Magic Quadrant for Email Security Platforms

16 December 2024 - ID G00806896 - 25 min read

By Max Taggett, Nikul Patel, **and 2 more**

Email security platforms provide protection against spam, phishing and business email compromise. Buyers should evaluate the following ESP vendors first on the quality of detections, and second on the presence of additional security capabilities and infrastructure support capabilities.

Market Definition/Description

Gartner defines an email security platform as a product that secures email infrastructure. Its primary purpose is the removal of malicious (phishing, social engineering, viruses) 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. They may integrate as a secure email gateway (SEG) for predelivery protection or as an integrated cloud email security (ICES) solution for postdelivery protection.

Email security platforms protect an organization's email infrastructure from social engineering, phishing, business email compromise, spam, malware attacks and data theft. Email security platforms are deployed independently, but integrated with other network and endpoint security controls to improve the overall risk posture of the organization. Email security platforms offer cybersecurity teams visibility into email-related security incidents for investigation and remediation.

Mandatory Features

Mandatory features of an email security platform include:

- Message, body and header scanning for phishing and spam
- Attachment inspection and quarantine or disarming
- URL analysis and protection
- Email data protection, including encryption and data loss prevention features

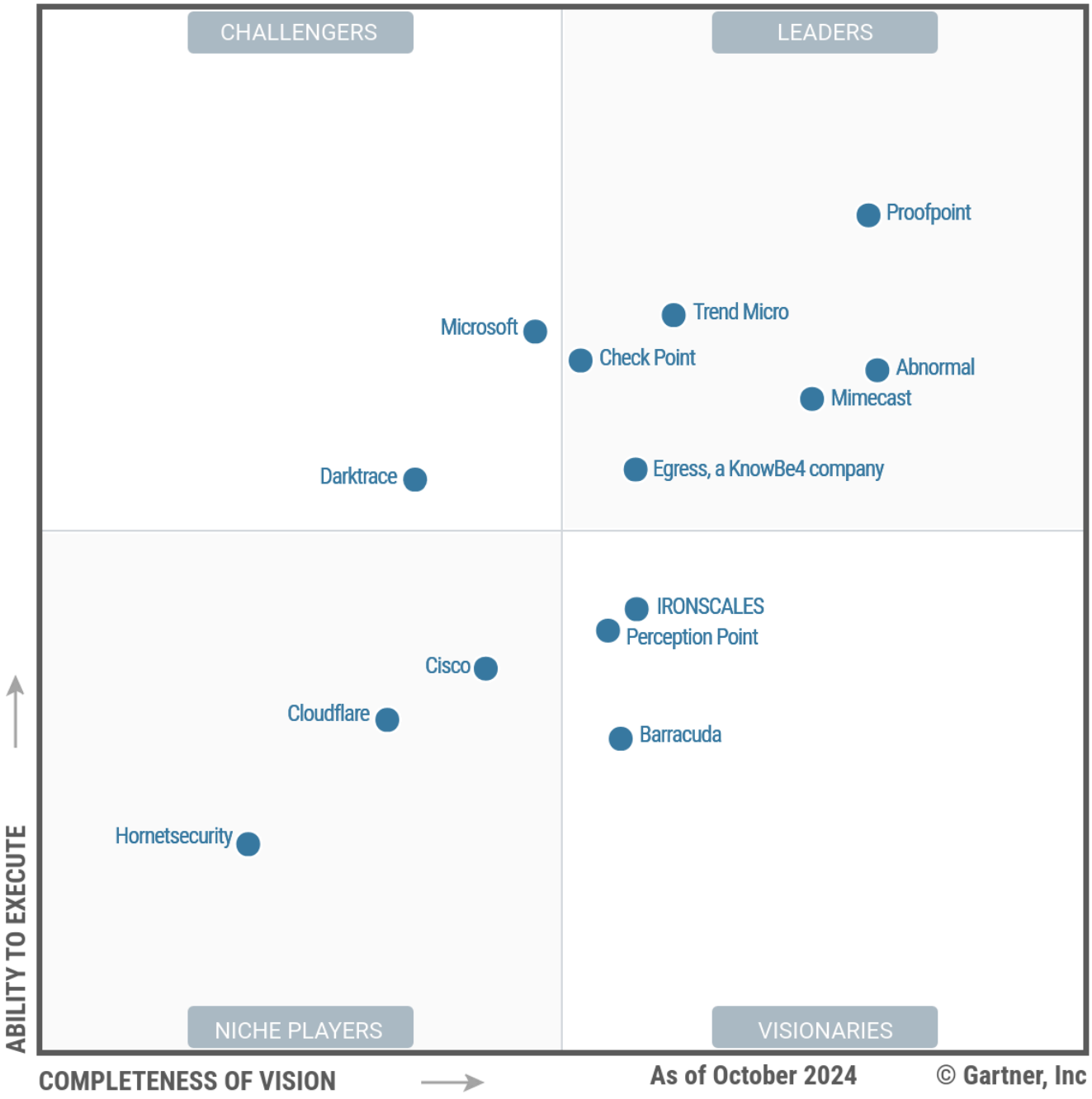
Common Features

Common features of an email security platform include:

- DMARC/domain keys identified mail (DKIM)/sender policy framework (SPF) management
- Account takeover prevention
- Collaboration/productivity tool protection
- Awareness training
- Message transfer agent (MTA)

Magic Quadrant

Figure 1: Magic Quadrant for Email Security Platforms



Gartner

Vendor Strengths and Cautions

Abnormal

Abnormal Security is a Leader in this Magic Quadrant. The Abnormal Human Behavior AI Platform baselines user behavior to identify and remediate threats. It also maintains a proprietary vendor database to track business communications patterns and identify supply chain attacks.

Abnormal has advanced its integration with third-party tools, including SIEM, ITSM and EPP tools, enabling investigation and remediation from outside of its platform. It has also integrated AI chatbot functionality for improved prereporting phishing triage.

The Abnormal Human Behavior AI Platform suits a wide variety of organizations focused on core email security and a higher degree of automated email security functions.

Strengths

- **Market responsiveness:** Abnormal Security's market responsiveness is bolstered by strong customer feedback loops and feature developments aligned with customer and market demands.
- **Innovation:** Abnormal innovates through rapid introduction of new features, internal processes and support structures.
- **Sales strategy:** Abnormal's sales strategy prioritizes long-term deals and scores above average compared with other vendors in this Magic Quadrant.

Cautions

- **Overall viability:** Abnormal lacks the depth of experience and history found in other vendors in this Magic Quadrant.
- **Geographic strategy:** Despite broad language support for detection, Abnormal does not have a significant global presence and offers limited resources for organizations with geographic and regulatory requirements.
- **Operations:** Abnormal has a less established global sales capability, employs fewer analytic support personnel and has fewer certifications compared with other Leaders in this Magic Quadrant.

Barracuda

Barracuda Networks is a Visionary in this Magic Quadrant. Barracuda Email Protection is the company's flagship ESP product, composed of Email Gateway Defense and a number of individual security and infrastructure-focused products. Barracuda delivers security and infrastructure functions that include encryption, impersonation protection, archiving and continuity services.

Barracuda's click-time URL rewriting capabilities, web filtering modules, and in-browser end-user education are representative of Barracuda's emphasis on protecting against browser-based phishing attacks.

Barracuda Email Protection suits managed service providers (MSPs) and smaller organizations with multiple tenants.

Strengths

- **Market understanding:** Barracuda shows a strong awareness of emerging attack vectors and how to address the challenges that MSPs and small and midsize businesses (SMBs) face.
- **Overall viability:** Barracuda maintains strong revenue and continues to add to its employee count.
- **Product strategy:** Barracuda's roadmap is geared toward improving usability for MSPs and SMBs.

Cautions

- **Product:** Barracuda's product offers limited analytic depth in advanced detection techniques.
- **Customer experience:** Barracuda's customer relationship management and customer feedback lag behind other vendors in this research.
- **Innovation:** Barracuda is unlikely to shape the market based on its current focus and capabilities.

Check Point

Check Point Software Technologies is a Leader in this Magic Quadrant. Its flagship ESP product is Harmony Email & Collaboration (HEC). The company also offers Check Point Horizon XDR/XPR, one of a limited number of extended detection and response (XDR) products with native email security integration, bolstering Check Point's value to organizations seeking a comprehensive workspace security vendor.

Check Point's email offering includes data loss prevention (DLP) capabilities and DMARC management from within the console. It also offers a phishing simulation and training module that can target specific user groups with disarmed versions of live phishing campaigns.

HEC suits organizations prioritizing ease of use, cost and pursuing security vendor consolidation.

Strengths

- **Sales execution/pricing:** Check Point provides simple and reasonably organized packages at lower prices than other vendors in this Magic Quadrant.
- **Market understanding:** Check Point has a good understanding of the email security market's evolving threat landscape and its own competitive advantage in the market.

- **Product:** Check Point's threat detection capabilities are strong compared with other vendors in this Magic Quadrant.

Cautions

- **Sales strategy:** Check Point lacks strong competitive displacement programs and strong incentives for long-term contracts.
- **Customer experience:** Check Point's customer relationship management practices lag behind other vendors in this research.
- **Operations:** Check Point has a smaller team dedicated to email security products than other vendors in this research.

Cisco

Cisco is a Niche Player in this Magic Quadrant. Cisco's Secure Email consists of its Secure Email Gateway and Secure Email Threat Defense products. Cisco Secure Email Gateway delivers all core gateway functionalities. Cisco Secure Email Threat Defense provides additional threat detection capabilities delivered through ICES.

Cisco offers support for decreasingly common on-premises email infrastructure while simultaneously investing in the expansion of its ICES integrations through the acquisition of Armorblox in 2023 to augment its threat detection capabilities.

Cisco's flagship ESP product suits global organizations invested in the broader suite of Cisco security offerings looking to simplify integration, operations and procurement.

Strengths

- **Sales strategy:** Cisco offers bundling options across its Breach Protection and User Protection suites, an expanded sales structure and a broad network of value-added resellers (VARs).
- **Operations:** Cisco boasts a broad geographic footprint, as well as depth of experience in product management and workforce distribution.
- **Overall viability:** Cisco has a long history in the email security space and continues to invest in its future via targeted acquisitions that address evolving BEC and social engineering threats.

Cautions

- **Customer experience:** Cisco's customer relationship management and customer feedback lag behind other vendors in this research.
- **Product:** Cisco's ESP relies on two distinct products to deliver SEG and ICES implementations. Cisco facilitates certain workflows through its XDR platform, introducing complexity across multiple interfaces.
- **Market responsiveness:** Cisco's roadmap focuses on the continued development of its most recent email security platform, with less emphasis on its gateway-specific product.

Cloudflare

Cloudflare is a Niche Player in this Magic Quadrant. Cloudflare Email Security is available as a stand-alone product, as well as part of Cloudflare's single-vendor SASE platform, Cloudflare One, which provides additional protections against web-based attacks targeted through email.

Cloudflare's value proposition for its email security platform, including its PhishGuard managed services, is heavily focused on phishing protection.

Cloudflare Email Security suits enterprises considering vendor consolidation strategies specific to single-vendor SASE, and those in need of data protection for web-based applications and collaboration platforms.

Strengths

- **Market understanding:** Cloudflare understands the holistic needs of the email security market.
- **Geographic strategy:** Cloudflare's large and growing global footprint supports client localization requirements across multiple regions.
- **Overall viability:** The growth of Cloudflare's email security team and its strategic position within Cloudflare's overall roadmap support its long-term viability.

Cautions

- **Operations:** Cloudflare's operations score is impacted by broad leadership changes in several areas, introducing the potential for uncertainty around the future direction of email-specific initiatives.
- **Sales execution:** Cloudflare's email security bundling is better suited to single-vendor SASE customers than email security customers due to the composition of its product packages.
- **Innovation:** Email security is underrepresented in Cloudflare's corporate vision and commitment to innovation.

Darktrace

Darktrace is a Challenger in this Magic Quadrant. Darktrace's /EMAIL platform is its flagship email security product. Darktrace's email security detection engine is focused primarily on identifying threats through its AI, including NLP and behavioral analysis, instead of traditional security measures like signatures and sandboxing. While Darktrace provides coverage on some adjacent security functions such as DLP and misdirected mail, its strongest value proposition is the augmentation of other email security platforms.

Darktrace also has /IDENTITY to expand protection coverage to productivity tools such as Microsoft 365 and Google Workspace; /Proactive Exposure Management for phishing simulations and risk scores for users; and /NETWORK, /CLOUD and /OT for threat detection and investigations.

Darktrace's flagship ESP product is well suited to organizations with existing ESPs in search of improved detection against business email compromise (BEC) and spear phishing attacks.

Strengths

- **Operations:** Darktrace has a broad geographic presence and larger-than-average sales and customer support teams.
- **Overall viability:** Darktrace has grown its email security business at a faster rate than other vendors in this research.
- **Sales execution:** Darktrace performs well with first-time email security buyers and has strong renewal rates.

Cautions

- **Product:** Darktrace lacks certain features and integrations that are present in other ESPs in this Magic Quadrant.
- **Vertical/industry strategy:** Darktrace's focus on a highly usable but lightly configurable interface limits its suitability for verticals with more advanced technical specifications.
- **Innovation:** Darktrace is unlikely to reshape the market with its innovations based on its modest commitments to R&D infrastructure.

Egress, a KnowBe4 company

Egress, a KnowBe4 company, is a Leader in this Magic Quadrant. Its flagship ESP product, Egress Intelligent Email Security, is composed of three offerings: Egress Defend (inbound phishing protection), Egress Prevent (outbound/DLP/misdirected) and Egress Protect (encryption). These can be bought individually or bundled.

Egress' recent acquisition by KnowBe4 bolsters its ability to drive security and awareness education to the inbox and creates significant cross-selling opportunities with existing KnowBe4 customers.

Egress Intelligent Email Security is suitable for organizations in search of transparent LLM usage through social engineering attack prevention, DLP, and security and awareness training content.

Strengths

- **Product strategy:** Egress' product roadmap aligns well with customer requirements in the areas of DLP and core email protection.
- **Sales execution/pricing:** Egress' product bundles are simple, logically grouped and aligned with customer requirements.
- **Overall viability:** Egress' expansion of its workforce and acquisition by KnowBe4 improves its long-term viability.

Cautions

- **Product:** Egress lacks the depth of features and configurability available from other vendors in this research.
- **Geographic strategy:** Egress lacks a significant footprint outside of Europe and North America, and its administrative console is in English only.
- **Marketing strategy:** Egress' focus on user education could limit its attractiveness to email security customers with a broader focus.

Hornetsecurity

Hornetsecurity is a Niche Player in this Magic Quadrant. Its flagship ESP product, 365 Total Protection, offers comprehensive email security for the Microsoft 365 environment.

Hornetsecurity acquired Vade, an AI-based email security platform, in March 2024, bolstering its detection capabilities for BEC and spear phishing. Hornetsecurity offers email archiving and email continuity services as part of its ESP solution's complete protection offering.

365 Total Protection suits European organizations with good support and language capabilities.

Strengths

- **Sales execution:** Hornetsecurity provides consistent year-to-year pricing and no-cost support.
- **Sales strategy:** Ad hoc contract renewals provide customers with a level of flexibility that is uncommon in the market.
- **Operations:** Hornetsecurity's acquisition of Vade early in 2024 contributed to the addition of key personnel in both leadership and functional areas.

Cautions

- **Product:** Hornetsecurity's ESP lags behind other evaluated vendors' platforms in detection and administrative capabilities, as well as in end-user experience functions.
- **Customer experience:** Hornetsecurity's customer relationship management lags behind other vendors in this research.
- **Product strategy:** Hornetsecurity's roadmap does not fully address current and future market requirements.

IRONSCALES

IRONSCALES is a Visionary in this Magic Quadrant. IRONSCALES' Email Security Platform provides advanced threat detection against BEC and spear phishing attacks. It includes a small range of additional security tools for collaboration security, account takeover protection and user education.

The addition of IRONSCALES' AI security assistant provides further support to cybersecurity functions as a first-level phishing triage service. IRONSCALES also leverages its product capabilities for protection against high-volume hate speech.

IRONSCALES' flagship ESP product is suitable for SMBs globally that are seeking native behavior-based end-user training and phishing simulation capabilities. It especially suits those organizations whose existing ESPs fail to properly address social engineering or lack effective automation for phishing workflows.

Strengths

- **Customer experience:** IRONSCALES has strong customer relationship management processes and positive customer feedback.
- **Market responsiveness:** IRONSCALES demonstrates an ability to adapt to emerging needs, as evidenced by its delivery of an end-user-facing chat assistant and improvements to graymail handling.
- **Innovation:** IRONSCALES has strong internal processes around R&D that support innovation and enable the delivery of new-to-market features ahead of other vendors in this research.

Cautions

- **Operations:** IRONSCALES' operations are staffed to support primarily midsize enterprises. Larger organizations should validate IRONSCALES' ability to support their requirements.
- **Vertical/industry strategy:** IRONSCALES lacks strategic initiatives targeting specific verticals or industries.
- **Product:** IRONSCALES lacks common options for deployment and configuration, as well as common infrastructure support features.

Microsoft

Microsoft is a Challenger in this Magic Quadrant. Microsoft delivers email security through Exchange Online Protection (EOP) and Microsoft Defender for Office 365, which are intertwined with its widely deployed Exchange and Exchange Online email infrastructure. EOP is a core component of Microsoft's E3 and E5 licensing packages, making it the most broadly accessible security product on the market.

Defender for Office 365 is easily accessible and integrated. Ideally, it is used with the rest of Microsoft's extensive suite of products.

Microsoft's ESP is well-suited to organizations committed to the full suite of Microsoft products and a mature email security and infrastructure function.

Strengths

- **Overall viability**: Microsoft controls a significant portion of email infrastructure and security market share, and commands a stronger corporate position than other vendors in this Magic Quadrant.
- **Geographic strategy**: Microsoft provides broad geographic support for its products.
- **Market understanding**: Microsoft has a particularly strong understanding of the email security market due to its position as a major email infrastructure provider.

Cautions

- **Customer experience**: Microsoft's customer relationship management lags behind other vendors in this research and customer feedback indicates variable service and support.
- **Sales strategy**: Microsoft's sales strategy bundles email security with non-email security products to a higher degree than other vendors in this Magic Quadrant.
- **Innovation**: Microsoft's innovations generally rely on developments in adjacent security areas, such as XDR and Copilot for Security, instead of the direct development of email security capabilities.

Mimecast

Mimecast is a Leader in this Magic Quadrant. Mimecast Advanced Email Security offers both gateway and API integration, as well as add-on modules for advanced threat protection such as its DMARC Analyzer and collaboration security. It also offers features for infrastructure support functions such as archiving and continuity services.

Mimecast recently acquired Elevate Security for improved human risk management, and Code42 for enhanced insider threat detection and response.

Mimecast's combined ESP offering suits a broad range of organizations, especially those prioritizing email archiving and human risk management.

Strengths

- **Operations**: Mimecast is well-staffed to support its global operations with above-average personnel counts for technical customer support, product management and analytic roles.
- **Sales strategy**: Mimecast's sales strategy benefits from packaging reconfigurations that align well with customer requirements and improved VAR partnering strategies.
- **Geographic strategy**: Mimecast offers broad language support and above-average, regionally aligned support infrastructure.

Cautions

- **Product**: Mimecast's implementation of language analysis is underdeveloped compared with other vendors in this research.

- **Sales execution/pricing:** Mimecast's discount programs and vertical-specific pricing are poorly defined.
- **Market understanding:** Mimecast's vision for the future of email security diverges from other vendors in this research through its focus on human risk mitigation.

Perception Point

Perception Point is a Visionary in this Magic Quadrant. Its flagship ESP product, Advanced Email Security, is available as a package that includes all capabilities and services baked into a single offering, with complementary managed service and incident response offerings by the vendor.

Perception Point's additional security for other workspace applications includes a secure browser extension, collaboration application security and secure document-sharing platforms to enhance workspace security.

Advanced Email Security is more suitable for SMBs that prioritize ease of use and managed services, as well as other organizations that do not have a fully matured internal SOC and incident response team.

Strengths

- **Market understanding:** Perception Point shows strong awareness of the needs of SMBs, especially those affected by skills gaps and workforce shortages.
- **Customer experience:** Perception Point has strong customer relationship management processes.
- **Sales strategy:** Perception Point offers flexibility in contract length and simple bundling options that are well-suited to smaller organizations.

Cautions

- **Overall viability:** Slower-than-average growth and limited availability of financial information about Perception Point create uncertainty regarding the company's long-term viability.
- **Operations:** Perception Point has a smaller employee base than other vendors in this research, and larger enterprises should confirm Perception Point's ability to support their requirements.
- **Geographic strategy:** Perception Point's geographic strategy is mostly limited to North America and Europe.

Proofpoint

Proofpoint is a Leader in this Magic Quadrant. Its flagship ESP product, Proofpoint Threat Protection, includes risk dashboards, email fraud defense and DLP capabilities that are among the market's most comprehensive offerings in their respective categories.

Proofpoint's acquisition of Tessian in December 2023 strengthened its outbound protection capabilities.

Proofpoint Threat Protection suits a broad range of organizations, especially large enterprises and those looking for a full-featured security platform.

Strengths

- **Product:** Proofpoint offers a broad set of platform tools and strong detection capabilities.
- **Market responsiveness/record:** Proofpoint's feature expansions, such as the introduction of misdirected mail protection, align with emerging threats and customer requirements.
- **Sales strategy:** Proofpoint's packaging aligns with security buyers' focus on comprehensive inbox security, and the vendor continues to add sales channels such as AWS Marketplace.

Cautions

- **Market understanding:** Proofpoint underestimates the strength of its ICES competition and the market demand for the flexibility provided by API-integrated vendors.
- **Product strategy:** Proofpoint's integration of Tessian emphasizes a need for customer experience roadmap items, such as a unified dashboard, which may impact the delivery of new functionality.
- **Sales execution/pricing:** Proofpoint's pricing is higher than that of other vendors in this research.

Trend Micro

Trend Micro is a Leader in this Magic Quadrant. Its flagship ESP product, Trend Vision One Email and Collaboration Security, can be combined with the vendor's extensive suite of add-on solutions in the ESP segment, such as XDR for Email.

Trend Micro offers additional email security capabilities, such as DLP and encryption, as well as security and awareness training features.

Trend Micro's flagship ESP product suits a broad range of organizations worldwide, including clients pursuing security vendor consolidation and those looking for integrated workspace security capabilities.

Strengths

- **Product:** Trend Micro offers versatile implementation, architecture design and administrative capabilities while maintaining a high degree of usability.
- **Market responsiveness:** Trend Micro has a strong process for collecting and channeling customer feedback to feature improvements.
- **Sales strategy:** Trend Micro's competitive displacement programs and cross-sell identification strategy are among the most aggressive in this Magic Quadrant.

Cautions

- **Innovation:** Trend Micro's R&D focus operates globally, but some feature deliveries are slightly lagging those of other vendors in this research.
- **Overall viability:** Trend Micro's email security business has grown at a slower rate than that of other vendors in this research.
- **Vertical/industry strategy:** Trend Micro lacks strategic initiatives targeting specific verticals or industries.

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 analytic tools (including but not limited to large language models, natural language processing or social graph analysis) for content analysis focused on preventing business email compromise.
- Must have a minimum of 10,000 customers *or* a minimum 1 million mailboxes protected.
- Have a combined market share in North American, European, the Middle East and African markets exceeding 40%.

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 platform'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 administration of marketing operations and 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
Marketing Execution	Low
Customer Experience	Medium
Operations	Medium

Source: Gartner (December 2024)

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 2024)

Quadrant Descriptions

Leaders

Leaders have a strong vision for the future of ESPs, balanced with the Ability to Execute on those visions. While Leaders may vary in product efficacy or functionality, their services offered are consumable by broad swathes of the email market and have strong commitments to customer success. Leaders are early to identify new attack trends and move quickly to fill gaps created by an evolving threat landscape, either by innovation or acquisition. Leaders excel with technical capabilities, infrastructure that supports progressive product strategies, and an emphasis on customer success.

Challengers

Challengers exhibit operational capabilities, stability, visibility in the market, and strength in one or more technical product features. Their vision is unlikely to change the market. Challengers develop new capabilities in response to advancements made by vendors in the other quadrants, or focus on the development of other products in their portfolio. Challengers are practical choices for customers with established strategic relationships, but may lack “bleeding edge” functionality as the market shifts.

Visionaries

Visionaries address broadly applicable needs within the market that lack representation among other ESPs. Alternatively, they focus on addressing attack vectors or pain points that position them for broad adoption in the future. Visionaries may offer unique features, focused on a specific industry, or address a specific set of use cases to a greater extent than vendors in other quadrants.

Niche Players

Niche Players provide ESP technology that is adequate, but are likely not selected based on the strength of their detection technology. Reasons for selection may include lower total cost of ownership, integrations with existing infrastructure, beneficial integrations with an XDR, or regional support. Niche Players that primarily serve infrastructure support functions can provide value as an additional layer of security in conjunction with other ESPs.

Context

Efficacy is a primary concern of email security customers, especially for protection against email security threats like spear phishing and business email compromise. Natural language processing, large language models and social graph analysis represent a significant advancement in combating these attack methods. Customers should consider some combination of these technologies as prerequisites when building their email security platform shortlists, followed by additional security or infrastructure features.

The market has also seen significant change in representative vendors over the last decade, with a greater number of relatively small vendors seeking to gain market share by catering to specific use cases and security features. While many ESPs aim to be industry-agnostic, email security customers may find some email security vendors to be more suitable for use cases within their vertical.

Market Overview

Email infrastructure has predominantly transitioned to the cloud, increasing the market potential for vendors primarily delivering security outside the confines of traditional secure email gateway (SEG) implementation. Advancements in technology used in email security platforms (ESPs) have changed significantly over the last decade, especially with regard to three areas: implementation, social engineering detection and variations in product capabilities.

Integrated cloud email security (ICES) solutions most commonly refer to ESPs that utilize API connections to existing email infrastructure to monitor inboxes. While some may also utilize journaling to minimize detection times, the remediation function is the same. ICES solutions drastically reduce implementation complexity, timelines and, by extension, the ability to competitively compare the effectiveness of various ESPs. They have increasingly challenged the standard of in-line email security, meaning organizations must now consider the ideal implementation schema before finalizing their vendor selections.

Simultaneous to the rise of ICES solutions, advances in natural language processing (NLP) and the advent of large language models (LLMs) have changed both how organizations are attacked and how ESPs defend against social engineering attacks. Humans are increasingly incapable of identifying social engineering attacks as LLMs are refined for purpose by attackers. ESPs have increasingly developed capabilities to programmatically read and understand email content in the context of social engineering. Some vendors include social graph analysis to identify messaging patterns among social groups and identity context to improve fidelity on suspicious mail. Gartner considers these to be essential components for the future of email security.

Features and product lines have become more fluid as new entrants to the email security market cater to specific customer profiles or market segments. Examples include managed services, data loss prevention (DLP), data classification and automation. The concept of a “full-service platform” will mean different things to different organizations, making comprehensive requirement collection a key activity.

Together, the rise of ICES vendors and advancement of social engineering detection has led to increased merger and acquisition activity in the email security space. Buyers seem to be split between two camps: Email security vendors acquiring functionality as opposed to developing it in-house; and vendors in adjacent security spaces expanding the scope of their own security platforms.

Acronym Key and Glossary Terms

BEC	business email compromise

ESP	email security platform
DMARC	domain-based message authentication, reporting, and conformance
DLP	data loss prevention
ICES	integrated cloud email security
LLM	large language model
NLP	natural language processing
SEG	secure email gateway
SOC	security operations center
VAR	value-added reseller

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and

organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.