ESG SHOWCASE

Email Security in a State of Transformation

Big Changes Happening in Email Security

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

ABSTRACT: A lot has changed about email security in the past two years. The threat landscape has evolved dramatically, email services have moved to the cloud, and socially engineered attacks have become commonplace. As organizations continue to migrate on-premises email solutions to the cloud using platforms like Microsoft Office 365 and G Suite, email security requirements are changing too. With many assuming the native security controls included with cloud-delivered email will be adequate, most are realizing that additional, third-party email security controls are necessary to secure critical business communications and the data stored within an organization's email infrastructure. This paper explores the changing threat landscape, the move to cloud-delivered email and the email security controls needed to protect the modern email infrastructure.

Overview

Email continues to be the pervasive means of digital business communications. The use of mobile email access has further enabled workers to engage in business activities throughout their lives, including 41% of workers who reported answering emails during a child's event and 63% who reported reading email while in the car.[1]

With 90% of organizations now operating email from cloud-delivered providers, including Microsoft Office 365 and Google G Suite,[2] new types of email security threats have emerged. Email attacks are no longer limited to mass-emails preying on only the most vulnerable users.

Email is an open door into our organizations and the people who work within them. As an open means of communication, attackers regularly leverage email and phishing tactics as a path to reach unsuspecting users who can help them gain access to sensitive information and carry out malicious activities. Email is regularly used as an entry point to carry out more complex attacks that leverage other threat vectors, escalating the importance of combining email security controls with endpoint, network, and cloud security that enable security teams to see and understand these complex attacks.

With 71% of organizations reporting issues relating to either inbound attacks, sensitive data loss, gaps in backup and recovery, gaps in availability, or compliance issues,[3] many lack the security that they once had with their on-prem email solutions. Further, as a cost control, 42% of organizations have opted out of more advanced native security controls, utilizing only the limited security controls available in the Office 365, E3 license.[4]

[1] Source: ESG Research Report, *2019 ESG Digital Work Survey*, December 2019.
[2] Source: ESG Research, *Trends in Email Security: Security Controls and the Move to Cloud-delivered Email*, February 2020.
[3] Ibid.
[4] Ibid.

To combat these issues, organizations are realizing that additional third-party controls are necessary to protect against today's sophisticated attacks, including business email compromise, spoofing, and other phishing-based attacks.

Challenge: Highly Targeted Phishing and Impersonation/Spoofing Attacks

Modern email attacks are often targeted and highly socially engineered, involving multiple targets over long periods of time. Most involve some type of impersonation or spoofing techniques used to trick users into unknowingly engaging with criminals to facilitate criminal activity.

Bad actors use social engineering techniques to determine the targeted names of people in specific roles and how to best communicate directly with them using simple inbound email.

Phishing is the most common type of email threat,[5] and it's often used to steal credentials and other sensitive data. In preparation for phishing attacks, bad actors use social engineering techniques to determine the targeted names of people in specific roles and how to best communicate directly with them using simple inbound email.

Executive names and contact information can be easily harvested by criminals. Using this information, criminals impersonate superiors, instructing unsuspecting trusted employees to carry out malicious or criminal actions such as the transfer of funds.

Challenge: Credential Theft/Business Email Compromise

Impersonation techniques are often used to trick users into sharing credentials and other sensitive data with criminals. Using impersonated websites and spoofed domains, attacks fool users into believing that they are interacting with known, reputable websites requesting username and password authentication. The use of simple, single password authentication leaves an opportunity for stolen credentials to become an open door for criminals.

Once criminals acquire credentials and other sensitive data, they gain access to email accounts where they can tap into internal conversations for additional context, enabling them to more accurately impersonate key employees and supply chain contacts. These techniques enable business email compromise attacks, including wire transfer fraud, payroll fraud, payment fraud, and supply-chain fraud.

Challenge: Sensitive Data Loss

Organizations lose sensitive data daily when email users misaddress emails or mistakenly include the wrong documents as email attachments. With 39% of organizations having no policy or controls in place for sharing sensitive data via email,[6] intellectual property and sensitive customer data is at risk.

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.[7]

With 39% of organizations having no policy or controls in place for sharing sensitive data via email, intellectual property and sensitive customer data is at risk.

[5] Source: ESG Master Survey Results, *Application and Email Security Trends,* September 2019.
[6] Ibid.
[7] Source: Ponemon Institute, *Cost of Insider Threats Global Report*, 2020.

Further, most company-sensitive data is stored in long-term email mailboxes and archives, where it is at risk of theft when email compromise occurs.

Challenge: Siloed Security Data

With 60% of organizations reporting the use of at least 25 security tools[8] for email, endpoint, network, and cloud security, security analysts struggle to assemble data to gain a clear understanding of attacks.

Email attacks are all too often the entry point for more complex attacks, involving lateral movement into core business applications. Email security tools alone lose visibility into these complex attacks, requiring analysts to piece together information from other security controls to understand an attack.

Integrating and aggregating security data from multiple security controls is challenging and often not possible due to misaligned data definitions and schemas. In addition, this approach requires significant time and resources to accommodate, which many SecOps teams can't afford. Out-of-the-box integrations are often limited, and most require customization and analyst intervention to carry out remediations.

What's Needed

A broad set of email security capabilities are required to secure against the modern email threat landscape. These capabilities must be tightly integrated and share common policies and management to ensure efficient, effective controls.

- A layered, integrated approach – Modern email security requires a layered, integrated approach that can work *together* with endpoint, network, and cloud security controls to stop sophisticated attacks, including phishing, business email compromise, ransomware, spoofing, and malware.
- Threat intel – With a rapidly changing threat landscape, access to the latest, email-specific threat intel is more important than ever to ensure that new attacks are identified and stopped.
- Multifactor authentication – With credential theft on the rise, verifying the identity of email users becomes critical. Multifactor authentication ensures that only authorized users can gain access to email accounts as well as other network entry points, protecting against unauthorized email access through the use of stolen credentials.
- Cloud and on-prem support – With organizations often running hybrid email deployments leveraging both cloud-delivered and on-prem solutions, security controls need to support both cloud-delivered and on-prem email with common interfaces.
- Data loss protection – The ability to classify, detect, and protect sensitive information data loss is a must, especially in support of industry and government regulations. DLP protects against both unintentional and intentional data loss.
- Enhanced native controls – As email security providers build out their own email security controls, the solution must easily integrate and add value without conflict.
- Extensible architecture – In support of organizations' growing security needs, the solution must expand and scale easily.

[8] Source: ESG Master Survey Results, *Enterprise-class Cybersecurity Vendor Sentiment*, March 2020.

- Flexibility – As infrastructure and policies evolve, the solution must be customizable to incorporate new controls and requirements as organizations change and grow.
- Automated security awareness training – With business email compromise and other types of phishing attacks, humans play an integral role in the success of the attack. Regular security training and security awareness assessment can reduce the success rate of these kinds of attacks, in addition to preparing users for new, unknown attack types.

Figure 1. Closing the Gap with a Layered Approach to Security

Source: Enterprise Strategy Group

Introducing Cisco Email Security

Cisco Email Security provides a layered email security solution that protects against email attacks, including phishing, spoofing, business email compromise, ransomware, and malware. Utilizing Cisco Email Security, security analysts and email administrators have visibility into email activity, across all devices, locations, and users, where they can search for messages in real time, respond to critical calls, and rapidly respond if an incident occurs.

Cisco Email Security leverages threat intelligence provided by Cisco's Talos threat research team (recognized as the largest private threat research team in the world), to keep email safe as new threats are discovered.

Cisco Email Security includes Data Loss Prevention (DLP), protecting sensitive information from inadvertently being shared, while encrypting sensitive data in transit (supporting industry and government regulations). All email traffic is inspected for sensitive information, so outgoing emails that include sensitive data can be blocked if they include unapproved content. A more advanced, full-featured DLP capability is also available as an additional subscription.

Advanced Phishing Protection, Domain Protection, and Security Awareness subscriptions are also available, providing a robust, full-featured email protection solution.

Full feature parity is provided across cloud, virtual, on-premises, or hybrid deployments, supporting organizations as their deployment needs evolve or change.

A Core Component of Cisco SecureX Security Platform. Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio, increasing visibility and automating workflows to speed threat detection and response. SecureX aims to streamline operations, enabling security analysts to view threat history and trajectory across Cisco Security products like Next Gen Firewall (NGFW), Advanced Malware Protection (AMP),Cisco Email Security, Umbrella, and WSA through a single console. This integrated approach goes a long way in reducing investigation and response times.

The Bigger Truth

Email threats have become prolific, sophisticated, and unpredictable. Adversaries are heavily leveraging phishing and other sophisticated attacks within cloud-delivered email solutions for successful business email compromise attacks, causing significant productivity and financial loss.

Modern email solutions need a comprehensive layered approach to security, working in concert with other security controls, including endpoint, network, and cloud, to defend against sophisticated attacks. These controls need to be integrated and backed by the latest threat intelligence.

Innovations from companies like Cisco are delivering layered email security solutions as part of a fully integrated security platform to protect organizations against the modern 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