May 2020

Introducing Cloud Mailbox Defense

Innovating The Way to Protect Office 365 Email

In this issue

Welcome 2

Moving to Cloud Email Platforms; Efficiencies and Hazards 3

Research from Gartner Market Guide for Email Security 8

Welcome

It's increasingly evident that email continues to be the number one threat vector for cyber-attacks. As the primary communication method for business, it remains a security challenge for all organizations regardless of size or how the email platform is deployed. This business-critical function continues to be weaponized. Email attacks are constantly evolving and are more pervasive than ever, forcing businesses to seriously evaluate their security posture. This far too often happens, unfortunately, after a business has been compromised causing negative financial impact, serious productivity loss, or both. For those organizations migrating their email platforms from traditional on-premises deployments to the cloud, an exponentially expanded threat landscape demands a dynamic and effective email security solution.

The 2020 Cisco CISO Benchmark Report validates these concerns from the highest levels of a wide range of organizations. According to the report, the most common causes of downtime are malware and malicious spam.[1]

Cisco Email Security provides a layered email protection which keeps your on-premises or cloud-based email safe and productive by stopping phishing, spoofing, business email compromise and other common cyber threats. It protects against malicious content and prevents attacks and loss of sensitive information.

Comprehensive threat intelligence from Cisco Talos, the largest non-government threat detection team in the world, is the foundation of our product and a key differentiator. While doing threat research and working with third party intelligence organizations, Talos also aggregates security telemetry from most Cisco security products and transforms it into consumable vector-specific intelligence.

Multiple layers of protection mean threats are blocked faster. And, real-time telemetry increases response time to mitigate risks more quickly. Integration into the SecureX platform provides enhanced visibility and automation across the entire Cisco Security product suite providing the protections that ensure businesses function securely.

Source: Cisco

[1] Cisco's 2020 CISO Benchmark Report

Moving to Cloud Email Platforms; Efficiencies and Hazards

Gartner's 2019 Market Guide for Email Security reaffirms that an increasing number of organizations are migrating their email platforms to the cloud. The increased productivity this provides organizations is incredibly valuable. Other benefits include access to up to date tools, reduced maintenance, and a shorter window to consume new features.

According to Gartner, "by 2021, Gartner expects 70% of public and private companies to be using cloud email services."[2] That access to email from anywhere and on any device means it is essential that organizations protect themselves from increasingly prevalent threats. Due to email being such a prominent attack vector, Gartner specifically states that "Security professionals have known for years that, due to its importance as an attack vector, email security requires a layered approach."

Cisco Email Security fully represents this model of protection. Using real time threat intelligence and telemetry from Cisco Talos, Cisco Email Security responds to evolving threats and keeps cloud-based email safe and productive by stopping phishing, spoofing, ransomware, business email compromises and other cyber threats. Additional subscription services provide the complementary layers that create the comprehensive protection the solution provides. Exemplifying Gartner's CARTA approach, these layers address the four key areas of protection and according to Gartner, "Email security refers collectively to the prediction, prevention, detection and response framework used to provide attack protection and access protection for email." These subscription products include multifactor authentication using Duo, Advanced Malware Protection (AMP), Advanced Phishing Protection, Domain Protection and Security Awareness.

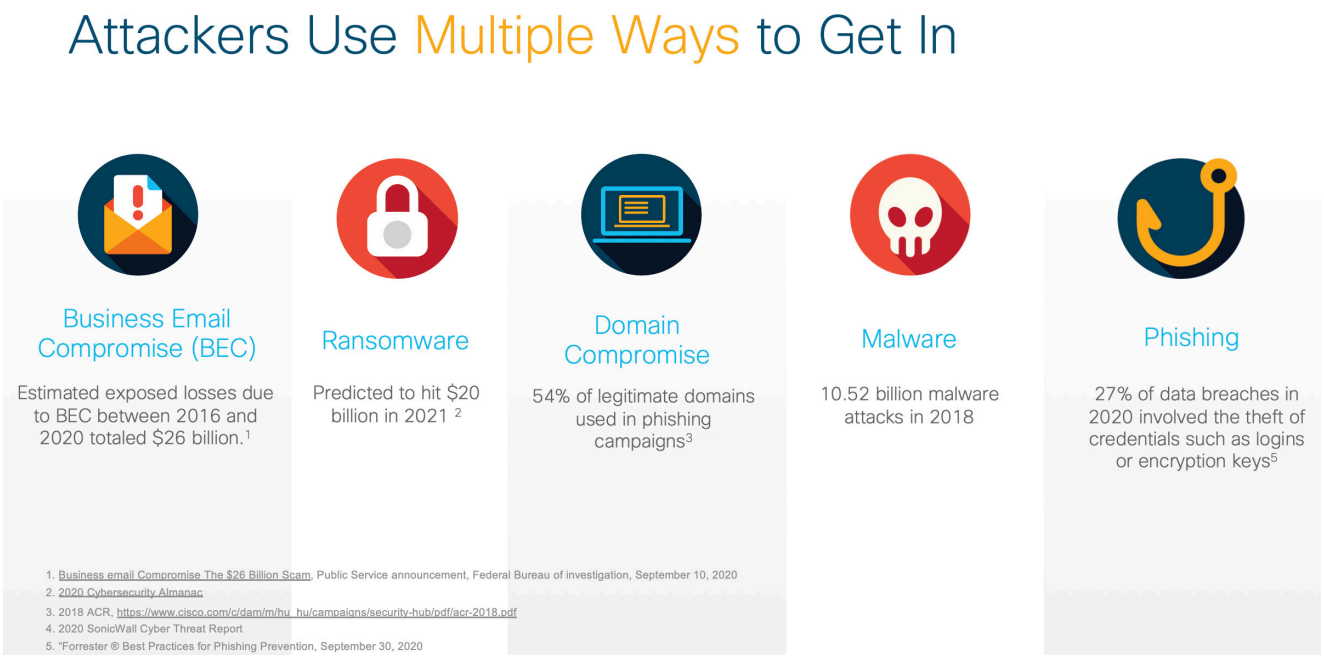
Cisco Email Security mirrors Gartner's guidance of layering inbound, outbound, and internal detection and remediation capabilities.

It's become evident that some cloud email platforms are more vulnerable than others. In fact, according to Gartner, by 2020, 50 percent of organizations using Office 365 will rely on non-Microsoft security tools to maintain consistent security policies across their multivendor "SaaSscape."[3] And, Office 365 account takeover through credential phishing is one of the top three most common email threats.[4]

Cloud Mailbox Defense; Moving Closer to the Mailbox

As more organizations move to Office 365 and allow for a work-from-anywhere approach, scanning every message associated with cloud mailboxes becomes even more important. As security boundaries change, move or retire, we must move security closer to what doesn't change: the email and the inbox. To compound the issue, customers who rely solely on the

Top Email Security Threats



native cloud-based email security, make it easier for attackers to be successful. Attackers now only need to compromise a consolidating security surface.

In the accompanying Market Guide for Email Security, Gartner coined a new market term for email security solutions that provide that additional layer of security – Cloud Email Security Supplements (CESS). CESS solutions are defined as focusing "on specific threats, often in the realm of hard-to-detect phishing and can leverage full access to cloud-hosted inboxes via APIs for detection and remediation." And, it recommends that security leaders, "supplement gaps in the ATD [advanced threat detection] capabilities of an incumbent SEG [Secure Email Gateway] by adding a CESS tailored for this purpose, if replacement is not an option."

Cloud email platforms' core competency is not security. In an effort to provide greater protection for the Office 365 email platform, Cisco developed Cloud Mailbox Defense. This new product offering is an integrated cloud-native security platform for Office 365 that focuses on simple deployment, easy attack remediation, superior visibility, and best-in-class threat intelligence from Cisco Talos. It addresses weaknesses in Office 365 security by blocking advanced email threats like ransomware, business email compromise (BEC), phishing, spoofing and spam by leveraging proven Cisco Email Security technologies.

Full conversation and message trajectory views allow insight into email traffic within your O365 mailboxes, thereby providing better contextual information needed to make an appropriate judgement. Cloud Mailbox Defense will provide a full, graphical email conversation stack showing the entire scope of compromised messages – whether inbound, outbound, or internal user-to-user messages.

According to Gartner's recent Business Email Compromise report, they recommend upgrading SEG solutions to include internal email protection.[5] Specifically, Gartner suggests that a Cloud Email Security Supplement be added to existing cloud email solutions like Office 365.

Cloud Mailbox Defense Defined

Cloud Mailbox Defense can quickly remediate threats – either automatically or manually – using the most modern and effective tools available without interrupting the regular delivery of messages. Leveraging the advanced, mature and stable email security products that Cisco's customers rely on for their ongoing security, Cloud Mailbox Defense imbeds these features into O365.

Cloud Mailbox Defense is built using modern, open APIs to allow flexible integration into an organization's email administration, security operations, and incident response processes.

Cloud Mailbox Defense provides simplified and effective security with:

- **Lower total cost of ownership and higher SOC productivity**
  Cloud Mailbox Defense is designed with simplicity in mind. Because there are no required changes to mail flow, it can be deployed without the administrative overhead of altering MX records

or email architecture. Because the configuration is minimal and the interface so intuitive, no specialized training is required, and operations can immediately triage and remediate threats.

- **Protection against account takeover attacks**
  Because Cloud Mailbox Defense scans and remediates against internal messages, we can spot lateral movement and internal malware propagation that can occur after an account takeover. Outbound malware and spam is given the highest priority and administrators are alerted immediately when this type of behavior is detected.

- **Direct Integration with Microsoft's Cloud**
  Cloud Mailbox Defense allows organizations to augment native Office 365 security controls by leveraging the industry leading security intelligence of Cisco Talos. By integrating directly with Microsoft's cloud, we can bring Cisco security as close to the mailbox as possible. Further integration with SecureX provides visibility across the entire Cisco Security portfolio and increases automation.

Cloud Mailbox Defense Use Cases

- Efficacy improvement
  - Traditional SEGs not only lack visibility into user-to-user traffic, but also the ability to protect it. Cloud Mailbox Defense extends protection past the perimeter to achieve both.
- Protecting organizations of all sizes.
  - For those smaller organizations with limited resources to allocate toward email security, Cloud Mailbox Defense simplifies the experience and provides a format that requires little prior knowledge or oversight. Larger organizations can benefit from the increased intelligence provided by Cloud Mailbox Defense in combination with their existing SEG; whether with Cisco Email Security or another solution.
- Simplifying mail flow
  - A traditional SEG has a complex set of controls – which many organizations need. But, with that robust feature set comes the need for specialized knowledge and another system to maintain. With Office 365 and Cloud Mailbox Defense only, the entire process is simplified – with all mail flowing through Office 365 · and, can be managed by the existing Office 365 administrator.
- Ensuring compliance and privacy
  - Using Cloud Mailbox Defense's architecture, full email message content never leaves Azure. Only metadata (e.g. sender, recipient, subject) leave the Azure environment to be searched. This maintains a strict level of compliance and customer privacy.

Calls to Action

Cisco Cloud Mailbox Defense is uniquely positioned to lead in the CESS space.

Learn more about Cisco Email Security and Cloud Mailbox Defense at cisco.com/go/emailsecurity

---

[2] Gartner, Market Guide for Email Security, 6 June 2019, Peter Firstbrook, Neil Wynne
[3] Gartner: How to Enhance the Security of Office 365 (2017)
[4] Gartner, Market Guide for Email Security, (2020)
[5] Gartner, Protecting Against Business Email Compromise: March 19, 2020

Research from Gartner

Market Guide for Email Security

Large-scale migration of email to the cloud has necessitated a strategic shift in how to secure this communication channel. Security and risk management leaders must adopt a continuous adaptive risk and trust assessment mindset to protect inboxes from exposure to increasingly sophisticated threats.

Key Findings

- The adoption rate and gravitational pull of Google and Microsoft toward their respective cloud office systems is forcing security and risk management leaders to evaluate every product in their email security architectures against the native capabilities these vendors claim to provide.
- Impersonation and account takeover attacks are increasing and causing direct financial loss, because users place too much trust in the identities associated with incoming email and are inherently vulnerable to deception and social engineering. This growing problem can only be reduced through education, social graph impersonation filtering, improved indicators of identity in email and suspicious email workflow.
- The email security market is starting to adopt a continuous adaptive risk and trust assessment (CARTA) mindset and acknowledge that perfect protection is not possible. As a result, vendors are evolving or emerging to support new detect and response capabilities by integrating directly with the email system via API.

Recommendations

Security and risk management leaders responsible for email security should:

- Adopt a CARTA strategic approach to email security by layering inbound, outbound, and internal detection and remediation capabilities.
- Leverage incumbent email security products by verifying and optimizing their capabilities and corresponding configurations. This will serve as the start of a gap analysis to determine where supplementation or replacement may be required.
- Address gaps in the advanced threat defense capabilities of an incumbent secure email gateway (SEG) by adding a cloud email security supplement (CESS) tailored for this purpose, if replacement is not an option.
- Invest in user education and implement standard operating procedures for financial and sensitive data transactions commonly targeted by impersonation attacks.

Strategic Planning Assumptions

By 2023, 65% of organizations will inspect their intradomain email traffic for advanced threats, which is a major increase from 7% in 2019.

By 2022, at least one major secure email gateway (SEG) vendor will "end of life" its on-premises components.

Market Definition

Email security refers collectively to the prediction, prevention, detection and response framework used to provide attack protection and access protection for email. Email security spans gateways, email systems, user behavior and various supporting processes, services and adjacent security architecture. Effective email security requires not only the selection of the correct products, with the required capabilities and configurations, but also having the right operational procedures in place (see Note 1).

Market Description

Email is the most commonly used channel for opportunistic and targeted attacks, as well as a significant point of egress for sensitive content. Thirty-two percent of breaches covered in the 2019 Verizon Data Breach Investigations Report involved phishing, and 94% of malware incidence was delivered via email.[1] Attacks have evolved from massive distribution of standard malware to a combination of more-sophisticated techniques to achieve the attacker's objectives. To achieve their goals, attackers can quickly change their tactics. They will adapt distribution to the best spam botnets, use attachment types that best evade detection and change message body content to best convince recipients to act. Common controls, such as standard, reputation-based, anti-spam and signature-based antivirus, are fine for widespread attacks and scam campaigns, but they're not good enough for protection against more-targeted, sophisticated and advanced attacks. More than ever, modern email security requires innovation and a shift in mindset to combat the evolving threat landscape.

Market Direction

Cloud Office Adoption and Duopoly

Enterprise adoption of cloud office systems — for which cloud email is a key selling point — is now mainstream (see Note 2). By 2021, Gartner expects 70% of public and private companies to be using cloud email services.[2] Google's G Suite and Microsoft's Office 365 have created a cloud office duopoly — a market almost entirely dominated by two vendors. Cloud mail is accessible from any device and any location, leaving inboxes potentially exposed. Organizations that want to limit access to managed devices, Internet Protocol (IP) geolocations or other forms of adaptive access must find the right balance between increasing security and inhibiting the users from leveraging the benefits of a widely accessible email product.

As Google and Microsoft exert a strong gravitational pull in the cloud office market toward their respective suites, we are seeing this force two major market changes.

Organizations Are Evaluating All Products in Their Email Security Architectures Against the Native Capabilities That Google and Microsoft Claim to Provide

Microsoft Office 365 includes Exchange Online Protection (EOP) with all plans. EOP is an anti-spam, anti-phishing and anti-malware service. Microsoft also offers Office 365 Advanced Threat Protection (ATP) to add more anti-phishing capabilities, as well as advanced attachment and URL-based threat defense. Office 365 ATP is included in some pricing plans and available for others as an extra cost option. Furthermore, data loss prevention (DLP), email encryption and enterprise digital rights management (EDRM) are available in some pricing plans. This enables organizations to monitor, encrypt, block or apply rights management to messages based on policy (see "What You Need to Know About Security in Office 365" in the Gartner Recommended Reading section).

Google G Suite natively provides anti-spam, anti-phishing, signature-based anti-malware, and — only in the Enterprise and Education plans — DLP capabilities in Gmail for inbound and outbound email, along with Secure/Multipurpose Internet Mail Exchange (S/MIME) for outbound encryption. It also offers several settings that can be used to enhance protection against advanced URL-based attacks and domain and display-name-spoofing impersonation tactics. G Suite is beta testing network sandboxing capabilities to thwart advanced malware-based threats, although these will ultimately be available only to customers on the G Suite Enterprise and G Suite Enterprise for Education editions. Gmail Confidential Mode enables the application of several EDRM capabilities to messages (see "What You Need to Know About Security in G Suite" in the Gartner Recommended Reading section).

Despite Google's and Microsoft's continued investment in G Suite and Office 365 security improvements, some Gartner clients report dissatisfaction with natively available capabilities and are, therefore, choosing to supplement with third-party products, as discussed in the Representative Vendors section.

The Market for On-Premises Email Security Products Continues to Shrink

As more organizations accept and become familiar with cloud platforms, the demand for on-premises

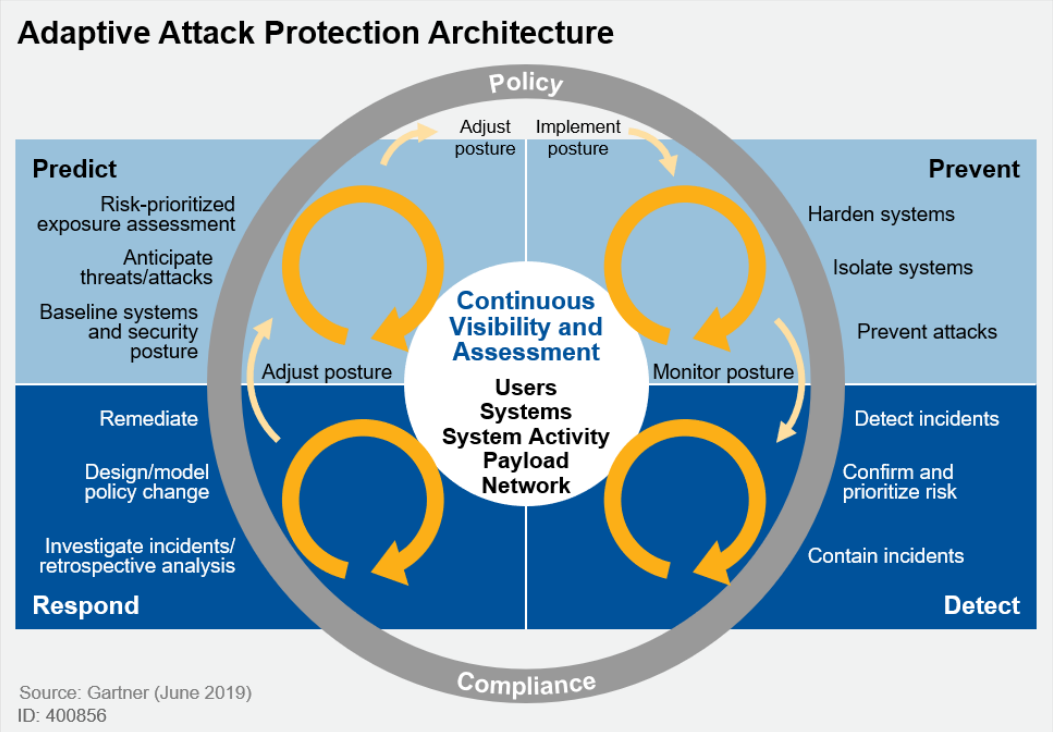
products has diminished. Traditionally, the two main concerns about cloud deployment are availability and security. Google and Microsoft consistently demonstrate acceptable availability (often better than can be achieved on-premises) and have long streaks with no major security breaches. This goes a long way toward assuaging those concerns.

Organizations that have migrated to cloud email and those that are planning a migration are overwhelmingly choosing cloud-delivered email security products. Vendors can harness the processing power of the cloud for better defense against advanced threats, while incorporating proper due diligence and numerous control attestations to satisfy most regulatory and privacy concerns. Of course, some organizations with unique requirements will continue to keep SEG implementations on-premises, due to residual privacy, data sovereignty, legal, integration support and network design concerns.

Adopting a Continuous Adaptive Risk and Trust Assessment Mindset

The email security market has begun to adopt a continuous adaptive risk and trust assessment (CARTA) mindset in response to the dissolving perimeter (see Figure 1). CARTA is a strategic approach to security that balances security friction

Figure 1. Adaptive Attack Protection Architecture



with transaction risk. A key component of CARTA is continuous assessment of risk and trust, even after access is extended. At its core, CARTA is an acknowledgment that perfect attack prevention, perfect authentication and invulnerable applications were never possible. In the futile pursuit of perfection, security infrastructure and processes became constraining and cumbersome, slowing down the organization and the speed of innovation.

Positioned in front of the email system, SEGs have been the traditional email security perimeter. However, increases in account takeover attacks and an acknowledgment that perfect protection is not possible, have amplified the interest in intradomain email protection. Attackers are increasingly seeking authenticated access to mailboxes, which they can use to phish other users in the same email system, bypassing perimeter security. Moreover, as attackers become more sophisticated, email admins are realizing that a second layer of complementary detect and response capability may be necessary. As a result, products are evolving and new vendors are emerging to provide detect and response capabilities that integrate directly with the email system.

Via API access, these products inspect the email server or archives for threats that may have evaded perimeter security and remove malicious messages from inboxes. In addition, a detect and response mindset requires a focus on the workflow to rapidly address user-submitted suspicious emails. As organizations increase user education as part of a balanced effort to thwart phishing attempts, the volume of user-generated submissions can overwhelm security operations centers (SOCs), resulting in increased demand for automated workflow and end-to-end submission resolution process.

The velocity and creativity of attacks will continue to grow, and attackers will exploit a variety of tools, tactics and techniques against an ever-increasing diversity of targets to achieve a growing range of goals. In a CARTA-inspired email security architecture, security controls are always monitoring, assessing, learning and adapting, based on the relative levels of business risk, threat intelligence and trust that are observed.

Mobile Device Prevalence

The use of mobile devices for email affects the risk of email threats as well. Many VIP users are power users of email on mobile devices, and they consider this as an ideal way to communicate quickly and around the clock. The use of mobile devices for email is good news for preventing some attack techniques. Because well-maintained mobile devices are less susceptible to malware than traditional endpoints, the impact of malicious attachments and URLs is less critical. Nevertheless, mobile device users are at least as susceptible as, and arguably even more susceptible than, full desktop users to attacks such as credential phishing and business email compromise (BEC).

The most important negative effect of the use of mobile devices on email security is client application limitations. Both the email clients and the browsers used on mobile devices make it hard for users to check for phishing indicators. Gartner strongly recommends including mobile devices explicitly in awareness programs.

Market Analysis

Email is the most commonly used attack vector in targeted attacks and untargeted attacks. Even if many attacks need other channels (typically the web) for full compromise of a client endpoint, in most cases, email is the first to deliver:

- The initial URL, in the form of a link to an exploit kit or phishing website
- The attachment, in the form of a dropper or payload
- The starting point for a social engineering attack, such as in the case of BEC or credential phishing attacks

Email threats have become sophisticated to evade detection by common email security technologies, particularly those that rely only on standard antivirus and reputation. Email threats are also being blended, combining social engineering, identity deception, phishing sites, malware and exploits. Note 3 discusses the reasons for the popularity of email among attackers. Note 4 provides examples of three common email threats.

Security and risk management (SRM) leaders must revisit their organizations' email security architecture in the light of current email threats, such as sophisticated malware, links to exploit kits, credential phishing and BEC. Security professionals have known for years that, due to its importance as an attack vector, email security requires a layered approach. However, only a few vendors innovate their products at a pace that is similar to the attackers'. Even when vendors have innovated, their customers have often failed to deploy the latest versions in a timely fashion to mitigate the latest threats.

Technology innovations should be complemented by investments in security awareness training, especially to combat email threats that are payloadless (that is, they don't contain an attachment or a URL). Organizations should simulate attacks via anti-phishing behavioral conditioning (APBC), measure, and provide training and notification to users. User awareness is not 100% effective, of course, but neither is such awareness an optional layer. Educated users can form an effective defense against many email threats, including some of the more sophisticated ones. SRM leaders should document an email security policy, covering the sensitivity of corporate email addresses and what the intended use of corporate email is. Make notification of suspicious email messages as easy as possible, and strive for a culture that has a healthy distrust of email messages.

Differentiating Capabilities

The following capabilities can be used as primary differentiators and selection criteria for email security products. Due to the lack of independent testing, SRM leaders should conduct a thorough proof of concept (POC) in vendor selection (see Note 5).

To Protect Against Attachment-Based Advanced Threats

Network Sandbox

A network sandbox is used to inspect attachments and URLs that cannot be identified as benign or malicious using other methods. The network sandbox should

cover an extensive set of file types (including zip, wsf, js and macros that are commonly used in attacks) and embedded URLs. In addition, it should have strong anti-evasion capabilities. It should also accurately identify malware that attempts to detect that it is being run in a virtualized sandbox environment.

Content Disarm and Reconstruction

Content disarm and reconstruction (CDR) is also referred to as "content sanitization." It breaks down files into their discrete components, strips away anything that doesn't conform to that file type's original specification, ISO standard or company policy, and rebuilds a "clean" version. This near-real-time process is an effective and efficient approach to removing malware and exploits from files. Although sandboxing and almost all other techniques depend on detection, CDR protects against exploits and weaponized content that have not been seen before.

To Protect Against URL-Based Advanced Threats

URL Rewriting and Time-of-Click Analysis

Rewrite URLs before they are delivered to the user for stronger protection than time-of-delivery URL inspection. This can be used to:

- Disarm the URL (i.e., turn it into a nonclickable version of the URL)
- Replace with text (e.g., "embedded URL removed for security reasons")
- Redirect the URL to the URL inspection service for time-of-click analysis protection

URLs in attachments are generally left untouched by most SEGs, although several have this on their product roadmaps.

Web Isolation Services

Redirected URLs can also be directed to a special type of secure web gateway (SWG), which is typically referred to as an "isolation service." Similar to CDR, SWGs proxy web transactions and reformat content to remove any security risks and provide a clean rendering of the website content to the client browser. Users can interact with the website; however, active content is executed in a remote server, and only clean content is rendered to the user.

To Protect Against Impersonation and Social Engineering Tactics Used in URL-Based, Attachment-Based and Payloadless Advanced Threats

Display Name Spoof Detection

This detects spoofed messages based on email headers and the sender names. Some products support the fuzzy matching of sender names with a list of names that the email security administrator can predetermine — typically, a list of VIPs (such as senior executives) likely to be targeted. Other solutions use a social graph to monitor all sender recipient relationships and seek near-match deviations combined with keyword analysis of commonly used keywords in BEC attacks.

Domain-Based Message Authentication, Reporting and Conformance on Inbound Email

This enforces domain-based message authentication, reporting and conformance (DMARC) on inbound email traffic to protect internal users from receiving spoofed external messages from domains that have implemented DMARC in rejection mode. This also checks the alignment of the domains used in message header FROM and SMTP envelope MAIL FROM email addresses.

Lookalike Domain Detection

This detects the use of lookalike domains, also referred to as "cousin domains." Most, if not all, SEGs allow administrators to include a list of lookalike domains that should be flagged. Some products do fuzzy matching on domains to detect such scams, whereas others require customers to upload their own lists of lookalike domains.

Anomaly Detection

This detects anomalous messages, based on sender, recipient, envelope, content, history and other context to thwart BEC and account takeover attacks. Threats increasingly fly under the radar of traditional, reputation-focused and signature-based products. Anomaly detection may be able to identify these more-sophisticated attacks. Using email telemetry/intelligence enables non-rule-based detection of spam and phishing, even if few messages are sent.

Anomaly detection leverages three main ingredients. The first is metadata, which includes the reputation of the sender address, sending domain and IP — global, as well as for the organization. It also includes the identity deception attempts of sender (lookalike, reply-to, etc.), and authentication (e.g., Sender Policy Framework [SPF], DomainKeys Identified Mail [DKIM] and DMARC evaluation). The second is content — typically, a specific activity request with some urgency, attachments and URLs. Content may be detectable, because it is reused across organizations; however, this is typically not the case in targeted attacks. The third ingredient in anomaly detection is historic communication: What was the typical communication between this sender and recipient and their domains?

Additional Differentiating Capabilities

Anti-Phishing Behavioral Conditioning

As phishing-based attacks continue to become more sophisticated and evade even advanced machine-learning-based, anti-phishing technologies, end-user training becomes more important to provide a human layer for protection. APBC focuses on reducing the frequency with which employees click on URLs in phishing emails. Although each vendor provides a unique offering, the basic approach is the same:

- Phishing emails are sent to employees.
- Employees who click on the URLs therein are immediately pushed into a computer-based training (CBT) session.
- URL click rates are recorded for longitudinal trend analysis.

The use of APBC as part of a security awareness program is important to help identify key pockets of risk in the enterprise audience, deliver social

engineering attacks, and provide just-in-time training and teachable moments. However, SRM leaders must understand that there is no end to this program.

Attack strategies change quickly — the bad actors are always several steps ahead — and the audience needs continuous reinforcement in this area. The frequency should be monthly at least, and potentially greater for higher-risk profiles (see "Three Critical Factors in Building a Comprehensive Security Awareness Program" in the Gartner Recommended Reading section).

Graymail Handling

This is an area in which many SEGs require further investment. Most products can identify graymail — that is, solicited bulk email messages that the recipient "opted in" for at some point in the past. However, many lack methods for end users to configure the handling of these messages, based on their individual and subjective preferences. Favor products with secure unsubscribe features. Some attacks masquerade as graymail and hide a malicious URL in a seemingly innocuous unsubscribe link. Products may offer a safe unsubscribe capability that effectively replaces the links in such messages with a secure one.

Data Protection

Outbound email security features (e.g., DLP, email encryption and EDRM) are critical for intellectual property protection and regulatory compliance (such as Payment Card Industry [PCI] and Health Insurance Portability and Accountability Act [HIPAA] data). These capabilities should be weighed appropriately in buyer analyses. Although they can be used separately, DLP and encryption are typically used in a complementary approach. Users should be provided with readily available email encryption options that empower them to make the right decision when handling sensitive data via email. However, if they inadvertently or intentionally fail to do so, then the DLP inspection engine for outbound messages can block or remediate this as a fail-safe.

Postdelivery Protection and M-SOAR

Organizations should evaluate vendors that have added detection and response capabilities to address threats that were not initially caught by the SEG and were allowed to land in a user's inbox. Using API integrations with cloud email systems (such as Office 365) or plug-ins for email clients (such as Outlook), these vendors can attempt to "claw back" a malicious message by removing it from the user's inbox after initial delivery. This message may have already been opened by the user. Hence, the product should also be able to alert relevant personnel and products (e.g., administrators, SOCs, endpoint detection and response [EDR] or security information and event management [SIEM]) about potential compromises for remediation or recovery. As interoperability among products improves, automated remediation actions can be taken in real time to decrease incident response time and the level of human effort required.

The challenge of security analysts spending a significant part of their time on phishing investigation and response has resulted in an interesting evolution

of capabilities to help improve this. Most security orchestration automation and response (SOAR) vendors have some form of phishing response playbooks. Generic SOAR products often require adjustments and integrations with SIEM and email security products to become effective tools for SOC analysts. With the exception of mature SOCs, the use of full, generic SOAR for phishing incident response is costly and difficult — therefore, it's rare.

As an alternative to full-featured SOAR products, email security vendors have begun to offer orchestration and automation tooling focused on email. These mail security orchestration, automation and response (M-SOAR) capabilities are characterized by:

- A focus on email threats
- Less orchestration focus — Even though some vendors do this too, most M-SOAR is focused on the vendor's product and email platform
- Simplicity — They are simpler to use and to buy than SOAR, and they often come as an additional license to SEG or other email security products

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

A list of representative vendors (see Note 1) is provided in the categories described below. This is not, nor is it intended to be, a list of all the vendors or offerings in this market. It is not, nor is it intended to be, a competitive analysis of the vendors discussed. Several vendors provide email security capabilities that span multiple categories. However, each vendor is listed only once in what Gartner considers to be its predominant category, based on market perception, customer usage and product heritage.

SEGs

For inbound email threats or outbound exfiltration attempts, SEGs continue to be the front line of defense for one of the largest attack surfaces. This remains true, even as many organizations migrate their email to the cloud. SEGs are expected to provide a versatile and broad range of capabilities that, at a minimum, should include the following:

- A message transfer agent (MTA), as well as API-based modes for intradomain message scanning and remediation
- Anti-spam and signature-based anti-malware
- Marketing and graymail classification, as well as personalized controls for management of these types of messages
- Network sandboxing and/or CDR for advanced, attachment-based threat defense
- Rewriting and time-of-click analysis for advanced, URL-based threat defense
- Context inspection, display name spoof, lookalike domain and anomaly detection for advanced, impostor-based threat defense

- DLP and email encryption (pull/push methods beyond Transport Layer Security [TLS]) for outbound content to satisfy corporate and regulatory policy requirements
- Cloud-based delivery

Some products may also offer email continuity and archiving, as well as on-premises and hybrid delivery model architectures. Some SEG vendors have integrated APBC capabilities into their products, primarily through acquisition (see Note 6 for notable examples).

Global SEGs (see Table 1) have broad geographic distribution of their customers, as well as their sales, support and data center coverage.

Table 1. Representative Vendors for Global SEGs

Vendor
Barracuda
Cisco
Forcepoint
Fortinet
Google
Microsoft
Mimecast
Proofpoint
Symantec
Trend Micro
Source: Gartner (June 2019)

Regionally focused SEGs (see Table 2) have their predominant business operations and customer bases in the same geographic regions, particularly in Europe. Gartner anticipates that these vendors will continue to expand their geographic reach.

Table 2. Representative Vendors for Regionally Focused SEGs

Vendor
Censornet
Clearswift
Kiwontech
Retarus
Spamina (part of the Hornetsecurity Group)
Source: Gartner (June 2019)

Cloud Email Security Supplements

Cloud email security supplements (CESSs) focus on specific threats, often in the realm of hard-to-detect phishing, and can leverage full access to cloud-hosted inboxes via APIs for detection and remediation. Most of these products focus on phishing, but some go well beyond to include sandboxing and URL rewriting/time-of-click analysis, thereby directly competing with SEGs. Some CESS vendors claim to be replacing SEGs; however, for most organizations, the SEG remains the workhorse of their email security architecture. Generally, the use of a SEG is preferred because it stops inbound attacks closer to the attacker. This prevents unwanted email from taking up bandwidth and storage, and its processing does not compete with the processing of the email system. (See Note 7 for situations in which a CESS can provide substantial additional security.)

When considering a CESS, carefully assess the features and deployment options, because they can vary widely (see Table 3). SRM leaders should be aware of the differences between the in-line SEG approach and products that leverage APIs to integrate with the inboxes in cloud email systems (see "How to Build an Effective Email Security Architecture").

Table 3. Representative Vendors for CESSs

Vendor
Agari
Area 1 Security
Avanan
Cyren
GreatHorn
Graphus
Inky
IRONSCALES
Perception Point
Vade Secure
Source: Gartner (June 2019)

APBC

With the increase in email threats that fly "under the radar" (that is, attacks that leverage smart social engineering and identity deception techniques), user awareness training is a significant component in any successful email security architecture. Email security awareness — referred to as "anti-phishing behavioral conditioning" (APBC) — trains users through attack simulations, the measurement of results, and training and notification. Users should be trained to spot identity deception and phishing attempts by carefully analyzing the email sender address, reply-to address, embedded URLs, attachments and specific calls to action. Most vendors (see Table 4) offer a user-friendly, phishing-reporting function within their email clients. A subset of these vendors offers technologies to assist with triaging reported messages.

Table 4. Representative Vendors for APBC

Vendor
Cofense
Infosec Institute
Inspired eLearning
KnowBe4
MediaPRO
PhishLabs
Terranova Security
Source: Gartner (June 2019)

Email Data Protection Specialists

Email was never designed to be a secure communication medium, and organizations continue to struggle to protect sensitive email content in transit and at rest. Email data protection products protect the confidentiality and integrity of email messages by enabling the transmission of sensitive information to intended recipients with the starkly reduced possibility of disclosure or alteration. Although more than 60% of client organizations leverage the DLP and email encryption capabilities of an SEG, there can still be a need for specialist products, particularly for customer-facing use cases in which a frictionless experience is critical (see Table 5).

Table 5. Representative Vendors for Email Data Protection Specialists

Vendor
DataMotion
Echoworx
Egress Software Technologies
Tessian
totemo
Virtru
Zix
Source: Gartner (June 2019)

Market Recommendations

SRM leaders responsible for email security should do the following:

- Adopt a CARTA strategic approach to email security by layering inbound, outbound, and internal detection and remediation capabilities. In a CARTA-inspired email security architecture, security controls are always monitoring, assessing, learning and adapting, based on the relative levels of business risk, threat intelligence and trust that is actually observed. Implementing CARTA will be a multiyear journey. Prioritize intradomain message protection as an important starting point. There are many account takeover scenarios in which an attacker can leverage intradomain messages to move laterally and compromise internal resources. Without some way to effectively scan intradomain emails, these attacks could affect the organization. Protect against internal spread using technologies that integrate with the email system (cloud and/or on-premises).
- Fully leverage incumbent email security products by verifying and optimizing their capabilities and corresponding configurations. This can serve as the start of a gap analysis to determine where, if any, supplementation or replacement may be required. Required capabilities may already be available from your SEG vendor, for example, but you may need to purchase a license for the additional features. Many of the rules and settings in email security products need continued maintenance and verification to ensure that new attacks are blocked.
- Supplement gaps in the ATD capabilities of an incumbent SEG by adding a CESS tailored for this purpose, if replacement is not an option. Not all SEG vendors include best-of-breed ATD capabilities. Furthermore, many organizations are not able to pursue a “rip and replace” approach, due to the implications for DLP and email encryption. These are typically separate initiatives that are tied to business processes and stakeholders, so they add additional time to a technology migration. Should this be the case for your incumbent SEG, consider supplementing it with a product that provides additional protection.
- Prioritize vendors that directly address the human element by using APBC. Choose vendors that offer this capability natively or have integration opportunities with security awareness vendors. For example, a click on a URL may immediately initiate a redirect to a short training/awareness session. Also, users that are recipients of more targeted attacks should receive, even if all attacks are blocked, more focused attention from awareness campaigns.

- Assess business requirements for DLP email encryption and EDRM over the next three years, and evaluate products accordingly. Although it is not optimal, DLP capabilities from SEGs or email data protection specialists can be implemented independently of enterprise DLP to satisfy email-specific aspects of regulatory compliance, enforce acceptable usage or enable automatic email encryption. For IP protection, however, buyers of email-centric DLP capabilities must understand how they integrate with a more holistic enterprise data management strategy.

- Adopt a multipronged approach that spans technical, procedural and educational controls to achieve effective mitigation of malicious messages, such as phishing attacks. (Refer to the Gartner Recommended Reading section for the latest "fighting phishing" research, which discusses the full scope of the inbound phishing threat and identifies effective mitigation strategies.)

Evidence

The findings and recommendations in this research were derived from more than 1,250 Gartner client interactions from June 2017 through May 2019 on the topic of email security.

[1] Verizon 2019 Data Breach Investigations Report

[2] "Public companies' unstoppable march to cloud continues with almost 25% — of any size, industry and region — having moved to a cloud email platform. Application leaders can use this research to evaluate Google G Suite and Microsoft Office 365 as cloud email solutions, and to guide deployment plans." (See "Survey Analysis: Cloud Email Adoption Growth Continues but With Large Regional/Industry Variations.")

Note 1. Representative Vendor Selection

Representative vendors were selected on the basis of one or both of the following:

- Client interest via searches on Gartner.com and inquiries about that vendor for email security

- Vendors that are offering email security capabilities in ways that are unique, innovative and/or demonstrate forward-looking product strategies

Note 2. Cloud Office Systems

Cloud office systems include creative, collaboration, communication, social, coordination and data services, along with APIs that enable integration with other systems. Microsoft Office 365 and Google G Suite are the primary examples. At a minimum, cloud office systems include capabilities for email, social networking, file synchronization and sharing, document creation and editing, screen sharing, IM, audioconferencing, and videoconferencing. Most buyers start with a subset that includes email. The broad term "cloud office systems" is a generic label. The term "Microsoft Office" refers to a specific range of products from Microsoft.

Note 3. The Popularity of Email as a Target for Attackers

There are various reasons for the popularity of email among attackers:

- **User trust:** Email is massively used by consumers and businesses. Many users have an abundant trust in senders, message body content, links and attachments. For many users, the sheer volume of messages received is too high to spend a huge amount of time checking everything. Therefore, people tend to open and consume quickly, and generally do not report issues.

- **Inexpensive:** Sending masses of unsolicited email messages can be achieved at low cost. It is possible to hire a 10,000-node bot for few hundred dollars. In addition, there are thousands of free email services for attackers to choose from if they want to conduct nonautomated attacks.

- **Usable for most attack types:** Email can be untargeted and opportunistic (as spam is), but also lends itself well to targeted attacks.

- **Elusive:** Mailboxes and domains can be registered by anyone accessing the internet, and attackers leverage many techniques to evade detection by email security products. For example, they may change sender IP addresses quickly and spread attacks across many senders to remain undetected.

- **Vulnerable:** Attackers abuse inherent weaknesses in protocols and email technology. Spoofing sender names and domains is trivial in many ways. For example, email senders are typically not authenticated, and the reply-to address need not equal the visible sender address. Moreover, most email clients lack clear visual indicators of good or bad email messages or sender reputation. This complicates the verification of received messages, even for aware users.

Note 4. Examples of Three Common Email Threats

Threat No. 1. Ransomware Spreading Through Spam: The first example of a quite-common email threat is ransomware. Not all ransomware spreads through email — we see some attackers using exploit kits through web drive-by and adware. However, some of the most successful ones have relied on email, and many are expected to do so in the future.

Locky is a well-known family of ransomware that successfully spreads through spam. To spread, Locky hitches a ride with spam campaigns, sometimes targeting millions of inboxes in a single day. Typical spam campaigns show great spikes of activity, sometimes due to a new ransomware campaign. Locky does not use identity deception.

The payload for these example ransomware families is typically carried in the form of attachments; however, the types of attachments change over time. Attackers choose the types that are most successful at infecting the machine. Although earlier versions of Locky used Word files with macros (which served as the downloader for the actual payload), later versions carried the whole attack in a compressed archive attachment with malicious scripts. Of course, the body

of the message is intended to entice the user to open the attachments and, optionally, enable macros or conduct other follow-up actions to install the malware. For that purpose, attachments often appear to be invoices from well-known organizations.

Common, widespread ransomware can be blocked by the SEG, the email server security product and the endpoint. The true multilayer defense-in-depth architecture will be effective against widespread ransomware attacks in attachments.

For completely new types of attacks, the assessment is slightly different. Advanced countermeasures in the form of network sandboxes, URL rewriting, CDR or file type whitelisting may be required to block such attacks. Advanced endpoint security technologies may catch some of these at the last layer of defense.

In addition to technologies, aware users play a significant role in the protection against widespread attacks, but an even more significant role for more-sophisticated attacks.

Threat No. 2. BEC: The second example is BEC, a threat also referred to as "business email spoofing" or "CEO fraud." The best-known example of BEC consists of messages seemingly originating from a VIP user, targeting an internal employee and requesting wire transfer. Other BEC scams have gone after W2 forms for subsequent tax return fraud, unpublished financial reports and other sensitive information. BEC scams are typically set up cleverly, spoofing email names, using lookalike domains, communicating at awkward times, citing a message history and using convincing arguments.

BEC is one of the fastest-growing email security threats for a few reasons. First, it flies under the radar for many technical detection techniques. It is low-volume and highly targeted, and attacks generally do not leverage attachments or URLs that could indicate its nefarious objectives. Second, attacks pay off. Even though attackers have to spend time on activities such as identifying targets (long live social media), writing personalized messages (no more bad spelling) and copying branded signatures of actual messages, the reward for a successful scam is usually quite high. Examples of such scams have been documented and run in the tens of millions of dollars.

Compared to ransomware, the situation for protection against BEC looks bleak. Strong SEG and email server security products combine sender reputation with outlier anomaly detection, content analysis, lookalike domain detection and recipient relevancy to detect and tag such messages. Organizations' SEGs that do not have these capabilities will need a replacement. Or they should use a gateway focused on BEC detection as an additional layer of defense or a BEC detection product that integrates with the email server. The user, as in the previous scenario, plays a significant role.

Other countermeasures fall out of scope for technical controls, but are powerful for BEC prevention. Standard operating procedures, also commonly referred to as "internal controls," greatly reduce the risk of BEC. Incorporate segregation of duties and out-of-band verification for specific calls to action that involve financial processes (such as wire transfers) or sensitive information (e.g., W2 forms).

Threat No. 3. Office 365 Account Takeover Through Credential Phishing: The final example is a threat that is becoming increasingly popular among attackers. The attacker sends phishing emails to Office 365 users. Users who fill out their credentials have their mailboxes taken over, and the attack spreads laterally within the organization and to others related to the victim. Because the messages seem to originate from a trusted sender and are executed by human attackers, these messages are hard to distinguish from genuine messages.

SEGs, especially the ones with time-of-click protection that go beyond malware and exploits and effectively check for phishing sites, can play a role. Often, URL assessment at time of click requires a sandbox to detect advanced phishing attacks.

Integrated protection, because it has historical data on communication patterns, can use its social graph to flag anomalous messages as suspicious. It will not always be able to pre-emptively block such messages. Products can also use APIs to analyze and correlate anomalous login events with communication patterns.

Because an increasing number of organizations are targeted by, or have already fallen victim to, account takeover attacks, it is important for SRM leaders to swiftly implement preventive measures. These include requiring two-factor authentication for mailbox access and adaptive access for managed devices across all email clients.

Note 5. Using a POC in Email Security Product Selection

Don't overreact if the POC process of the incoming vendors shows large-scale improvements over the incumbent product. One of the largest challenges faced in the email security market is difficulty in building reliable, independent, recurring email protection testing, in particular with spam and phishing detection. There are no reliable monthly tests for spam and phishing results of all the top vendors, as compared with anti-malware tests provided by organizations such as AV-TEST or Av-Comparatives. SE Labs periodically tests several email security products, but not on a monthly basis, and focuses mainly on malware and phishing. The challenges are vendor participation, as well as the ability to come up with current and relevant spam and phishing samples.

During POCs, ensure that your incumbent product has all the ATD capabilities enabled and properly tuned. The new products should not be scanning quarantine, deleted, spam or other folders where you are possibly storing emails that have malware, spam or phishing emails for possible false positive detection. Another consideration to factor into the POC process is how the testing is being done — in-line or parallel (journaling).

Note 6. Notable APBC Acquisitions by SEG Vendors

- Ataata has been acquired by Mimecast.
- Blackfin has been acquired by Symantec.
- Phishline has been acquired by Barracuda.
- Wombat Security has been acquired by Proofpoint.

Note 7. Situations in Which a CESS Can Provide Substantial Additional Security

A CESS is a viable, additional line of defense for an organization that:

- Requires on-demand scanning of mailboxes, generally as a secondary scan at low-use times
- Wants to quickly manage outbreaks that spread through email
- Demands detection methods that use historical communication patterns (for example, to build social graphs in defense against phishing)
- Has substantial intradomain email traffic without routing through an SEG
- Uses applications that have programmatic access to the mail server
- Has users who regularly post messages in public folders
- Does not use an SEG

Gartner Research Note G00400856, Neil Wynne, Peter Firstbrook, Published 6 June 2019

Contact us

For more information contact us at:

cisco.com/go/cmd