ESG SHOWCASE

Closing Security and Resiliency Gaps in M365

Date: October 2022 **Author:** David Gruber, Principal ESG Analyst

ABSTRACT: As companies and government entities depend on cloud communication and collaboration platforms to enable employees, partners, and suppliers to work together, any service disruption has a direct and immediate impact on business operations. Yet end-users are being more targeted than ever, with human error involved to some degree in more than 90% of successful security breaches.[1] As attackers leverage the ubiquity of Microsoft 365 and its connection to workers in an attempt to evade other controls, security and IT teams are investing in additional, layered security and operational resiliency solutions to mitigate risk.

Overview

Microsoft 365 (M365) is the most popular business productivity platform in the world, with an estimated 345 million paid seats.[2] The benefits are clear: lower costs from cloud hosting, user-friendly tools for employees, and collaboration capabilities that make remote work more productive.

The risks, however, are not as widely understood. M365's popularity has created an irresistible target for cybercriminals, making it the most attacked platform in the world. Homogenous technology invites risk, and, as such, M365 is massively targeted and often exposed to attacks that leverage the M365 platform itself. In a threat landscape that leaves no margin for error, this critical mechanism demands the strongest possible protection.

Despite ongoing investment in native controls by cloud business platform providers, security and IT teams report weaknesses in both security and resilience, motivating many to add layered controls to reduce the success rate of attacks and mitigate the risk of operational disruption. Broad solutions offered by vendors like Mimecast help keep M365 secure and resilient.

Supplemental Security and Resiliency Controls

While Microsoft offers multiple native security capabilities within both its popular E3 and E5 offerings, many security teams are supplementing these capabilities with layered security and resilience solutions to further reduce operational and security risks. There are two common approaches to supplemental strategies:

- Purpose-built cloud supplements – These specialized, cloud-specific supplemental solutions are purpose-built to close gaps in Microsoft 365 native controls. Organizations that depend solely on cloud-delivered email and collaboration solutions are often a good fit here. Implementation is fast and easy. While

Reducing Operational and Security Risk

While Microsoft offers native security controls. many security teams are supplementing these capabilities with layered security and resilience solutions to further reduce operational and security risk.

[1] Source: Mimecast, *Confronting the New Wave of Cyberattacks: The State of Email Security 2022*.

[2] Source: Office365forITpros, *Office 365 Reaches 345 Million Paid Seats,* April 2022.

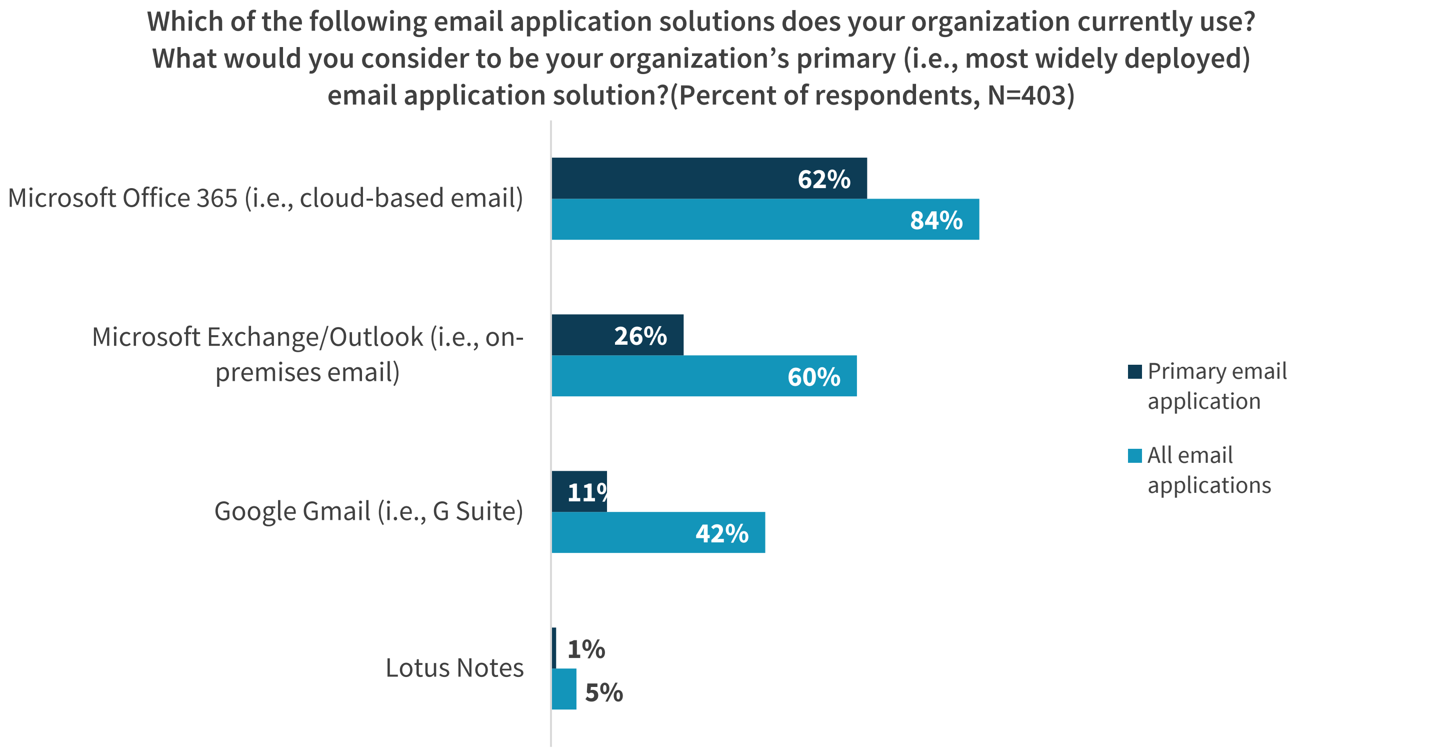
This ESG Showcase was commissioned by Mimecast and is distributed under license from TechTarget, Inc.

connectivity models for these solutions vary, some report performance concerns in products that leverage API connectivity models, resulting in additional windows of risk and operational delays for end-users when emails are clawed back for re-inspection. Integrated cloud email security solutions are available from multiple vendors, in addition to supplemental solutions that can strengthen data protection and platform resiliency.

- Hybrid email and collaboration security and resiliency platforms – These solutions support hybrid cloud and on-prem email and collaboration environments, offering IT and security teams the ability to apply and manage policies and exceptions through a single, consistent management mechanism for both cloud and on-prem email and collaboration tools. These solutions can offer both flexibility and scalability for organizations who have more dynamic, diverse environments, including more complex administrative needs; more complex account hierarchies; or hybrid environments, combining cloud-email with one or more on-premises email implementations. A more limited number of vendors offer this scope of capabilities and implementation models, and those that do have evolved, matured, and often assembled multiple, innovative solutions over longer periods of time.

Despite the popularity of cloud-delivered email and collaboration solutions, 60% of organizations report the continued use of on-prem email solutions, either in conjunction with cloud-delivered email, or as their primary email solution (see Figure 1).[3] In these cases, many are looking for more comprehensive solution providers that can extend security and resiliency controls across both cloud and on-prem environments, supporting shared, consistent policy management models.

Figure 1. Cloud-based Email Prevails, but Many Still Run Hybrid Environments



Source: ESG, a division of TechTarget, Inc.

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

Where IT and Security Teams Are Adding Layered Controls

- Enhanced cloud email security: In support of a rapidly growing, more advanced threat landscape, organizations are adding additional, layered security mechanisms capable of detecting and stopping more advanced attacks that involve communication and collaboration mechanisms.

- Operational resiliency: Email service disruption has broad and dramatic impact on all facets of business operations, motivating many to add additional mechanisms to ensure 100% uptime. Supplements typically can't provide this capability as they sit behind the core email provider and are therefore unavailable during email service disruption.

- Data loss protection: The ability to back up and restore email inboxes and content is a must, not only to minimize damage in the event of a successful attack, but also to simplify compliance with increasingly complex regulations.

- Consolidation: Reducing complexity by consolidating services with trusted vendors has become a priority for IT and security teams that are stretched to their limits. As organizations add layered controls to strengthen native cloud services, many are looking to more comprehensive platform providers capable of supporting multiple layered controls in a single solution.

- Scalability and flexibility: As IT and security teams evolve to more complex email and collaboration solution environments, many are looking for consolidated policy and management options that can be applied across hybrid environments, while addressing future scalability and growth requirements.

- Security stack collaboration: Complex threats involving multiple threat vectors require email and collaboration controls to work together with other security controls to inform advanced threat detection. Bidirectional sharing of intelligence and detections fuels more effective threat protection.

The Mimecast System

Mimecast offers layered email security controls for organizations with all types of needs, delivering world-class email security efficacy with total deployment flexibility. Customers can choose between two deployment options based on their specific objectives and requirements.

Mimecast Email Security, Cloud Gateway

A secure email gateway (SEG) in the cloud, Mimecast Email Security, Cloud Gateway is designed to secure any type of email environment, even the most complex. Offering advanced administration capabilities and a range of complementary solutions and integrations, it's ideal for IT and security teams that want to control risk and tame complexity. The solution supports M365 and Google Workspace, as well as on-premises and hybrid deployments.

Mimecast Email Security, Cloud Integrated

Operating as an integrated cloud email security solution, not requiring an MX record change, Mimecast Email Security, Cloud Integrated is purpose-built to enhance and extend M365 protections. Deploying in minutes and providing optimized protections out of the box, it's ideal for IT and security teams that want to bolster M365 while simplifying email security administration.

The Bigger Truth

Cloud business platforms like M365 have become essential for doing business but keeping them secure and resilient has never been more challenging. A constant and evolving threat escalation involving these platforms creates an imperative for IT and security teams to strengthen controls.

While native controls provide coverage against many threats, comprehensive coverage requires a performant, layered security model, capable of detecting and stopping all types of threats without adding friction to end-user productivity. Third-party solutions can mitigate risks by offering both additional security and resilience to keep users working, providing redundancy when a cloud email provider experiences an outage.

While many integrated cloud email security solutions address specific security gaps within the native controls offered within cloud-delivered email solutions, few are able to deliver the level of comprehensive security and resiliency needed by more discerning organizations. Integrated, comprehensive solutions addressing all facets of email security and operations are helping these organizations leverage a single solution to mitigate the risks of operational disruption and protect sensitive data (in motion and at rest), while simplifying IT and security operations.

ESG recommends considering layered solutions from vendors like Mimecast that can deliver the security, performance, and resilience needed to protect and scale with business operations.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

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