Gartner Reprint

Clip source: Gartner Reprint

Perception Point Analyse 2023 Gartner

Market Guide for Email Security

Published 13 February 2023 - ID G00760247 - 21 min read

By Ravisha Chugh, Peter Firstbrook, **and 1 more**

The migration to cloud email platforms continues along with a significant increase in the number of phishing attacks. Security and risk management leaders should evaluate the native capabilities offered by cloud email systems and ensure that they are adequate to prevent sophisticated attacks.

Overview

Key Findings

- As organizations continue to adopt cloud email systems there is a shift in communication beyond email to other collaboration platforms introducing threats that may not be protected by incumbent email security tools.
- Impersonation and account takeover attacks via business email compromise (BEC) are increasing and causing direct financial loss, as users place too much trust in the identities associated with email, which is inherently vulnerable to deception and social engineering.
- Vendor consolidation and integration of email security with other security tools (such as security service edge [SSE] and endpoint detection and response [EDR]) enable improved detection and response capabilities of security threatsas part of an extended detection and response (XDR).

Recommendations

As a security and risk management leader responsible for email security, you should:

- Supplement the native capabilities of your existing cloud email solutions with third-party security solutions, to provide phishing protection for collaboration tools and to address both mobile- and BEC-type phishing scenarios.
- Use email security solutions that include anti-phishing technology for targeted BEC protection that use AI to detect communication patterns and conversation-style anomalies, as well as computer vision for inspecting suspect URLs. Select products that can provide strong supply chain and AI-driven contact chain analysis for deeperinspection and can detect socially engineered, impersonated, or BEC attacks.
- Prioritize integration of email security solution APIs to enable integration of email events into a broader XDR or security information and event management (SIEM)/security orchestration, analytics and reporting (SOAR) strategy.

Strategic Planning Assumptions

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

By 2026 credential loss will be the No. 1 effect of phishing attacks.

Market Definition

This document was revised on 20 March 2023. For more information, see the Corrections *page on gartner.com.*

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 solutions provide both inbound and outbound email security by blocking phishing attacks and preventing data exfiltration. The core capability of an email security solution includes spam protection, malware protection, malicious links and attachments protection, and BEC protection. Many can also address outbound email security use cases through email data loss prevention (DLP) and email encryption capabilities. Additional capabilities include security awareness training, domain-based message authentication reporting and conformance (DMARC), and email encryption.

This Market Guide focuses on three main types of email security solutions (see Figure 1):

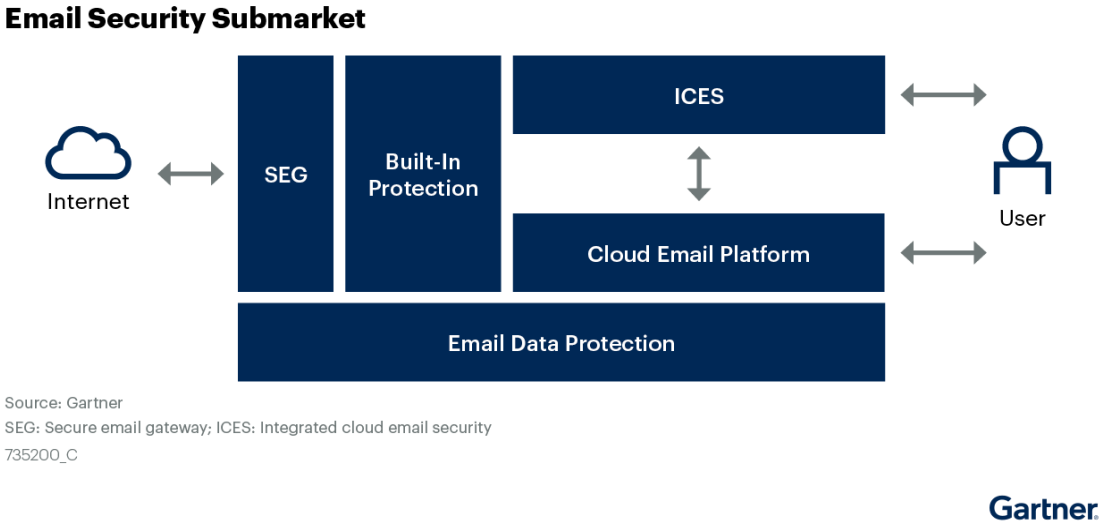
- **Secure email gateway (SEG) —** Email security for both inbound and outbound email has traditionally been provided by SEG solutions either as an on-premises appliance, a virtual appliance or a cloud service. SEGs process and filter SMTP traffic, and require organizations to change their Mail Exchange (MX) record to point to the SEG.
- **Integrated cloud email security (ICES) —** The adoption of cloud email providers (e.g., Microsoft and Google) that provide built-in email security hygiene capabilities is growing. Advanced email security capabilities to supplement these native 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 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 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 misdirected 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

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]Cloud adoption continues, with an estimated 70% of organizations using cloud email solutions (see Note 1). Microsoft and Google continue to dominate the market and the capabilities they provide are decent but insufficient for some sophisticated attacks.

Microsoft, in particular, continues to make 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 effectiveness tests. It is possible to evaluate Microsoft Defender for Office 365 against other incumbent third-

party solutions. But this is only half the evaluation because it doesn't identify what was stopped by the existing solution that Microsoft wouldn't have blocked.

Integrated solutions that use APIs to examine emails are gaining momentum, augmenting either an existing SEG offering or the built-in protections. 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 existing controls, the value can be seen quickly (see Note 2). The solutions also benefit from visibility of internal traffic and can use historic email history to quickly build machine learning (ML) baselines for improved detection. Recently, some SEG vendors like Proofpoint and Mimecast have also started to provide ICES solutions and claim to provide enhanced artificial intelligence (AI)/ML capabilities. However, there is no additional capability that these vendors provide in comparison to other core ICES vendors. IBM's Cost of a Data Breach 2022 Report highlighted that 19% of total data breaches are due to compromised and stolen credentials resulting in an average of $4.5 million losses.[2] So, most ICES vendors also focus on account takeover detection and remediation.

Increasingly, mail security orchestration automation and response (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). In addition, most of the 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.

With the shift to remote and hybrid working, communication is moving beyond just email to include collaboration tools such as LinkedIn,MicrosoftTeams, Slack etc., with users outside the organization. Attackers can potentially use these for phishing and malware distribution. Although email is still the most common attack vector, many attackers use emails to begin the communication and then move it to Slack, Teams or any other collaboration platforms. Several vendors' solutions can use their API integrations into collaboration platforms to filter malicious content or suspicious interactions. Many of these solutions use ML and NLU capabilities to analyze the communications across multiple channels and prevent attacks.

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 ML to analyze communication patterns to prevent inbound phishing are also being used to detect potentially misdirected emails.

Most email today uses transport-level encryption between mail systems, but 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 due to usability issues. SEGs commonly include encryption, but the usability differs greatly. Newer solutions that provide end-to-end encryption prioritize usability.

Market Analysis

Compare Existing Capabilities With Native Capabilities Provided by Google and Microsoft

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

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

Google Workspace offers a simple three-tier model which 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 Office 365 is expensive. However, there are various different bundles and add-ons that can be used to add 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 integration 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 Purview Information Protection and Microsoft Defender for Endpoint can provide improved overall visibility and security, forming 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,Trend Micro and others have all recently updated or added email security components. Often, these are API-based ICES solutions.

SEGs

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

- URL rewriting
- Multi-antivirus (AV) scanning
- Sandbox integration
- Spam quarantine with end-user digests
- Graymail handling
- BEC protection
- 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 domain name spoofing aimed at employees, partners and customers, but deployment, configuration and maintenancecan be challenging depending on the size and number of domainsin an organization. Professional services are often needed to assist with the 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 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 the end users 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 typically 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. ICES solutions also provide account takeover protection which analyzes user behaviors and various other factors such as login behavior, locations, authentication methods etc. They detect and alert which account has been compromised and take remediation actions if required. Remediation may include blocking the account, password reset or other customer-defined playbooks etc.

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 from opening it before it is scanned. 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, by 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. A number of vendors now offer this MSOAR capability as a managed service, as well as integrating it into other SOAR tools.We also see that there is a requirement of privacy and legislative laws for security products in mainland China (see Note 3).

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.

Email 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 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. Several 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 data breach vector, especially for accidental data loss. Misdirected recipients are the primary cause. Few solutions exist to specifically address this, but with the growth of AI/ML 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.

Another common risk is sensitive information stored in email repositories. Attackers and malicious insiders can directly exploit the emails stored in the email servers of Microsoft and Google. Vendors such as Material Security solve this issue by identifying and redacting the messages containing sensitive data in the mailboxes. Further, users can access redacted emails on demand after an authentication step. This helps in managing the risk of data loss from stored email.

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

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

A list of representative vendorsis 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.

A companion tool is also available that includes a larger set of 42 representative vendors and their capabilities (see Tool: Vendor Identification for Email Security).

Table 1: Representative SEG Vendors

Vendor	Product Names

Barracuda Networks	Barracuda Email Protection Advanced Barracuda Email Protection Premium Barracuda Email Protection Premium Plus Barracuda Email Gateway Defense Barracuda Impersonation Protection Barracuda Incident Response Barracuda Security Awareness Training
Broadcom (Symantec)	Symantec Email Security.cloud Symantec Email Threat Detection and Response Symantec Messaging Gateway

Cisco	Cisco Secure Email Threat Defense Cisco Secure Email Cloud Gateway Cisco Secure Email Gateway Cisco Secure Email Domain Protection Cisco Secure Email Encryption Service Cisco Secure Awareness Training
Fortinet	SaaS — FortiMail Cloud — Gateway SaaS — FortiMail Cloud — Gateway Premium Physical Appliances — FortiMail

Microsoft	Exchange Online Protection Microsoft Defender for Office 365 Plan 1 Microsoft Defender for Office 365 Plan 2
Mimecast	Email Security, Cloud Gateway Email Security, Cloud Integrated
Proofpoint	P0 Core Threat Protection P1 Advanced Threat Protection P1+ Complete Threat Protection PX Microsoft 365 Protection Proofpoint Enterprise Data Loss Prevention Proofpoint Managed Service for Email Security
Sophos	Sophos Email

Trellix	Trellix Email Security
Trend Micro	Trend Micro Cloud App Security Trend Micro Email Security Trend Micro Smart Protection for Office 365 Trend Micro XDR for Users Deep Discovery Email Inspector

Source: Gartner (February 2023)

Table 2: Representative ICES Vendors

Vendor	Product Names
Abnormal Security	Abnormal Cloud Email Security Platform
Armorblox	Inbound Email Protection Outbound Email Protection

Cellopoint	Secure Microsoft Office 365 Secure On-Premises Email Platform
Check Point Software Technologies (Avanan)	Anti-Phishing Software Anti-Malware and Ransomware Software Full-Suite Protection
Cloudflare	Cloudflare Area 1 Email Security (formerly Area 1 Horizon)
Cofense	Cofense Reporter Cofense PhishMe Cofense Intelligence Cofense Triage
Darktrace	Darktrace Antigena Email
Egress	Egress Defend Egress Prevent Egress Protect

Fortra (Agari)	Agari Phishing Defense Agari Phishing Response Agari Brand Protection Agari Active Defense
GreatHorn	GreatHorn Cloud 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 IRONSCALES email security

Perception Point	Advanced Email Security Advanced Internal Email Security Advanced Collaboration Security
Tessian	Tessian Cloud Email Security Platform Tessian Defender Tessian Guardian Tessian Enforcer Tessian Architect
Vade	Vade for M365

Source: Gartner (February 2023)

Table 3: Representative EDP Vendors

Vendor	Product or Service Names
Echoworx	Echoworx Email Encryption Platform

Trustifi	Trustifi Outbound Shield Trustifi Inbound Shield Trustifi Account Compromise Detection
Zivver	Zivver Secure EmailZivver Secure File Transfer
Zix	Secure Cloud

Source: Gartner (February 2023)

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 todetect anomalies.
- Evaluate built-in email security capabilities provided by cloud email systems and augment it with third-party solutions for handling sophisticated attacks.
- Ensure that the solution has multifaceted protection for credential theft, as well as computer vision to analyze URLs that are impersonating common log-on pages.
- 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, as these solutions create communication graphs and baseline user activity to detect suspicious behavior.
- Invest in solutions that can use their API integrations into collaboration platforms to filter malicious content or suspicious interactions.

- Invest in user education with a particular focus on BEC-type attacks with no payload, and implement standard operating procedures for the handling of financial and sensitive data transactions commonly targeted by impersonation attacks.
- Reinforce training with context-aware banners and in-line prompts to help educate users.
- Ensure that user-reported unwanted emails are automatically resolved by the integrated MSOAR capability.
- Integrate email events into a broader XDR or SIEM/SOAR strategy by choosing vendors that have integrations with these security tools.
- Protect the corporate brand by implementing DMARC for protection against exact domain spoofing attacks on partners and customers. Seek out providers that can monitor DMARC rejects and host Sender Policy Framework (SPF) records.
- Consider the solution's role in a data security governance framework to protect sensitive data sharing with DLP, encryption and stored data discovery.

Evidence

The findings and recommendations in this research were derived from more than 1,500 Gartner client interactions between October 2021 and December 2022.

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

[2]Cost of a Data Breach 2022 Report, IBM.

Note 1: 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 2: 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 significant 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 the 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 for any of 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).

Note 3: Privacy and Legislative Laws for Security Products in Mainland China

Regarding the multilevel protection scheme (MLPS) certification, Gartner has observed a significant rise in activity throughout China. Risk-driven cybersecurity controls and documented governance and oversight were complying with these cybersecurity

standards triggered by social stability and national security concerns. If you do business in China, you should look for solutions compliant with the MLPS certification process, or you risk having audits and police-led inspections.

As a simple rule, the Chinese government is required to keep Chinese data in the country, making email security approaches specifically challenging as cloud-based ICES and SEG solutions require a geo-location in mainland China, hence the still significant embrace of traditional on-premises solutions.While vendors like Microsoft provide a solution hosted via a third party in mainland China, other vendors like Cellopoint are focused on the mainland China market. Their focus is on implementation, certification and specialized BEC capabilities for the double-byte character set, including simplified and traditional Chinese.

Is this content helpful to you?