ESG SHOWCASE

Consolidating Email Security

Email Security Is Drowning Security Teams

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

ABSTRACT: Email security is in a state of transformation. As email attacks have become more sophisticated and targeted, organizations have continued to layer multiple security controls to a point where security teams are drowning in complexity. Email has become a preferred path for adversaries to circumvent other technical security controls, heightening the importance of email security as a top-5 priority in most organizations.[1]

This growing complexity is dragging down security and IT teams, particularly those with only a handful of security professionals, as they focus on managing tools instead of on core risk reduction objectives. Emerging consolidated and integrated security platforms are helping these organizations reduce complexity while stopping the modern adversary. Mimecast's Email Security platform is one such solution that is helping organizations achieve new levels of both efficacy and efficiency.

Overview

Email security is no longer limited to an edge-oriented control. While secure email gateways (SEGs) continue to play an important role in the email security stack, new attack strategies have caused organizations to implement additional layered controls beyond just stopping inbound spam and phishing. These additional controls add protection against insider threats, domain spoofing, business email compromise, malicious web traffic, website cloning, and other emerging email-related attack strategies. Further investments in security awareness training help email users participate in attack prevention through education and awareness of common and emerging threats.

The growth of these traditionally independent controls has resulted in huge cost and complexity challenges, in addition to the creation of silos of security data that require post-processing to support security operations. This pattern is consistent with the increasing complexity of the overall security stack, driving organizations to demand convergence and consolidation wherever possible. According to ESG research, these factors, together with the continuing security skills gap, are motivating 64% of organizations to increase their spending on integrated email and broader security solutions.

> **Reducing Cost and Complexity**
>
> Only a small number of vendors can offer integrated, holistic security platforms capable of protecting against the rapidly expanding email threat landscape while reducing cost and complexity.

A new approach that consolidates and simplifies email and associated web security controls while increasing protection against the modern adversary is needed. No longer will single specialized security control silos provide protections from cybercriminals who simultaneously leverage channels such as email and the web in campaigns. While the email security vendor landscape is extensive, only a small number of vendors can offer integrated, holistic security platforms capable of protecting against the rapidly expanding email threat landscape, while at the same time reducing cost and complexity.

[1] Source: ESG Master Survey Results, *Trends in Email Security*, June 2020. All ESG research references in this white paper have been taken from this master survey results set.

The Transformation of Email Security

57% of organizations believe that email security is going through a significant state of transformation and will reevaluate all available email security controls in the next year. This dramatic statistic is driven by three key factors:

1. The move to cloud-delivered email – 90% of organizations are currently using a cloud-delivered email platform in some capacity, with 84% utilizing Microsoft Office 365.
2. The growing email threat landscape – The email threat landscape has accelerated to unprecedented levels and variety, leading to the need for additional security controls capable of keeping up with emerging threats.
3. Gaps in native security controls – 71% report gaps in native cloud-delivered security controls, and therefore use additional third-party controls to close the gaps.

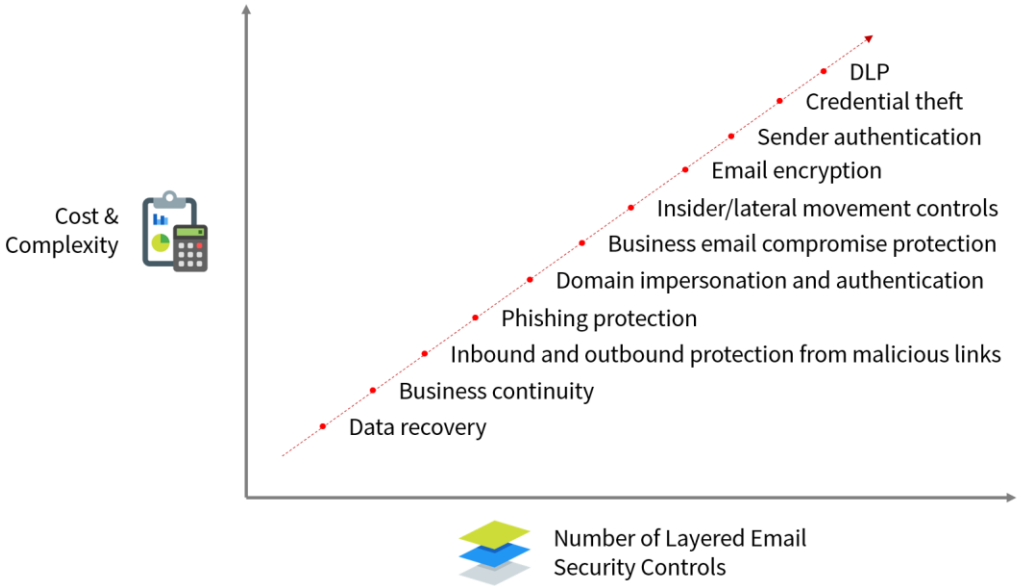
Additional Third-Party Controls Still Needed

While many previously believed that native security controls included in cloud-delivered email solutions would secure their organizations, 50% later realized the need to supplement with additional, third-party controls to close gaps.

As organizations migrate email to the cloud to drive down cost and complexity while shifting CapEx to OpEx, adversaries are doubling down on how they leverage email to compromise them. While many previously believed that native security controls included in cloud-delivered email solutions would secure their organizations, 50% later realized the need to supplement with additional, third-party controls to close gaps.

While in the past, most previously depended on a secure email gateway (SEG) as the foundation of their email security strategy, the use of multiple, layered email security controls has now become a best practice. Yet as multiple third-party controls are added (for email encryption, DLP, phishing, business email compromise, domain impersonation and authentication, inbound and outbound protection from malicious links, credential theft, insider/lateral movement controls, sender authentication, data recovery, and business continuity), cost and complexity rise.

Figure 1. Cost and Complexity Are on the Rise



Source: Enterprise Strategy Group

As security teams come to better understand the strengths and weaknesses of native email security controls included with cloud-delivered email solutions, most are reevaluating current strategies, controls, and tools. With email security considered a top-5 priority for 69% of organizations and with 64% planning on additional investments in net-new security controls, significant change is underway.

The Move to Integrated Email Security Platforms

Security architects now have the option of using more comprehensive email security platforms to protect from the email threat vector. While assembling a "custom" email security stack from multiple vendors will likely always be an option, it more often will result in an overly complex environment, requiring continuous integration and management investments. As platform vendors emerge, organizations can leave that effort to the vendor, turning their attention instead to managing the organization's security strategy and risk management program.

What's Needed

Integrated, adaptive controls – Modern email security platforms must combine and integrate a broad array of email security controls, combining pre-delivery filtering, east/west, post-delivery controls and remediation, and domain spoofing support together with web security and filtering controls, to protect against the rapidly expanding and varied email threat landscape.

Turnkey solutions – Deployment must support hybrid (cloud and on-premises) email management with ease while automatically aligning policies across systems.

Threat intelligence – Threat intelligence must underly the platform, supporting all aspects of automated protection and remediation as well as broader security ecosystem integration.

Integration and extensibility – Open APIs and off-the-shelf integrations enable full security stack integration, including with SIEMs, SOARs, endpoints, firewalls, and other third-party security controls and services.

Integrated security services – Adversaries leverage phishing and fake, copycat websites that mimic trusted brands to steal credentials and commit other forms of fraud. Extending core email security capabilities to add integrated brand exploit protection services that can monitor for similar domains and fake sites, shutting them down to stop malicious use of respected brands.

Unified email and web security – With so many email attacks, such as phishing-based credential harvesting, leveraging spoofed web properties as an integral part of the campaign, web security must be tightly integrated with email security controls.

Platform Benefits

When email security is delivered as a fully integrated platform, organizations achieve threat detection and prevention, leading to better security posture, simplified deployment and management, better governance, and significant cost savings. IT and security teams spend less time managing tools and more time focusing on core objectives, including performance, resilience, and risk reduction.

Introducing Mimecast's Email Security Platform

Mimecast's Email Security is supported by a comprehensive cloud-based platform that offers multi-zoned protection and integrates with an organization's larger security stack. It provides specific security controls at the email perimeter, inside the network and the organization, and beyond the organization's 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 or 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 remediates attacks and other unwanted emails post-delivery, eliminating threats in data at rest in mailboxes in email archives, and even in files on employees' desktops.

A Comprehensive, Cloud-based Platform

"Mimecast has provided essential solutions that have met our business needs and requirements in legal and compliance, archive, message hygiene, message tracking, URL threat protection, DLP, reporting, alerting, disaster recovery, and many other features all within a single manageable dashboard."

- Doug Blankenship, Enterprise Architect, H Lee Moffitt Cancer Center and Research Institute

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

Beyond the Perimeter

Looking outside the organization, Mimecast continuously finds and shuts down fraudulent websites and helps stop unauthorized direct email domain spoofing used in phishing and other impersonation attacks. Using the DMARC DNS Authentication standard, the Mimecast service can stop attackers from abusing an organization's email domains 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 discover, block, and take down fraudulent websites, in many cases, before the attacker has launched an attack that leverages them.

Integrating the Security Stack

While integrating the email security stack itself improves the efficacy and efficiency associated with the email threat vector, integrating email security with the broader security stack strengthens the overall security posture. Prebuilt integrations and 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, feed critical intelligence to other parts of an organization's security infrastructure, and improve overall situational awareness.

The Bigger Truth

Email security is in a state of transformation. Cloud-delivered email, largely via Microsoft 365, together with a far more sophisticated and focused adversary has exposed too many organizations to successful phishing attacks. Adding more, narrowly specialized tools isn't helping; complexity is drowning security teams.

Consolidation of security tools is not a new idea. While best-of-breed strategies were once preferred, platform vendors – particularly those that are cloud-based - have come a long way in increasing overall efficacy while also helping organizations achieve new levels of efficiency with their tightly constrained staffs.

Security teams are demanding consolidation, but without losing efficacy. And the move to the cloud is the time to do it.

With users continuing to depend on email, and by extension the web, as a primary means of communication from a diverse set of devices, security teams must respond with security controls that can protect these devices and users against a complex and sophisticated threat landscape. Security teams are demanding consolidation, but without losing efficacy. And the move to the cloud is the time to do it.

With emerging integrated email and web security platforms now available, organizations should be directing their attention to consolidating their email security systems by adopting these platforms as broadly as possible. When email security is delivered as a fully integrated platform, organizations achieve threat detection and prevention, leading to better security posture, simplified deployment and management, better governance, and significant cost savings. With this transformation, IT and security teams can spend less time managing tools and more time focusing on core objectives, including performance, resilience, and risk reduction.

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