FORTRA

GUIDE (EMAIL SECURITY)

From SEG to CEG: Moving from the Secure Email Gateway to Cloud Email Gateway

Redefining the Email Security Landscape with a Best-in-Class Solution

Executive Summary

The Time for Next-Generation Cloud-Based Email Security is Now

While the legacy secure email gateway (SEG) is a good option for those industries, such as defense and other aspects of government, that require on-premise appliances to ward off common email attacks like spam, viruses, malware and ransomware, there is a need to augment your email architecture for a new generation of rapidly evolving advanced email attacks that use identity deception methods to trick recipients. With business email compromise scams, spear phishing attacks, and data breaches, along with other types of crime, cybercriminals are seeing massive success to the tune of $12.5 billion in the United States in 2023 alone.

At the same time that cybercriminals are evolving their tactics, businesses are moving en masse to cloud-based platforms such as Microsoft Office 365 or Google Workspace. These platforms provide native support for anti-spam, virus and malware blocking, email archiving, content filtering, and even sandboxing, but they lack when it comes to protecting against advanced email threats that use identity deception techniques to trick recipients.

This move to cloud-based email and the onslaught of zero-day attacks that successfully penetrate the inbox are shifting email security from signature-based inspection of email on receipt to continuous detection and response using machine learning to detect fraudulent emails and to hunt down latent threats that escaped initial detection or have activated post-delivery.

As a result, Fortra's new integrated cloud email security platform (ICES) has emerged – Fortra Cloud Email Protection. With innovative features like deep content inspection, identity threat detection and global inbox threat intelligence, Cloud Email Protection delivers the capabilities you need to stop advanced threats. Fortra's deep content inspection augments traditional security appliances like SEGs. Also, our advanced data science leverages a combination of machine learning (ML) models, Large Language Models (LLMs), and neural networks to detect suspicious markers or anomalies in email header data. Finally, our global threat intelligence feeds monitor indicators of compromise and user-reported data continuously enriches the platform to stop the advanced email threats that other legacy controls miss.

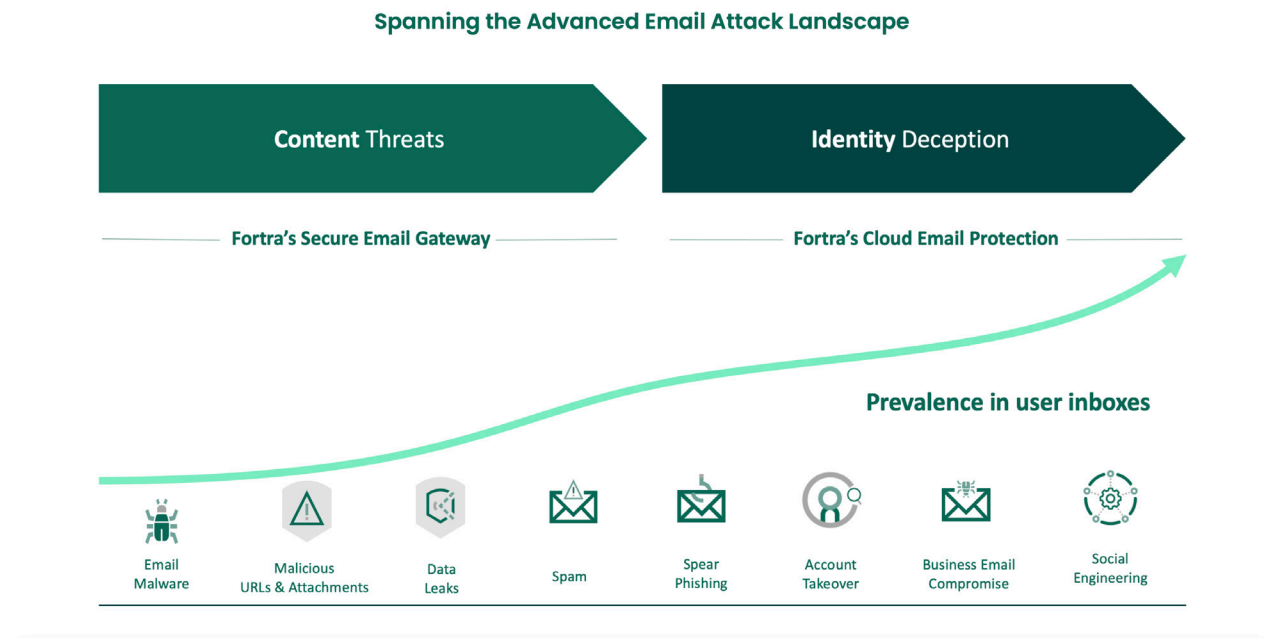
There is little doubt that email and the threats against it are changing fast. Email security must do the same.

The FBI estimates that nearly 21,500 victims lost $2.9 billion in 2023 from business email compromise in the United States alone.

Table of Contents

An Enemy in the Inbox

Identity Impersonation Has Changed the Game



The ubiquity of email, as well as the known limitations in its technology, has made the channel vulnerable to cybercriminals for decades. In the early 2000s, the secure email gateway (SEG) and various anti-malware/anti-virus vendors stopped the majority of these attacks as they focused on signature-based inspection of incoming message content. SEGs assessed the reputation of the sending infrastructure in order to identify and disrupt spam, virus and worm attacks, and scattershot credential phishing attacks. Leading SEGs still rely on detecting the "bad" or malicious content like malware, keywords, or high volumes of attacks from a single IP address.

While this approach stumped cybercriminals for quite some time, they eventually evolved to send new types of threats. Second-generation SEGs and phishing defense solutions leveraged malware sandboxes and new forms of dynamic analysis to counter them. Unfortunately, cybercriminals evolved email-based threats faster than most of the email security industry, changing their approach once again to using sophisticated identity deception techniques and attacks with no detectable payload, both which can easily bypass most legacy defenses.

A New Kind of Attack

Instead of relying on malicious links or software, a new generation of well-funded, increasingly networked cybercriminal operations has evolved the techniques used for email-based attacks from content deception to identity deception.

Exploiting security gaps in the underlying email protocols or the user interface constraints of email clients, attackers are able to send email messages that leverage the identity markers of trusted people and use deception techniques informed by social engineering to manipulate recipients into taking a desired action such as wiring money or divulging sensitive information. These messages hide in plain sight, easily bypassing legacy security systems undetected, and use personal and professional context to defraud businesses and individuals.

Making matters even worse, attackers are increasingly leveraging popular cloud platforms and services, and even compromised user accounts, to launch these attacks. By using Google and Microsoft infrastructure, cybercriminals prevent organizations and current email security solutions from blacklisting the services, given the tremendous volume of legitimate email that they send.

Some Limitations of Awareness Training

Perhaps the most obvious solution to defending against human vulnerability is simply to train end users how to spot fake emails—showing them which rules to apply to inspect emails in their inbox. While security awareness training is critical to a holistic enterprise anti-phishing strategy, it is not foolproof. In fact, Fortra's Terranova 2023 Gone Phishing Tournament findings reported that 10.4% of all phishing simulation email recipients clicked the message's phishing link – that's a 3.4% increase compared to the previous year's metric results! Even with a security awareness training and phishing simulation program, a well-crafted targeted email attack using personal context is likely to fool users into opening the email and clicking on malicious links.

Furthermore, security awareness training will likely result in an uptick in reported phishes, some of which will turn out to be false positives. Clearly, a better solution is needed not only for email security, but for triage, response and remediation as well.

Angles of Attack

Key Identity Deception Techniques

With identity-based email attacks posing a serious threat to individuals and organizations in every sector, it is critically important to understand how cybercriminals use identity deception techniques to evade existing security controls.

The key to any identity-based attack is impersonation—manipulating components of an email message to exactly match or bear an extremely close similarity to identity markers in a legitimate message. The most common message components that have these identity markers are the "From" header, the Subject header, and the body of the message.

The Parts & Parcel of Email Parsing: Email Header Data

Here is a breakdown of the various components embedded in email header data:

From

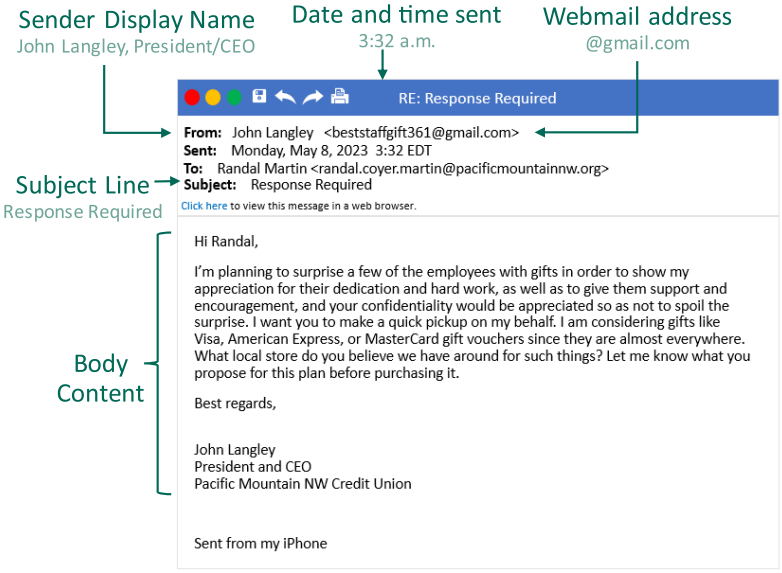
The "From" field, or Sender Display Name, is who the message is sent from [header.from]. This field can be easily forged and is why we suggest ensuring you only open email that has been authenticated by SPF and DKIM.

To

This displays who the message is addressed to, but may not contain the recipient's email address.

Subject

The subject line is generally the high-level topic of the message being sent as created by the sender.



Local Part

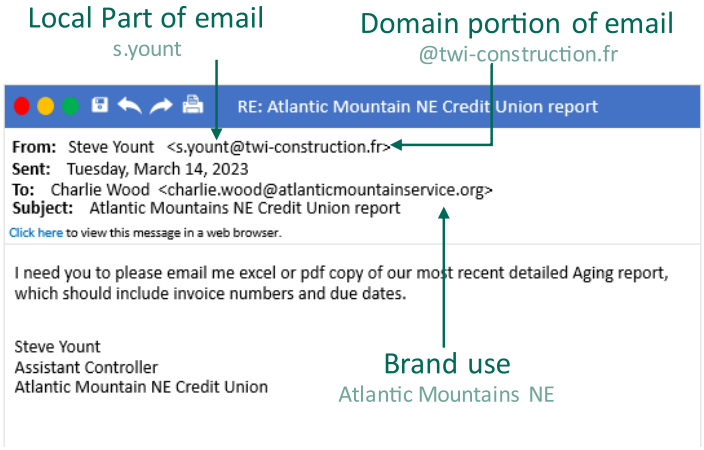
Also called the email prefix, it is the unique identifier or username that comes before the @ symbol in an email address (i.e., the person or entity within an organization that the email is sent directly to).

Email Domain

The email address that follows in brackets after the "From" field shows the actual email domain from which the email was sent.

Brand Use

This is a technique used by threat actors that includes the sending company's name with the goal of legitimizing the email communication.



In addition to the header data, the machine learning models also consider other email characteristics and data, including, but not limited to:

- The sender's infrastructure
- The number of days IP address has been used to send from on behalf of domain
- The number of emails sent using the same "Local Part" of email
- The number of emails using the same Display Name
- Intent of the email (examine nature of content, like Subject Line)
- Matching Address Group and Display Name
- Character text used in the Local Part of email (Latin vs. Cyrillic)
- SPF/DKIM/DMARC records
- And others

Once all of this data is evaluated and scored, Cloud Email Protection produces Reputation and Authenticity scores.

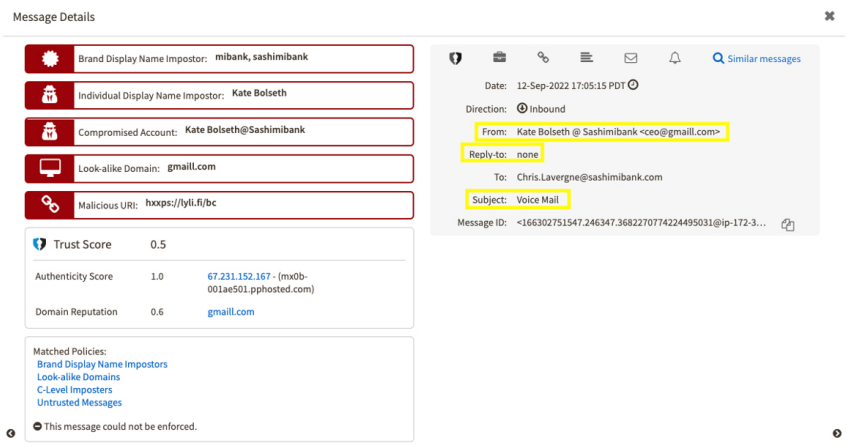
This basically determines if the email was part of a previously unidentified targeted attack, or if it was simply an anomaly. For example, if there was an email that received a very low Authenticity score but a high Reputational score, the models would suggest that there was likely a spoof of a highly reputed domain. The models will then output a "final" Trust Score based on the unique combination between the two model scores on a scale of 0 – 10–where generally a score of 0 -1 is untrustworthy; a 1.1 - 5 rating is suspiciious, and a >5 rating signifies a trusted communication.

Real Example

This malicious email attempts to impersonate a CEO. While the sender's name and the company name look legitimate, if you look at the fields highlighted in yellow there are indicators of impersonation, specifically:

1) The "From" address which has <ceo@gmaill.com> with Gmail's sending domain name being misspelled, which is actually a look-alike domain;

2) The "From" address also has "Kate Bolseth" as the sender identity from Sashimibank, however she is the CEO of Fortra, not Sashimibank;



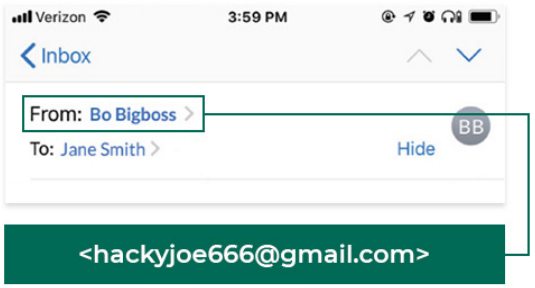
3) The Reply-To address of "none";

4) The subject line of "Voice Mail", representing a fraudulent vishing attempt employing a very generic subject.

This message passed SPF authentication due to relaxed SPF alignment in the domain's DMARC policy. However, this message was given an overall trust score of 0.5 by Cloud Email Protection because it has matched multiple policies associated with impersonation at the bottom, including Brand Display Name Imposters (Sashimibank), Look-alike Domains (gmaill), C-Level Imposters (i.e. Kate), and thus, a label of "Untrusted Message".

Display Name Deception

Of these components, the display name in the "From" header is the most commonly recognized identity marker, as it is displayed prominently in most email clients. It is also the marker that is most commonly abused, since the sender of a message can specify any value for the display name. Indeed, this kind of technology continues to be the tactic of choice for cybercriminals, accounting for 53% of all email attacks.



Cybercriminals simply need to insert the name of a trusted individual or brand into the display name field within Office 365, G Suite, Yahoo, or any other cloud-based email platform. Since its point of origin is an established and widely used hosted email service, these attacks easily evade most SEG defenses, and then trick their recipients since the name matches one they are familiar with—either a brand they trust or a specific person within their organization.

Compromised Accounts

The second most common form of identity deception is also the most harmful. Known as a compromised account attack, this approach is used in one out of every four new email scams, and it is by far the most difficult to detect and stop. A key driver of this attack modality is the rapidly expanding online marketplace for stolen email account login credentials belonging to high-value targets.

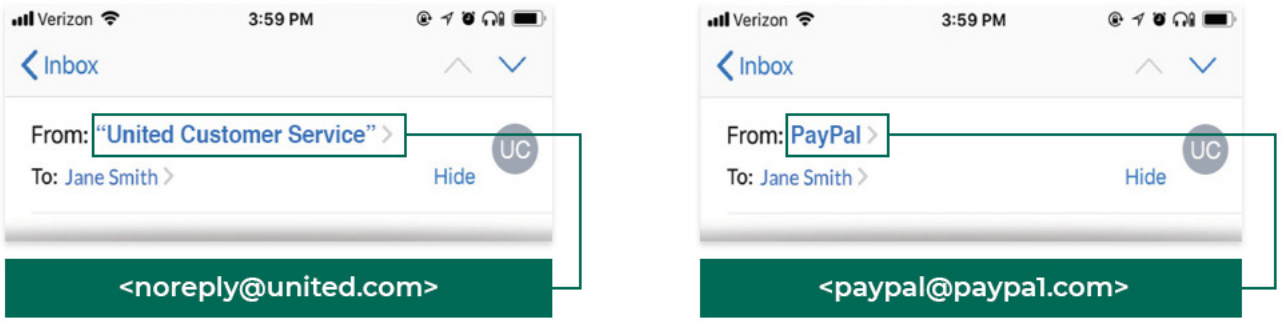
Here again, traditional email security controls are defenseless because these attacks are launched from a legitimate email account within a legitimate domain—perhaps even from the same domain as the target. These attacks are especially damaging because each new compromised account can lead to more. A successful compromised account not only gives fraudsters the ability to impersonate the email account's owner, but it also gives them access to the individual's contacts, ongoing email conversations, and historical email archives. This makes it possible to craft new scams that appear entirely legitimate—coming from the actual account with all the background information needed to make perfect sense.

Look-Alike Domains

The remaining identity deception technique includes look-alike domains. Here, threat actors can use common misspellings, homoglyphs, or Cyrillic characters that appear similar to the original characters in an impersonated domain to a company or a trusted service such as DocuSign, Dropbox, or Microsoft itself. While large services and corporations often register look-alike domains as "defensive domains" themselves to prevent this attack, they can never register every permutation. In addition, if the organization has not implemented the email authentication level needed to block the use of the look-alike domain, attacks can still spoof the look-alike domain, no matter who legally owns it.

By only slightly changing the domain, criminals can easily trick recipients who may not notice an extra letter or have the foresight to focus on the sending domain. Indeed, something a simple as changing a lowercase l in an email to an uppercase I can appear to be the same visually, but have an entirely different digital destination.

Despite their differences, each of these forms of identity deception is designed to bypass legacy security controls and ultimately convince recipients that the message was sent by an identity they know and trust. Once the email security system has been bypassed, cybercriminals have struck gold by taking advantage of a much weaker defense—humans themselves.



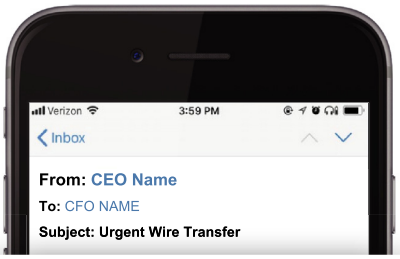
$37.4 Billion and Counting

The Economics of Impersonation-Based Email Attacks

The result of these new identity deception-based email attacks is that business email compromise, data breaches, and consumer phishing are costing businesses and consumers billions.

Big Business in Business Email Compromise

These attacks are seen on a daily basis through CEO wire fraud schemes, partner invoice scams, or payroll diversion scams, with most organizations receiving hundreds or thousands of per year. Unfortunately, it only takes one to lose millions of dollars. However, it's not just huge enterprises that are discovering how easy it is to be scammed. According to the IBM/Ponemon's Cost of a Data Breach Report, the average global cost of a successful phishing attack is $4.76 million––money that goes straight into the pockets of criminals.



Nearly **$3 Billion** 2023 Actual Losses due to BEC

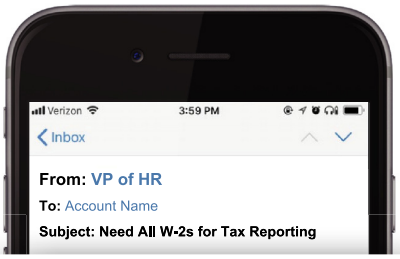
Source: Statista, Apr. 3, 2024

Data Breaches Continue to Concern

Business email compromise isn't the only major player, with a recent Comcast Business survey finding that between 80-95% of all breaches start with a phishing email. These breach-focused attacks use spear phishing or social engineering techniques to gain access to sensitive data such as employee W-2 or direct deposit information.

Consumer Phishing Hits Hard

These attacks are not just targeted at employees, as consumers have been hit just as hard. In fact, according to the FTC's recent Data Book, one in four people reported losing money to fraudulent scams, with a median loss of $500 per person – the primary vector of which being email. In these attacks, cybercriminals impersonate trusted brands in order to defraud their customers, as well as other consumers and businesses. The negative headlines and reputational damage from these incidents can make the organization's legitimate emails toxic to consumers who want to avoid falling victim to a scam, and the resulting impact on email-based revenue streams can be catastrophic.

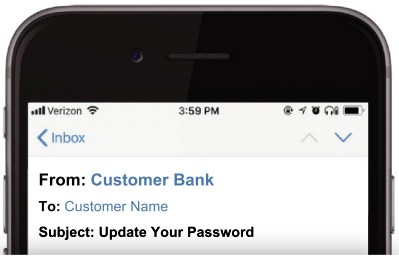


$4.45 Million 2023 Average Data Breach Cost

Source: Ponemon/Identity Theft Resource Center

Getting One Step Ahead

To counter these types of threats and those that come after them, the next generation of email security must take a fundamentally different approach to the secure email gateways and phishing defense solutions that are currently on the market. As cybercriminals move to outsmart current email security technology, organizations must move with them to a solution that uses identity markers to distinguish identity-based email attacks from legitimate email traffic and stop them before they reach the inbox.

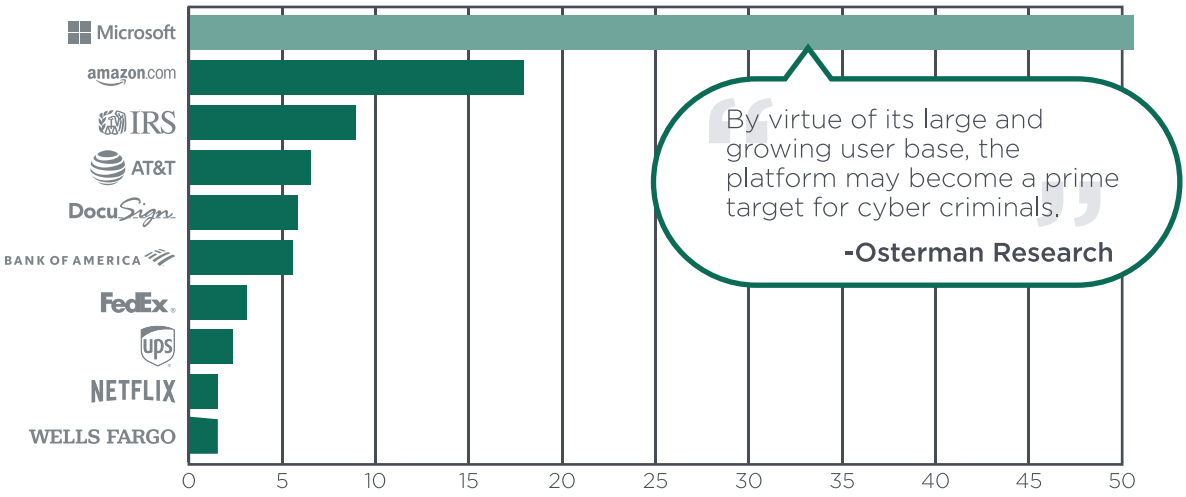


$52 Million 2022 Actual Losses due to Phishing

Source: FBI/IC3

Entering the Cloud

Microsoft is Still Most Impersonated Brand—And Biggest Target



Based on the millions of attacks stopped and analyzed by Fortra, Microsoft itself rises to the top when it comes to impersonation in identity deception-based email attacks. According to Infosecurity Magazine, Microsoft was impersonated in 38% of all brand phishing attacks in Q1 2024.

Whether it's a malicious email disguised as a Microsoft Office 365 password update, or an invitation to edit a OneDrive document linking to a spear phishing page, the Microsoft ecosystem can be a key enabler for attacks on any organization. And as more businesses transition to the cloud, it also makes for a target-rich environment.

Inherent Threats in Cloud-Based Email

Display name deception is exceptionally easy within cloud-based environments, and building target lists is simplified since organizations are all within a searchable directory. When criminals succeed at infiltrating an Microsoft 365-based email account, they gain a powerful launching pad for new attacks.

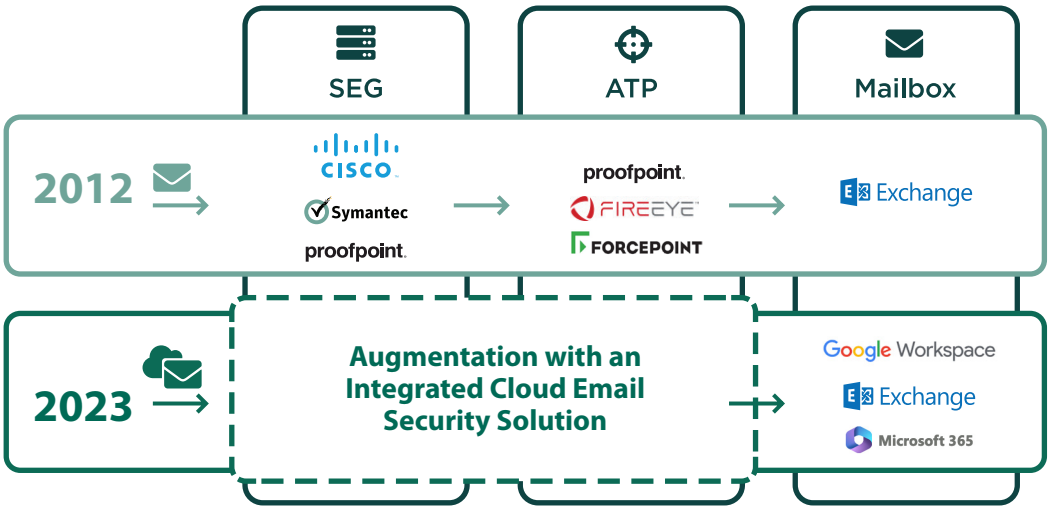
By leveraging a ubiquitous and trusted infrastructure, cyberthieves can continuously test attack methodologies until they're able to successfully circumvent security controls. And since users are frequently prompted to log in to connected services such as SharePoint, OneDrive and Azure, phishing attacks aimed at harvesting credentials to these services can go unnoticed.

Once access is gained to a compromised account owner's contacts and archived messages, hackers are free to launch executive impersonation scams, request fraudulent wire transfers, steal valuable IP, and redirect employee paychecks, amongst other crimes. By taking it one step further, fraudsters are also able to wage fresh identity deception-based email attacks on outside organizations, using legitimate accounts to target both internal and external victims.

For organizations that have made the transition to hosted email services, these factors should serve as ample warning about the rapidly evolving threats targeting their cloud-based email operations—as well as the need for a new paradigm for email security.

Built-In Security is Not Enough

Consolidating Legacy Controls is Just the Beginning



As organizations modernize their email infrastructures by transitioning to cloud email platforms, they shed layers of costly infrastructure from on-premises equipment, software, and maintenance resources.

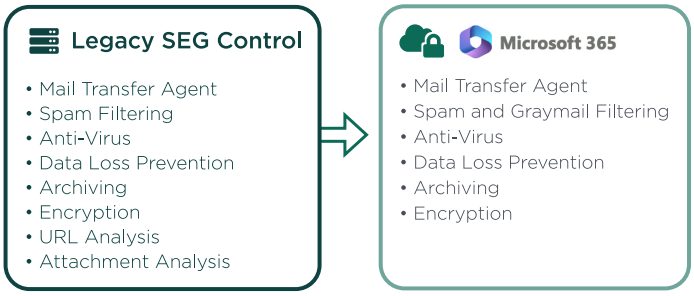
At this point, about 94% of global enterprises have moved their email in the cloud with services like Microsoft Office 365 and Google Workspace, where much of the core functionality of legacy SEGs and ATPs has been built directly into the platform.

Many capabilities of the traditional secure email gateway such as anti-spam, anti-virus, and malware protection are now being delivered in new cloud email platforms. This is a natural and expected evolution that is commonplace across all IT applications. It simply makes sense to develop new technologies in a better way than the preceding technologies, and in the case of email, this means integrating services into the base platform that in the past were bolted on.

Designed to assess incoming emails by analyzing content and infrastructure reputation, these platform-native controls are proving essential to ferreting out spam, malicious URLs and malware, certain keywords, or a high volume of attacks from a single IP.

The Capabilities Built into Cloud-Based Email

Today, nearly all the functionality of the legacy secure email gateway has been integrated as native capabilities of platforms, such as Microsoft Office 365, Google Workspace, and others. Microsoft's anti-malware and anti-spam features are often recognized by the marketplace as more impactful than the major SEGs, including:



Mail Transfer Agent: Message routing is core to email and as organizations leverage Microsoft 365 to manage all their mailboxes globally, they need the flexibility to define email delivery paths. Microsoft's integrated MTA allows each organization to set up complex mail flows to ensure email delivery complies with specific regulatory or business needs.

Anti-Virus, Spam, and Graymail Filtering: For years, Microsoft 365 trailed in anti-virus, spam, and graymail filtering efficacy. However, through on-going research and integration of several anti-virus and antispam engines focused on zero-day spam variants, URL analysis, bulk email categorization, and accelerated signature database updates, Microsoft has achieved parity to industry leaders.

Data Loss Prevention, Encryption, and Archiving: Microsoft recognized that in order to achieve full adoption of Microsoft 365 product tiers, organizations needed help meeting compliance requirements associated with their business. The DLP, encryption, and archiving integrations native to Office 365 enable organizations to limit the exchange of sensitive data, ensure that authorized data is sent securely, and preserve a record of all email sent and received for legal purposes. However, having a legacy SEG or just M365 still falls short of what Fortra's ICES platform – Cloud Email Protection – can do, as the below table depicts:

Functionality	M365 E3 Tier	Fortra SEG (Deep Content Inspection)	Fortra Cloud Email Protection (Data Science, Identity Threat Detection & Email Threat Ops)
Anti-virus	√	√	
Anti-spam	√	√	
Stop & block policy enforcement	√	√	
Stop & block DLP controls	√	√	
B2B/B2C encryption	√	√	
Sandboxing to protect from malware & APTs		√	
Active content sanitization to protect from malware & APTs		√	
Adaptive DLP to protect from data loss & compliance violations		√	
Data redaction of sensitive data *(e.g., IP, PII, PCI, etc.)*		√	
Automated document sanitization of metadata & version history		√	
Anti-steganography to sanitize images of hidden data		√	
Optical Character Recognition (OCR) to extend data protection		√	
Advanced BEC & brand impersonation protection		√	√
Advanced URL & Attachment analysis		√	√
Threat investigation			√
Automated incident response & remediation			√
Next-generation anti-phishing & spoofing			√
Security awareness training			√

While Microsoft 365 covers each of these elements of security, it is not prepared to stop the next generation of email threats. This is why a new security infrastructure should be included—one purpose-built to layer on top of M365 and other cloud-based email to prevent identity-based threats and other zero-day attacks.

Today, the increasing sophistication of these attacks is calling into question not only the efficacy of the on-premises SEG, but the return on investment thesis as well. Considering that the cloud email platforms already provide the basic email security features of the SEG, more organizations are finding that pairing M365 with new capabilities provides higher efficacy at lower cost.

Fortra's Cloud Email Protection is a next-generation approach to advanced email security, using real-time intelligence informed by trillions of emails flowing across the globe to continually detect incoming threats, as well as those that activate post-delivery. Cloud Email Protection differs in several remarkable ways from legacy security controls and adds to the built-in controls in cloud-based platforms to include a higher layer of protection.

Built on Data Science

The Science Behind the Scenes of Cloud Email Protection

Fortra's Cloud Email Protection combines a multitude of models that interpret, analyze, and assign individual scores to each message component. For example, the table below lists several of these models and the parts that they score:

It's important to understand how the models behind Cloud Email Protection data science work. Three machine learning paradigms are used to parse and analyze inbound email data:

Model Repository		
Parts	**Attack Type**	**Model**
Domain	Malicious domain	Domain Reputation
Sending Infrastructure	Sender impersonation	Authenticity
Full header from, subject line	Brand imposter	BDNI
Full header from, address groups	Individual imposter	IDNI
Subject line	Approach attempt, scam	Subject Line (types, suspiciousness)
URLs	Malicious URLs	URL Classifier
*All**	Webmail scams	Webmail Catcher
*All**	Multiple emails, one actor	Campaign Detection
*All**	-	Overall Risk Score
*All**	Services	Service Abuse Detector (SAD)
*All**	Spam	Spam Account Protector (SAP)

Figure 2: *All* above in the Parts column indicates that the scores are aggregated to determine attacks like Webmail scams, targeted email campaigns, and combine them to assign an overall risk score.

1) Feature-Engineered

In feature-engineered machine learning models, domain experts define the individual measurable properties (e.g., the features) of input data that are instrumental in making predictions or performing tasks. These models excel in scenarios, like email security, where domain expertise plays a vital role in understanding the problem. Also, expert-designed features provide greater interpretability, meaning it can be easier to analyze and improve the model's performance. With deep expertise in email trust as co-founders of the DMARC standard for email authentication back in 2012, Fortra's experts have applied their combined decades of knowledge and these tried and true models to create hundreds of features that are considered by the feature-engineered models within Cloud Email Protection.

2) Neural Networks

Neural networks are used to automatically learn complex patterns and features from data. This allows them to handle a greater diversity of data, which is useful in areas like email security where a broad range of file types, images, text, etc. are encountered. In some scenarios, they can capture subtle patterns and nuances in the data that would be missed by feature-engineered models.

3) Large Language Models

Large Language Models (LLMs) are designed to understand language in a human-like fashion. They are trained on massive amounts of text data to learn patterns, relationships, and contextual information in language, and then making judgments about them – this makes them ideal for natural language processing (NLP) tasks.

In practice, Fortra's Data Science team uses a pre-train and fine-tune paradigm, adapting pre-trained models to various downstream tasks, such as:

- Analyzing specific text-based email components, such as subject lines and body content
- Task-specific functions, such as determining message type or level of suspiciousness
- Identifying groupings or clusters in email data
- Creating data lakes with labeled data that can be used by other models
- Ingesting feeds of useful data–like lists of suspicious domains and IP address groups

A good illustration of Cloud Email Protection employing LLMs is the analysis of email subject line intent. Instead of parsing features when an email is received, the subject line is encoded and then analyzed to determine the type of subject line and determine its level of suspiciousness. The Subject Type model ascertains what the language resembles the most (e.g., an automated service notification, a marketing email, a scam, an approach attempt, etc.). Then, the Subject Suspiciousness model determines if the subject phrase is suspicious, unsuspicious, or perhaps just overly aggressive in its marketing message or jargon. The outputs of these two models are then analyzed by an ensemble model that considers both determinations to provide an overall measurement of the subject line's intent.

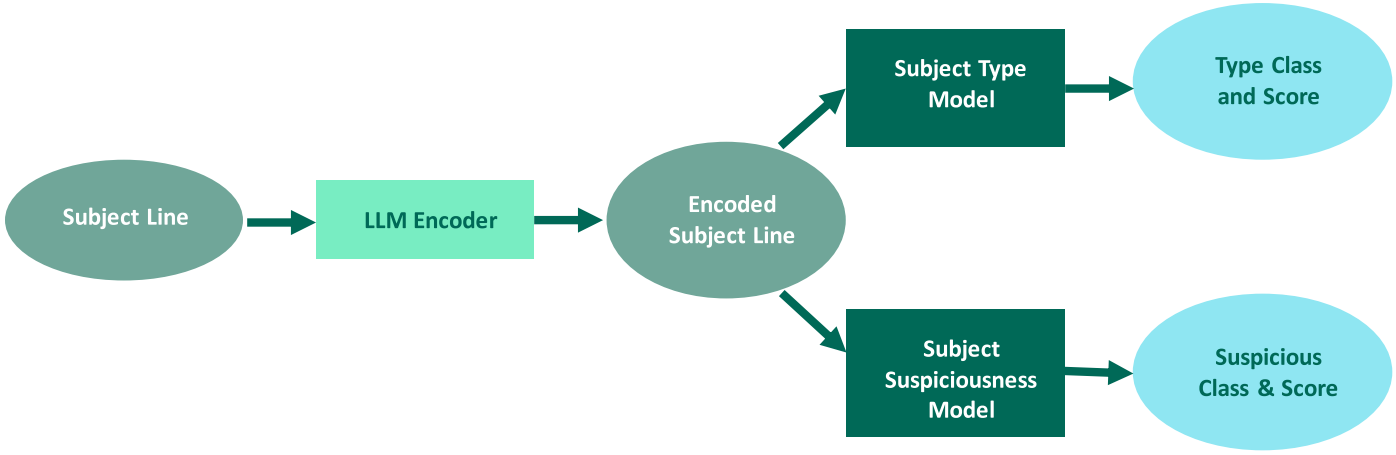


Figure 3: A visualization of the Subject Line attribute using LLM pre-training to assign a score based on its Type/Category & Suspiciousness levels.

Every machine learning paradigm has strengths and weaknesses. Also, the science of machine learning continues to advance and create opportunities to perform tasks more accurately and efficiently. For these reasons, it is critical to understand the task objective and select the ideal machine learning paradigm to perform the task well. This is especially true for applications of machine learning that can impact the operation of business processes, which could potentially bottleneck the flow of inbound and outbound communications.

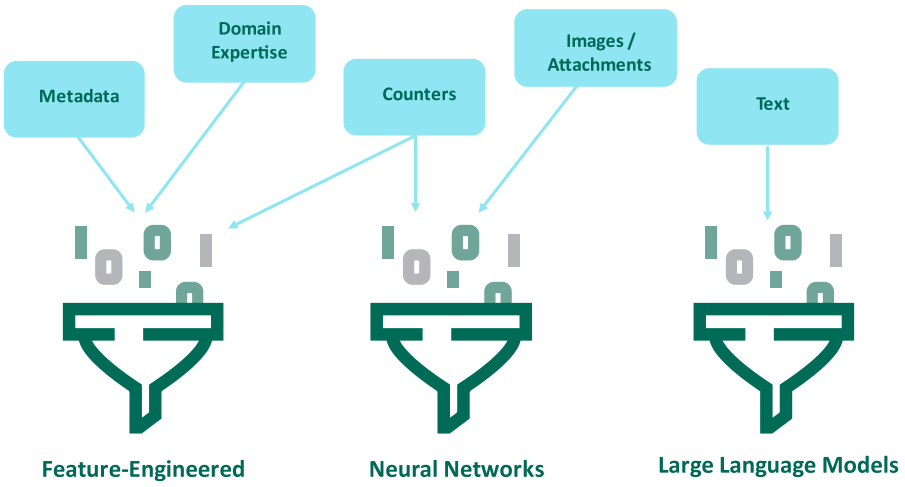
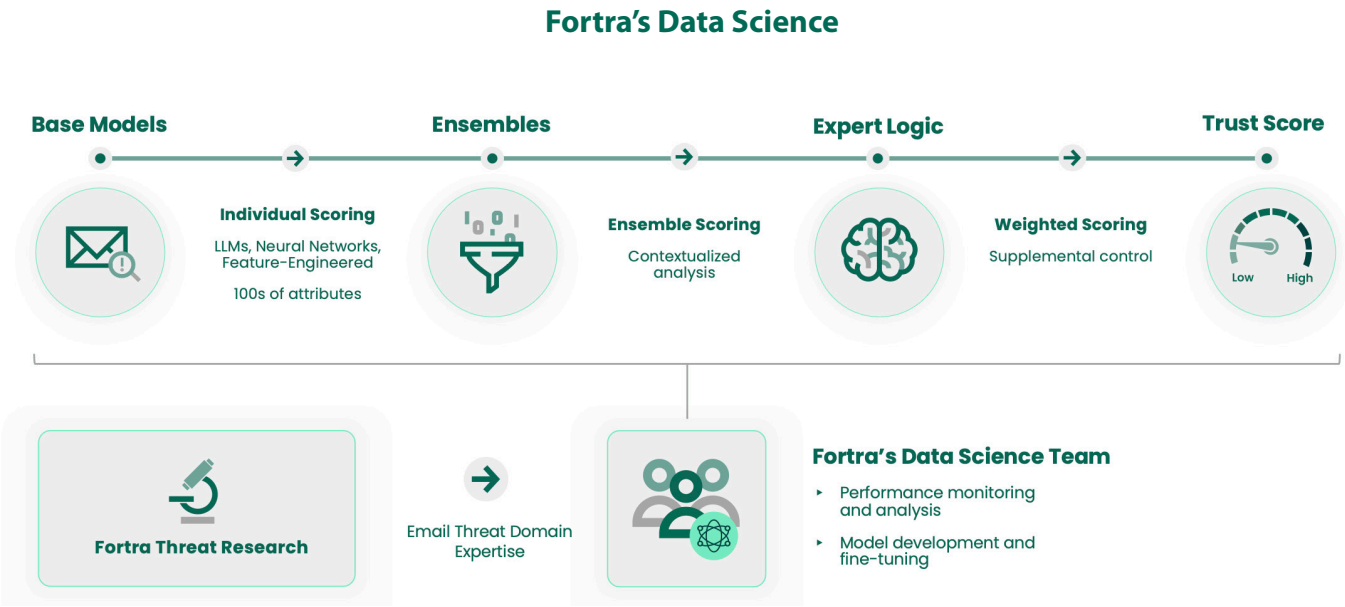


Figure 4: Each ML paradigm has strengths and weaknesses. It is important to utilize the ML paradigm that is best suited for the task.

Does Logic Come into Play?

AI and ML technologies, including those used in Cloud Email Protection, are a major leap forward. They provide unique insights into data and are a powerful way to find threats that would otherwise go undetected. That said, no artificial intelligence technology gets it right 100% of the time. Even the most sophisticated AI technologies require logic that supplements and provides boundaries. This is especially true for applications in business-critical production systems like email.

This is where expert logic from Fortra's Data Science team comes into play. Our data scientists have a deep understanding of how Fortra's models operate individually, and as parts of the whole. They also constantly monitor and evaluate performance. This team develops and maintains a control layer of expert logic that supplements Fortra's machine learning models while ensuring optimum performance.

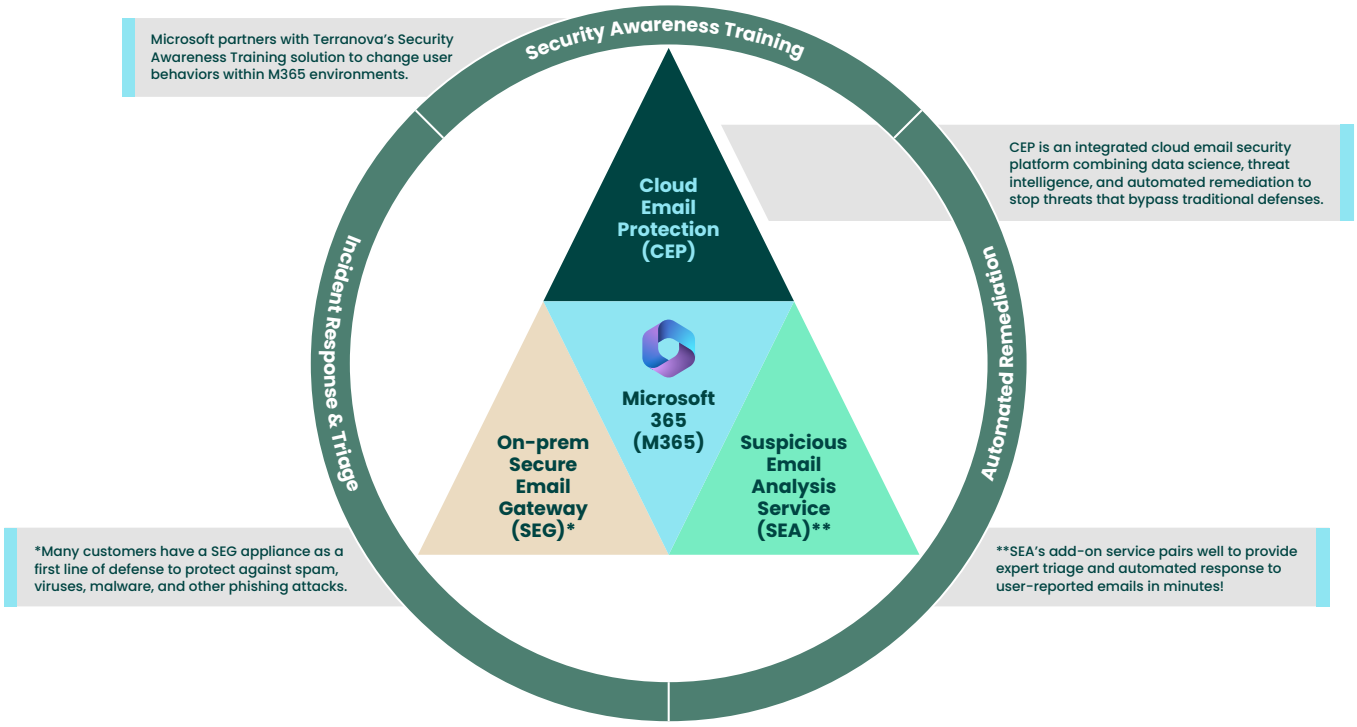


Prevent Zero-Day Attacks Every Day

It is this combination of a human-labeled big data, semi-automated learning algorithms, and real-time cloud-based delivery that makes the data science behind Cloud Email Protection smarter and more reliable with each email analyzed. This dynamic approach to email security outsmarts fraudsters even as they change behavior—moving from domain to domain, jettisoning blocked accounts, reformulating email messages, switching out display name strategies, recompiling malware, and more.

It is also an approach that can't readily be faked or spoofed because a fraudster typically doesn't have a trusted pattern of communications with those they are intent on attacking. Even in scenarios where accounts have been compromised, behavioral anomalies can be detected. And once organizations adopt the Agari solution, there are simply easier targets in organizations that use less-effective alternatives. By leveraging data science and AI to block malicious messages and become a hardened target, attackers tend to turn their attention toward easier prey.

Better Together: Microsoft 365 + Fortra Email Security



With the legacy secure email gateway capabilities now present in Microsoft Office 365 and other cloud-based platforms, as well as the new security features available with the Fortra Email Security solution suite, this combination is all organizations need to ensure that employees and consumers alike can open, click, and trust everything in their inbox.

Fortra's Cloud Email Gateway includes all the capabilities needed for any modern organization to fight cybercrime, including email authentication to prevent spoofing, context inspection to stop zero-day attacks, URL and attachment analysis to stop known attacks, and automated post-delivery remediation to quickly remove malicious emails that get through initial controls.

After all, email and the threats against it are changing fast. Fortra is here to ensure that email security does the same.

Fortra Email Security's Full Suite of Solutions

As the Head of Email Security from one of our manufacturing customers stated in relation to Microsoft 365's limitations, "Don't rely on M365 alone. Explore building a multi-layered approach to strengthen your security posture and reduce the volume of phishing attacks. Most attacks start with an employee, and then a chain reaction occurs. If a malicious email never gets delivered, there is little threat to the business. Fortra stops threats before they can ever get to our employees.

To understand more about how Fortra Email Security products protect against threats from staging and pre-delivery that target employees, partners, and customers and helps remediate those that bypass all defenses or activate post-delivery, let's explore the entire suite of solutions:

- **Cloud Email Protection:** Using Advanced Data Science, Global Inbox Threat Intelligence, Email Threat Operations and more, this new integrated cloud email security (ICES) platform protects against advanced email threats that bypass traditional security controls through a combination of data science to identify unknown threats, global inbox intelligence to counter emerging threats, and automated remediation that purges detected threats across the email environment.

- **Agari DMARC Protection:** By automating the process involved with deploying and managing the implementation of Domain-based Messaging, Authentication, Reporting, and Compliance (DMARC) protocols, Agari DMARC Protection makes it easy to prevent cybercriminals from impersonating an organization in phishing attacks targeting its customers, as well as other consumers and businesses.

- **Suspicious Email Analysis:** Expert triage and automated response to user-reported emails, ensuring real threats are quickly identified and mitigated.

- **Secure Email Gateway:** Full-featured gateway that delivers spam protection, anti-phishing, sandboxing, DLP, and other capabilities in an on-prem or virtual appliance.

- **Security Awareness Training:** Transforms end users into a powerful layer of security via engaging training courses, realistic simulations, and gamified learning.

- **Threat Intelligence Service:** Disrupts threat actors, prevents fraud, and enriches security controls by delivering critical insight before attackers strike.

Discover How Fortra Can Improve Your Current Email Security Infrastructure

As your last line of defense against advanced email attacks, Fortra stops attacks that bypass other technologies—protecting employees and customers, while also enabling phishing response teams to quickly analyze and respond to targeted attacks. Book a demo today to discover how much money you can save by adding Fortra to your email security environment. https://emailsecurity.fortra.com/demo

Calculate the ROI of Implementing Fortra

Discover how much money you can save by adding Fortra's Cloud Email Protection to your email security environment with our custom ROI analyzer. https://emailsecurity.fortra.com/resources/roi-calculator/cloud-email-protection

FORTRA

Fortra.com

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.