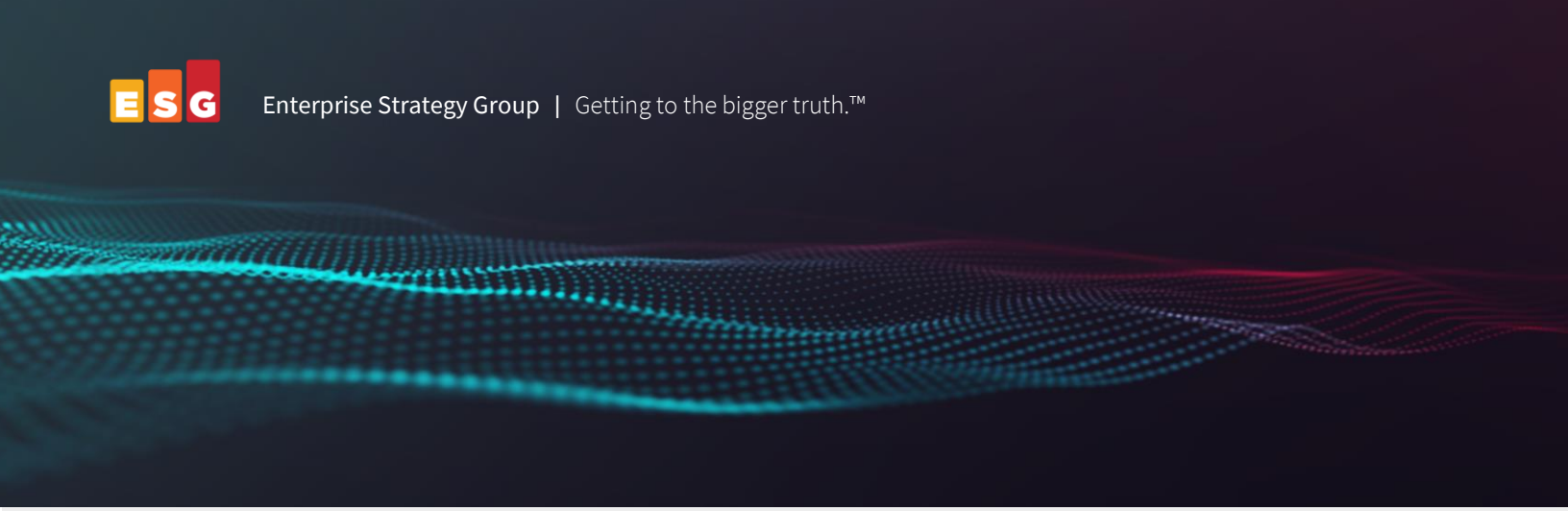


ESG WHITE PAPER

Closing Critical Gaps in Microsoft 365 Native Security Tools

The Imperative for Additional Third-party Security Controls

By Dave Gruber, ESG Senior Analyst

August 2021

This ESG White Paper was commissioned by Tessian and is distributed under license from ESG.

Contents

Executive Summary

Email continues to be the backbone of enterprise communications and is considered the most critical infrastructure to daily operations for most. Cloud-delivered email infrastructure has rapidly become the preferred approach to enable email communications, with over 1.3M companies depending on Microsoft 365.[1]

For many, handing over email infrastructure to a cloud service provider means transferring and trusting email security and resilience to the provider. Yet as phishing, which was involved in 43% of breaches in the past year,[2] continues at epidemic levels, over two-thirds (69%) of respondents to an ESG research survey report that email security has become one of their top 5 cybersecurity priorities, with 18% citing email security as their most important cybersecurity priority.[3]

While cloud-delivered email providers promise security and resilience, most fall short of what many security and IT teams would consider adequate. Further, adversaries are capitalizing on these homogenous security systems to bypass controls. As a result, ESG research found that 62% of organizations are reevaluating all security controls currently available natively, with many turning to third-party email security and resilience solutions to supplement native controls.[4]

Organizations that are planning to move or have recently moved to cloud-based email should strongly consider the use of third-party email security solutions to ensure that critical email infrastructure and data are adequately secured against the expanding email threat landscape.

The Move to Cloud-delivered Email Solutions

As organizations move core operating infrastructure to the cloud, enterprise email is ripe for transformation. Significant numbers of organizations have already migrated inboxes to popular cloud email solutions, with Microsoft Office365 leading the pack, but like the days of on-premises email, organizations need to plan for how to ensure security and resilience of their email solution. Moving to the cloud does not inherently address this issue.

Cloud-delivered email benefits align to the same, well-known benefits of the cloud, including the reduction of operating infrastructure management cost and the move from CapEx to OpEx. For most, email infrastructure is critical to daily operations; however, few view their choice of email solution as a means of operational differentiation, so outsourcing makes sense for most, like many other areas of operational IT infrastructure.

Not a Panacea

Cloud-delivered email solutions aren't a panacea. Moving on-prem email solutions to the cloud replaces the operational infrastructure but doesn't necessarily fully replace security controls.

But cloud-delivered email solutions aren't a panacea. Moving on-prem email solutions to the cloud replaces the operational infrastructure but does not offer complete security controls. Additionally, new risks emerge with the use of this approach to email infrastructure. Moving to Office365 is basically lifting and shifting an on-prem exchange infrastructure to the cloud—without comprehensive security controls.

And while most cloud-delivered email solutions offer basic security controls, they often lack many of the controls that today's corporate security teams mandate.

[1] Source: Statista, *Number of Office 365 company users worldwide as of June 2021, by leading country*, June 2021.

[2] Source: Verizon, *2021 Data Breach Investigations Report*, 2021.

[3] Source: ESG Research Report, *Trends in Email Security*, August 2020.

[4] Ibid.

As part of moving to cloud-delivered email, security teams need to play a key role in ensuring the necessary levels of security against malware, ransomware, phishing, and data exfiltration are in place.

The Evolution and Persistence of Phishing Attacks

Phishing attacks continue unabated, with an ongoing high incident rate of email phishing to remind security teams that cyber adversaries will default to those methods that have proven most effective. Phishing was involved in 36% of breaches in 2021, up from 25% last year.[5]

Yet even with these high numbers, not all phishing attacks are reported. Duped users are often not aware that they were phished or may be too embarrassed to report the incident. In either case, such situations increase dwell time and increase the potential for the spread of malware, data loss, or both. But in fairness to end-users, cybercriminals are employing socially engineered targeted attacks that are extremely difficult for some knowledge workers to identify (as they are so timely and accurate). Such attacks are new ways for criminals to monetize fraudulent phishing attacks, often leveraging pretexting that can lead to well-orchestrated business email compromise (BEC) attacks.

This type of fraud is perpetrated via spoofed emails that fool users into taking other actions, beyond simply clicking on a malicious link. Instead, recipients are often instructed to make payments, based on the direction to do so from an impersonated executive or impersonated vendor email. These types of BEC attacks have resulted in appreciable financial loss. In a recent public service announcement from the FBI, total losses due to successful business email compromise campaigns are estimated at $1.8B.[6] These attacks are further examples of fraud at scale.

Phishing is Often Only the First Step

Successful credential phishing attacks can lead to email account takeover (ATO) that allows the external cybercriminals to later appear as legitimate insiders, facilitating BEC, data exfiltration, and ransomware. As a frequent early tactic used in the kill chain, early phishing detection can thwart these more complex, sophisticated attacks before they get underway.

Phishing attacks are often just the first step in a campaign, as is the case with those that are designed to steal login credentials, often by exploiting the social networking aspect for how we use cloud services. For example, because the use of file sharing services, such as Box, Dropbox, One Drive, etc., is common, users are accustomed to receiving emails from others to access shared files. This creates the perfect opportunity for bogus emails to lead a user to a bogus login page as a means to capture credentials that are then used in the next step of an attack campaign. Bogus emails instructing a subordinate to transfer monies is even more believable because of the legitimacy of the sender's email address. These successful credential phishing attacks can lead to email account takeover (ATO), enabling cybercriminals to later appear as legitimate insiders, facilitating BEC, data exfiltration, and ransomware. As a frequent early tactic used in the kill chain, early phishing detection and prevention can thwart these more complex, sophisticated attacks before they get underway.

Email as a Path for Ransomware

Ransomware ranks as a top-3 risk concern, with 77% of organizations classifying ransomware as a high or medium risk.[7] Ransomware begins with an initial compromise that is most often facilitated through email, using phishing techniques, malware attachments, or malicious URLs. As the first step in the attack chain, stopping the initial compromise prevents further privilege escalation, lateral movement, and, ultimately, encryption activities. As organizations become increasingly

[5] Source: Verizon, *2021 Data Breach Investigations Report*, 2021.

[6] Source: Federal Bureau of Investigation Internet Crime Complaint Center, *2020 Internet Crime Report*, 2020.

[7] Source: ESG Research Report, *Trends in Email Security*, August 2020.

concerned about the risks of successful ransomware attacks, and as ransomware attacks become highly targeted and orchestrated, new detection strategies require security controls to interoperate, sharing suspicious activities as attackers progress in the attack chain. Email security is paramount, stopping malicious attachments, credential theft, and reconnaissance activities early in the attack chain.

Sensitive Data Leakage

While most email security solutions are focused on inbound threats, outbound threats continue to evade controls. Sensitive data exfiltration facilitated through impersonation and ATO activity has become a common attack strategy. Unintentional or careless sensitive data loss also ranks as a significant concern, with 32% reporting the accidental loss of sensitive data as a result of email-borne attacks.[8] While many see these careless actions as simple mistakes, simple human error can often result in far-reaching consequences, including exposure of key intellectual property, protected customer data, and sensitive financial information.

Insider threat further creates risk, as employees knowingly leverage email to deliberately export sensitive information for personal use, including customer account information, sensitive financial models, templates, etc., to give themselves an edge on their next career opportunity. Further, sensitive data leakage occurs when employees violate policies or evade controls by sending personal emails containing sensitive data externally using personal file sharing and other communication mechanisms.

Modern Email Controls Must Protect Against Both Inbound and Outbound Threats

Email is a bi-directional communications mechanism and, as such, requires thorough controls on both the inbound and outbound side.

Email is a bi-directional communications mechanism and, as such, requires thorough controls on both the inbound and outbound side.

Unpacking Microsoft 365 Native Security Controls in E3 and E5

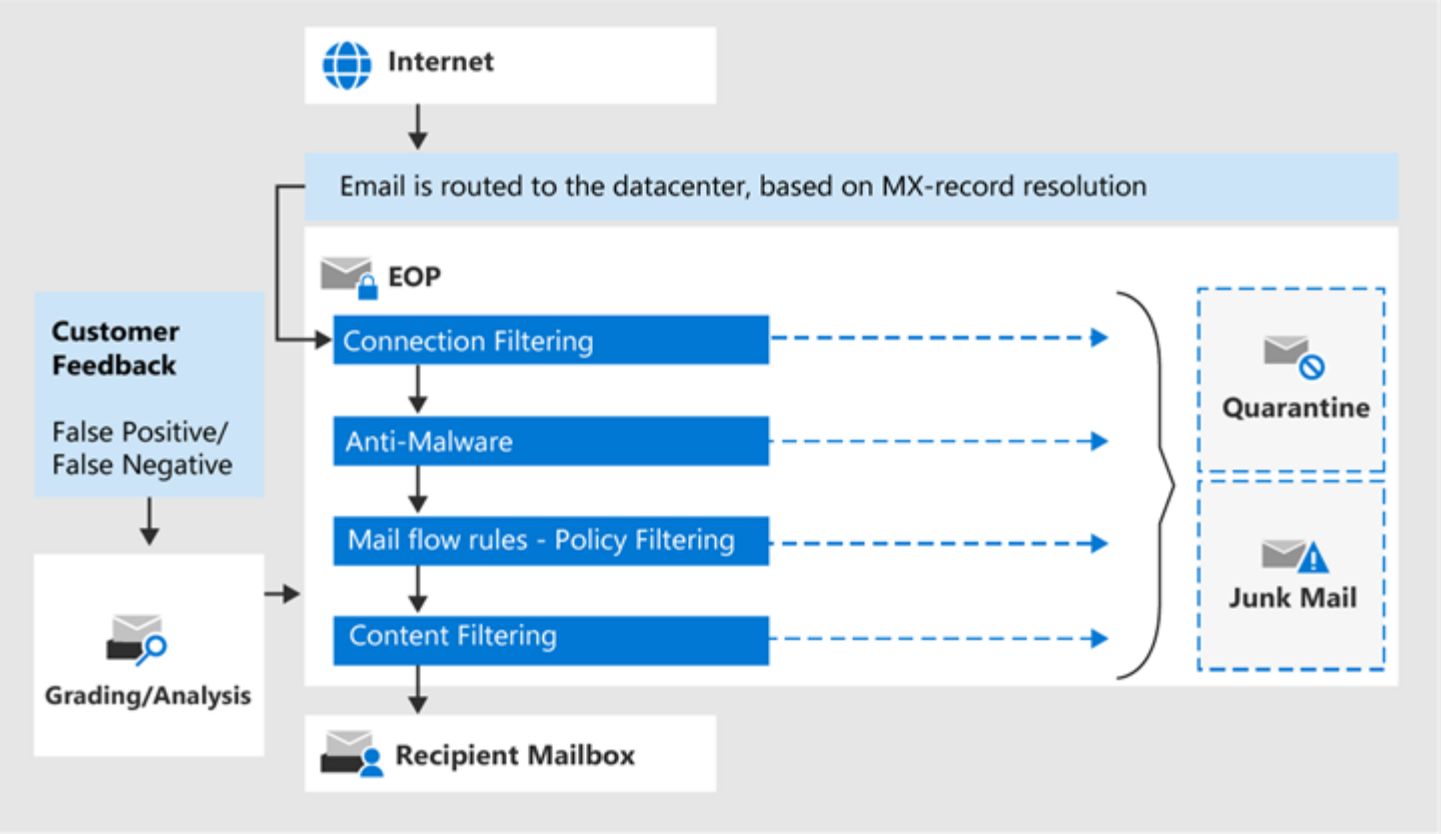
While Microsoft has invested significantly in strengthening security controls for Microsoft 365 (M365), organizations report continuing gaps in the controls included in both E3 and E5 licensing bundles.

M365 leverages Exchange Online Protection (EOP) in both the E3 and E5 bundles to filter email for malicious links, spam, and basic phishing attacks. Email security included with the E3 bundle depends solely on EOP, filtering based on sender reputation; the inclusion of malware; whitelisting/blacklisting; and content filtering looking for high-confidence spam, phishing, high-confidence phishing, bulk (anti-spam policies), or spoofing (spoof settings in anti-phishing policies). A global network of EOP data centers further protects users from outages.

The EOP architecture (see Figure 1) moves individual emails through a series of filters, governed by both preset and configurable security policies. This process results in exclusions that end up in either quarantine or junk email folders.

[8] Ibid.

Figure 1. Microsoft Exchange Online Protection Architecture



Source: Microsoft.com

Architectural Challenges

Adversaries are continually working to evade email security controls. Evasion techniques often involve single-use URLs and malware images to avoid signature-based detection techniques. With Microsoft's strong emphasis on signature-based detection of malware, malicious URLs, and known bad senders, adversaries are frequently able to evade native M365 security controls. This emphasis on detecting malicious "payloads" of emails (malware in attachments or malicious URLs) often leaves organizations highly vulnerable to attacks that do not contain known malicious payloads, such as social engineering and BEC attacks. More sophisticated detection techniques utilizing behavioral analytics, relationship graphing, and other methods providing individual message context are required to identify these types of attacks.

Advanced email-borne threats often require a deep, contextual understanding to determine when impersonation and other ATO-related techniques are in use. Rules-based methods lack the ability to detect these user relationships, fueling many to implement a behavioral approach that can deeply understand the unique context of each employee's actions.

Microsoft 365 E3 Gaps

Email Security

While EOP provides many valuable security features, it is limited in its ability to protect against more sophisticated email attacks, such as social engineering (or "spear-phishing"), business email compromise, account takeover, and many types of ransomware. Detecting these types of more sophisticated attacks requires both behavioral analytics and a contextual

understanding of individual communication activities, which don't exist in EOP. So, while native controls are effective at detecting mass/generic phishing campaigns, they are less effective at detecting highly targeted attacks. For example, EOP uses block lists to detect spam and known malware. Safe Links (available in E5) rewrites URLs and checks them against known lists of malicious URLs before allowing the user to visit the link.

Data Loss Prevention

45% of organizations report that more than 40% of their sensitive data flows through their email application.[9] Minimal data loss protection capabilities are included in the E3 bundle, relying on end-users to manually label documents as sensitive to protect them. Relying on end-users to accurately and consistently classify content puts organizations at risk. On the other hand, applying blanket policies and blocking sensitive information is highly disruptive to users' productivity and can be an immense burden on security teams. Further, companies that opt for applying a default classification to all documents and emails end up with the same label being applied to everything, while lacking any new visibility into sensitive data. As a result, organizations most often resort to tracking and post remediation instead of proactive detection and real-time response. Additionally, E3 lacks capabilities natively to detect and manage insider risk (for example, preventing data theft by departing employees). Native controls also often lack the ability to properly classify non-Microsoft data and files, requiring admins to use workarounds to achieve consistent protection.

Microsoft 365 E5 Gaps

Email Security

Microsoft 365 E5 bundle includes additional security features by adding the Microsoft 365 Defender endpoint security solution. Additional protection against phishing and ransomware is provided through more advanced malicious URL and attachment protection, including link re-writing and attachment sandboxing. Both approaches, however, can still be vulnerable to new URLs and attacks without "payloads."[10] Microsoft Defender depends on multiple scan engines to detect malware attachments and malicious URL links, leveraging both signature matching and machine learning to perform behavioral analysis. Because BEC and ATO impersonations often contain no malicious links or attachments, these threats can commonly escape this approach.

Impersonation Detection

Very basic impersonation rules for internal or pre-specified domains are also provided but lack the ability to protect against impersonation from outside counterparties, often used by attackers. Rules-based approaches to impersonation detection lack contextual understanding of relationships and subject matters, focusing primarily on protecting an organization's own domains and users, leaving them vulnerable to impersonations of counterparties. When defense depends on simplistic rules coverage, it can be easy for a mildly intelligent attacker to understand how to get around the rules. Without language analysis, detecting signs of social engineering is very difficult or impossible, as is detecting compromised external senders commonly used in BEC attacks. Rules-based approaches can also generate significantly more false positives.

Contextual Understanding Matters

Rules-based approaches to impersonation detection lack contextual understanding of relationships and subject matters, focusing primarily on protecting an organization's own domains and users, leaving them vulnerable to impersonations of counterparties.

[9] Source: ESG Research Report, *Trends in Email Security*, August 2020.

[10] Source: Microsoft.com, *Exclusive settings in anti-phishing policies in Microsoft Defender for Office 365*.

Data Loss Prevention

Data loss prevention is included in the E5 bundle for emails, Teams, and files. Advanced email encryption functionality is also provided, as well as email retention policies. Customer keys for Office 365 are also supported. Some level of insider risk management capabilities is also included.

Context Matters in DLP

Detecting misaddressed emails and emails with unintended attachments requires a contextual understanding of the parties exchanging email. Without this context, misaddressed emails and unintended attachments are often missed.

M365 Email DLP capabilities are, however, not context-aware (meaning that they lack context between parties exchanging email), resulting in an inability to proactively identify wrong recipients or unintended inclusion of attachments. M365 detection instead utilizes a rules-based approach to define DLP policies and classify data (regex pattern matches, proximity of certain keywords to the matching patterns, exact data matching, and fingerprinting). These techniques alone are often unable to detect when email recipients are misaddressed or when wrong attachments are involved.

Additionally, because these capabilities rely on rule-based techniques or trainable classifiers to align specific data types with DLP policies and to label data (using Azure Information Protection), effectively detecting sensitive information in unstructured data can be problematic (legal, mergers and acquisitions, work orders, bidding documents, and other non-Microsoft formatted files), resulting in users exfiltrating sensitive data and additional false positives.

While encryption is often mistakenly perceived as a solution to solve for misdirected emails, recipients included by mistake can still often decrypt emails to gain access to sensitive data. User experience/friction when encrypting emails can also be a barrier to use.

While E5 provides increased security capabilities over E3, organizations continue to report gaps in spear-phishing, BEC, account takeover, and many types of ransomware protection, motivating many to invest in additional third-party email security controls.

What's Needed

Email security has long been focused on inbound filtering and the monitoring of user activities looking for well-known patterns of misuse. Yet email usage patterns are more often unique to individual users, those that they communicate with, what they communicate, and how they communicate. This individual usage context is required to detect and stop many of today's more sophisticated attacks such as spear phishing, BEC, and ATO.

Much of this personal context can be derived through behavioral analytics of historical email, including the analysis of who, what, and when emails were sent in the past. When individual historical patterns, along with context, can be matched against future activity, modern email threats can be detected and stopped, often with little to no user or administrator involvement.

Modern email controls must protect against both inbound and outbound threats, including intentional and unintentional data leakage. These advanced security capabilities must be able to complement native, cloud-delivered email security controls, allowing organizations to supplement and close the gaps without introducing friction, avoiding any delivery and transmission delays.

The Bigger Truth

While cloud-delivered email solutions have provided significant benefits for many organizations, they continue to lack the depth of email security controls needed by many organizations today. Packaging and licensing options further complicate what levels of security are provided, leaving many vulnerable post-migration to cloud-delivered email implementations.

Security teams need to get involved early and must play a role in both the selection and implementation process to ensure corporate communications and data are adequately protected. Third-party solutions can mitigate risks by closing gaps in native, cloud-delivered email security controls, providing the security needed to protect users from modern email attacks.

Microsoft 365, the dominant cloud-delivered email solution adopted today, may lack critical security controls needed for certain organizations, therefore motivating many to add supplemental security solutions to close gaps. Whether in the planning stage, implementation stage, or post-implementation, third-party email security controls should be considered with all cloud-delivered email solutions.

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