

Solution Showcase

Cisco Email Security

Date: October 2018 **Author:** Mark Bowker, Senior Analyst and Adam DeMattia, Director, Custom Research

Abstract: Companies are increasing the urgency level with which they view email security. Organizations are vulnerable, and the stakes are high. ESG believes these heightened demands will result in the lion's share of cloud-delivered email users exploring supplemental third-party email security solutions.

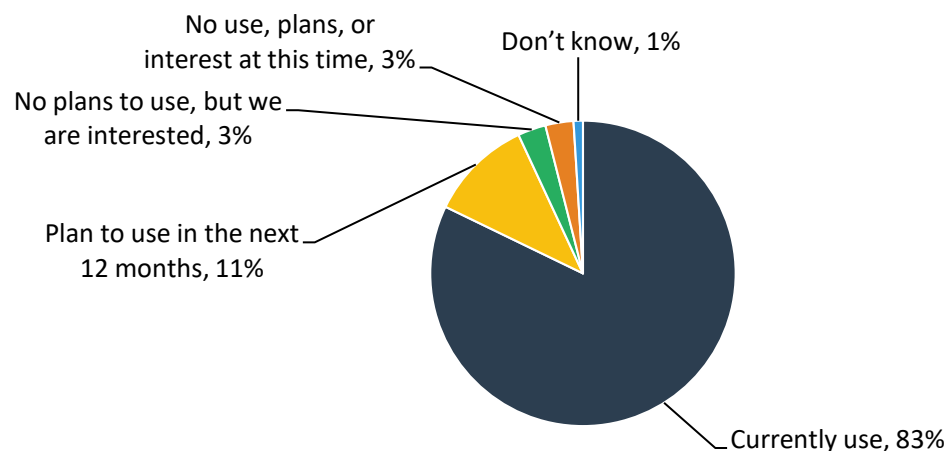
Email Is the Number One Attack Vector

Email remains a primary source of communication and collaboration for businesses and a primary target for a security breach. According to Verizon's Data Breach Investigations Report (DBIR), 98% of incidents and 93% of breaches involved phishing and pretexting scams. So how are businesses improving their security posture as email migrates to a cloud service while spoofing, phishing, business email compromise (BEC), and sophisticated social engineering attacks are on the rise?

As the email threat landscape intensifies, organizations have rapidly transformed how they consume email via the adoption of SaaS-delivered email like Office 365 and Gmail. In fact, 83% of respondents report their organization currently uses cloud-hosted email services today and an incremental 11% expect to do so in the next 12 months (see Figure 1).¹

Figure 1. Use of Cloud-hosted Email Services Is Widespread

What is your organization's usage of Office 365, Gmail, or any other similar cloud-hosted email service as a corporate-sanctioned email offering? (Percent of respondents, N=200)



Source: Enterprise Strategy Group

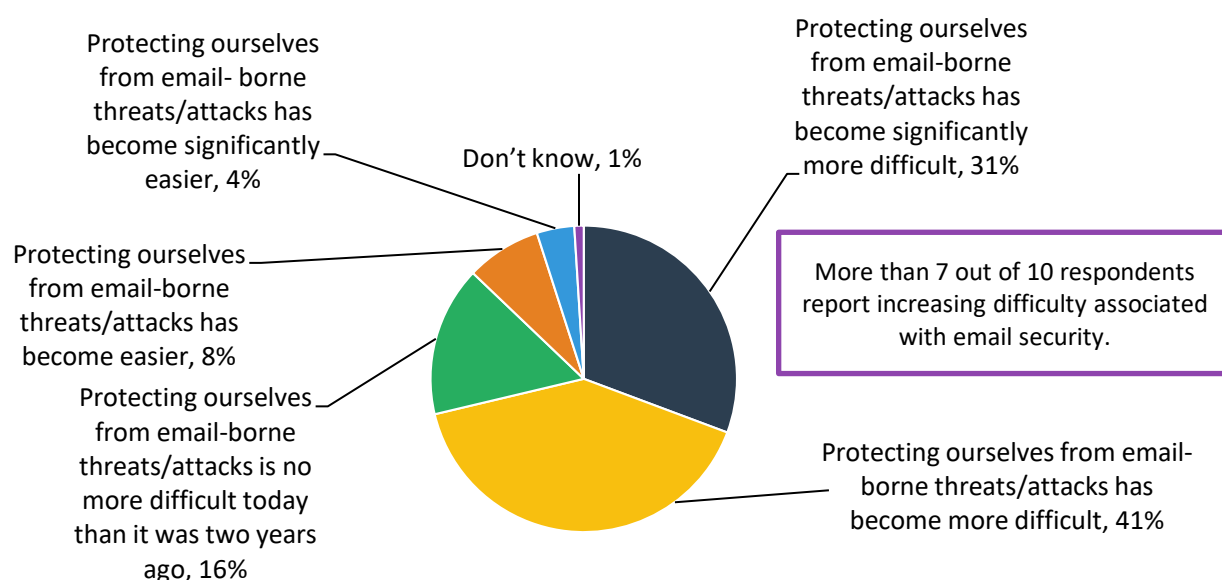
¹ Source: ESG Custom Research Commissioned by Cisco Systems Inc., October 2018. All ESG research references and charts in this solution showcase have been taken from this custom research.

However, as with any major technology transformation, the shift has created confusion in the market, specifically related to security. When ESG asked respondents if they felt the native security features offered by cloud service providers were adequate for their requirements, respondents were nearly evenly split: While 57% said yes, 43% reported they felt their organization would need to add supplemental third-party controls. This division denotes uncertainty in the market. The rapid adoption of cloud-based email has companies quick to roll out technology without considering the potential security risks.

To help measure the urgency level companies are setting on email security, ESG research began by asking respondents if email-borne threats are getting harder to defend against. This trend was soundly validated by respondents, with seven out of ten reporting increasing difficulty associated with email security over the last two years (see Figure 2).

Figure 2. Protecting Against Email-borne Threats Getting Harder

How – if at all – has the difficulty of protecting your organization from email-borne cybersecurity threats/attacks changed over the last two years (e.g., social engineering, phishing, business email compromise, fileless attacks, etc.)? (Percent of respondents, N=200)



Source: Enterprise Strategy Group

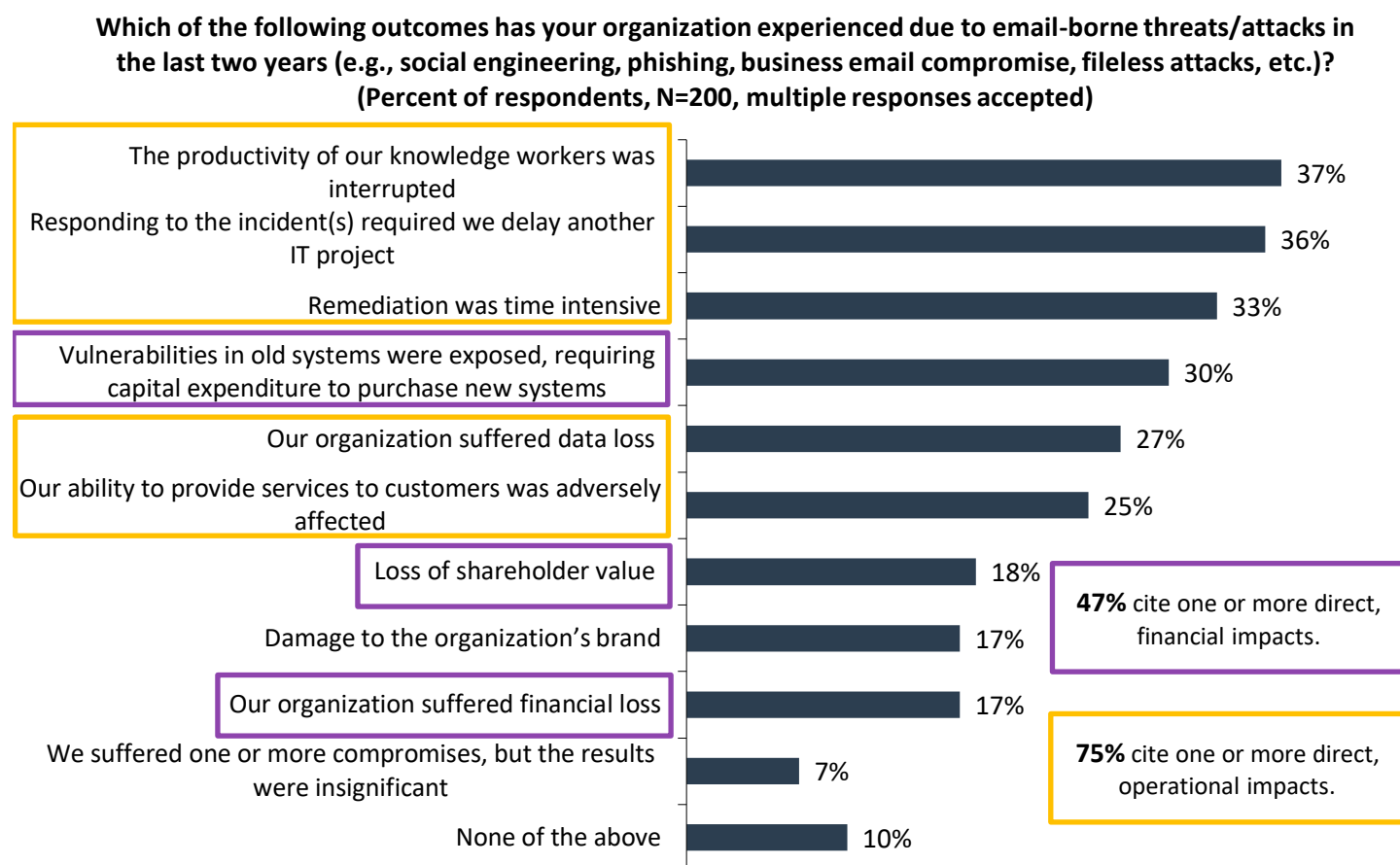
Qualitatively, the research shows that security practitioners feel their jobs are becoming more difficult with respect to email security. The research also shows quantitatively that this assessment is correct. ESG asked respondents what percentage of all employees at their organization they believe have fallen victim to a phishing or other socially engineered email attack in the last 12 months. The median response was 8% of employees. In this research, the average organization was comprised of approximately 6,800 employees. That means that the typical organization represented in this research experienced email compromise over 540 times in the last 12 months—and each of those compromises could have a devastating impact on the organization.

The research also discussed the tangible impact of email-borne threats. Respondents report the negative outcomes experienced are both serious and varied (see Figure 3). Three-quarters of respondents reported their organization has experienced one or more significant operational impacts in the last two years: from lost productivity through IT project delays stemming from time intensive remediations to customer service disruptions. Nearly half of respondents reported their organization has experienced a significant financial impact like expensive capital outlays needed to remediate risk or

even shareholder losses. Finally, it is worth noting that less than one out of five respondents reported their organization hadn't experienced a serious impact.

This data shows that organizational vulnerability is significant, and the stakes are high.

Figure 3. The Impact of Email Compromise Is Significant

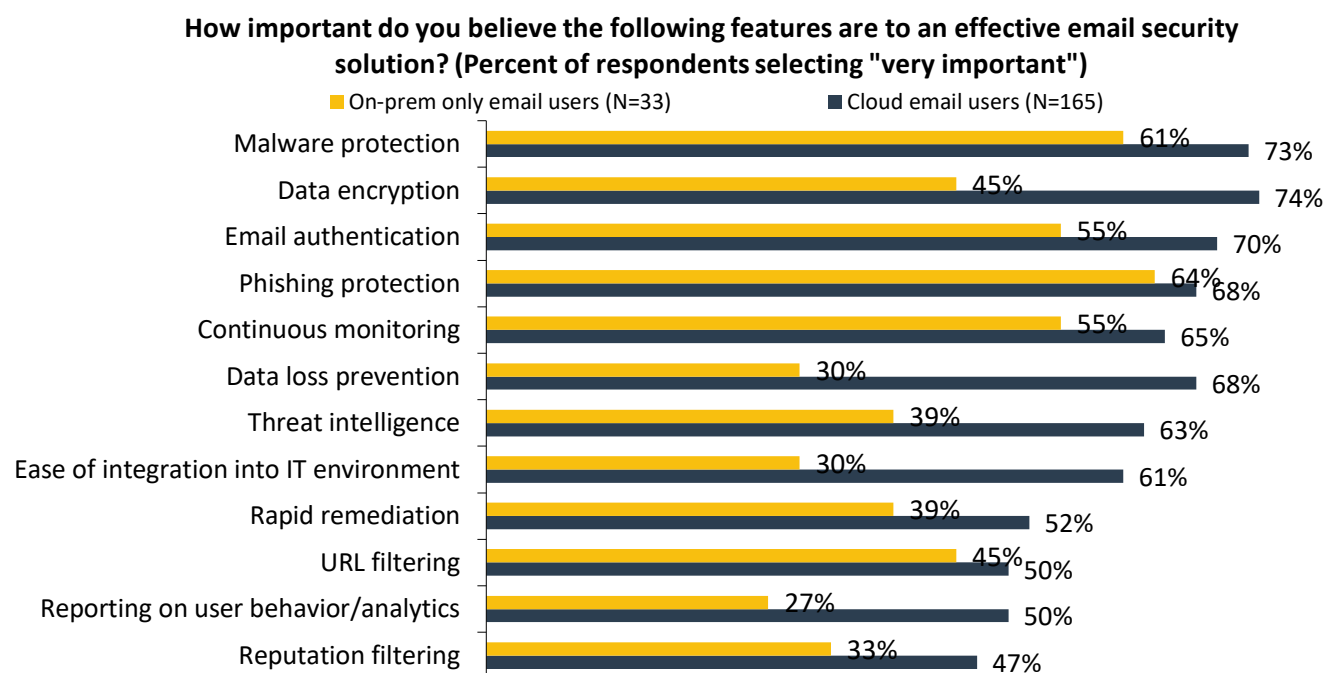


Source: Enterprise Strategy Group

While respondents were split about the effectiveness of security services included with cloud-delivered email, they were unified in their opinion that effective email security must be multifaceted. ESG asked all respondents about the importance of various email security features and, for every feature included in the survey, more than 90% of respondents agreed the feature was very important or important. Specifically, the features respondents were most likely to report being very important were malware protection (72%), data encryption (70%), phishing protection (68%), email authentication (68%), and continuous monitoring (64%).

With respect to email security requirements, ESG observed an interesting trend: Organizations that have adopted cloud-based email have much higher email security demands. As shown in Figure 4, these respondents were much more likely to report that they believe data encryption, DLP, threat intelligence, ease of integration, and in-depth reporting capabilities are very important email security features. Ultimately, ESG believes these heightened demands will result in the lion's share of cloud-delivered email users being highly likely to explore supplemental third-party email security solutions.

Figure 4. Differences in Email Security Preferences, by Cloud-hosted Email Use



Source: Enterprise Strategy Group

Moving Beyond the Basics with Cisco Email Security

Cisco Email Security provides the first layer of defense against threats and secures outbound data. It protects against spam, impostors, and infected files—no matter when they become malicious—and blocks risky URLs to prevent attacks. It prevents loss of sensitive information or secures it in transit to ensure compliance.

The threat detection from Cisco Talos, the largest security intelligence network in the world, is the foundation for Cisco Email Security. Multiple layers of protection means threats are blocked faster. Real-time visibility into all email communications helps IT respond to incidents sooner. Cisco Email Security enables secure email use to keep business moving.

In addition to the base email security product, Cisco offers protection through these subscriptions:

Cisco Advanced Phishing Protection helps stop the latest emerging threats that use identity deception such as business email compromise attacks with no payload, attacks that use compromised accounts, and social engineering attacks. Machine learning techniques for identities and baselining behavioral models drive a real-time understanding of senders.

Cisco Domain Protection correlates information into a report for visibility into keeping a company's brand safe. This enables companies to capture visibility into which third-party senders are sending email on their behalf and whether they are DMARC compliant. Protection is provided to reduce the likelihood of the brand being used to send out phishing emails.

Cisco Advanced Malware Protection (AMP) provides a repository to check against in the event an infected file comes in through the email system. The AMP architecture checks a file in the event of a disposition change from clean or unknown to malicious and notifies the customers retrospectively about every inbox where the associated message was delivered.

Additionally, Cisco provides URL intelligence with its web security products, including Umbrella, to provide knowledge of web-based attacks and methods to prevent attacks from infected links.

The Bigger Truth

Businesses' dependence on "out of the box" protection from cloud providers has created a level of uncertainty when facing email attacks. Additionally, businesses need more protection to improve their security posture and should consider integration with existing security investments, including network security and content security across their entire environment. They need a security platform that provides multiple layers of security for cloud, virtualized, on-premises, or hybrid consumption models and protection across the organization.

Cisco Email Security has a history of on-premises protection via email appliances and has advanced with IT and business trends to protect cloud email deployments. Continued investment and innovation into the Cisco product line should instill confidence in protecting the business' most used communication method: email. Cisco's real-time visibility into email activity across all devices, locations, and users helps reduce investigation and response times, freeing IT professionals to focus on network uptime.

Cisco Talos shares intelligence from other Cisco Security products and enables security professionals to see a threat once and block it everywhere. The Cisco Security portfolio of integrated products and open architecture gives companies the ability to have a multifaceted, layered approach to security.

The negative impacts of email compromise on the business are having a significant economic and operational effect on companies today, as demonstrated in Figure 3. Furthermore, keeping pace with the ever-changing threat landscape is proving to be a futile effort without a partner like Cisco that can share intelligence across its portfolio of security products and help companies quickly react and respond to threats as they happen.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



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

© 2018 by The Enterprise Strategy Group, Inc. All Rights Reserved.

