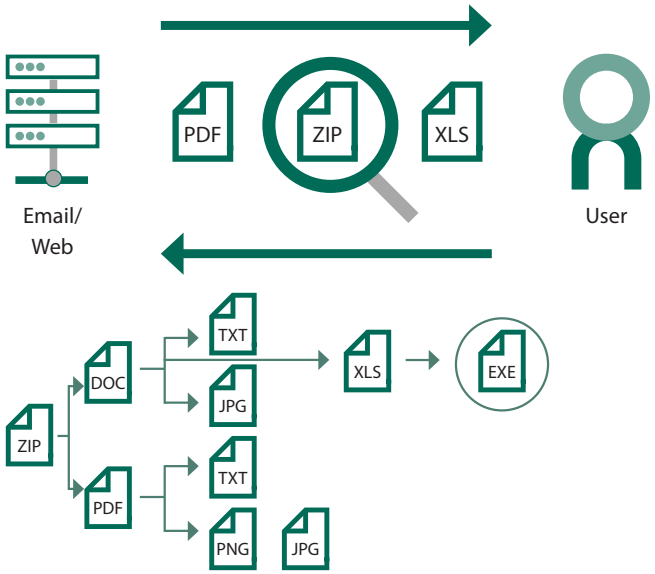
Once the message content is fully extracted, rules can be applied to inspect the content to determine what should be done with the message. Then it's checked using a powerful keyword search engine that supports all language sets, supports simple word, phrase, regular expressions, and compound conditions. Many products can look for simple keywords in messages, but few people consider that these security measures can be bypassed with a simple "Print Screen" operation. Fortra's SEG then employs OCR software to extract text can from the images to make sure sensitive data is not being leaked.

All of this provides a highly accurate and flexible approach where messages can be blocked, held, or delivered with warnings — all based on policies that satisfy even the most stringent requirements.

Closing the Gaps on Internal Threats

To make matters worse, images can be used to carry data by concealing valuable intellectual property or hiding malware in plain sight by using **steganography tools** to exfiltrate information. This may sound like something only used by spies and hackers, but in 2022, an employee of General Electric (GE) was convicted of conspiracy to commit economic espionage by downloading, encrypting, and hiding the files in a digital image of a sunset which he then emailed to his personal email account. According to court documents, the encryption process took less than 10 minutes.

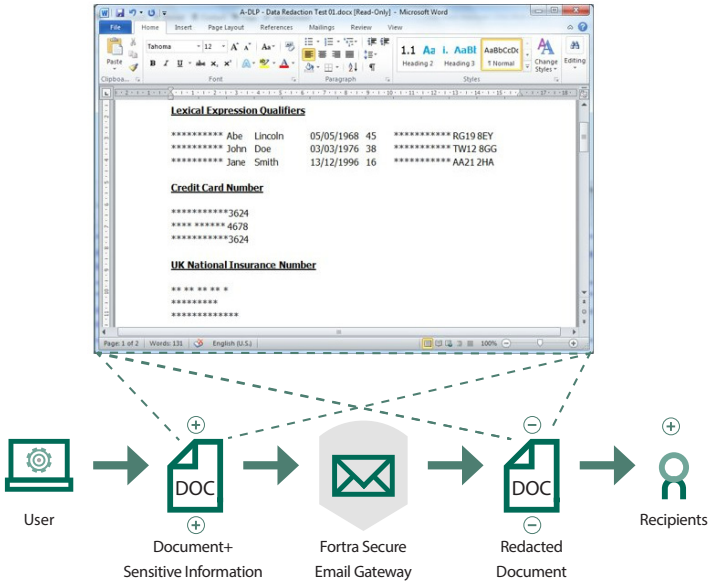
The shocking and quick way this breach was performed is exactly why added email security is vital to the protection of your organization. Fortra's DCI engine sanitizes image files to ensure data or malware has not been embedded using steganographic tools.



Protecting Data with a Better Content Safeguard

In a nutshell, Fortra's SEG can detect information that shouldn't be there. The data might be deliberately exfiltrated or someone could be sending out some content that may contain a hidden worksheet.

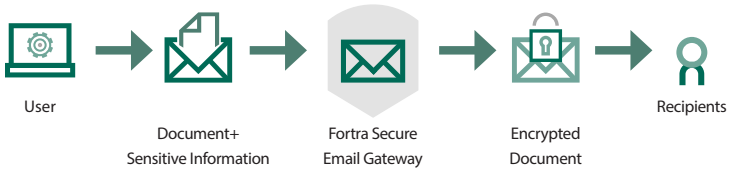
The SEG can clean content to ensure that no sensitive data is being exfiltrated either deliberately or accidentally. Images can be rebuilt to remove any data added by steganography tools. Documents can have sensitive text automatically redacted, even images within documents can have sensitive content redacted from the image and then replaced in the document. Document properties (metadata) can be cleaned; for example, you may want to remove the "Author" name from all publicly available documents.



The illustration displays how an attachment in an email containing sensitive information was redacted by the SEG.

Encryption that Keeps Business Moving

Another part of the Fortra's SEG is encryption, which automatically provides security and regulatory compliance needed to keep data secure in transit while avoiding delays and mistakes. The SEG encryption options allow policies to be based on sender, recipient, subject content, message body, attachment types, attachment content, message header, or document metadata.



By providing multiple options to send data securely, organizations can choose the best method to deliver content to third parties with the most appropriate encryption method. Fortra's SEG uses the following methods:

Transport Layer Security (TLS)

Secures messages over the internet between servers; is completely transparent to end users, and therefore, widely used.

Password-Protected Files:

Wraps the sender's message & attachments into a password-protected Zip file or PDF, which is delivered to the recipient. Password for recipient provided via different format—SMS or secondary email.

Secure MIME (S/MIME):

A standard for sending secure messages, widely used in Europe, that uses public key cryptography, where users are given both a private & public key which are mathematically linked so that an encrypted message with a public key can only be opened by the recipient using the corresponding private key.

Pretty Good Privacy (PGP):

"Pretty Good Privacy" is a similar mechanism to S/MIME where users have both private and public keys, but they use different sets of algorithms.

Web Pickup Over SSL:

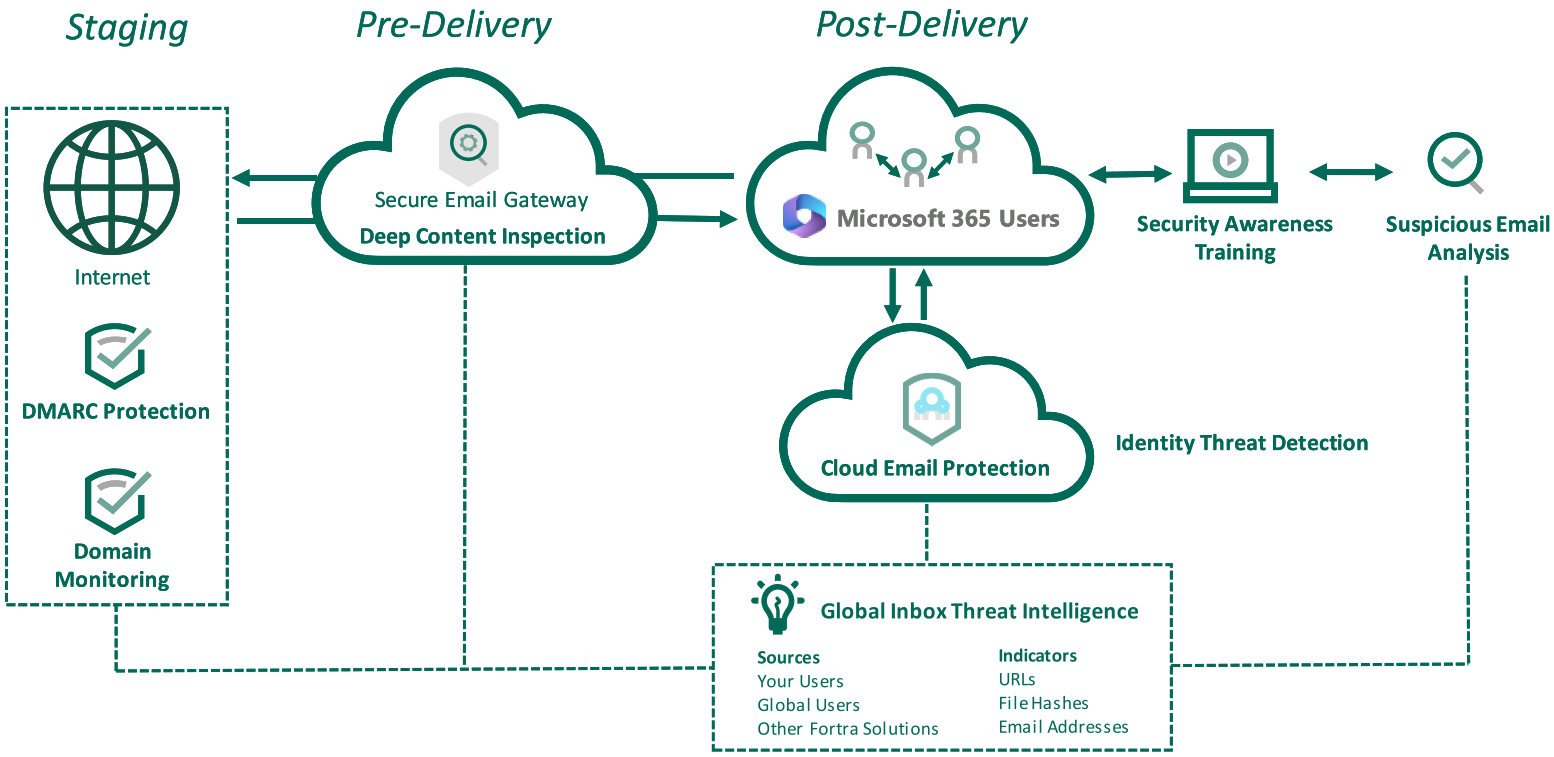
The hosted email portal allows senders to send messages using a webmail-style mail client & respond to the sender in a secure fashion, typically used for low message volume to users of all levels.

Method	Usage Frequency		Recipient		Level of security
	Regular	Adhoc	Business	Consumer	
TLS	✔	✔	✔	✔	Over Network
Password	✔	✔	✔	✔	Over Network
S/MIME & PGP	✔		✔		To User
Web Portal Pickup		✔	✔	✔	To User

A Solid Combination

There is no doubt that M365 possesses many email security protections, but it also comes with shortfalls. These shortfalls have very real consequences. Protecting enterprises against data and financial loss with integrated and adaptive email security through layered security fills gaps left by an existing email platform such as M365. Fortra's CEP uncovers identity deception and protects against phishing attacks, while Fortra's Continuous Detection & Response effectively reports and alleviates burdens on IT departments. Through the SEG, protection from inbound, outbound, and internal messages are achieved including content attacks and data loss. All of this can be done through the cloud, on-premises, or hybrid.

Fortra Advanced Email Security can be deployed alongside M365 to ensure your organization's valuable information remains secure — whether it's housed on-premise, in the cloud, or in a hybrid environment. It's the help your enterprise needs, without the email security hassles and headaches you don't.



Ready to strengthen your email security? Schedule a demo at a time that works for you.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-corp-gd-0324-r3-vm