Market Guide for Email Security

Published 7 October 2021 - ID G00735200 - 19 min read

By Mark Harris, Peter Firstbrook, **and 2 more**

Continued increases in the volume and success of phishing attacks and migration to cloud email require a reevaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for the changing landscape.

Overview

Key Findings

- The adoption of cloud email systems continues to grow, forcing security and risk management leaders to evaluate the native capabilities offered by these providers.
- Solutions that integrate directly into cloud email via an API, rather than as a gateway, ease evaluation and deployment and improve detection accuracy, while still taking advantage of the integration of the bulk of phishing protection with the core platform.
- Vendor consolidation and integration with other security tools enable improved detection and response capabilities (aka extended detection and response [EDR]).
- Ransomware, impersonation and account takeover attacks are increasing and causing direct financial loss, as users place too much trust in the identities associated with email inherently vulnerable to deception and social engineering. The evolution in threats has led to increased demand for other techniques and services, such as domain-based message authentication, reporting and conformance (DMARC), cloud access security broker (CASB)/API integrations, continuous awareness and mail-focused security orchestration, automation and response (MSOAR).

Recommendations

Security and risk management leaders responsible for email security should:

- Use email security solutions that include anti-phishing technology for business email compromise (BEC) protection that use AI to detect communication patterns and conversation-style anomalies,

as well as computer vision for inspecting suspect URLs. Consider products that also include context-aware banners to help reinforce security awareness training.

- Invest in user education and implement standard operating procedures for handling financial and sensitive data transactions commonly targeted by impersonation attacks. Remove as many targeted ad hoc processes from email as possible.
- Take advantage of emerging APIs to Integrate email events into a broader XDR or security information and event management (SIEM)/security orchestration, analytics and reporting (SOAR) strategy.
- Ensure that email is included in your data protection strategy by examining the types or data shared externally via email and putting appropriate controls in place.

Strategic Planning Assumptions

By 2023, at least 40% of all organizations will use built-in protection capabilities from cloud email providers rather than a secure email gateway (SEG), up from 27% in 2020.

By 2025, 20% of anti-phishing solutions will be delivered via API integration with the email platform, up from less than 5% today.

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, content security, 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.

Market Description

Email security covers a wide range of capabilities and solutions. This Market Guide focuses on three main types of email security solutions (see Figure 1).

- **SEG:** Email security for both inbound and outbound email has traditionally been provided by SEG solutions either as an on-premises appliance, a virtual appliance or a cloud service. SEGs process and filter SMTP traffic, and require organizations to change their MX record to point to the SEG.
- **Integrated cloud email security (ICES):** The adoption of cloud email providers (Microsoft and Google) that provide built-in email hygiene capabilities is growing. Advanced email security capabilities are increasingly being deployed as integrated cloud email security solutions rather than as a gateway. These solutions use API access to the cloud email provider to analyze email

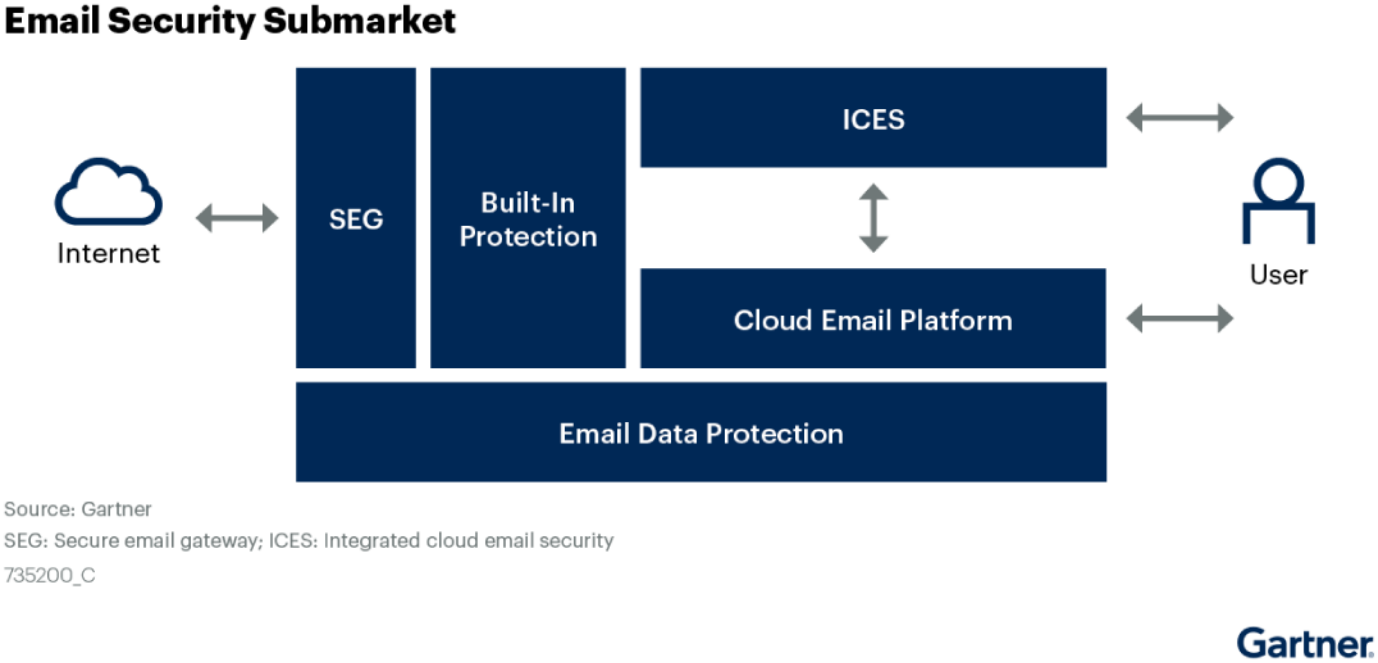
content without the need to change the Mail Exchange (MX) record. Integrated solutions go beyond simply blocking known bad content and provide in-line prompts to users that can help reinforce security awareness training, as well as providing detection of compromised internal accounts. Initially, these solutions are deployed as a supplement to existing gateway solutions, but increasingly the combination of the cloud email providers' native capabilities and an ICES is replacing the traditional SEG.

- **Email data protection (EDP)**: Email is fundamentally unsecure, and email data protection solutions add encryption to track and prevent unauthorized access to email content before or after it has been sent. EDP can also help prevent accidental data loss due to misdirect recipients.

Adjacent markets that often overlap with email security and are not covered by this Market Guide include:

- Security awareness training
- Information archiving
- Email continuity services

Figure 1: Email Security Submarket



Market Direction

Cloud adoption continues, with an estimated 70% of organizations using cloud email solutions (see Note 2). The recent HAFNIUM attack on Microsoft Exchange Servers and the move to remote

working has added to the growth. Microsoft and Google dominate the market and continue to enhance and improve the built-in capabilities that they provide.

Microsoft, in particular, has made significant investments in improving protection effectiveness and providing better configuration guidance. This makes it harder for SEG vendors to differentiate, especially as comparing detection rates is difficult and time-consuming, with very few independent tests of effectiveness. It is possible to evaluate Microsoft Defender for Microsoft 365 to compare the incumbent third-party solution versus Microsoft. But this is only half the evaluation, because it doesn't identify what was stopped by the existing solution that wouldn't have been blocked by Microsoft.

Integrated solutions that use APIs to examine emails are gaining momentum, augmenting either an existing SEG offering or the built-in protection. Many of these solutions use sophisticated anomaly detection techniques like natural language understanding (NLU), natural language processing (NLP) and image recognition. The direct integration makes these solutions easy to evaluate and prove value, and because they are behind any existing controls, the value can be seen quickly (see Note 3). The solutions also benefit from visibility of internal traffic and can use historic email history to quickly build machine learning baselines for improved detection.

Rather than specifically focus on simply blocking, solutions now include conditional banners that inform users to help them make decisions. This reinforces security awareness training and simplifies reporting suspect messages across all device types. Increasingly, MSOAR capabilities are offered to rapidly triage user-reported phishing messages as a managed service, either directly from the vendor or through a managed security service provider (MSSP).

With the shift to remote and hybrid working, communication is moving beyond just email to include collaboration tools such as Microsoft Teams and Slack with users outside the organization. These have the potential to be used by attackers for phishing and malware distribution. Several vendors' solutions can use their API integrations into such collaboration platforms to filter malicious content or suspicious interactions.

Inbound threats are the main driver for implementing email security, but outbound data loss, especially accidental data loss (misdirected emails) is increasingly a concern. Indeed, human error remains the most common reason for email data breaches. Compliance and privacy concerns go beyond simply blocking outbound personally identifiable information (PII) and can include reputation damage from careless distribution of intellectual property (IP). Solutions that use machine learning (ML) to analyze communication patterns to prevent inbound phishing are also being used to detect potentially misdirected emails.

Most email today is transport-level encrypted between mail systems; however, as more sensitive information is shared, the need to secure that communication in the message store becomes increasingly important. Email encryption tools have been available for a long time, but have only been

adopted by about 40% of organizations. SEGs commonly include encryption, but the usability differs greatly. Newer solutions that provide end-to-end encryption prioritize usability.

Market Analysis

Email continues to be a significant attack vector for both malware and credential theft through phishing. An estimated 40% of ransomware attacks start through email. [1] As the threat changes, it's important to reevaluate the capabilities and effectiveness of the current solution compared to new products. This is especially true as the incumbent solution may not be investing in new detection technologies.

Compare Existing Capabilities With Native Capabilities Provided by Google and Microsoft

Both Google and Microsoft provide the basic email hygiene capabilities, including:

- Blocking emails from known bad senders
- Scanning attachments with AV
- Blocking emails with known bad URLs
- Content analysis to identify spam

While Google Workspace has less sophisticated controls and fewer features, the simple three-tier model is very appealing to many organizations that have chosen Google Workspace as their collaboration platform. Microsoft's licensing can be complex, and the E5 license that contains Microsoft Defender for Microsoft 365 is expensive. However, there are various different bundles and add-ons that can be used to add the advanced capabilities. Exchange Online Protection (EOP) is included in all plans and provides the basic anti-spam, anti-phishing and anti-malware capabilities.

Microsoft has continued to invest in Microsoft Defender for Office 365, which includes more-advanced protection capabilities including safe links and safe attachments, and integrates with the other security tools from Microsoft. It also covers Microsoft SharePoint, Teams and other Office clients. Eighty percent of organizations are looking to consolidate security vendors, and the close integration between Microsoft 365, Microsoft Azure Active Directory (Azure AD), Microsoft Information Protection and Microsoft Defender for Endpoint can provide improved overall visibility and security, and forms part of Microsoft's XDR strategy.

Other security vendors are also making investments in email security capabilities as part of their own XDR strategy. Cisco, F-Secure, Kaspersky, Trend Micro and others have all recently updated or added email security components. Often, these are API-based ICES solutions.

Several email security vendors are also investing in integration with other security tools such as endpoint protection platforms (EPPs), endpoint detection and response (EDR), SIEM and SOAR. These provide a set of APIs that not only allow the sharing of information, but also can initiate response and remediation actions.

SEGs

SEGs are still the most common deployment of email security. SEGs are deployed as an appliance or a virtual appliance, but most often as a cloud service. SEG solutions provide the basic email hygiene capabilities as well as more advanced protection capabilities, such as:

- URL rewriting
- Multi-AV scanning
- Sandbox integration
- Spam quarantine with end-user digests
- Graymail handling
- Impersonation protection for key individuals (CIO/CFO)
- Postdelivery clawback

SEGs also provide outbound capabilities such as:

- Data leakage prevention for compliance, either blocking or reporting PII being sent
- Email encryption, transport layer security (TLS), or push or pull encryption.
- Large message sending, through a secure portal, often linked to the encryption

DMARC prevents exact name domain spoofing aimed at employees, partners and customers, but can be complicated depending on the size and number of domains in an organization. Professional services are often needed to assist with implementation and ongoing monitoring of DMARC. Some vendors also offer adjacent services like email archiving, continuity services and security awareness training.

A number of SEG vendors have added, or are in the process of adding, API-based integrations either as alternatives or enhancements to existing solutions, allowing for better visibility into internal email, the ability to add context-aware banners, and creating relationship graphs and ML models to improve detection.

Integrated Cloud Email Security

As built-in security from Microsoft and Google has improved, threat actors are also getting more sophisticated, often targeting them using fake login pages as a way of harvesting credentials. Sophisticated email threats include compromised websites and weaponized documents used to deploy malware. Many ransomware-as-a-service gangs use email as the initial entry point. Beyond malware, business email compromise and account takeover threats continue to rise, with significant financial losses as a result. These are often very difficult to detect because they contain no links or attachments and rely on social engineering to defraud the recipient. In the case of account takeover, there isn't even any indication in the message headers, so, for all intents and purposes, it's a legitimate email.

To combat these, email security solutions use a variety of more-advanced detection techniques, including NLU, NLP, social graph analysis (patterns of email communication) and image recognition.

Previously, Gartner separated API products into two categories: cloud email security supplements (CESSs) that focused on specific threats to enhance existing predelivery solutions, and integrated email security solutions (IESSs) that implemented more of the traditional controls found in an SEG. This distinction is no longer needed as the supplement solutions have now grown to have a more complete set of functionality. ICES products can be predelivery or postdelivery depending on which APIs are used. Predelivery is usually implemented as a connector and intercepts email before it reaches the user's inbox. Postdelivery analyzes emails after they have been delivered, and some products effectively "hide" the message to prevent the user opening it before it is scanned, while others simply rely on being able to scan the email before the user reads it. Postdelivery can be implemented using APIs on their own or a combination of APIs and journaling.

ICES solutions go beyond simply blocking email, adding context-aware banners warning users. This means that the threshold for false positives can be higher and can also reinforce security awareness training. Often, a mechanism for reporting phishing is included, either as part of the email client or as another banner inserted into the email body. Emails reported by the user can then be processed by MSOAR tools to assist in the automatic reclassification of emails and removing them from inboxes. Although this simplifies the processing of reported emails, it can still put a burden on overstretched IT security teams, and a number of vendors now offer this MSOAR capability as a managed service, as well as integrating into other SOAR tools.

ICES tools are able to move messages into built-in classification mailboxes, such as "Promotions" or "Junk" folders. Some are able to learn or modify classification based on whether a user moves a message from one folder to another, thus removing the need for complex policy management.

Data Protection

Data leakage prevention rules have been part of SEGs for many years: Emails can be blocked, redirected or encrypted based on analysis of their content. These capabilities are often part of a wider DLP portfolio. The pandemic has led to an increased reliance on email as a communication method, requiring more than simple gateway data protection. The ability to secure, track and

potentially redact sensitive data shared in email with partners, clients and/or customers becomes important, especially in light of continued regulations and privacy laws.

Although email encryption has been available for many years, the workflow is often very poor, meaning open rates of encrypted emails are historically low. Authenticating the recipient has always been the challenge, requiring users to create new accounts on messaging portals and leading to very poor open rates. With the widespread adoption of cloud email, authenticating users that are on the same platform (e.g., Microsoft 365) has simplified the process, but as soon as recipients are on different platforms, the issue remains.

A number of vendors focused on email data protection are looking to address this with simplified workflows and second-factor authentication. Secure messaging portals that store sensitive information separate from email is one solution, but that raises questions over data residency and where the keys are stored.

Email also continues to be the most common cause of data breach, especially accidental data loss. Misdirected recipients are the primary cause. Few solutions exist to specifically address this, but with the growth of ML/AI models to analyze emails for BEC, the same technology is being applied to detecting and warning users of misdirected emails. These warnings are either in the email client as the user is composing the email, or are sent as a “bounce” message requiring the user to confirm that the intended recipient is correct. Bounce messages are not as user-friendly, but they don’t require a plug-in to the email client to be deployed and managed, and the same workflow exists on mobile devices.

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 (see Table 1, Table 2 and Table 3). This is not, nor is it intended to be, a list of all the vendors or offerings in this market. It is also 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. Where appropriate, the high-level capabilities of each vendor are included; however, these capabilities are included for reference only and have not been ranked.

A companion tool is also available that includes a larger set of 56 representative vendors and their capabilities (see Tool: Vendor Identification for Email Security).

Table 1: Representative SEG Vendors

Vendor	Product Names
Barracuda	Barracuda Total Email Protection Barracuda Essentials Barracuda Sentinel Barracuda PhishLine Barracuda Forensics and Incident Response
Cisco	Cisco Secure Email Cloud Mailbox Cisco Secure Email Cloud Gateway Cisco Secure Email Gateway Cisco Secure Email Phishing Defense Cisco Secure Email Domain Protection Cisco Secure Email Encryption Service Cisco Secure Awareness Training
FireEye	FireEye Email Security (Server Edition) FireEye Email Security (Cloud Edition)
Fortinet	FortiMail Cloud — SaaS FortiMail — Virtual Machines FortiMail — Appliances
Microsoft	Exchange Online Protection Microsoft Defender for Office 365 Plan 1 Microsoft Defender for Office 365 Plan 2
Mimecast	Mimecast Perimeter Defense Mimecast Comprehensive Defense Mimecast Pervasive Defense

Vendor	Product Names
Proofpoint	P0 Core Threat Protection P1 Advanced Threat Protection P1+ Complete Threat Protection Proofpoint Enterprise Data Loss Prevention Proofpoint Managed Service for Email Security
Sophos	Sophos Email Sophos Email Advanced
Broadcom (Symantec)	Symantec email security.cloud Symantec Email Threat Detection and Response Symantec messaging gateway
Trend Micro	Trend Micro Cloud App Security with XDR Trend Micro Email Security Smart Protection for Office 365 Trend Micro XDR for Users Deep Discovery Email Inspector

Source: Gartner (October 2021)

Table 2: Representative ICES Vendors

Vendor	Product Names
Abnormal Security	Abnormal Integrated Cloud Email Security Platform

Vendor	Product Names
Agari	Agari Phishing Defense Agari Phishing Response Agari Brand Protection Agari Active Defense
Area 1 Security	Area 1 Horizon
Armorblox	Inbound Email Protection Outbound Email Protection
Avanan — A Check Point Software Technologies Company	Advanced Anti-Phishing Complete Malware Full-Suite Protection
Clearedin	Clearedin Cloud Email Security for Microsoft 365 Clearedin Cloud Email Security for Google Workspace Clearedin for File Sharing Clearedin for Slack Clearedin for Microsoft Teams
Darktrace	Darktrace Antigena Email Darktrace for Ransomware Darktrace for Microsoft

Vendor	Product Names
GreatHorn	GreatHorn Email Security Platform GreatHorn Account Takeover Protection GreatHorn Mailbox Intelligence GreatHorn Extended Monitoring Managed Services
INKY	INKY Phish Fence INKY Internal Mail Protection
IRONSCALES	Ultimate Core Core+
Perception Point	Advanced Email Security Advanced Internal Email Security Email Security Bundle Advanced Collaboration Security
Tessian	Tessian Human Layer Security Platform Tessian Defender Tessian Guardian Tessian Enforcer Tessian Human Layer Risk Hub Tessian Human Layer Security Intelligence
Vade	Vade for M365

Source: Gartner (October 2021)

Table 3: Representative EDP Vendors

Vendor	Product or Service Names
Echoworx	Echoworx Email Encryption
Egress	Egress Defend Egress Prevent Egress Protect
Trustifi	Trustifi Outbound Shield Trustifi Inbound Shield Trustifi Email Account Compromise Detection
Zivver	Zivver Secure Email and Secure File Transfer
Zix	Secure Cloud

Source: Gartner (October 2021)

Market Recommendations

SRM leaders responsible for email security should:

- Look for email security solutions that use ML- and AI-based anti-phishing technology for BEC protection to analyze conversation history to detect anomalies, as well as computer vision to analyze suspect links within emails.
- Include API-based ICES solutions when evaluating email security solutions. The simplicity of evaluation and additional visibility into internal traffic and other communication channels can reduce risk.
- Invest in user education and implement standard operating procedures for the handling of financial and sensitive data transactions commonly targeted by impersonation attacks. Reinforce

this training with context-aware banners and in-line prompts to help educate users. Ensure that user reports are acted on by using MSOAR solutions.

- Integrate email events into a broader XDR or SIEM/SOAR strategy by choosing vendors that have integrations with these security tools through APIs.
- Implement DMARC for protection against domain spoofing attacks.
- Don't rely on email as a way of carrying out secure transactions and sensitive data sharing by implementing data protection solutions.

Evidence

The findings and recommendations in this research were derived from more than 1,400 Gartner client interactions between June 2020 and June 2021.

[1] Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority, Coveware.

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 client inquiries about that vendor for email security
- Vendors offering email security capabilities in ways that are unique, innovative and/or demonstrative of 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 365 and Google Workspace 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: Using a POC in Email Security Product Selection

Don't be surprised if the proof of concept (POC) process of the incoming vendors shows large-scale improvements over the incumbent product. In the case of an SEG, the order in which the vendors are evaluated is important, if the solution is placed after the incumbent, it will always appear to catch

more. However, there is no guarantee that it would catch everything that the current solution does. ICES solutions are much easier to evaluate, but are always “second,” so will show benefits, but it’s important to determine the false positive rates as well. If the solution includes context-aware banners, they should not be too “noisy”; otherwise, the benefits diminish.

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 advanced threat detection (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).