Critical Capabilities for Email Security Platforms

15 January 2025 - ID G00806899 - 24 min read

By: Nikul Patel, Franz Hinner, Deepak Mishra, Max Taggett

Initiatives:Infrastructure Security; Build and Optimize Cybersecurity Programs

Security and risk management leaders can use this research to evaluate email security platforms for five key use cases: core email protection, outbound protection, security platform integration, power user capabilities, and managed service environments.

This Critical Capabilities is related to other research:

Magic Quadrant for Email Security Platforms

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- Most vendors in the email security platform (ESP) market are responding to the evolving email threat landscape by introducing advanced capabilities to defend against spear phishing attacks. These include business email compromise (BEC), vendor email compromise (VEC), QR code phishing (quishing) and account takeover (ATO).
- Solutions that include the ability to detect and protect against misdirected emails, data leaks and compliance violations are a differentiator for the outbound protection use case.
- Almost all vendors in the ESP market are enhancing their security capabilities to deliver a comprehensive platform that integrates with threat detection, investigation and response (TDIR) solutions. This expansion aims to reduce administrative burdens and boost overall security effectiveness.
- While most vendors offer cloud-delivered email solutions, fewer offer products that support hybrid environments and a high degree of customization requirements.
- Many vendors now offer managed email security services directly or through partners to supplement customers that face staffing constraints.

Recommendations

Security and risk management leaders responsible for infrastructure security and email protection should:

- Utilize an ESP that includes malware protection, antiphishing measures, impersonation defense, and internal email monitoring to safeguard against sophisticated email-based attacks.
- Plan to pilot vendors and assess their capability to detect and protect against misdirected emails, data leaks, compliance violations and ATO.
- Integrate security orchestration automation and response (SOAR) capabilities with your ESP to streamline event detection, analysis and remediation, thereby reducing response times, enhancing operational efficiency and lowering cybersecurity risks.
- Assess ESPs for integration compatibility across the incumbent security infrastructure to enable a more effective and efficient security environment.

- Address complex email security requirements by supplementing internal teams with managed services when they lack sufficient personnel and skills.

What You Need to Know

ESPs bolster the security of email infrastructure by preventing malicious or unsolicited messages. They also provide a variety of additional features — such as encryption, data loss prevention (DLP), and domain-based message authentication, reporting and conformance (DMARC) — to safeguard against data loss and BEC attacks. Furthermore, ESPs support detection and response functions to assist enterprises in threat investigation and remediation efforts.

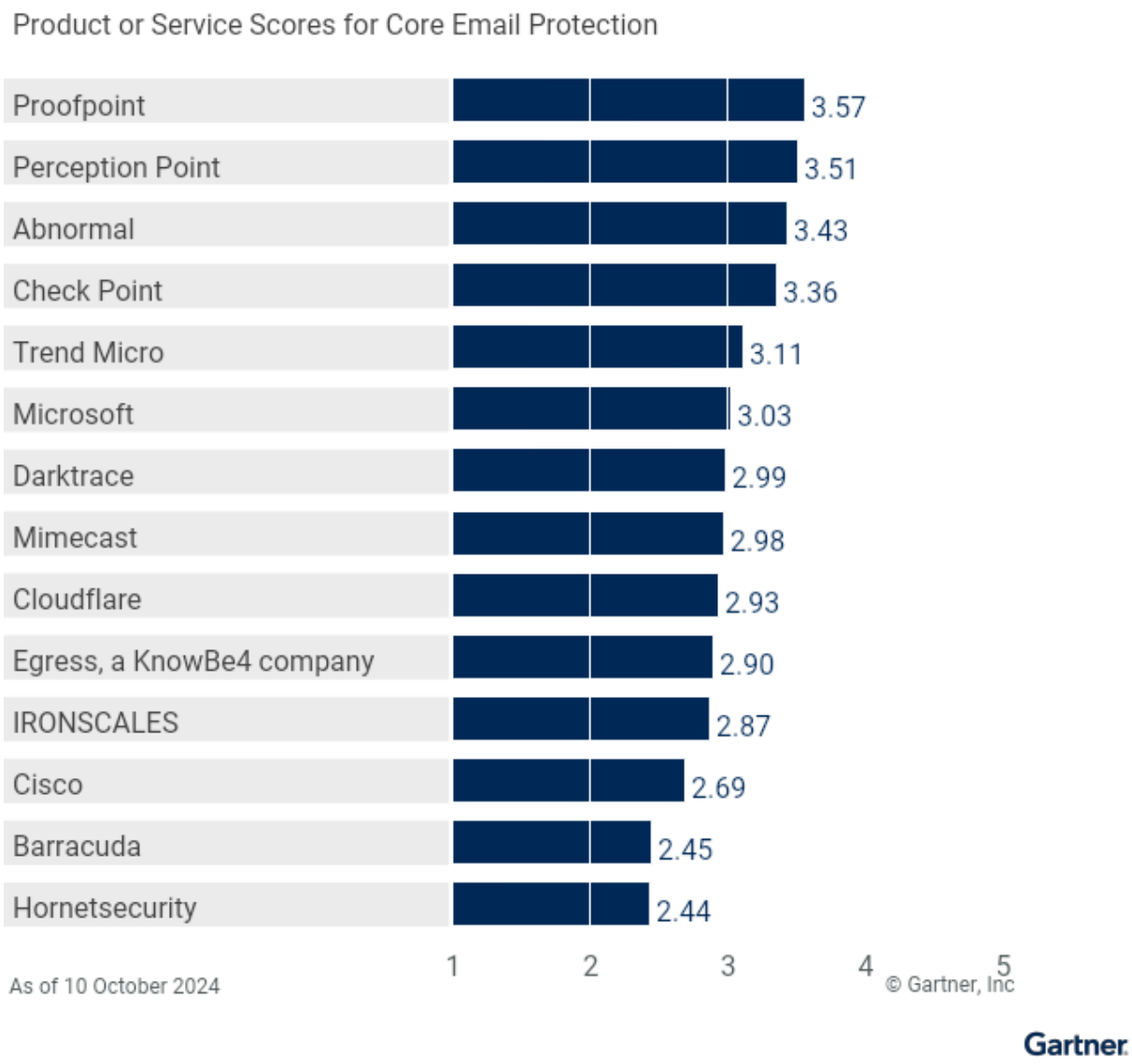
In today's market, spam and malware protection are standard features of ESPs. At the same time, vendors are investing in advanced technologies to detect social engineering attacks, including complex phishing threats like BEC, VEC and ATO. Vendors are also integrating with security information and event management (SIEM) and extended detection and response (XDR) tools to offer a unified view of security events and enable remediation across endpoints, email, identity, network, cloud and other security domains.

Buyers of modern ESP products expect strong threat protection as the foundational element of these offerings. Many organizations are evaluating ESP products to address threats such as BEC, VEC and ATO that bypass traditional secure email gateways. Their aim is to improve effectiveness against advanced phishing threats. The growing complexity of managing email alerts, along with the need to maintain a dedicated email security function and address cybersecurity skills gaps, is driving increased demand for managed security services. Clients looking to augment their existing email security function, or to offload the administration of the function externally, expect these services.

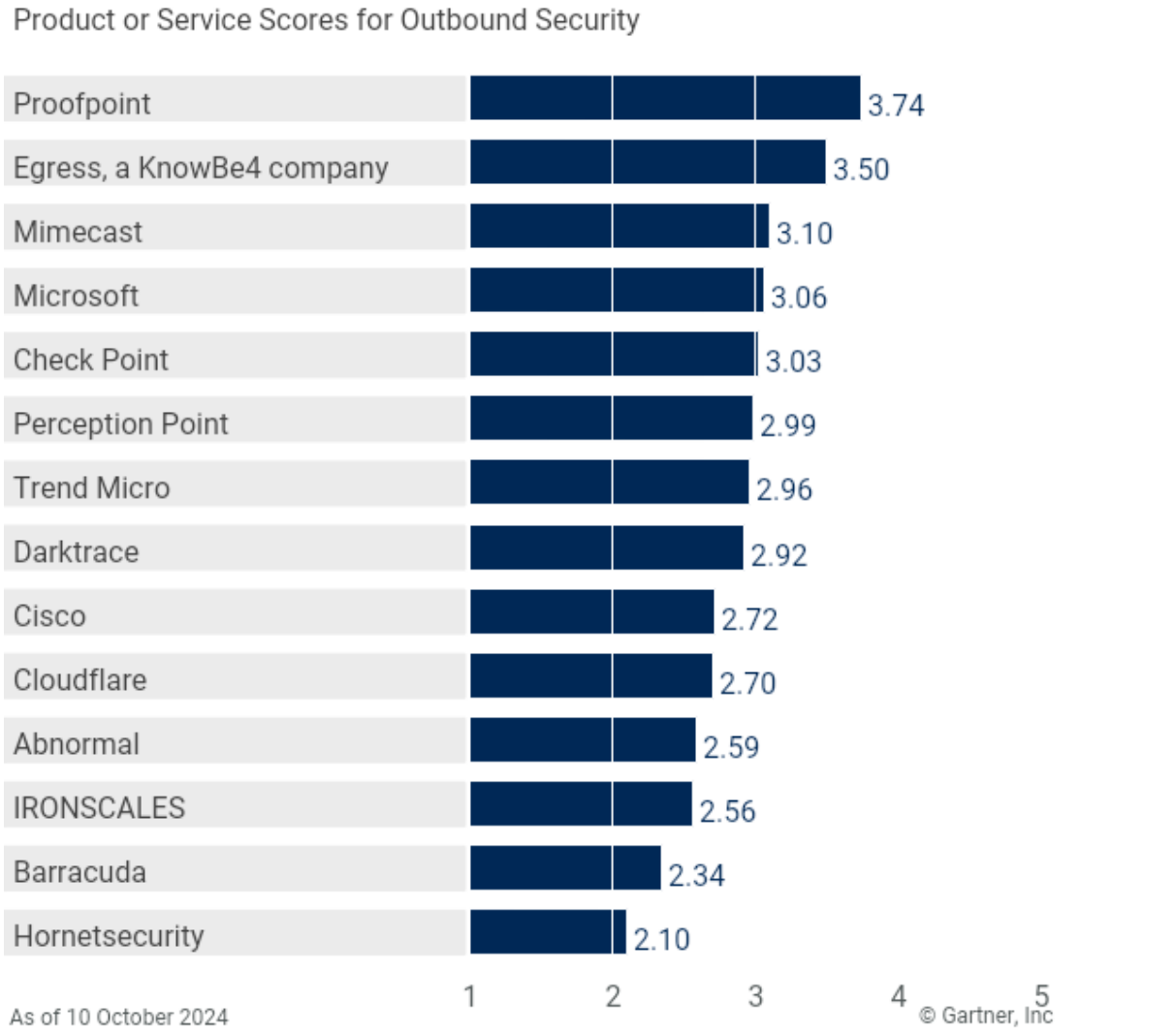
Analysis

Critical Capabilities Use-Case Graphics

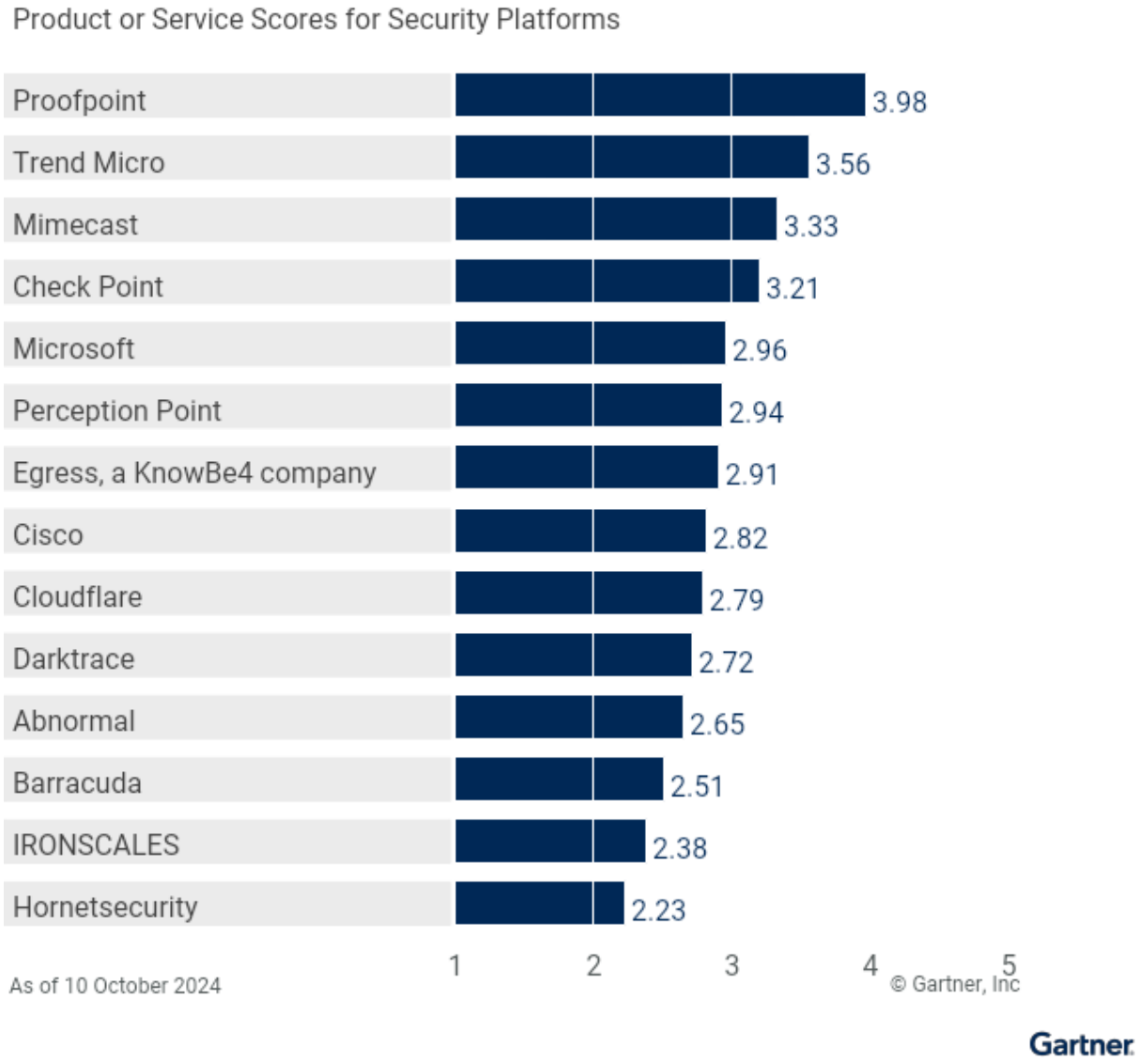
Vendors' Product Scores for Core Email Protection Use Case



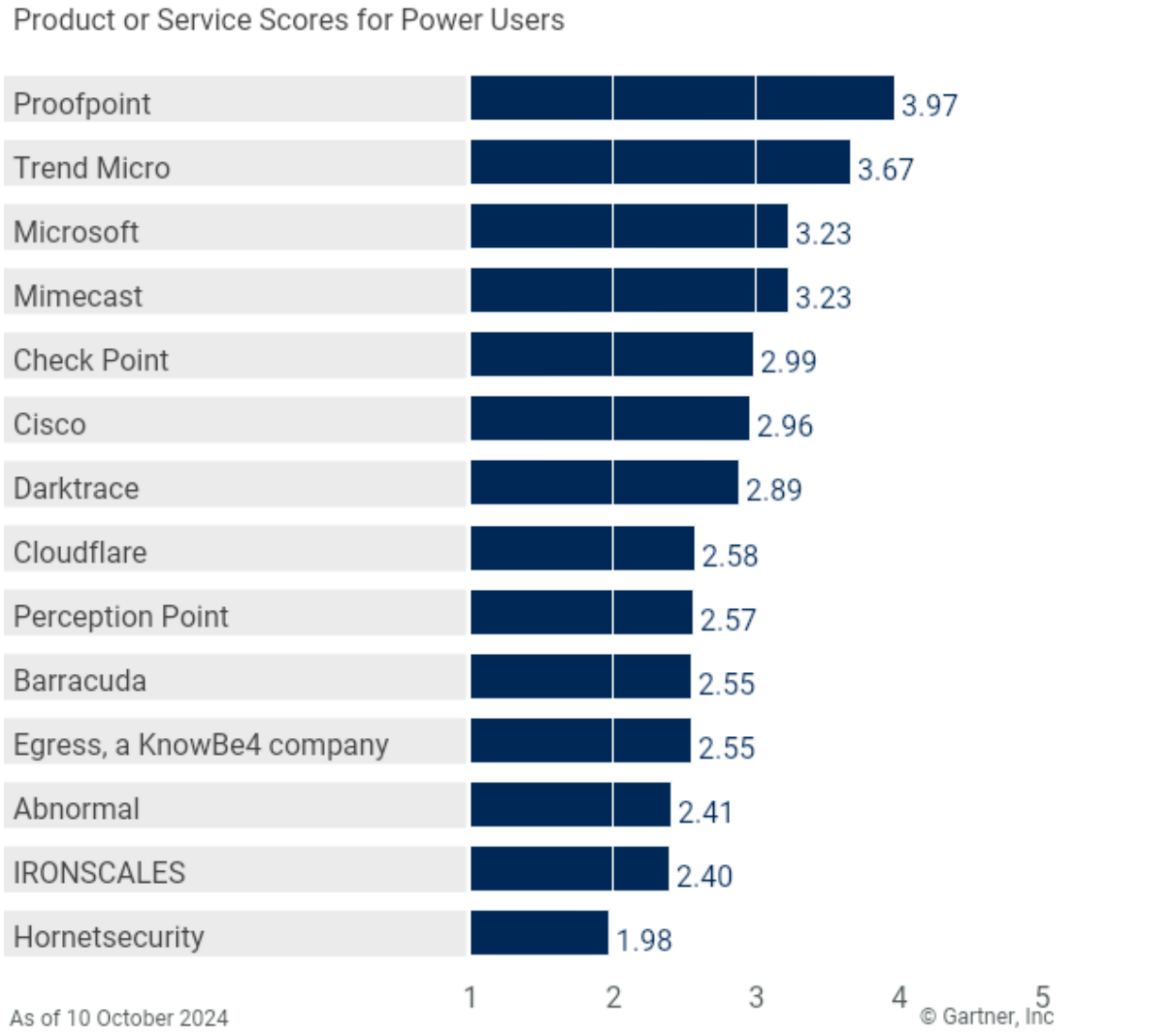
Vendors' Product Scores for Outbound Security Use Case



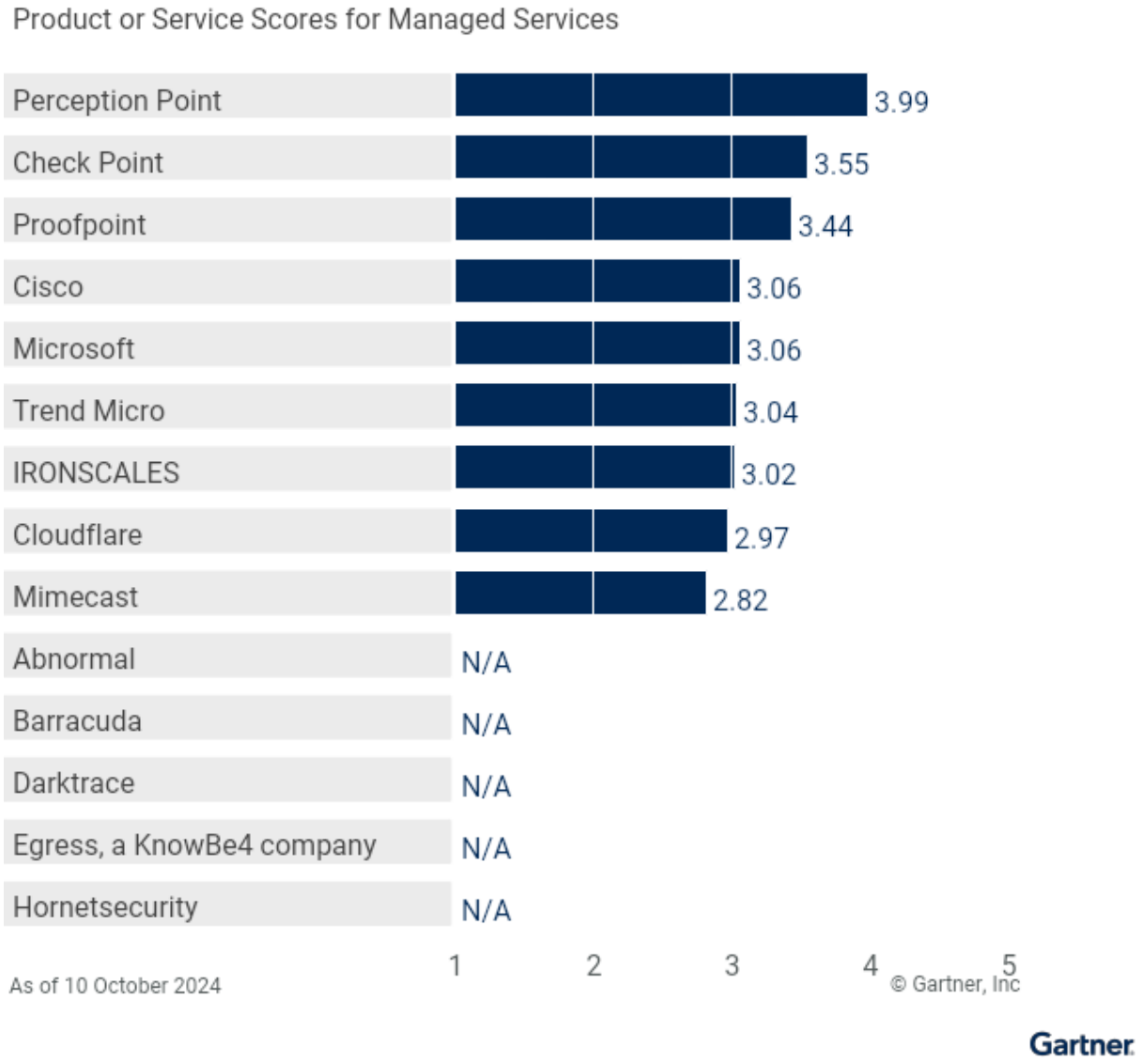
Vendors' Product Scores for Security Platforms Use Case



Vendors' Product Scores for Power Users Use Case



Vendors' Product Scores for Managed Services Use Case



Vendors

Abnormal

The Abnormal Human Behavior AI Platform is well-suited for organizations seeking strong AI-based email protection capabilities. It excels in the core email protection use case by providing effective email protection through detailed analysis of social graphing anomalies, content analysis capability, excellent support for deployment and onboarding, and a user-friendly interface. The platform is also appropriate for organizations looking to protect outbound emails from email ATO threats. Furthermore, its detection capabilities are enhanced by covering various collaboration platforms such as Microsoft Teams, Slack and Zoom.

Abnormal Security's platform score for the outbound security use case is somewhat negatively impacted by a lack of native DLP and encryption capabilities. It performs below average in the power users use case due to lack of DMARC management, message/mail transfer agent (MTA) and on-premises deployment functionality. Abnormal was not assessed in the managed service use case because direct vendor-delivered managed service offerings are needed. Instead, the vendor relies on its service partner ecosystem.

Barracuda

The Barracuda Email Protection platform is suitable for organizations of all sizes seeking comprehensive email security integrated with a broader security ecosystem. The platform extends protection to Microsoft 365 applications, including Exchange Online, OneDrive, Teams and SharePoint, and supports email encryption and DLP capabilities. Barracuda provides strong deployment and onboarding support, although it could improve its coverage for the power users use case in certain areas.

As part of core email protection, Barracuda Email Protection offers multilayered security that effectively blocks various email threats. However, its security operations integration capabilities may have room for improvement, relative to some competitors. Barracuda offers managed services options through its MSP program, allowing partners to provide managed email protection services to their customers. However, it lacks direct vendor-managed services and, therefore, was not considered in the vendor managed services use case as the quality of service varies by partner organization.

Check Point

Check Point Harmony Email & Collaboration (HEC) is suitable for organizations of all sizes seeking a comprehensive security platform, including a managed service offering. Check Point excels in core email protection with advanced threat detection, including content and artifact analysis, ease of use, and deployment and onboarding capabilities. It also supports identifying threats across various collaboration platforms like Microsoft Teams, Slack and Google Workspace.

Check Point's ESP performs well in the outbound security use case due to its strong threat detection for misdirected emails, DLP and encryption capabilities. The broad integrated security suite and mature security operations integration capability enhances its coverage of the security platforms use case. Check Point excels in the managed security services use case, thanks to its vendor-managed services, advanced security features and strong geographic support capabilities.

Cisco

Cisco Secure Email is well-suited for organizations seeking an ESP integrated with their broader security ecosystem and secure email gateway functionalities. Cisco excels in power user scenarios with strong infrastructure support and MTA/on-premises deployment options. Cisco also excels in managed services, offering direct vendor-delivered solutions and robust global support. Its worldwide presence ensures consistent service quality.

Cisco lags leading competitors in the core email protection use case in advanced content analysis, and in usability, deployment and onboarding processes. In the security platforms use case, Cisco performs slightly below average due to multiple management consoles, which can fragment user experience, creating a disorganized analyst workflow. The vendor instead relies on its extended detection and response (XDR) solution to unify security operations.

Cloudflare

The Cloudflare Email Security platform is suitable for organizations of all sizes seeking integrated email protection as part of Cloudflare's comprehensive security ecosystem, and for those looking for additional protection against multichannel phishing attacks. Its coverage of the core email protection use case is bolstered by robust content analysis, threat detection and ease of deployment.

In the security platforms use case, Cloudflare demonstrates a comprehensive zero-trust approach, combining email security with other capabilities including, browser isolation, DMARC management and robust security operations integration. Despite its below-average managed services capability, Cloudflare's PhishGuard — a managed service focused on phishing protection with demonstrably strong geographic support — shows promise.

Darktrace

Darktrace's /EMAIL platform is suitable for organizations looking to enhance their existing email security solution with a solid, advanced, AI-driven core email protection capability. Darktrace performs well in the core email protection use case because of its robust AI and behavioral-based threat detection capabilities. It extends protection to a range of collaboration applications such as Microsoft 365 (including Teams), Slack and Zoom. Darktrace performs well in the outbound security use case due to its ability to detect unusual behavior and content changes in email and Microsoft Teams.

Darktrace's performance in the security platforms use case is below average due to the platform's lack of DMARC management, encryption and security awareness training functionalities. Its coverage of the power users use case lags market leaders due to lack of deep customization and infrastructure support capability. Darktrace does not offer a vendor-managed service, but instead provides options through its MSP program. This allows partners to provide managed email protection services to their customers. Due to variations of services, the vendor was not assessed in the managed service use case.

Egress, a KnowBe4 company

Egress Intelligent Email Security is a strong choice for organizations using advanced behavioral-based inbound and outbound email threat protection, with a focus on human risk management. Egress excels in both core email protection and outbound security use cases thanks to its robust content analysis capability, focusing on AI-powered threat detection, misdirected emails, prevention of data loss caused by human error and encryption.

In terms of the core email protection use case, Egress offers advanced phishing threat detection, contextual machine learning and social graph analysis to understand individual behavior and detect threats. It also provides continuous education using real-time teachable moments, including contextual banners and prompts delivered at the point of risk. Egress' performance in the power users use case is below average due to lack of DMARC management, MTA and on-premises deployment functionality. Egress was not assessed in the managed services use case because direct vendor-delivered managed services are needed. Instead, the vendor relies on its service partner ecosystem.

Hornetsecurity

Hornetsecurity's 365 Total Protection is particularly suitable for small and midsize organizations seeking to enhance their existing Microsoft 365 email security and compliance. Its performance in the security platforms use case is boosted by its flexible email archiving solutions, which include retention periods from six months to 30 years, continuity solutions, encryption capabilities and AI-powered threat detection. Hornetsecurity lags competitors in core email protection due to relatively low scores for content analysis coverage and ease of use. It also lags in the outbound email security use case due to subpar DLP and content analysis capabilities.

Hornetsecurity's coverage of power user scenarios makes it unsuitable for organizations looking for a high degree of customization and infrastructure support capability. Hornetsecurity was not assessed in the managed services use case because it lacks direct vendor-delivered managed services. The vendor instead relies on its service partner ecosystem.

IRONSCALES

IRONSCALES' Email Security Platform is suitable for small and midsize organizations seeking a product that provides AI-powered advanced threat detection, security operations center (SOC) automation and an adequate managed service capability. Its performance in the security platforms use case is enhanced by the solution combining AI-driven email security with security awareness training, and ATO protection functionality. It also enables secure collaboration applications such as Microsoft Teams.

IRONSCALES performs well in the managed services use case thanks to its vendor-managed service offering and broad language support, designed for easy MSP management supporting regional language requirements. In the outbound security protection use case, IRONSCALES lags the majority of its competitors in this evaluation due to lack of advanced DLP, monitoring of outbound email and artifact analysis capability. IRONSCALES ' performance in the power users use case is below average due to limited security operations integration and infrastructure support capabilities.

Microsoft

Microsoft's ESP solution, delivered via Exchange Online Protection and Microsoft Defender for Office 365, is suitable for organizations of all sizes globally seeking an email security solution as part of a broader security platform. Microsoft excels in the security platforms use case, thanks to its strong integration with Microsoft 365, Defender, Entra and Sentinel. It also excels in the power users use case due to its breadth of security capabilities. These include DLP, encryption and security awareness, antiphishing, and attack simulation training. At the same time, it offers a high degree of customization for administrative configuration.

Microsoft's recent introduction of a direct vendor-delivered managed service, coupled with its strong geographic support capability, contributed to its decent performance in the managed services use case. In the core email protection use case, Microsoft benefits from advanced investigation and response capabilities, integration with SIEM/SOAR solutions, and global threat intelligence. However, it lags market leaders due to lack of advanced content analysis capability and preset security policies for ease of use.

Mimecast

Mimecast Email Security suits organizations of all sizes, especially those looking for a comprehensive solution providing email security, collaboration security and outbound protection. Mimecast's performance in the security platforms use case is enhanced by its solid security operations integration capability and broad security capabilities, which include DMARC management, encryption and security awareness training. It also excels in the power users use case due to its platform's support of granular controls and high degree of customization.

Mimecast's coverage for the outbound security use case is solid because of its DLP, outbound threat protection, and content and artifact analysis capabilities. However, its coverage of the core email protection use case lags leading competitors in advanced content analysis capability. Mimecast trails competitors in the managed services use case due to lack of full coverage of service across all solution offerings.

Perception Point

Perception Point's Advanced Email Security is particularly suitable for organizations of all sizes seeking a comprehensive email and collaboration security platform with AI-powered threat detection and managed services. The platform excels in the managed services use case due to its vendor-delivered managed service and 24/7 managed incident response, packaged with its core email protection. Perception Point also excels in the core email protection use case thanks to its robust content and artifact analysis, deployment and onboarding, and continuity and performance capabilities. Furthermore, it enhances its detection capabilities by covering various collaboration platforms such as Microsoft Teams and Slack.

However, Perception Point's coverage of the outbound security use case lags market leaders due to lack of native email DLP functionality and content analysis to identify misdirected emails. The vendor's performance in the power users use case is somewhat compromised by lack of on-premises deployment, MTA and detailed administrative configuration capabilities.

Proofpoint

Proofpoint Threat Protection suits organizations of all sizes, especially large enterprises and those seeking coverage across all security outcome use cases assessed. The platform excels in core email protection due to its robust AI-powered threat detection, multilayered content analysis and advanced sandboxing capabilities. It also extends protection for messaging and cloud collaboration apps, including Microsoft 365 (including Teams), Google Workspace and DropBox.

Proofpoint excels in the outbound security use case due to its advanced threat protection, DMARC management, DLP and encryption offerings. In the power users use case, Proofpoint demonstrates a strong infrastructure support capability that includes support for on-premises deployment, SMTP relay, strong API integration, granular controls, highly customizable policies and detailed administrative configuration features. Proofpoint's performance in the managed services use case exceeds most competitors due to its direct vendor-managed service and strong geographic support capability.

Trend Micro

Trend Micro's Trend Vision One Email and Collaboration Security is suitable for organizations of all sizes seeking a comprehensive email and collaboration security platform with advanced threat protection and robust core email protection. It performs well in the core email protection use case due to its AI-powered threat detection, phishing and BEC protection, and advanced sandboxing capabilities. Core email protection also extends protection capabilities for collaboration applications, including Microsoft 365 (OneDrive, SharePoint), Microsoft Teams, Google Workspace, Box and DropBox.

Trend Micro's coverage for both the security platforms and power users use cases is bolstered by its support for cloud, hybrid and on-premises deployment, DMARC management and reporting services, monitoring for outbound threats and strong customization features. Trend Micro performs fairly well in the outbound protection use case thanks to its artifact and content analysis capability, including DLP and autoredaction of misdirected emails. The vendor trails market leaders in the managed services use case due to its lack of in-house geographic support, instead relying on the Trend Partner Program.

Context

Email continues to be a vital open communication and collaboration tool in most organizations, serving as a repository for a significant portion of an organization's unstructured data. It is also the primary target for attackers, making it a critical component of any workplace security strategy. However, not all organizations have the same resources or requirements for an email security platform.

Most ESPs have evolved beyond basic anti-malware and phishing protection. Buyers should prioritize solutions that offer robust defenses against sophisticated email threats like BEC, VEC and quishing. These solutions should employ a combination of machine learning techniques in their detection logic. Organizations concerned about both accidental and intentional data loss are looking for solutions that emphasize outbound email protection. Furthermore, the rise in credential theft and misuse is driving demand for solutions designed to protect against ATO attacks.ESPs are essential for security operations and XDR strategies due to the ongoing threat of phishing. They should be integrated into a comprehensive workspace security platform rather than functioning as isolated products (see Securing Hybrid Work: Adopting the Right Workspace Security Strategy). Security and risk management leaders, including CISOs, aiming to consolidate workspace security should prioritize integrating ESPs into a broader platform approach.

Large enterprise power users typically seek scalable solutions that offer a comprehensive range of features and extensive policy controls. Integration with SOC tools and automation to improve security operations and incident response workflows are crucial capabilities for these users. Additionally, some vendors provide solutions tailored to mature organizations, addressing specific use-case requirements such as on-premises, cloud and hybrid deployments, MTA functionality, and enhanced customization options.

With the increasing frequency and complexity of phishing attacks, it is essential that organizations effectively manage email alerts, triaging and responding to threats. Organizations with limited resources are increasingly relying on managed services to optimize the use of their ESPs.

Market Definition

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)

Product/Service Trends

ESPs safeguard organizations from email-based threats and are increasingly expanding their capabilities to prevent malicious or unsolicited messages across other collaboration platforms. These platforms offer a range of features, including anti-malware, anti-spam, antiphishing, BEC protection and spear phishing defenses. Typically delivered as cloud-based services, ESPs may also offer on-premises or API-based deployment options to suit various organizational needs.

Critical Capabilities Definition

Deployment and Onboarding

The initial deployment and onboarding of the solution, initial policy configuration, and solution tuning from an administrative standpoint.

Security Operations Integrations

The ability to meet diverse organizational security needs by offering and integrating a variety of proprietary security controls, as well as connecting with threat detection, investigation, and response (TDIR) platforms to facilitate more cohesive security operations workflows.

Content Analysis

The ability of the vendor to provide capabilities to protect the user's mailbox from advanced phishing, impersonation and account takeover attacks.

Artifact Analysis

The ability of the vendor to provide protection capabilities including URL/file scanning, anti-spam, malware and message metadata analysis.

Ease of Use

The ease of use of the administration console based on analyst workflow, interface intuitiveness, end-user reporting and alert workflow.

Continuity and Performance

The ability of the ESP to complete its analysis without delaying mail flow or allowing malicious mail to dwell in the inbox for extended periods of time due to scanning, analysis or vendor-related outages.

Infrastructure Support

The vendor's ability to offer additional email infrastructure capabilities, including MTA and email archiving for long-term retention, compliance, reporting and recovery.

Outbound Protection

The provider's ability to monitor against misdirected email flow and data exfiltration scenarios.

Managed Services

The provider's ability to deliver various managed security services.

Geographic Support

The vendor's ability to support the global customer base through regional offices, service and support centers, partners and product localization, including regional data storage.

Use Cases

Core Email Protection

This use case reflects core ESP functionality, inbound protection, anti-spam/malware/phishing filtering, URL defense and BEC protection.

It's suited for organizations that rely on strong email protection and detection capabilities to ensure the safety of the user's inbox.

Outbound Security

This use case reflects the platform's ability to provide outbound protection for all mail leaving the corporate boundary.

It includes DLP, encryption, credential leakage, impersonation, account takeover and outbound mail scanning. This use case is suited for organizations with strict requirements connected to regulation and compliance, an emphasis on data security or significant brand impersonation concerns.

Security Platforms

This use case reflects a broad set of natively integrated ESP product capabilities in a single platform.

It's suited for organizations seeking to augment staff, leverage automation and optimize workflows in a "single pane of glass" without the need to manage multiple vendor relationships.

Power Users

This use case reflects ESP product capability to support on-premises deployment option, MTA and extensive customization or advanced features.

It's suited for organizations that must satisfy architectural and regulatory requirements and have staff dedicated to the operation and maintenance of their email infrastructure. These organizations are mature, well-staffed, and can integrate and operate ESP solutions in-house, rarely requiring MSS/MDR support.

Managed Services

This use case reflects managed service delivery for ESP.

It's suited for severely understaffed organizations that see technology as an operational necessity and prefer deploying solutions with managed service add-ons that best complement their minimal security staff.

Inclusion and Exclusion Criteria

To qualify for inclusion in this Critical Capabilities report and companion 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%.

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	Core Email Protection	Outbound Security	Security Platforms	Power Users	Managed Services
Deployment and Onboarding	10%	2%	5%	12%	7%
Security Operations Integrations	0%	10%	50%	38%	0%
Content Analysis	40%	20%	10%	0%	8%
Artifact Analysis	40%	20%	10%	0%	8%
Ease of Use	5%	6%	0%	0%	0%
Continuity and Performance	5%	0%	0%	5%	15%
Infrastructure Support	0%	0%	15%	45%	0%
Outbound Protection	0%	42%	10%	0%	0%
Managed Services	0%	0%	0%	0%	52%
Geographic Support	0%	0%	0%	0%	10%
As of 10 October 2024					

Source: Gartner (January 2025)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	Abnormal	Barracuda	Check Point	Cisco	Cloudflare	Darktrace	Egress, a KnowBe4 company	Hornetsecurity	IRONSCALES	Microsoft	Mimecast	Perception Point	Proofpoint	Trend Micro
Deployment and Onboarding	3.5	2.8	3.1	2.3	3.5	2.9	2.9	2.3	2.2	3.3	3.3	3.4	3.6	4.3
Security Operations Integrations	2.8	2.7	3.6	2.8	3.1	2.5	3.0	2.5	2.2	2.6	3.7	3.1	4.3	4.0
Content Analysis	3.7	2.3	3.8	2.9	3.0	3.3	3.0	2.4	3.0	3.1	2.9	4.0	3.4	2.9
Artifact Analysis	3.0	2.3	2.8	2.5	2.6	2.4	2.5	2.5	2.7	2.9	2.9	3.1	3.6	3.0
Ease of Use	3.8	3.5	4.0	2.3	2.5	3.5	4.0	2.6	3.9	3.2	3.3	3.1	3.3	3.4
Continuity and Performance	4.1	3.0	4.2	3.6	4.3	4.9	4.1	2.4	3.5	2.7	3.3	3.5	4.8	3.0
Infrastructure Support	1.6	2.3	2.3	3.2	1.7	3.0	1.9	1.4	2.5	3.8	2.8	1.8	3.7	3.3
Outbound Protection	1.6	2.1	2.5	2.8	2.5	3.0	4.3	1.6	2.2	3.2	3.1	2.4	3.9	2.6
Managed Services	1.5	1.5	3.5	3.1	2.7	1.8	1.8	1.4	3.2	3.0	2.5	4.6	3.1	3.0
Geographic Support	2.4	3.0	3.5	3.1	2.3	3.1	1.8	2.3	2.2	3.8	3.3	2.7	3.0	2.6
As of 10 October 2024														

Source: Gartner (January 2025)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

(Enlarged table in Appendix)

Use Cases	Abnormal	Barracuda	Check Point	Cisco	Cloudflare	Darktrace	Egress, a KnowBe4 company	Hornetsecurity	IRONSCALES	Microsoft	Mimecast	Perception Point	Proofpoint	Trend Micro
Core Email Protection	3.43	2.45	3.36	2.69	2.93	2.99	2.90	2.44	2.87	3.03	2.98	3.51	3.57	3.11
Outbound Security	2.59	2.34	3.03	2.72	2.70	2.92	3.50	2.10	2.56	3.06	3.10	2.99	3.74	2.96
Security Platforms	2.65	2.51	3.21	2.82	2.79	2.72	2.91	2.23	2.38	2.96	3.33	2.94	3.98	3.56
Power Users	2.41	2.55	2.99	2.96	2.58	2.89	2.55	1.98	2.40	3.23	3.23	2.57	3.97	3.67
Managed Services	N/A	N/A	3.55	3.06	2.97	N/A	N/A	N/A	3.02	3.06	2.82	3.99	3.44	3.04
As of 10 October 2024														

Source: Gartner (January 2025)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Acronym Key and Glossary Terms

ATO	account takeover
BEC	business email compromise
DMARC	domain-based message authentication, reporting, and conformance
DLP	data loss prevention
ESP	email security platform
MSP	managed service provider
MSS/MDR	managed security services/managed detection and response
MTA	mail transfer agent
SIEM	security information and event management
SOC	security operations center
TDIR	threat detection, investigation, and response
VEC	vendor email compromise
XDR	extended detection and response

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

How Products and Services Are Evaluated in Gartner Critical Capabilities

Magic Quadrant for Email Security Platforms

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Core Email Protection*	*Outbound Security*	*Security Platforms*	*Power Users*	*Managed Services*
Deployment and Onboarding	10%	2%	5%	12%	7%
Security Operations Integrations	0%	10%	50%	38%	0%
Content Analysis	40%	20%	10%	0%	8%
Artifact Analysis	40%	20%	10%	0%	8%
Ease of Use	5%	6%	0%	0%	0%
Continuity and Performance	5%	0%	0%	5%	15%
Infrastructure Support	0%	0%	15%	45%	0%
Outbound Protection	0%	42%	10%	0%	0%
Managed Services	0%	0%	0%	0%	52%
Geographic Support	0%	0%	0%	0%	10%
As of 10 October 2024					

Source: Gartner (January 2025)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*Abnormal*	*Barracuda*	*Check Point*	*Cisco*	*Cloudflare*	*Darktrace*	*Egress, a KnowBe4 company*	*Hornetsecurity*	*IRONSCALES*	*Microsoft*	*Mimecast*	*Perception Point*	*Proofpoint*	*Trend Micro*
Deployment and Onboarding	3.5	2.8	3.1	2.3	3.5	2.9	2.9	2.3	2.2	3.3	3.3	3.4	3.6	4.3
Security Operations Integrations	2.8	2.7	3.6	2.8	3.1	2.5	3.0	2.5	2.2	2.6	3.7	3.1	4.3	4.0
Content Analysis	3.7	2.3	3.8	2.9	3.0	3.3	3.0	2.4	3.0	3.1	2.9	4.0	3.4	2.9
Artifact Analysis	3.0	2.3	2.8	2.5	2.6	2.4	2.5	2.5	2.7	2.9	2.9	3.1	3.6	3.0
Ease of Use	3.8	3.5	4.0	2.3	2.5	3.5	4.0	2.6	3.9	3.2	3.3	3.1	3.3	3.4

Continuity and Performance	4.1	3.0	4.2	3.6	4.3	4.9	4.1	2.4	3.5	2.7	3.3	3.5	4.8	3.0
Infrastructure Support	1.6	2.3	2.3	3.2	1.7	3.0	1.9	1.4	2.5	3.8	2.8	1.8	3.7	3.3
Outbound Protection	1.6	2.1	2.5	2.8	2.5	3.0	4.3	1.6	2.2	3.2	3.1	2.4	3.9	2.6
Managed Services	1.5	1.5	3.5	3.1	2.7	1.8	1.8	1.4	3.2	3.0	2.5	4.6	3.1	3.0
Geographic Support	2.4	3.0	3.5	3.1	2.3	3.1	1.8	2.3	2.2	3.8	3.3	2.7	3.0	2.6
As of 10 October 2024														

Source: Gartner (January 2025)

Table 3: Product Score in Use Cases

Use Cases	*Abnormal*	*Barracuda*	*Check Point*	*Cisco*	*Cloudflare*	*Darktrace*	*Egress, a KnowBe4 company*	*Hornetsecurity*	*IRONSCALES*	*Microsoft*	*Mimecast*	*Perception Point*	*Proofpoint*	*Trend Micro*
Core Email Protection	3.43	2.45	3.36	2.69	2.93	2.99	2.90	2.44	2.87	3.03	2.98	3.51	3.57	3.11
Outbound Security	2.59	2.34	3.03	2.72	2.70	2.92	3.50	2.10	2.56	3.06	3.10	2.99	3.74	2.96
Security Platforms	2.65	2.51	3.21	2.82	2.79	2.72	2.91	2.23	2.38	2.96	3.33	2.94	3.98	3.56
Power Users	2.41	2.55	2.99	2.96	2.58	2.89	2.55	1.98	2.40	3.23	3.23	2.57	3.97	3.67
Managed Services	N/A	N/A	3.55	3.06	2.97	N/A	N/A	N/A	3.02	3.06	2.82	3.99	3.44	3.04
As of 10 October 2024														

Source: Gartner (January 2025)