Magic Quadrant for Email Security

1 December 2025 - ID G00826513 - 30 min read

By Max Taggett, Nikul Patel

Email security vendors are rapidly bolstering social engineering detection capabilities in response to the escalating pace of phishing and business email compromise (BEC) attacks. Buyers must consider complementary or supplemental email security solutions to align with best practices for combating modern email threats.

Market Definition/Description

Gartner defines an email security solution as a product that secures email infrastructure. Its primary purpose is to protect against malicious messages (phishing, social engineering, malware) or unsolicited messages (spam, marketing). Other functions include email data protection; domain-based message authentication, reporting and conformance (DMARC); investigation; and remediation through a dedicated console. Email security solutions may also support nonemail collaboration tools, such as those for document management and instant messaging.

Email security tools protect an organization's email from spam, phishing, malware attacks, account takeover and data loss. They may provide capabilities for data loss prevention, encryption, domain authentication and security education, as well as advanced protections against business email compromise. Email security platforms give cybersecurity teams visibility into email-related security incidents, support investigation and automated remediation, and enable management of both inbound and outbound email delivery. Email security solutions often integrate with other network, identity and endpoint security controls, and may also support collaboration tools and email relay capabilities.

Mandatory Features

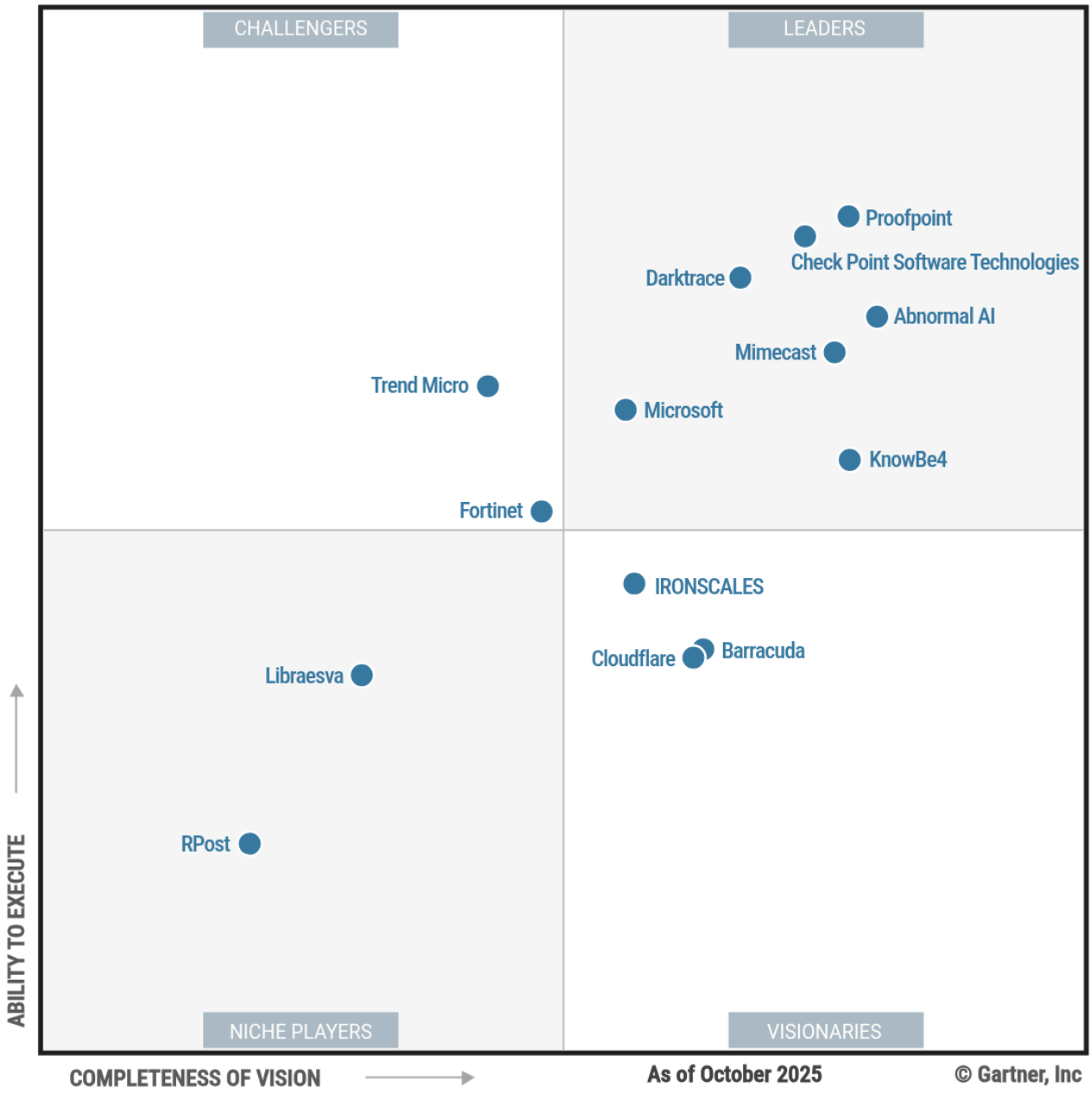
- Spam filtering
- Attachment inspection for malware/ransomware and subsequent quarantining or disarming
- URL analysis and protection
- Phishing detection/prevention

Common Features

- DMARC, DomainKeys Identified Mail (DKIM) or Sender Policy Framework (SPF) management
- Outbound protection features, such as DLP and misaddressed sender identification
- Account takeover prevention
- Collaboration/productivity tool protection
- Threat intelligence integration
- Awareness training and phishing simulation
- Message transfer agent (MTA)
- Email data protection, including encryption and data loss prevention features
- Managed detection and response
- Brand Indicators for Message Identification (BIMI) support

Magic Quadrant

Figure 1: Magic Quadrant for Email Security



Gartner

Vendor Strengths and Cautions

Abnormal AI

Abnormal AI is a Leader in this Magic Quadrant. The Abnormal Behavior Platform uses behavioral baselines to identify and remediate threats, and incorporates vendor-specific social graphing to track business communications patterns and detect vendor email compromise.

Over the past year, Abnormal has expanded its product portfolio to include phishing simulation training for security awareness use cases, along with enhancements to its detection engines and AI agent-enabled reporting. The company has maintained strong

momentum by continuing to focus on complementing native email security tools. It has also expanded its government-sector reach through FedRAMP Moderate authorization.

Abnormal's solution is suitable for organizations focused on core email security and automation for email security workflows.

Strengths

- **Marketing execution:** Abnormal's investments in marketing activities support its visibility and brand recognition among Gartner clients.
- **Customer experience:** Abnormal has strong customer relationship management processes, as supported by client feedback and Peer Insights that indicate positive customer experience and product capabilities.
- **Sales strategy:** Abnormal's sales strategy incentivizes long-term deals and no-cost competitive displacement of professional services, appealing to customers in a volatile economy.

Cautions

- **Geographic strategy:** Abnormal lacks a distributed global presence, with relatively fewer sales resources, partners, and customers in regions outside of North America and Europe compared to other leaders in this Magic Quadrant.
- **Market responsiveness:** The company's recent product and feature developments, namely Abnormal AI Data Analyst and AI Phishing Coach, fail to expand its coverage of email security's most significant threats.
- **Operations:** Abnormal has fewer employees and resources in key functional areas, such as product management and threat intelligence research, than other leaders in this Magic Quadrant.

Barracuda

Barracuda is a Visionary in this Magic Quadrant. Barracuda Email Protection is the company's flagship email security product, composed of Email Gateway Defense and several security and infrastructure-focused products. The product delivers security and infrastructure functions, including encryption, impersonation protection, archiving, and continuity services.

Over the past year, Barracuda has expanded its content and artifact analysis capabilities and improved detection parity across deployment methods. The company continues to focus heavily on security information and event management (SIEM) and extended detection and response (XDR) efficiencies to drive broader Barracuda product adoption and maintains a strong customer base among small businesses.

This solution is especially suitable for managed service providers (MSPs) and smaller organizations with multitenant requirements.

Strengths

- **Innovation:** Barracuda commits significant resources to research and development and is an active contributor of threat intelligence to the market.
- **Overall viability:** Barracuda maintains healthy revenue and modest changes in headcount.
- **Market understanding:** The company demonstrates strong awareness of emerging attack vectors and the challenges faced by MSPs and small and midsize businesses (SMBs).

Cautions

- **Product:** Barracuda continues to lack analytic depth in detection and incident reporting compared with other solutions in this Magic Quadrant.
- **Customer experience:** Customer relationship management and feedback processes lag behind those of other vendors in this Magic Quadrant, as supported by client feedback that indicates a variable customer experience.
- **Sales strategy:** Barracuda's sales strategy leads to shorter contracts that are dependent on partner performance.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. Its flagship email security product, Harmony Email & Collaboration (HEC), integrates with Check Point Horizon XDR/XPR.

Over the past year, Check Point expanded its headcount and budgets and integrated technologies from Check Point's nonemail security acquisitions to strengthen its email security capabilities. The company also released new security features that expanded its

ability to service larger organizations, such as archiving, Domain-based Message Authentication, Reporting, and Conformance (DMARC) support, as well as natural language queries to improve usability.

HEC is well-suited for organizations that prioritize ease of use, cost-efficiency, and all-in-one workspace security platforms.

Strengths

- **Overall viability:** Check Point continued to grow its email security function and revenue over the last year.
- **Customer experience:** The company has strong customer relationship management practices, as supported by client feedback and Peer Insights that indicate a positive customer experience.
- **Product:** Check Point provides an intuitive interface with broad feature coverage across email security use cases.

Cautions

- **Sales strategy:** Based on Gartner end-user client inquiries, Check Point is less commonly included on client shortlists compared to other leaders in this Magic Quadrant.
- **Vertical strategy:** Check Point's strategies for vertical-specific differentiation are less focused than those of other leaders in this Magic Quadrant.
- **Geographic strategy:** Check Point's ability to provide region-specific services, such as data sovereignty or localized infrastructure, trails other leaders in this Magic Quadrant.

Cloudflare

Cloudflare is a Visionary in this Magic Quadrant. Cloudflare Email Security is available as a stand-alone product or as part of Cloudflare One, the vendor's secure access service edge (SASE) platform, which adds protections against web-based attacks delivered through email.

Over the past year, Cloudflare has focused on developments to expand analytic visibility, including an embedded Remote Browser Isolation feature for better visibility into URL-based lures, employing new methods for malicious link identification, and free DMARC management and posture checking. The company continues to position its email security

product as complementary to its SASE-led workspace security strategy, with an increasing emphasis on its suitability as a stand-alone product.

Cloudflare Email Security is a strong fit for organizations seeking cost-conscious protection against advanced email attacks or vendor consolidation opportunities.

Strengths

- **Product strategy:** Cloudflare's product roadmap focuses on increased usability and features that improve its value proposition against its closest email security competitors.
- **Marketing strategy:** Cloudflare's marketing strategy leverages a variety of channels to communicate its value as a secure email gateway (SEG) augmentation.
- **Geographic strategy:** Cloudflare maintains a global footprint and supports client localization requirements across multiple regions.

Cautions

- **Market responsiveness:** Cloudflare's share of the email security market is lower than that of Leaders or Visionaries in this Magic Quadrant.
- **Sales execution:** The company's bundling and packages appear designed to facilitate SASE adoption and lack well-defined discount strategies.
- **Innovation:** Cloudflare's innovation focus is limited to areas that complement its SASE offering.

Darktrace

Darktrace is a Leader in this Magic Quadrant. Darktrace / EMAIL provides a broad set of email security capabilities designed to target advanced threats. Email security is tightly integrated with Darktrace's / NETWORK and / IDENTITY products and offers out-of-the-box integrations with many network, endpoint, and identity security tools. / EMAIL also covers data loss prevention (DLP), misdirected mail, and DMARC management.

Over the past year, Darktrace expanded its capabilities and strategy, significantly improving both vision and execution potential. The company released domain-specific language models for sensitive data detection, expanded collaboration app coverage, and added DMARC management to its offerings. Following its acquisition by Thoma Bravo, Darktrace made key additions to its email leadership team, enhanced its partner network, and

achieved FedRAMP High Authority to Operate status to improve suitability for government use cases.

/ EMAIL is best suited for organizations seeking improved threat detection and response workflows and a simple licensing model.

Strengths

- **Operations:** Darktrace's headcount, especially in the areas of technical customer support and analytic roles, increased significantly over the past year, surpassing other leaders in this Magic Quadrant.
- **Product strategy:** Darktrace's product roadmap is aligned with the emerging needs of its target customers.
- **Market understanding:** The company's product roadmap is well-positioned to create opportunities against its targeted competition and increase its value proposition as an augmentation to native email controls.

Cautions

- **Sales strategy:** Darktrace's adjustments to pricing have yet to shift observed Gartner client sentiment.
- **Marketing strategy:** The company's marketing investments are less aggressive in both spend and targeting compared to those of other leaders in this Magic Quadrant.
- **Geographic strategy:** Darktrace lacks language support and depth of regional customizations compared to other leaders in this Magic Quadrant.

Fortinet

Fortinet is a Challenger player in this Magic Quadrant. Fortinet's FortiMail Workspace Security provides a range of email security tools such as DMARC, encryption, and DLP capabilities, along with strong integrations into Fortinet's security platform.

Over the past year, Fortinet completed its acquisition of Perception Point, adding advanced detection capabilities to its existing email security appliance and SEG. Fortinet's integration of Perception Point has increased automation for incident response workflows and centralized alerts.

Fortinet is well-suited for existing Fortinet customers pursuing workspace security strategies and seeking strong file-based malware detection.

Strengths

- **Overall viability:** Fortinet maintains a strong corporate financial position and continues to invest in email security developments.
- **Marketing strategy:** The company utilizes a variety of channels to communicate its competitive takeout programs to potential customers.
- **Sales execution:** Fortinet offers competitive pricing and renewal rates and performs well in cross-selling to its existing customers.

Cautions

- **Market responsiveness:** Fortinet's email security market share trails leaders in this Magic Quadrant.
- **Product strategy:** In the past year, Fortinet's product strategy necessarily focused on the acquisition and integration of Perception Point and is now catching up to the market on certain detection and response functions, such as social graphing and improved account takeover capabilities.
- **Operations:** Fortinet has fewer personnel assigned to functional email security areas, such as technical customer support, analytic roles, and product management, than other vendors in this Magic Quadrant.

IRONSCALES

IRONSCALES is a Visionary in this Magic Quadrant. IRONSCALES Email Security provides advanced threat detection against business email compromise and spear phishing, along with account takeover protection, user education, and innovative collaboration security capabilities.

Over the past year, IRONSCALES has differentiated itself by releasing deepfake protections for Microsoft Teams. The company also introduced graymail filtering, DMARC management, and additional automation capabilities.

IRONSCALES is well-suited for organizations with low tolerance for social engineering or those lacking effective automation for phishing workflows.

Strengths

- **Sales execution:** IRONSCALES' pricing is competitive across organization sizes and has a transparent pricing and discounting structure.
- **Market responsiveness:** The company proactively addresses gaps in the market, such as anticipating the need for and delivering deepfake detection ahead of other email security vendors.
- **Innovation:** Internal processes around R&D support innovation and enable the delivery of new-to-market features ahead of other vendors in this research.

Cautions

- **Operations:** IRONSCALES remains one of the more lightly staffed vendors in this Magic Quadrant and serves fewer enterprise-size clients than other leaders.
- **Sales strategy:** Based on Gartner end-user client inquiries and Peer Insights customer feedback, IRONSCALES is less frequently included on competitive email security provider shortlists compared to other vendors in this Magic Quadrant.
- **Product:** The company's emphasis on innovation leads to less emphasis on depth in areas such as DLP.

KnowBe4

KnowBe4 is a Leader in this Magic Quadrant. Its flagship product, KnowBe4 Cloud Email Security, includes four offerings: Defend for inbound phishing protection, Prevent for outbound DLP and misdirected mail, Protect for encryption, and PhishER for mSOAR. KnowBe4's recognition as a security and awareness training (SAT) vendor provides additional opportunities for existing SAT customers evaluating new email security vendors.

Over the past year, KnowBe4 completed its acquisition and integration of Egress, focusing development on improving deployment workflows and detection models. KnowBe4's roadmap contains opportunities to realign with leaders in the email security market, supported by outbound security and DLP features that align well with vertical-specific use cases.

KnowBe4 Cloud Email Security is well-suited for organizations seeking easy-to-use DLP, encryption and native security, and awareness training.

Strengths

- **Product strategy:** KnowBe4's roadmap contains increasingly common features among Magic Quadrant leaders, such as account takeover protection and collaboration protection.
- **Vertical strategy:** The company's vertical strategy aligns with the strengths of its product and has a clear path to vertical expansion.
- **Overall viability:** KnowBe4 is well-funded, exhibits year-over-year revenue growth, and its completed acquisition of Egress indicates a likelihood of continued investment in email security.

Cautions

- **Product:** KnowBe4 continues to lag leaders in the Magic Quadrant in its depth of features, exacerbated by rapid evolution in the email security market over the past year.
- **Customer experience:** Customer relationship management and feedback processes lag behind those of other vendors in this Magic Quadrant, as supported by client feedback that indicates a variable customer experience.
- **Marketing strategy:** KnowBe4's product messaging and positioning are not differentiated from other vendors included in this MQ.

Libraesva

Libraesva is a Niche Player in this Magic Quadrant. Libraesva Email Security offers a privacy-focused email security solution designed to meet regulatory and compliance requirements for data localization. With more than a decade of experience in the market, Libraesva focuses on detecting threats in the inbox rather than expanding the breadth of use cases supported.

The company primarily services European organizations, offering a strong customer experience and essential add-ons such as DMARC.

Libraesva is well-suited for organizations seeking a greater degree of control over vendor access to their data and on-premises-compatible, locally run models.

Strengths

- **Sales strategy:** Libraesva's clients pursue multiyear contracts at a higher rate than those of other leaders in this Magic Quadrant.
- **Market understanding:** The company shows above-average market understanding by proactively addressing gaps in the market, such as deploying modern detection techniques and implementing privacy-focused local language models.
- **Sales execution:** Libraesva offers simple packaging and competitive pricing.

Cautions

- **Innovation:** Libraesva's research and development resources lag behind those of other vendors, making regular competitive innovations unlikely.
- **Operations:** The company has a smaller employee base than other vendors in this research, impacting its ability to effectively support the needs of larger enterprises.
- **Market responsiveness:** Libraesva is slow to respond to emerging customer needs and requirements compared to leaders in this Magic Quadrant.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Its flagship email security product, Microsoft Defender for Office 365, is tightly integrated with the Exchange email infrastructure. It is available as a stand-alone solution or included in Microsoft 365 license bundles with varying features, making it the most accessible security product on the market.

Over the past year, Microsoft introduced solutions for new attack types, augmented social engineering protections, and expanded its protections for Microsoft Teams. The company also prioritized initiatives to combat perceptions of Defender's effectiveness and encourage administrators to utilize Microsoft dashboards as their primary workflow through benchmarking reports and customer-facing performance dashboards.

Microsoft Defender for Office 365 is well-suited for organizations that are invested in Microsoft 365 and pursuing an integrated workspace security offering, and those with mature email security and infrastructure functions.

Strengths

- **Overall viability:** Microsoft is a large, well-funded vendor with a substantial presence and a long history of investment in email infrastructure and security.

- **Operations:** Broad first- and third-party support and training are available for all products.
- **Market responsiveness:** Microsoft's continued product evolution demonstrates the ability to respond to emerging threats and customer pain points, such as email bombing.

Cautions

- **Customer experience:** Customer relationship management lags behind other vendors in this research, and customer feedback indicates variable service and support degrade the overall customer experience.
- **Sales strategy:** Email security is bundled with nonemail security products to a higher degree than other vendors in this Magic Quadrant.
- **Product strategy:** Microsoft's product strategy is not fully aligned to meet future market needs, focusing on features that improve efficiency more than security, such as recently released effectiveness dashboards.

Mimecast

Mimecast is a Leader in this Magic Quadrant. Mimecast Email Security offers both gateway and API integration, with add-on modules for advanced threat protection, such as DMARC Analyzer and collaboration security. Infrastructure support features include archiving and continuity services.

Over the past year, Mimecast continued the integration of last year's acquisitions, Code42, Elevate Security, and Aware, into its human risk management portfolio, enhancing its account takeover and SAT products.

Mimecast's email security products are suitable for a broad range of organizations, especially those prioritizing email archiving or infrastructure support capabilities.

Strengths

- **Operations:** Mimecast is well-staffed to support global operations with strong personnel counts in technical customer support, product management, and analytics.
- **Sales strategy:** The company's sales strategy is strengthened by an expansive partner program and larger discounts on multiyear deals than those of other vendors in this Magic Quadrant.

- **Marketing execution:** Mimecast maintains a high degree of visibility by contributing narratives and advocating its competitive positioning in the email security market.

Cautions

- **Sales execution:** Mimecast's repackaging efforts over the last year have increased overall licensing complexity.
- **Customer experience:** The company's customer relationship management processes and support licensing lag behind those of other leaders in this Magic Quadrant.
- **Market understanding:** Mimecast's focus on human risk lacks a strong connection to email security outcomes.

Proofpoint

Proofpoint is a Leader in this Magic Quadrant. Its flagship email security product, Proofpoint Prime threat protection, includes risk dashboards, message authentication, and DLP capabilities that are among the most comprehensive in the market.

Over the past year, Proofpoint adjusted packaging for large enterprise customers, introduced competitive displacement programs targeting market leaders, and expanded its API offering to reach more customers.

Proofpoint is a strong fit for a broad range of organizations, especially large enterprises and those seeking a full-featured security solution.

Strengths

- **Product:** Proofpoint offers a broader set of email security and infrastructure tools than its competitors and strong detection capabilities.
- **Market responsiveness:** The company services clients across all sizes and industries and continues to expand its portfolio in response to the market, such as with collaboration security.
- **Overall viability:** Proofpoint's size and financial position contribute to its long-term viability in the email security space.

Cautions

- **Geographic strategy:** Proofpoint lacks the geographic diversity and expansion strategy of other Magic Quadrant leaders.
- **Marketing strategy:** The company's marketing strategy lacks specificity in how it targets and differentiates itself from its competition.
- **Sales execution/pricing:** Proofpoint's pricing has increased significantly over the past year, as indicated by Gartner end-user client inquiries.

RPost

RPost is a Niche Player in this Magic Quadrant. The vendor's flagship email security product is RMail PRE-Crime Preemptive Cybersecurity, with RPost Gateway serving as the primary means of inbound and outbound protection.

RPost differentiates itself by focusing on document rights management protection and has recently expanded inbox security capabilities to include semantic analysis.

RPost is well-suited for organizations whose external email workflows require strict management of documents and data.

Strengths

- **Sales execution:** RPost's pricing is lower than that of other vendors in this Magic Quadrant, with strong discounting strategies.
- **Geographic strategy:** The company's solution supports a wide variety of languages and is well-positioned for expansion beyond North America and Europe.
- **Vertical strategy:** RPost's vertical strategy aligns with its strengths in document rights management and DLP, targeting customers in insurance, legal, and government sectors.

Cautions

- **Product:** RPost's user experience, workflows, and BEC capabilities trail those of other vendors in this research.
- **Market responsiveness:** The company's feature developments are focused on its verified delivery and document rights management capabilities to a greater degree than emerging threats or market developments.

- **Product strategy:** RPost's product developments are unlikely to see widespread adoption or development from other vendors in this Magic Quadrant.

Trend Micro

Trend Micro is a Challenger in this Magic Quadrant. Its flagship email security product, Trend Vision One Email and Collaboration Security, offers DLP modules, collaboration security, and direct access to its XDR product.

Over the past year, Trend Micro has focused on stronger integration of email security with its security platform, enhanced support for file-based detections, and improved DMARC analysis and reporting.

Trend Vision One is suitable for organizations pursuing security vendor consolidation and holistic integrated workspace security.

Strengths

- **Product:** Trend Micro offers versatile implementation, well-designed workflows, and administrative capabilities delivered with a high degree of usability.
- **Customer experience:** The company has a strong process for collecting and channeling customer feedback into feature improvements.
- **Market understanding:** Trend Micro positions itself in the market to contrast positively against its closest competitors on workspace security.

Cautions

- **Market responsiveness:** Trend Micro's market share in email security remains low compared to that of other leaders in this Magic Quadrant.
- **Product strategy:** The company's product roadmap focuses on nonemail security advancement to a greater extent than other vendors in this Magic Quadrant.
- **Vertical/industry strategy:** Trend Micro's initiatives targeting specific verticals or industries are limited.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Libraesva
- RPost

Dropped

- Cisco failed to meet the technical requirements for inclusion in this Magic Quadrant.

Inclusion and Exclusion Criteria

To qualify for inclusion in this Magic Quadrant, each vendor:

- Must sell email security as a product line independent of any other solution or service.
- Must provide the capability to block or filter unwanted email traffic.
- Must provide file scanning to protect against malware.
- Must provide the capability to vet and protect against malicious URLs.
- Must utilize advanced analytics tools, including natural language processing, for message content analysis, and expose semantic analysis to end-user administrators.
- Must have a minimum of 10,000 customers or a minimum of 1 million mailboxes protected.
- The total number of customers in a single region outside of North America and Europe must not exceed 60% of a vendor’s total customer base.

Evaluation Criteria

Ability to Execute

Product/Service: Evaluation factors include core product and service capabilities, the depth and breadth of functionality, and support capabilities.

Overall Viability: Evaluation factors include overall financial health and the email security solution's contribution to revenue growth.

Sales Execution/Pricing: Evaluation factors include the execution of presales activities, the competitiveness of product and service pricing, client wins, and Gartner end-user client proposal reviews.

Market Responsiveness and Track Record: Evaluation factors include responsiveness to email security trends and needs, customer distribution, and customer integration in the development process.

Marketing Execution: Evaluation factors include the administration of marketing operations and the execution of marketing initiatives.

Customer Experience: Evaluation factors include customer relationship management (CRM), Gartner Peer Insights, and Gartner client interactions.

Operations: Evaluation factors include product management, certifications, training, and management of human resources.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria	*Weighting*
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	Low

Evaluation Criteria	*Weighting*
Marketing Execution	Low
Customer Experience	Medium
Operations	Medium

Source: Gartner (December 2025)

Completeness of Vision

Market Understanding: Evaluation factors include how vendors identify email security market trends, understand their buyers, and evaluate their competition.

Marketing Strategy: Evaluation factors include marketing-specific strategic projects, budgetary and administrative allocation, and communication channel expansions.

Sales Strategy: Evaluation factors include the attractiveness of product licensing and packaging options, deal strategies, competitive strategies, and Gartner end-user client interactions and consideration rates.

Offering (Product) Strategy: Evaluation factors include responsiveness to customer requests, product roadmap items, and applicability to the overall email security market.

Vertical/Industry Strategy: Evaluation factors include performance in specific industries and strategies for vertical expansion.

Innovation: Evaluation factors include commitments to R&D, competitive differentiation, and organizational innovations, with direct impacts on the consumer.

Geographic Strategy: Evaluation factors include performance in international markets, product localization, and geographic expansion strategies.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	Low
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	NotRated
Vertical/Industry Strategy	Low
Innovation	Medium
Geographic Strategy	Low

Source: Gartner (December 2025)

Quadrant Descriptions

Leaders

Leaders are recognized for strong market adoption, financial stability, and established integrations with major collaboration platforms. They may offer comprehensive or targeted solutions that blend traditional gateway functions with modern API-driven protection, and consistently achieve high feature attachment rates for add-ons. They often possess high-volume, established global customer bases across various enterprise sizes.

Challengers

Challengers possess broad security portfolios and significant market presence, often appealing to budget-sensitive customers with competitive pricing when bundled with their broader security portfolios. These providers are moving to bridge gaps in modern

architecture, leveraging their position to enable workspace security consolidation, reduce fragmentation, and offer compelling commercial models.

Visionaries

Visionaries focus on solving emerging and complex problems through innovative, AI-driven approaches such as deepfake prevention and advanced identity protection, rather than refining features that have generally reached maturity throughout the market. They often excel at reducing security operations center (SOC) burden through agentic AI and autonomous remediation capabilities, prioritizing deployment simplicity and low operational overhead. They demonstrate agility by being first to market with specialized threat defense capabilities.

Niche Players

Niche Players often focus on specific market segments, geographic regions, or unique technical requirements, such as data sovereignty or complementary security layers. Their strength lies in delivering high-quality solutions for defined customer profiles, including those that rely on managed security service providers (MSSPs) or require deep functionality across on-premises or hybrid infrastructures. Niche Players differentiate through specialized features, such as document rights management or compliance-focused products that augment larger security stacks.

Context

The high volume of sophisticated, email-enabled social engineering attacks, combined with the difficulty in consistently quantifying true detection efficacy across the market, justifies organizations utilizing multiple vendors for comprehensive protection. Diverse product offerings and specialized features give buyers flexibility both in vendor selection and in feature choice across email security solutions. Where feasible, organizations should consider deploying overlapping, multilayered email security solutions, pairing a core solution with specialized vendors to ensure complementary coverage against advanced or emerging threats.

As organizations consider an expanded email security stack, minimizing the total cost of ownership (TCO) of the combined tools and simplifying operations should remain priorities. Clients should emphasize these factors when evaluating secondary vendors, favoring

stronger integrations and streamlined workflows, such as unified quarantine or automation capabilities, to reduce administrative overhead. Competitive market dynamics and growing overlaps between products allow email security buyers that deploy multiple tools to effectively negotiate aggressive discounts. Organizations are encouraged to add cost-effective or niche solutions to proof-of-concept evaluations to support quantitative value comparisons against higher-priced offerings.

Market Overview

The email security market continues to evolve in both detection methodology and feature offerings. Email security vendors have increased customer counts, mailboxes protected, and revenue, coinciding with Gartner's SEG-specific estimates of 9% growth in marketwide revenue (see **Market Share: Security Software, Worldwide, 2024**). This growth is enabled by simple integrations that minimize the friction associated with email security tool changes and the rise of sophisticated email-enabled social engineering attacks.

Detection rates are an essential factor for email security buyers, though efficacy remains difficult to measure. Efforts by vendors to improve public perception of their product did little more than confuse narratives and ultimately led to a single conclusion: the use of overlapping, complementary solutions for email security may be preferable to relying on a single vendor.

At the same time, a volatile economy puts pressure on email security buyers to prioritize solutions based on cost and feature alignment. Email security buyers are increasingly prioritizing low TCO, which coincides with more aggressive pricing from some Magic Quadrant vendors. A narrative from last year's email security Magic Quadrant pointed to the diversity of vendor offerings and opportunities for buyers to find solutions that match their specific environment. Vendor capabilities have expanded as a result, yet buyers continue to prioritize "right fit" solutions when appropriate.

Product Evolution

The distinction between SEG and integrated cloud email security (ICES) vendors has begun to blur. Most SEG vendors now offer API deployment options in addition to a gateway. Vendors that previously deployed exclusively by ICES are increasingly introducing integration methods that allow their solutions to operate predelivery, either by mail exchange (MX) record or by modifying mailflow rules. While this technically qualifies them as

a SEG, vendors and buyers should consider the risks of processing large volumes of mail through solutions built for postdelivery analysis, such as increased delivery latency or service disruptions.

Many recent developments are deployment-type agnostic or delivered through blended approaches using both SEG and ICES from a single vendor, further blurring the lines between SEG and ICES deployments.

Functional focus areas and releases this year include:

- **Collaboration security:** Most vendors now offer some level of security for collaboration applications, with many releasing or extending the capability within the last year, bringing email protections to file shares, communications tools and SaaS applications such as Dropbox, Salesforce, SharePoint, Slack, and Teams.
- **AI-enabled phishing training:** Vendors are evolving phishing simulations with language models, automating the generation of phishing simulations and educational content built from the end user's own inbox.
- **Refinement of detection capabilities:** Vendors continue to improve detection engines with more accurate language models, expanded language support, and new signals generated from sources such as computer vision and dynamic webpage analysis.
- **Unified quarantine:** Deploying an ICES solution on top of Microsoft Defender for Office 365 previously resulted in a split quarantine, with each solution maintaining its own cache of detections. The development of a unified quarantine minimizes the time spent operating in different vendor dashboards.
- **Misdirected mail:** Advanced detection of misaddressed outbound mail occurs before it leaves the organization, validating recipients based on the alignment of the email content with analyses of previous conversations, with some vendors adding the ability to identify misattached files with similar analytics.

Differentiation

Usability and configuration depth: Despite vendor marketing promoting ease of use and automation, the actual flexibility, configurability, and depth of analysis vary significantly between vendors. Some solutions use black box approaches that obscure detection engine logic, which can complicate the investigation of false alerts. Others provide detailed

reporting on detection engine logic, malware analysis, and custom rule capabilities leveraging third-party indicators of compromise.

Use-case specialization: Vendors differentiate their products by introducing features that create specific niches in the market. These may address longstanding needs, such as encryption, DLP, or archiving and eDiscovery, or introduce specialized capabilities such as deepfake detection, email bombing, or authenticated email delivery. Prospective buyers should use Gartner's Critical Capabilities for Email Security to assess products against specific organizational use cases.

Platform integration: Only a small number of vendors offer a comprehensive single-vendor workspace security platform. Multiple vendors offer a more limited workspace platform, offering endpoint protection platforms or security service edge tools that are tightly integrated with the rest of their security offerings. Stand-alone email security vendors add value through custom endpoint detection and response (EDR), SASE, identity, or XDR integrations that support multivendor workspace security strategies.

⊕ Evaluation Criteria Definitions

Get The App

GET IT ON Google Play

Download on the App Store