TAG CYBER

ENTERPRISE BUYER'S GUIDE FOR CLOUD EMAIL SECURITY SOLUTIONS

DR. EDWARD AMOROSO, TAG CYBER

Abnormal

TAG CYBER

ENTERPRISE BUYER'S GUIDE FOR CLOUD EMAIL SECURITY SOLUTIONS

DR. EDWARD AMOROSO

This buyer's guide offers advice and insight into what modern enterprise teams should consider when reviewing and selecting a cloud email security solution. We include functional requirements and corresponding vendor questions to help buyers select the best tool for their environment.

INTRODUCTION

Enterprise security teams understand that email is a major target for adversaries. Email use involves every employee, partner, supplier and customer and includes data that can range from innocuous chatter to highly sensitive information. Furthermore, with the emergence of public cloud services, access to email provides an easier entry point to business applications such as Microsoft SharePoint and Microsoft Teams.

Traditional email security practices have focused on filtering malicious content from inbound emails. First-generation solutions primarily removed attachments that contained malware or viruses, and this evolved into second-generation secure email gateway (SEG) systems. The use of the SEG was an important step forward in protecting email, but it has proven insufficient for most enterprise email risks in recent years as the threat landscape has changed. Newer approaches have become necessary to block modern attacks.

In addition to threat actors changing their tactics, email itself has changed. The world has now transitioned from on-premises email systems like Microsoft Exchange to cloud-based email platforms like Microsoft 365 and Google Workspace. This change occurred quickly and has helped organizations increase productivity as they shift to a remote-first or hybrid work environment. The cybersecurity risks of cloud email, however, require a new type of defense—one that is different from traditional anti-malware and SEG-based protection.

In this buyer's guide for cloud email security solutions, we begin by explaining the cyber risks that are not addressed by Microsoft and Google. We then cover the requirements that buyers should include in their security planning for cloud email. Finally, we provide a set of specific questions that can be included in discussions with providers of modern cloud email security solutions that will be used in conjunction with Microsoft 365 and Google Workspace.

THE ADVANTAGES OF CLOUD EMAIL

Our assumption is that most readers will be fully aware of the business value of using cloud email. And certainly, some might choose to skip this section. Nevertheless, we feel obliged to share a summary of the major advantages that drive the use of such solutions. This helps ensure a set of baseline assumptions as we analyze options for integrating security onto this kind of infrastructure.

The salient aspect of cloud email is that it does not require organizations to host their own email infrastructure, as was the case with Microsoft Exchange. Traditionally, this was done by information technology teams in private, company-owned data centers. The administrative and security obligations, such as server management and vulnerability patching, were usually quite time-consuming and costly.

In contrast, modern cloud email services use a third-party hosting partner, almost exclusively Microsoft or Google, which provides email capabilities to enterprise users through cloud-hosted platforms. This new software-as-a-service (SaaS) approach offers major functional and usability advantages, including the following:

- ***Ubiquitous User Access*** — Users, including third parties, can more easily access cloud-hosted email from any device and generally across any type of transport, including the internet and 4G/5G networks or Wi-Fi.
- ***Reduced Operational Costs*** — The tangible hosting and infrastructure costs associated with electricity, cooling, physical security and staff can be amortized across all public cloud email service users, thus reducing costs for every enterprise customer.
- ***Straightforward Scaling*** — The ability to support user growth is much easier in a shared cloud email service because new users are simply given access to the SaaS platform using whatever provisioning process is desired.

Certain aspects of the shared cloud-based email service inherently help with cybersecurity. For example, disaster recovery for server malfunctions is usually supported via redundant architectures built into shared infrastructure from Microsoft or Google. Similarly, assurance that the most up-to-date protocols and patches are installed at the infrastructure level is typically part of the service level agreement for any cloud email platform.

In addition, Microsoft and Google have introduced a set of cybersecurity features (see sidebar) that match their business circumstances. Specifically, they have introduced protection capabilities that scale across their massive base of users, without being so aggressive as to create possible side effects for users who do not desire these additional security protections.

That said, the rapid pace of new email threats by adversaries exceeds the ability of both Microsoft and Google to keep up. Large providers simply cannot stay ahead of attackers in a threat landscape that evolves by the day. Buyers must therefore turn to more nimble, pure-play security providers for additional, but necessary, email protection.

NATIVE SECURITY IN MICROSOFT 365 AND GOOGLE WORKSPACE

The two dominant email platforms, Microsoft 365 and Google Workspace, include a range of native security protections that address spam, phishing, domain spoofing, malware attacks and more. Given the large customer bases for both services, these security features have been developed in the context of massive scalability requirements, and include the following:

- Microsoft's Exchange Online Protection (EOP) is a cloud-based filtering service that protects organizations against spam, malware and other email threats. EOP is provided to all Microsoft 365 organizations with Exchange Online mailboxes. It offers baseline protection, relying on malware signatures, static policies, heuristics and known indicators of compromise to detect email attacks. Microsoft offers additional advanced threat capabilities as part of Microsoft Defender for Office 365, accessible by purchasing different licenses and plans.
- Google Workspace offers baseline protection against spam, phishing and malware in all license plans. Like Microsoft, it uses malware signatures, static policies, heuristics and known indicators of compromise to detect email attacks. Google also offers advanced threat capabilities as part of different licensing plans. Both Microsoft and Google offer add-on capabilities like encryption to reduce email security risks. Some enterprise teams are beginning to use encryption, but it remains a comparatively little-used feature by many organizations.

While these native email security protections are useful as a foundation for enterprise email security, they have proven insufficient to handle advanced threats and other enterprise-level essentials, such as zero-day exploits, strict compliance requirements, the need for customization and handling the large volume of emails many businesses must manage.

SECURITY CHALLENGES OF CLOUD EMAIL

Despite the many commercial cybersecurity solutions available to protect endpoints, systems and data, malicious actors continue to succeed when attacking email services. In fact, it is not controversial to suggest that virtually every major cyberattack that has occurred in the past few years has involved some type of exploitable weakness in an email account or the improper use of email by some unsuspecting victim as part of the attack path.

With this in mind, below are the major security challenges that businesses of all sizes, types and sectors must understand before making decisions about their email platform. These challenges are not theoretical, but rather emerge based on more than a decade of serious global incidents—ranging from email mishandling by political operatives to phishing weaknesses that led to major enterprise breaches. The primary email security challenges are listed below:

- ***Financial Loss Risk*** — The potential for direct financial loss to institutions, enterprises and even individuals is high with respect to email security threats such as business email compromise (BEC).
- ***Access Risks*** — The potential emerges with email threats that an attacker can gain access to targeted networks and systems by compromising the email accounts of authorized individuals.
- ***Third-Party Risks*** — The risk of suppliers, partners and other third parties being directly or indirectly compromised through email has grown, impacting the security of the entire enterprise organization.
- ***Disclosure Risks*** — Sensitive customer or employee information can be lost, stolen or leaked through public cloud email systems whenever explicit controls are not present to prevent it.

- ***Integrity Risks*** — Information and email attachments can be modified, adjusted or corrupted by individuals and groups with unauthorized access to the cloud email environment.
- ***Disruption Risks*** — The blocking or disrupting of an important workflow or business process step is also a major concern and can be done by manipulating fake emails to corrupt processes such as a funds transfer.

These cybersecurity challenges are significant because they remain present in most contexts, despite the many years of experience enterprise teams have in dealing with email risk. Obviously, new tools are required to address this persistent cyber risk. The sections below provide a summary of the types of email security controls needed to secure the enterprise email environment.

UNDERSTANDING THE EVOLUTION OF CLOUD EMAIL SECURITY

Our present generation of email security has advanced considerably during the transition from early data center-hosted email to modern cloud-based email infrastructure. However, many organizations still lag in this transition and must begin to implement third-generation protection in order to stay secure against from modern attacks..

First-Generation Email Security

The first email security tools emerged in the 1990s when email became a preferred method of communication for businesses and governments. Cybercriminals quickly determined that viruses could be transported for attack propagation, as users at the time believed that inbound email was inherently secure.

Antivirus methods initially relied heavily on the use of attack signatures to detect viruses. Unfortunately, variants were quickly developed to sidestep the detection. This led to a cat-and-mouse game that enterprise teams quickly realized was not sustainable.

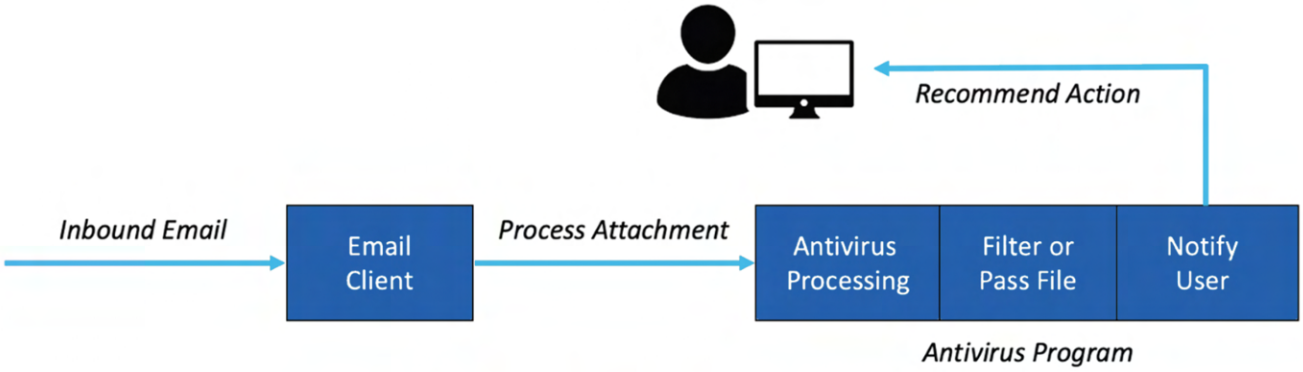

Figure 1. First-Generation Email Virus Attacks

Second-Generation Email Security

Despite the usefulness of antivirus software, the lack of authentication to verify the identity of sender domains soon became a problem. This prompted the eventual launch of Domain-based Message Authentication, Reporting, and Conformance, most popularly known as DMARC.

DMARC allows senders of email to bind their originating IP address to any email carrying their domain. While this was an important step in the evolution of security, it does not stop inbound email threats, particularly those that originate from free webmail addresses which pass DMARC checks—such as Gmail or Yahoo.

The ability to filter URLs and attachments as well as quarantine portals also emerged during this period, which enabled enterprise teams to manage email threats via temporary handling and analysis of emails.

This second generation of email security was characterized by attempts to be more proactive about viruses and malicious links that arrived in a recipient's inbox and was marked by the introduction of the secure email gateway (SEG). The SEG could be placed in line with email store-and-forward paths (via redirection) to provide higher levels of inspection and filtering coverage for emails sent and received.

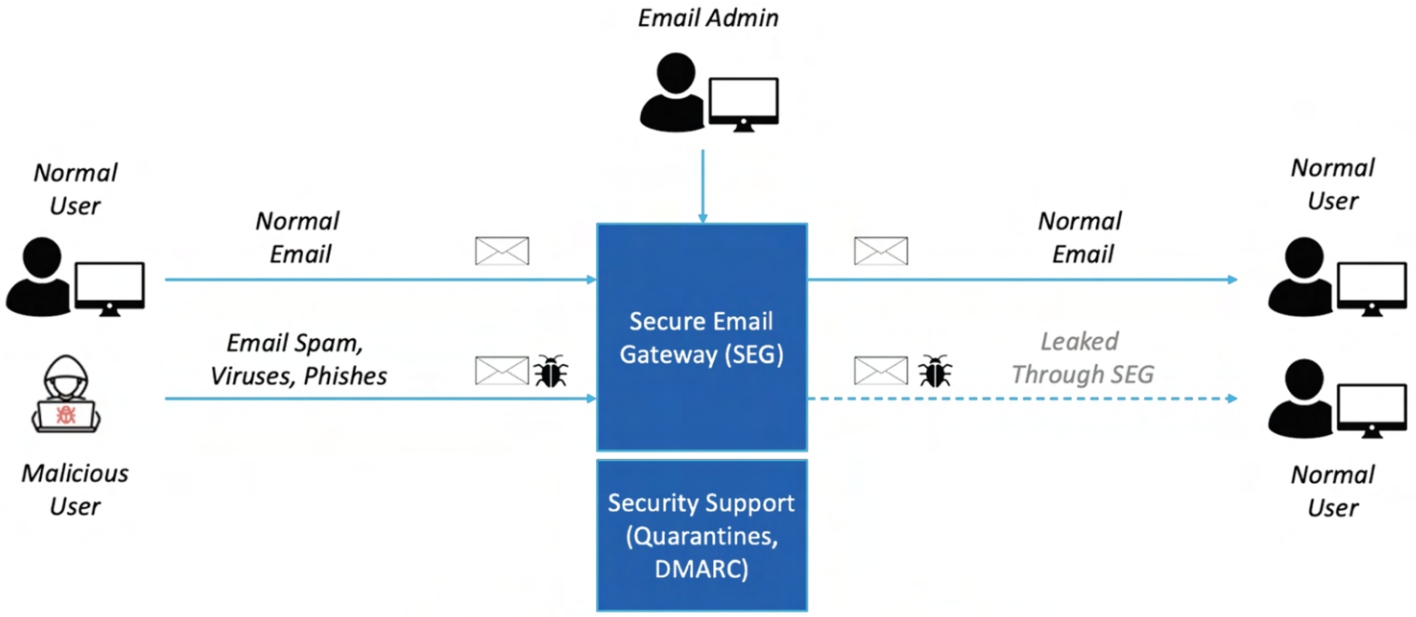

Figure 2. Second Generation SEG Filtering[1]

Third-Generation Email Security

To understand the third and current generation of email security, it is helpful to recognize that attacks have become even more sophisticated since the introduction of the SEG.

Threat actors have moved to highly advanced spear phishing and business email compromise attacks, which use social engineering tactics to impersonate high-profile executives, business associates and vendors. Traditional first- and second-generation email security solutions are incapable of handling the intensity of this threat—particularly when these emails are text-based without traditional indicators of compromise.

Modern, state-of-the-art platforms, which are almost completely built for the cloud email infrastructure, take full advantage of a behavioral approach and generally employ machine learning models that synthesize thousands of identity and behavior signals to assess risk in email. In doing so, they establish known baselines of legitimate communications to identify and block malicious emails—flipping the traditional model of looking only for known bad indicators on its head.

What makes the third generation particularly useful is that organizations can choose to combine it with existing SEGs to augment protection or remove the SEG entirely and rely on the behavioral AI platform for protection. By doing so, security teams have flexibility with both budget and team bandwidth to determine which approach works best for their unique situation and end users.

The ultimate goal for security teams is to establish a good protection architecture using the best commercial solutions available. Such cloud-based security providers should help deploy, implement and support the desired controls.

[1] Our diagram leaves out the actual email service to highlight the security aspect of the process. In addition, one might view our reference to "leaked" email as being "missed," but the reader is welcome to use any designation deemed more locally acceptable.

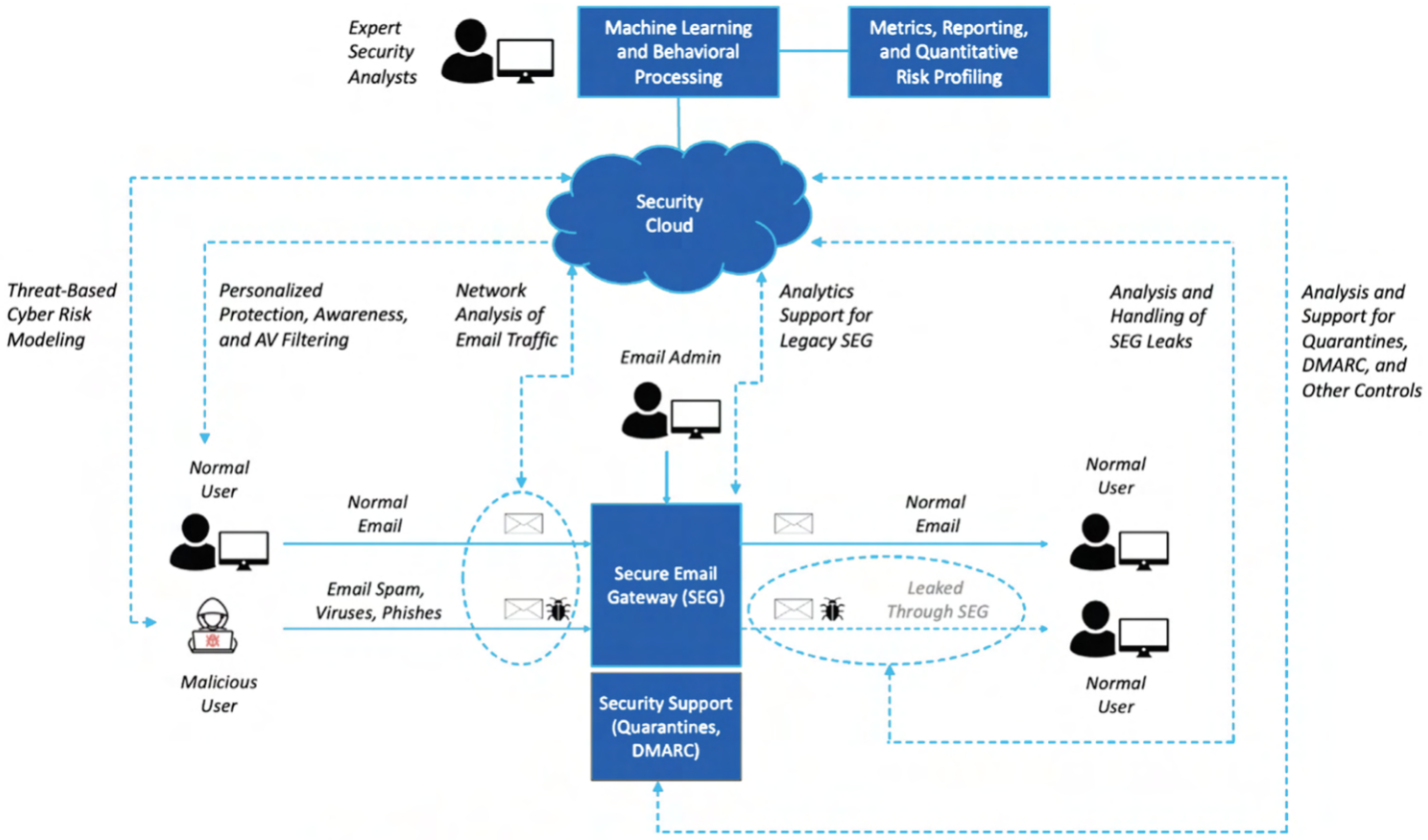

Figure 3. Third-Generation AI-Based Controls[2]

In the next section, we provide detailed guidance in the form of functional requirements and associated questions that buyers can use when selecting a world-class cloud email security platform.

[2] As with our previous diagrams, we focus on the security aspect here and do not represent the underlying elements of the actual cloud or on-premises email service or servers being used.

KEY FUNCTIONAL REQUIREMENTS FOR CLOUD EMAIL SECURITY

To assist with the evaluation process for cloud email security platforms, it helps to identify key functional requirements that connect with the most common enterprise use cases. The following requirements do not comprise a fully complete list, but rather serve as a starting point for locally tailored objectives:

Requirement 1: *Support to tailor detection to local conditions*: Each enterprise has a different network and set of assets that dictate different types of email security risks. A nuclear power company, for example, will have different email risks than an accounting firm. While most cloud-based security tools are industry-agnostic, security leaders should ensure that the vendor can meet their needs.

Requirement 2: *Email security must include third-party risk reduction*: Significant email security risks emerge from supply chain and partner channels. This is especially true for smaller organizations that may not have their own security teams or protection controls. Therefore, cloud email security solutions should have capabilities to address both internal and external threats.

Requirement 3: *Email security must shift both left and right*: Many security solutions focus on pure response to threats under the assumption that they are unavoidable. Good security platforms will actively try to prevent email threats before they occur, using machine learning to detect malicious emails that contain never-before-seen URLs or other indicators.

Requirement 4: *Dwell time for email threats must be addressed*: Modern cyberattacks often involve long dwell times for installed malware. Email security platforms should be cognizant of the techniques and tactics used in advanced persistent threats and have integration partners that can remediate them immediately.

Requirement 5: *Behavioral analytic support is required*: The need exists for algorithms that take user behavior into account when detecting threats. Biometrics in general offer excellent context for recognizing many types of advanced attacks and can be key to understanding when an internal user account has been compromised so it can be remediated immediately.

Requirement 6: *Spam and related fraud and abuse must be handled*: Any selected email security solution should address time-wasting inbound messages. This includes attention to spam and graymail, preferably based on user preference.

Requirement 7: *Email security solutions should help manage cloud-related configurations*: Many cloud email systems need security control assistance for their own user access and authentication support across installed third-party applications and multiple tenants.

VENDOR QUESTIONS TO INCLUDE IN EMAIL SECURITY DISCUSSIONS

To ensure that an organization is getting optimal protection for its cloud email, whether Microsoft 365 or Google Workspace, we offer the following requirements-based questions that are based on practical experience in this area.

The hope is that these questions can be posed to vendors during discovery calls or requests for proposals to reduce cloud email risk as part of the search for third-generation modern cloud email protection:

Question 1: Business Email Compromise *– Does your solution address business email compromise?*
Business email compromise (BEC) is often used as a catch-all term for email threats because it involves many different kinds of attacks such as invoice fraud, impersonation, social engineering and other types of unauthorized email use. These attacks can be difficult to detect because they are often text-based without malicious links or attachments. Cloud email security solutions should thus use other methods to understand when an email is sent from a compromised account or impersonated party.

Question 2: Phishing Risk *– Does your solution provide the means to reduce the risk associated with phishing attacks?*
Every security team understands the need to reduce phishing risks, making this feature essential in a cloud email security solution. Phishing attacks usually involve sending a legitimate-looking email that redirects a victim to a fake website that then steals credentials. Buyers should look for detection approaches that employ natural language processing (NLP)/natural language understanding (NLU) to assess phishing risks in email content.

Question 3: Supply Chain Risk *– Does your solution address supply chain risks that are enabled via email?*
Any cloud mail security platform should include controls that address the security risk associated with third-party suppliers, partners and other external groups. Cloud email security solutions should be able to develop an understanding of each of the organization's vendors and suppliers and offer federated insights about compromised senders that may be targeting multiple customers, recognizing when a third party may be compromised and using that information to detect increased risk.

Question 4: Ransomware Risk *– Does your solution provide a means to reduce the risk of ransomware?*
Ransomware can be delivered in a variety of ways, but the initial attack vector often involves the ransomware being embedded in an inbound email to establish a presence on an endpoint. Cloud email security solutions should therefore address this threat by employing world-class means to detect ransomware in emails and mitigate known vulnerabilities.

Question 5: Malware Risk *– Does your solution effectively identify and remove malware from email attachments?*
It is a well-known requirement that cloud email security solutions must include an effective capability for detecting and removing malware. Buyers should request details on how the vendor does this, including any use of advanced technologies that can safely identify and potentially disarm malware that might be inbound via email to the organization.

Question 6: Account Takeover Risk *– Does your solution support the remediation of compromised user accounts?*
Account takeover (ATO) threats can be accomplished by first stealing credentials to an email account through a phishing or brute force attack. Support for the reduction of ATO risk, and the ability to quickly remediate compromised accounts, is thus a mandatory cloud email security feature that is best achieved using combinations of security controls, including identity and behavioral attributes.

Question 7: Abuse Mailbox Capabilities *– Does your solution support notifications for fraud, abuse and phishing attacks?*
The deployment of fraud, abuse and phishing mailboxes is common for enterprise security teams, and it is wise to optimize the process with as much automation as possible. Useful intelligence is collected via users reporting into these types of mailboxes, so it is imperative to implement such a resource. World-class cloud email security platforms support this feature using automated workflow, analysis, reporting and even mitigation to ensure end-user engagement and provide automated remediation to reduce the time analysts must spend on email discovery and response.

Question 8: Spam and Graymail *– Does your solution filter unwanted mail such as spam and graymail?*
A useful component of modern cloud email security is the automated management of unwanted sales and marketing email solicitations, known as graymail, and widespread spam campaigns. The best cloud email security platforms will use advanced machine learning algorithms that can detect and provide policy-based handling of such messages on a per-user basis. Manual processes to find and delete spam simply do not scale for most organizations, and newer approaches can help security teams avoid this.

PROPOSED ACTION PLAN

The recommended next steps for any enterprise team hoping to reduce the security risks associated with their public cloud email service should include the following:

1. ***Tailor Requirements*** — The requirements offered above should be tailored to include locally relevant functional constraints for email security, including which public email service is being used, whether Microsoft or Google.
2. ***Contact Vendors*** — The questions offered above should also be tailored to provide a suitable means for evaluating pure-play email security vendors to augment protections offered by the public cloud email provider.
3. ***Engage a Platform*** — The platform should be engaged using either a stepwise, gradual introduction or a cutover for the entire email ecosystem. This is an organization-specific decision that will be guided by local IT and security best practices.
4. ***Integrate Visibility*** — The first step in the new platform engagement will be to take full advantage of the visibility offered by the add-on security. This can be integrated into the organization's full security stack including security information and event management.
5. ***Optimize Mitigations*** — Once visibility is established, the organization can engage in more significant controls, including any active mitigation that is included in the selected cloud email security platform.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Abnormal Security. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

TAGCYBER