ESG SHOWCASE

# Beyond the Perimeter

## The Need for Pervasive Email Security

**Date:** February 2020 **Author:** Dave Gruber, Senior ESG Analyst

**ABSTRACT:** As the number one threat vector for most organizations, email continues to be widely used by cyber criminals to penetrate organizations in support of a wide variety of cyberattacks. Unlike other attack vectors, email enables cybercriminals to directly leverage humans in an effort to bypass security controls and facilitate attacks. Recent business email compromise and other sophisticated phishing-related attacks all too often elude traditional email security controls, contributing billions of dollars to the pockets of criminals.

Many organizations are coming up short when protecting against modern email threats. A more comprehensive email security solution is needed—one that protects at the perimeter, inside the network and the organization, and beyond the perimeter. Mimecast's Email Security 3.0 strategy can help.

### Overview

Today's business users face an unprecedented number of daily emails, from a wide variety of senders, including coworkers, customers, prospects, suppliers, business service providers, and both internal and external cloud-delivered applications distributing machine-generated emails. While email plays a critical role in modern business communications and operations, it also provides attackers with a nearly open door to individuals who can help them bypass security controls and successfully carry out a large variety of attacks.

Email provides criminals with a flexible and ubiquitous attack vehicle, enabling a single email to deliver socially engineered content in conjunction with malicious links and attachments directly to unsuspecting and busy employees at any level within an organization. Supporting this unique threat vector, an entire attack tools and services industry used by non-technical cybercriminals has emerged.

While email security controls are among the oldest in the security stack, email threats have risen to new levels, requiring security teams to take another look at the effectiveness of existing email security controls against the growing email threat landscape.

**In the process of migrating from on-premises to cloud-delivered email, many security teams have let their guard down, making the false assumption that cloud-based email service providers can natively deliver the same robust security controls as specialized, third-party email security solutions.**

Further complicating email security, the recent move to cloud-delivered email systems (such as Office 365) has generated new opportunities for attackers to fool unsuspecting users by impersonating these and other trusted providers. In the process of migrating from on-premises to cloud-delivered email, many security teams have let their guard down, making

the false assumption that cloud-based email service providers can natively deliver the same robust security controls as specialized, third-party email security solutions.

A new, more comprehensive approach to email security is needed to address the move to the cloud and the growing email threat landscape.

## The Modern Email Security Threat Landscape

Today's email threat landscape continues to evolve as criminals test the limits of how far they can push employees to act on their behalf. Unlike so many other digital security controls, email centers around the human element, enabling attackers to gain access to and leverage unsuspecting end-users to assist with their attacks. While older attack techniques persist, newer, more creative techniques are exceeding the capabilities of traditional security controls, creating new challenges for security teams and end-users.

Further intensifying the situation, the ecosystem surrounding email attacks has enabled non-technical criminals to easily acquire and use attack software that enables virtually ANYONE to become a cybercriminal by virtue of easily packaged, simple-to-use, fully documented attack kits. This dynamic has quickly caused email to become the number one attack vector for most organizations.

### Sender and Organization Impersonations

Some defensive approaches depend heavily on the end-user's ability to discern bad from good. However, end-users are faced with new levels of complexity, receiving email communications from people they know and trust, from business services that they may not know, and from applications that provide machine-generated business information that's critical to their jobs. This varied, complex set of email senders means that email users are constantly challenged to verify whether emails are sent from trusted organizations and trusted people.

With a nearly open door for imposters to join this list, users are challenged with verifying the validity of each sender and whether to trust their communications. As attackers continue to impersonate trusted entities, end-users need to be on constant alert to recognize phishing and other malicious email communications without interrupting their busy workdays. This is essentially an impossible task.

### Business Email Compromise

Modern email attacks are often targeted and highly socially engineered, involving multiple people over long periods of time. Most involve some type of impersonation techniques—spoofing of branding, email senders, and web pages—in an effort to establish context and build trust while leading to criminal activity.

**Criminals often use simple social engineering techniques together with public databases to determine the names of targeted individuals in specific company roles.**

In preparation for business email compromise (BEC) and other phishing attacks, criminals often use simple social engineering techniques together with public databases to determine the names of targeted individuals in specific company roles. Executive names, contact information, and other business and personal information can be easily harvested by criminals and later used to target others with fake requests to carry out malicious or criminal actions, such as the transfer of funds or the planting of ransomware.

## Website and Email Domain Spoofing

Pixel-perfect, scraped, and otherwise impersonated websites and spoofed domains operating under attacker control are often used to further fool unsuspecting users into giving up login credentials and other sensitive information. With two-thirds of companies using cloud-delivered email services,[1] criminals often use widely available cybercrime toolkits to recreate impersonated Office 365, G Suite, banking, government, and many other types of login and password reset pages, combining them with phishing emails as the lure. The base internet has no built-in control mechanisms or centralized "police force" to prevent this type of fraudulent impersonation.

Stolen login credentials are used for a variety of purposes, including compromising email accounts such that criminals can listen in on internal and supply chain email communications. Criminals know that when they effectively impersonate supply chain contacts by inserting themselves into operational communications, they can successfully harvest confidential information, leading to wire transfer fraud, payroll fraud, vendor and supply chain fraud, and other BEC attacks.

**Criminals know that when they effectively impersonate supply chain contacts by inserting themselves into operational communications, they can successfully harvest confidential information, leading to wire transfer fraud, payroll fraud, vendor and supply chain fraud, and other BEC attacks.**

## Sensitive Data Loss

Unintentional loss of sensitive data through misaddressed emails or incorrect document attachments is both a policy and automated controls issue. 39% of organizations report having no policy or controls in place for sharing sensitive data via email,[2] leaving it up to employees to decide what can be shared. Further, most company-sensitive data is stored in long-term email mailboxes and archives where it is at risk of theft when email account compromise occurs.

Insider threats have been steadily increasing over the past three years, with employee or contractor negligence leading the way. 60% of companies have experienced an average of more than 20 incidents per year.[3] Most use email as the transport mechanism to exfiltrate data.

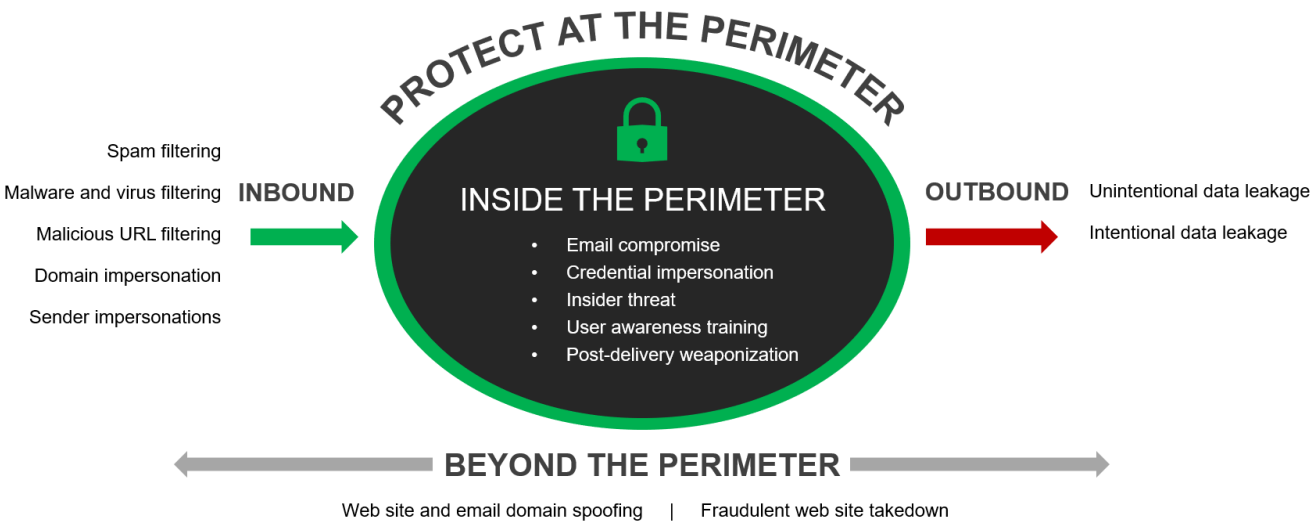
## Security Awareness

With email providing a direct communication link from bad actors to company employees, attackers will continue to use innovative new ways to deceive trusted employees into helping them criminally gain access to information and assets. While 60% of workers report that their companies offer cybersecurity training, one in five say they have personally experienced a cyber attack, with phishing reported as the most common.[4] While security is everyone's responsibility, few employees outside of IT and security teams are highly motivated to keep up on the latest threats.

[1] Source: ESG Master Survey Results, *Application and Email Security Trends*, September 2019.
[2] ibid.
[3] Source: Ponemon Institute, *Cost of Insider Threats Global Report*, 2020.
[4] Source: ESG Master Survey Results, *2019 Digital Work Trends Survey*, November 2019.

## What's Needed: A Pervasive Approach to Email Security

**Figure 1. Securing Email at the Email Perimeter, Inside the Network and Organization, and Beyond**




*Source: Enterprise Strategy Group*

### Security at the Email Perimeter

With the continued use of email as the number one transport mechanism for malware and other attacks, securing the inbound and outbound traffic at the email perimeter is highly relevant and important. Perimeter-based spam, virus, and phishing filtering also plays an important role in cutting down unwanted or inappropriate mass email marketing content. But these controls aren't enough.

With website and domain spoofing at an all-time high, perimeter-based inspection of URLs and web traffic is required to eliminate risks associated with phishing and other impersonation emails that trick users into visiting fake or malicious websites where login credentials and other sensitive data are stolen.

Unintentional data leakage also happens daily in most organizations, requiring automated, content-sensitive perimeter resident controls that can protect users from mistakenly sending sensitive data or attachments that contain sensitive or unencrypted data.

### Securing Inside the Network and the Organization

Email security is no longer just about filtering at the perimeter for spam, impersonations, malicious links, and malware. Email security controls must also operate inside the perimeter to detect inconsistent and abnormal behaviors, flushing out bad actors and insider threats, and providing tools to automatically remove malicious or unwanted emails from the inside.

With bad actors regularly using stolen credentials, they end up inside email environments—particularly as those email systems themselves have moved to the cloud—listening in on proprietary communications and impersonating trusted individuals using internal email addresses. Executive impersonation can convince even the most honest, trusted employee to carry out malicious activities, including the fraudulent transfer of funds and other digital assets. Internally focused security controls are needed to detect malicious email usage, flushing out these impersonations and stopping the spread of attacks internally.

Malicious and careless insider threats also continue to grow, requiring specialized, intelligent controls to distinguish when known users attempt to carry out malicious activities.

### User Training and Security Awareness to Strengthen the Human Firewall

With adversaries focusing on penetrating the human perimeter, ensuring that users are trained and up to date on the latest attack techniques—both email-centric and otherwise—becomes critically important as a human layer of defense. Businesses need automated training, awareness, and assessment tools to help email users stay current and keep organizations in compliance with policies and regulations.

**Internally focused security controls are needed to detect malicious email usage, flushing out these impersonations and stopping the spread of attacks internally.**

Attack testing and simulation tools are also needed to help verify users are informed and to identify when additional user training is needed, especially in the area of harder-to-detect attacks like spear-phishing.

### Securing Beyond the Perimeter

With fraudulent websites and email domains so heavily used to support phishing and other web-based attacks, securing beyond the organizational perimeter can help shut down the opportunity for attackers to fool users—in many cases before they have even launched the attack. Organizations need a mechanism to search the internet for fraudulent websites and web domains that are impersonating their brands. They need a means to report and initiate takedown requests, eliminating the opportunity for users to unknowingly give up credentials and other sensitive data.

**With fraudulent websites and email domains so heavily used to support phishing and other web-based attacks, securing beyond the organizational perimeter can help shut down the opportunity for attackers to fool users—in many cases before they have even launched the attack.**

In addition, as new attacks emerge, monitoring and enforcing how email sending domains are used will play an important role in keeping organizations secure. With so many services legitimately sending emails using their customer domains—Salesforce.com, Survey Monkey, Marketo—it isn't surprising that illegitimate players are jumping in to do the same.

## Introducing Mimecast's Email Security 3.0 Strategy

Mimecast's Email Security 3.0 strategy is supported by a comprehensive cloud-based platform that offers pervasive, multi-zoned protection and integrates with an organization's overall security technologies, making them smarter. The strategy provides specific security controls at the email perimeter, inside the network and the organization, and beyond the perimeter.

### Delivering Security at the Email Perimeter

Protecting inbound email, the Mimecast cloud-based gateway filters out spam, malware, malicious URLs, and domain and other impersonations. For outbound email, Mimecast's services stop unintentional and intentional data leakage and prevent bad actors from exfiltrating data and launching outbound attacks post-credential-theft.

### Delivering Security Inside the Network and the Organization

Mimecast monitors internal email traffic to identify and remove internal phishing and insider threats. The service also monitors and remediate attacks and other unwanted emails post-delivery, eliminating threats in data at rest in mailboxes and the email archive.

With email archives hosting much of a business' critical IP and digital assets, protecting the data there is critical.

In addition, to improve the organization's human firewall, Mimecast's integrated online security awareness training educates end-users about threats and how to identify and not fall for them. Simulated attack tools and other assessments and monitoring enable security teams to identify weaknesses and assess where additional training is needed.

### Beyond the Perimeter

Looking outside the organization, Mimecast continuously finds and shuts down fraudulent websites and helps stop direct email domain spoofing used in phishing and other impersonation attacks. Through the use of the DMARC DNS Authentication standard, the Mimecast service can stop attackers from abusing an organization's email domain as part of an email-based campaign. Similarly, by monitoring the use of an organization's web domains and pages on the web, as well as domains and pages that are similar, Mimecast can block and take down these fraudulent websites in many cases even before the attacker has launched an attack that leverages them.

### Integrating the Security Stack

Prebuilt integrations and extensive open APIs enable full security stack integration, including with SIEMs, SOARs, endpoints, firewalls, and other third-party security controls and services. Given the central nature of phishing and other email-borne threats, the Mimecast service can serve as an early-warning system and feed critical intelligence to other parts of an organization's security infrastructure and improve overall situational awareness. And conversely, detections and new information can be fed directly into the Mimecast service to maximize the protections it provides.

## The Bigger Truth

Email threats have become prolific, sophisticated, targeted, and unpredictable. Adversaries are leveraging email as a direct means to break into and spread around organizations by leveraging a common weak link, the human. End-users are often overwhelmed with the amount of and variation in senders associated with daily email communications. A heavily user-dependent approach to email security, as well as one using outdated security technologies, is no longer enough.

Modern email solutions need to provide a more pervasive approach to security, protecting at the email perimeter, inside the network and the organization, and beyond the perimeter. These controls need to be backed by the latest threat intelligence and integrated with other key security controls

Security vendors like Mimecast are delivering innovative, comprehensive solutions that can provide this level of pervasive email security, protecting organizations from the rapidly expanding email threat landscape.



**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188