Email Security

Martin Kuppinger
John Tolbert
December 14, 2023

LEADERSHIP
COMPASS
2023

This report provides an overview of the Email Security market and provides you with a compass to help you to find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing Email Security solutions.

Contents

Figures

Introduction / Executive Summary

Email has been a standard and preferred communication tool for 30 years. It will remain so for the foreseeable future. However, it is a prime vector for many kinds of cyber threats. To protect enterprise users against these threats, robust email security measures are essential. Here are some examples of the types of threats that can infiltrate an organization via email, which also illustrate the need for email security.

Phishing Attacks: Phishing emails are deceptive messages that attempt to impersonate real users or authoritative sources, luring recipients to click on malicious links or download malicious attachments. These attacks preface other attacker tactics and can lead to the compromise of enterprise users' devices and other sensitive information, such as login credentials, financial data, personally identifiable information (PII), and intellectual property (IP).

Malware: Attackers still use malicious software to take control of victims' systems. Malware can be disseminated via email attachments or links, infecting systems when opened. Malware can include viruses, ransomware, spyware, and Trojans/rootkits, each designed to exploit known or unknown vulnerabilities and likely to steal or encrypt data.

Spear phishing: This is a specialized and more targeted form of phishing. Spear phishing is when attackers perform reconnaissance on organizations and specific individuals within organizations to develop target lists and decide on tactics. The attackers then use this information to craft convincing emails and related content that make it harder to distinguish the spear phish emails from legitimate correspondence.

Business Email Compromise (BEC): The purpose of BEC attacks on employees is to get them to transfer funds or sensitive information under the guise of a trusted authority within the organization, such as a CEO or CFO or a specific employee's manager. These attacks often use social engineering tactics. BEC attacks can be related to spear phishing. Some brand protection services provide executive monitoring services to alert when these types of attacks could be forthcoming.

Spoofing and Impersonation: Email spoofing and impersonation tactics involve falsifying sender information to trick recipients into believing the email is from a trusted source. These attacks can be used to spread malware or gain access to sensitive data. Spoofing and impersonation tactics run the gamut from faking the account name to typosquatting to even compromising legitimate senders' accounts.

Email Bombing: This is a variation of a denial of service in some cases. Attackers flood a target's inbox with an overwhelming volume of emails, causing service disruptions and potentially leading to data loss or exposure. This method is also like MFA SMS/text fatigue, where attackers repeatedly hit an account hoping that the recipient will eventually give in and open a message and interact with its malicious content.

Data Leakage: Unauthorized data leakage can occur when employees inadvertently send sensitive information to unintended recipients. This could result from human error or malicious intent (either on the part of the employee or through manipulation by bad actors).

Zero-Day Exploits: Attackers may discover and exploit unknown vulnerabilities in email clients or servers, enabling them to deliver malware or compromise systems. Attackers may also simply use email to deliver zero-day exploits to victims.

Given the pervasive and evolving nature of these email-based threats, email security is something that all organizations must have.

Highlights

- Email security solutions must be an essential component of every organization’s security architecture
- Email is a primary vector for many cyber-attacks, and malicious actors are constantly evolving their techniques and payloads
- Malicious actors are using generative AI to create much more realistic phishing and spear phishing emails, leading to more incidents of business email compromise (BEC)
- Security vendors are also leveraging AI, including Machine Learning (ML) and Deep Learning (DL) algorithms for detecting anomalous and suspicious email and malicious content
- There are many attack patterns against email services as well as user inboxes, and email security solutions should be able to detect and stop such attacks
- Innovative features in this market include using browser isolation, Content Disarm and Reconstruction (CDR), integrated security awareness training and testing, email archive, and legal e-discovery
- Although email security is a long-established cybersecurity product area, new innovative approaches in the marketplace are welcome, which is why we see new entrants in the market within the last five years
- Additional consolidation is expected in this market, as some of the smaller or newer players will be acquired by the heavyweights to augment their email security offerings.

Market Segment

The market is composed of

- Secure Email Gateways (SEGs) that intercept the flow of email and add security using various technologies.

- Integrated cloud email security solutions that do not function as SEGs, but rather interoperate with email platforms via APIs. Some integrated cloud Email Security solutions serve as a modern replacement for SEGs.

- Built-in security capabilities in existing email systems; this includes integrated, cloud-based communication and collaboration platforms that integrate email security, for instance, the services provided by Microsoft and Google.

- Additional services not directly focusing on email, but essential for its security (encryption, browser isolation, sandboxing, etc.).

Delivery Models

For email security, there are three major approaches and deployment models that solutions can take: Secure Email Gateways, API-based solutions, and security solutions integrated into email platforms.

A **Secure Email Gateway (SEG)** can be a vital component of an organization's cybersecurity architecture designed to protect against email-based threats, including phishing attacks, malware, and other malicious content. SEGs are deployed in front of an organization's actual email servers by changing the MX (mail exchanger) DNS record. It can serve as the first line of defence by inspecting incoming and outgoing emails to ensure that only safe and legitimate messages reach the recipients. The following is a high-level description of how a SEG works:

- **Email Traffic Routing**: Incoming email is routed to the SEG, which is typically located at the perimeter of the network. Cleared traffic is sent on to actual email servers.

- **Content Filtering**: The SEG performs content inspection by analysing the email's headers (purported senders and intermediate servers), subject line, and body text. It checks for suspicious keywords, patterns, and known indicators of threats, such as URLs linked to phishing sites or malware distribution points.

- **Anti-Malware Scanning**: The SEG employs anti-malware engines to scan files in email attachments and embedded links. It checks these components for known malware signatures, use of known exploits, and behaviours associated with malicious code. If any malicious content is detected, it can be quarantined for analysis.

- **Phishing Detection**: Advanced SEGs utilize ML detection methods to determine phishing attempts. They assess the sender's reputation, look for signs of email spoofing, and analyse the email's content and context to alert administrators of suspicious messages. These messages can also be quarantined.

- **Sandboxing**: Some SEGs use sandboxing technology to divert email attachments to out-of-band sandbox environments to execute and analyse code to detect zero-day threats. This keeps suspicious email out of the network until the sandbox verdicts deem it safe or malicious.

- **Authentication Checks**: SEGs implement email authentication protocols like Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM), and Sender Policy Framework (SPF) to assess the legitimacy of incoming emails. This helps prevent email spoofing and impersonation attacks. Beginning in February 2024, Google and Yahoo will require senders of 5,000 or more messages to authenticate using these methods and will require unsubscribe options to allow recipients to opt-out.

- **URL Rewriting and Scanning**: SEGs may rewrite URLs in emails to direct them through a scanning service. The scanning service then checks these URLs in real-time for malicious content, to prevent users from clicking on harmful links.

- **Policy Enforcement**: Administrators should be able to define Data Leakage Prevention (DLP) style security policies within the SEG, fine-tuning what is allowed through and what should be blocked or automatically quarantined. These policies can be based on sender reputation, intended recipients, content, and other parameters.

- **Reporting and Logging**: SEGs provide detailed logs and reports to help administrators track email-related threats, understand attack trends, and adjust security policies. Logs should output to organizations' Security Information and Event Management (SIEM) systems.

- **Quarantine and Remediation**: Suspicious emails can be either quarantined for further analysis or blocked by the SEG according to policies. Administrators can allow users to access the quarantine area to review and release legitimate emails mistakenly flagged as threats.

API-based email security solutions allow organizations to use their preferred email platforms, whether on-premises, cloud-hosted, or in many cases, those delivered as SaaS. These solutions are addressable via secure APIs. The API calls may be configured within the hosting platform or connectors may be available which manage some of the configuration. These API-based solutions then perform similar functions as discrete SEGs, including real-time monitoring, content inspection, threat detection, sandboxing, DMARC/DKIM/SPF authentication, policy enforcement, automated remediation of threats, alerting, logging, and integration with other security solutions. They seem being well-suited for dealing with BEC (Business Email Compromise) types of attacks, which have become a major use case for these types of solutions. API-based email security solutions are designed to be highly scalable. They also have the advantage of being able to be updated as frequently as needed, due to the vendor hosting and maintaining the infrastructure.

Integration of these solutions can vary depending on the technical implementation as well as the customer infrastructure:

- Inline as sort of a cloud-based SEG that sits in front of the email system
- API-based pre-delivery analysis, where incoming mails are analysed via API-based access before hitting the inbox of the users
- API-based post-delivery analysis, where incoming mails are analysed when reaching the inbox of the users

The latter two approaches require the use of different types of APIs. Pre-delivery analysis is more powerful and effective from a security perspective. Many solutions in the market combine all variants, depending on the type of analysis run.

The third architectural option for email security is leveraging the built-in (or optional add-on) capabilities within major email service platforms such as Google's Gmail and Microsoft Outlook 365. Many organizations use these platforms for their email services, and both come with security features like those offered in SEGs or API-based email security solutions. Additionally, email service platforms offer Multi-Factor Authentication (MFA) for users and have Data Leak Prevention (DLP) functions that can help prevent exfiltration (either intended or unintended) of sensitive data and intellectual property.

Required Capabilities

Given the pervasive and evolving nature of these email-based threats, email security is something that all organizations must have. Effective email security solutions include the following components:

- Identification and blocking of unsolicited email communications (spam) using several technologies (content scanning, blacklisting, domain reputation, etc.), since spam is often used to disguise more malicious types of email.
- Classification and control of content and media considered inappropriate or in violation of corporate policies (white/blacklisting, industry classification, etc.).
- Identification and blocking of malicious and/or suspicious content (anti-malware) including malicious attachments, scripts, macros, as well as links to known malicious or compromised websites.
- Click-time protection against malicious links – using technologies like link rewriting, real-time analysis, browser isolation, etc.
- Post-delivery protection using additional out-of-band analysis like sandboxing, with the ability to remove content identified as malicious even after delivery to a user's inbox.
- Content Disarm and Reconstruction (CDR) – performed by disassembling attachments in common data formats, identifying hidden malicious blocks, and rebuilding sanitized documents without them (for popular formats like Office, PDF, image, and others).
- Data Loss Prevention (DLP) – applying corporate policies to outgoing emails and preventing sensitive or valuable information from exfiltration.
- Phishing protection – protecting users from social engineering types of attacks by analysing email sender, content, and other context, and preventing credential theft, ransomware deployment, etc.
- Business Email Compromise (BEC) protection – identifying and blocking malicious actors impersonating legitimate contacts to perform financial fraud, account takeover, identity theft, etc. Usually combines domain intelligence, user behaviour analysis, anti-phishing, might incorporate advanced AI-based semantic analysis.
- Email encryption and digital signatures – ensures that email content originates from trusted senders and is not tampered with in transit.
- eDiscovery / litigation hold – assists in legal proceedings, government investigations, etc. by providing specialized processes, workflows, data formats, etc.
- Backup / Archival – ensures business continuity after outages, ransomware attacks, etc. as well as compliance with regulatory frameworks.
- Monitoring and analytics – provide complete visibility into current and past email flows, assists in forensic investigations, provides alerts when threats or violations are detected.

Required integrations:

- Secure API exposure or pre-built connectors for IT Service Management (ITSM), SOAR, XDR, and reporting systems
- Quick, guided deployments for leading email systems like Microsoft, Google, Yahoo, ProtonMail, Zoho, etc.
- Integrations and tools for leading email clients such as Microsoft Outlook, Apple Mail, Gmail, Mozilla Thunderbird, etc.
- Processing and filtering of SMTP, IMAP, and POP traffic or integration to email services via APIs
- AI-/ML-based analysis capabilities
- Integration capabilities to secure email services, DLP, SIS, Information Classification, and other related systems, or provision of integrated capabilities in these areas.
- Advanced security features such as sandbox integration and email quarantine

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors to be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

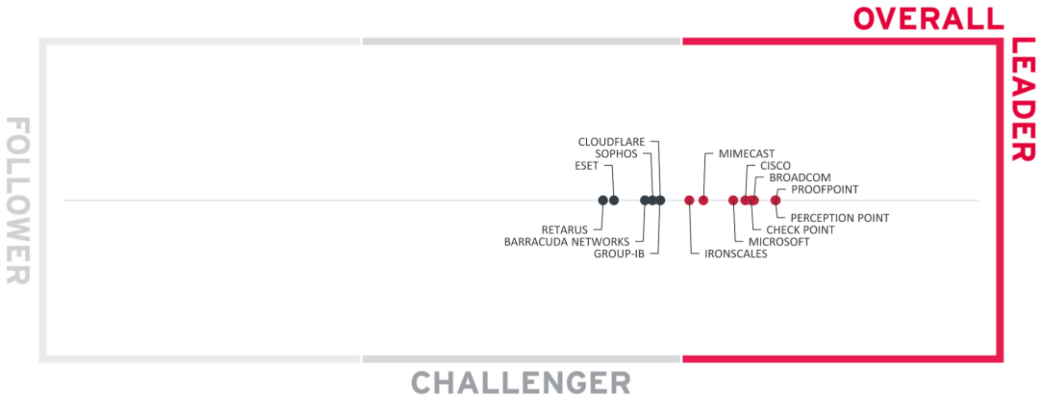


Figure 1: Overall Leadership rating for Email Security (graphic does not contain a y-axis, vendors to the right score stronger).

We find a close group of leaders in this analysis. Perception Point and Proofpoint are slightly ahead of a group of four other vendors, including (in alphabetical order) Broadcom, Cisco, Check Point, and Microsoft. While Broadcom, Cisco, Perception Point, and Proofpoint benefit from their strong placements across all leadership dimensions, both Microsoft and Check Point benefit from their strong market position, shifting them into the group of Overall Leaders. Two more vendors made it amongst the Overall Leaders, which are Mimecast and IRONSCALES, both delivering a good set of Email Security capabilities and innovation.

In the Challenger segment, we find the other vendors, with a group of four vendors positioned close to each other, consisting of (in alphabetical order) Barracuda Networks, Cloudflare, Group-IB, and Sophos. Following them closely we find ESET and Retarus, which both also have strong offerings and are of specific interest for European customers, being headquartered within the EU.

Overall Leaders are (in alphabetical order):

- Broadcom
- Check Point
- Cisco
- Ironscales
- Microsoft
- Mimecast
- Perception Point
- Proofpoint

Product Leadership

Product Leadership is the first specific category examined below. This view is based on the analysis of service features and the overall capabilities of the various services.

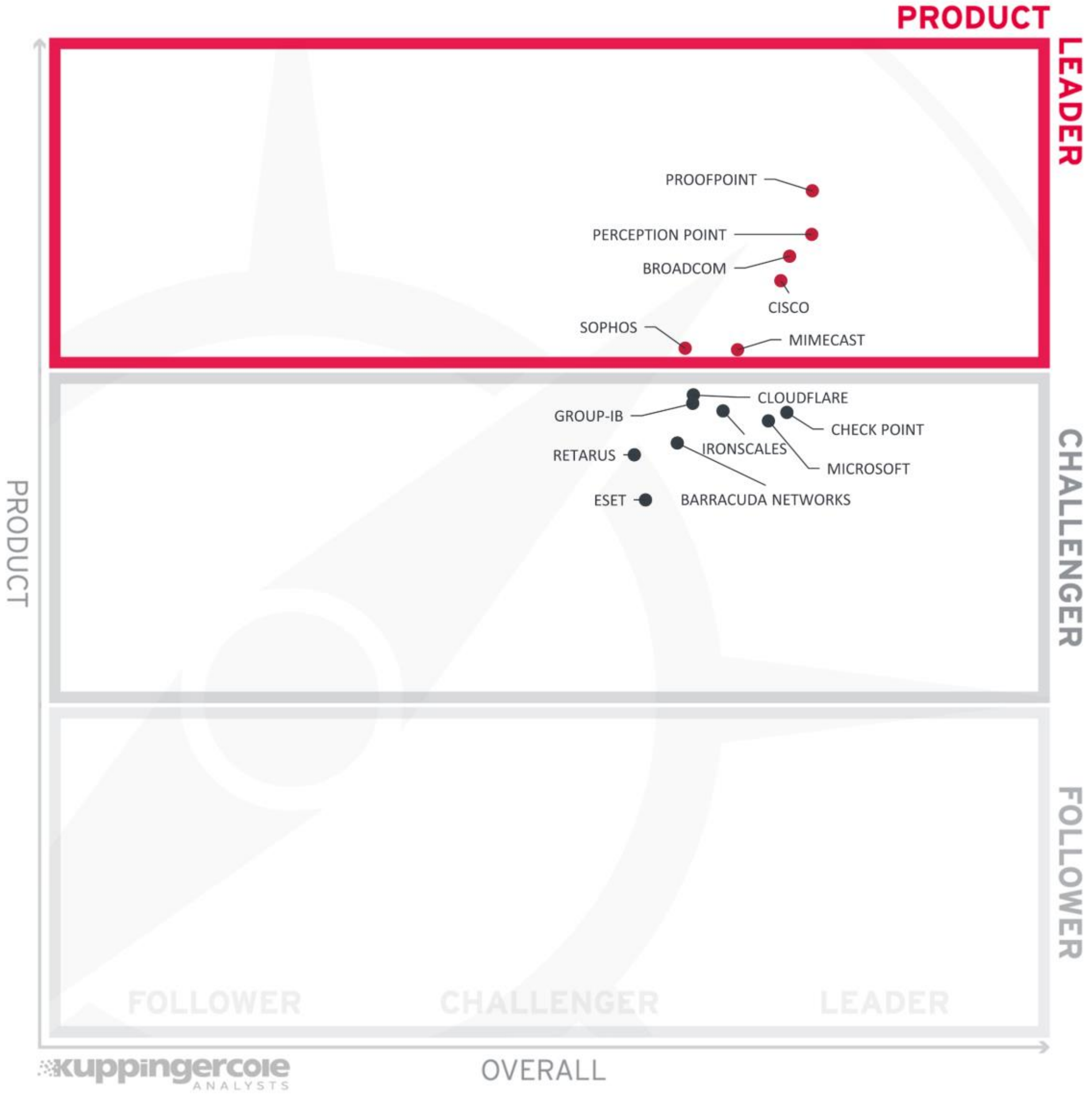


Figure 2: Product Leadership for Email Security.

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

We find a group of six vendors in the Leader segment, with Proofpoint being slightly ahead of Perception Point, Broadcom, and Cisco. Sophos and Mimecast also entered this segment. All vendors have feature-rich solutions for Email Security, supporting a wide range of use cases.

The Challenger section is packed, with many vendors being close to the Leader segment. At the top of this segment, we find (in alphabetical order) Check Point, Cloudflare, Group-IB, IRONSCALES, and Microsoft. Closely following them, we find Barracuda Networks, Retarus, and ESET. All these vendors provide strong solutions for Email Security. Customers are well-advised in a detailed analysis, also in the context of their specific use cases. Microsoft, for instance, is targeted at their own Microsoft 365 environment only, while Group-IB stands out with their forensic capabilities, while Cloudflare excels by their integration into the broader Cloudflare platform.

ESET, on the other hand, has its roots in the consumer market. They, as Retarus, distinguish themselves from others being European solutions that are of specific interest to certain groups of EU-based customers, including governmental agencies and regulated industries. Retarus also is very strong regarding their support for a wide range of email solutions including legacy email solutions and their email management such as archiving.

Product Leaders (in alphabetical order):

- Broadcom
- Cisco
- Mimecast
- Perception Point
- Proofpoint
- Sophos

Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

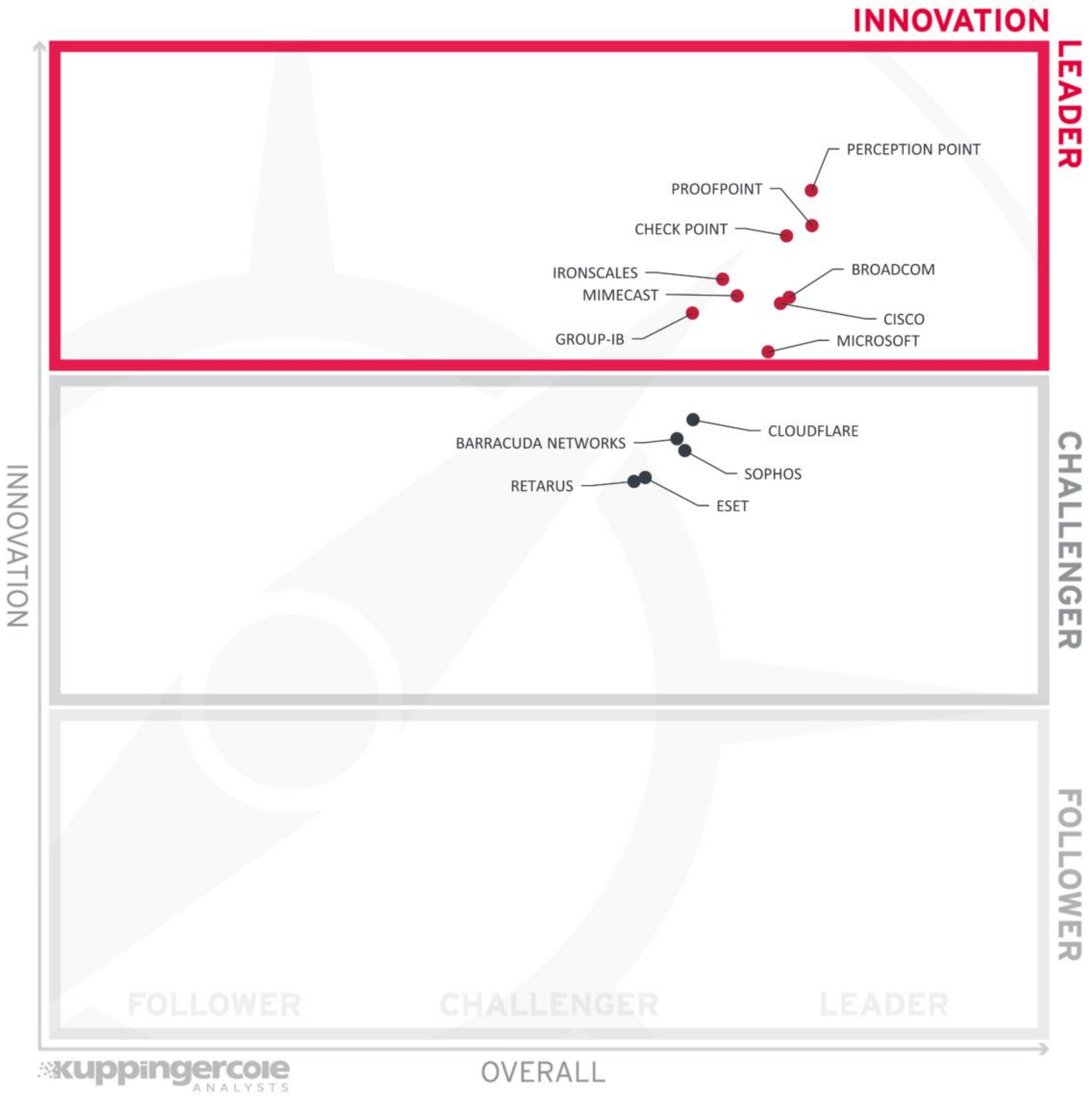


Figure 3: Innovation Leadership for Email Security.

We have rated several of the vendors as Innovation Leaders, given the significant amount of innovation we are observing in the market, both with the transition towards modern deployment models and integration into leading email platforms and with the use of AI and other technologies to tackle the ever-increasing threats customers are facing for their email-based communication. Many of the vendors also integrate Email Security with securing other communication channels such as Teams, Slack, and web-based interaction.

Perception Point stands slightly apart from the other vendors, followed by Proofpoint. Check Point is also strongly positioned regarding the innovative capabilities delivered. Broadcom, Cisco, Group-IB, IRONSCALES, and Mimecast are rated at an equal level, with Microsoft just making it into the group of Innovation Leaders. While providing a lot of strong features, Microsoft is focused on their Microsoft 365 platform only and does not support the level innovation for heterogeneous email environments as other vendors do.

Amongst the Challengers, we find Cloudflare, Barracuda Networks, ESET, Retaus, and Sophos, some of them being very close to entering the Leader segment. All are demonstrating a good level of innovation but lacking the breadth of innovation shown by some of the other vendors. ESET and Retarus are lagging in AI adoption.

Innovation Leaders (in alphabetical order):

- Broadcom
- Check Point
- Cisco
- Group-IB
- IRONSCALES
- Microsoft
- Mimecast
- Perception Point
- Proofpoint

Market Leadership

Lastly, we analyse **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

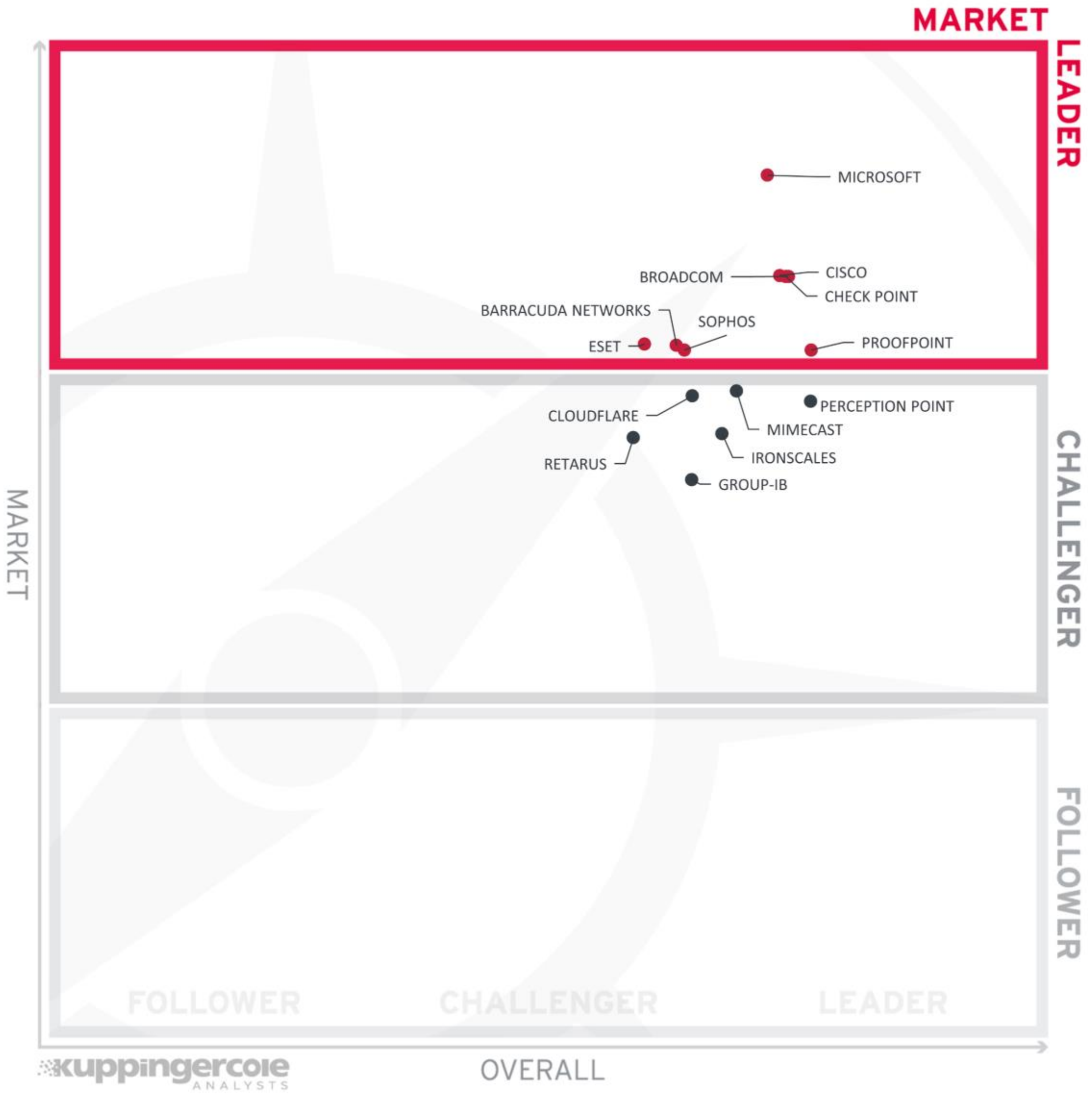


Figure 4: Market Leadership for Email Security.

It does not come as a surprise that Microsoft is dominating the market, based on their presence as a leader in email platforms. While this report focuses on the added, specialized capabilities in Email Security, beyond the built-in features, Microsoft has a strong position here as well, regarding their customer base, global presence, and partner ecosystem.

Following them, we find Broadcom, Cisco, and Check Point positioned at an equal level, all being strong in the enterprise business and in large accounts. Sophos, ESET, Barracuda Networks, and Proofpoint are next, all having a very large customer base also for their Email Security solutions.

On top of the Challenger section, we find Cloudflare – with their generic strength based on their platform approach -, Mimecast, and Perception Point. Close to them, we find the other vendors with IRONSCALES, Retarus, and Group-IB.

Market Leaders (in alphabetical order):

- Barracuda Networks
- Broadcom
- Check Point
- Cisco
- ESET
- Microsoft
- Proofpoint
- Sophos

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution which is both feature-rich and continuously improved. This is indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

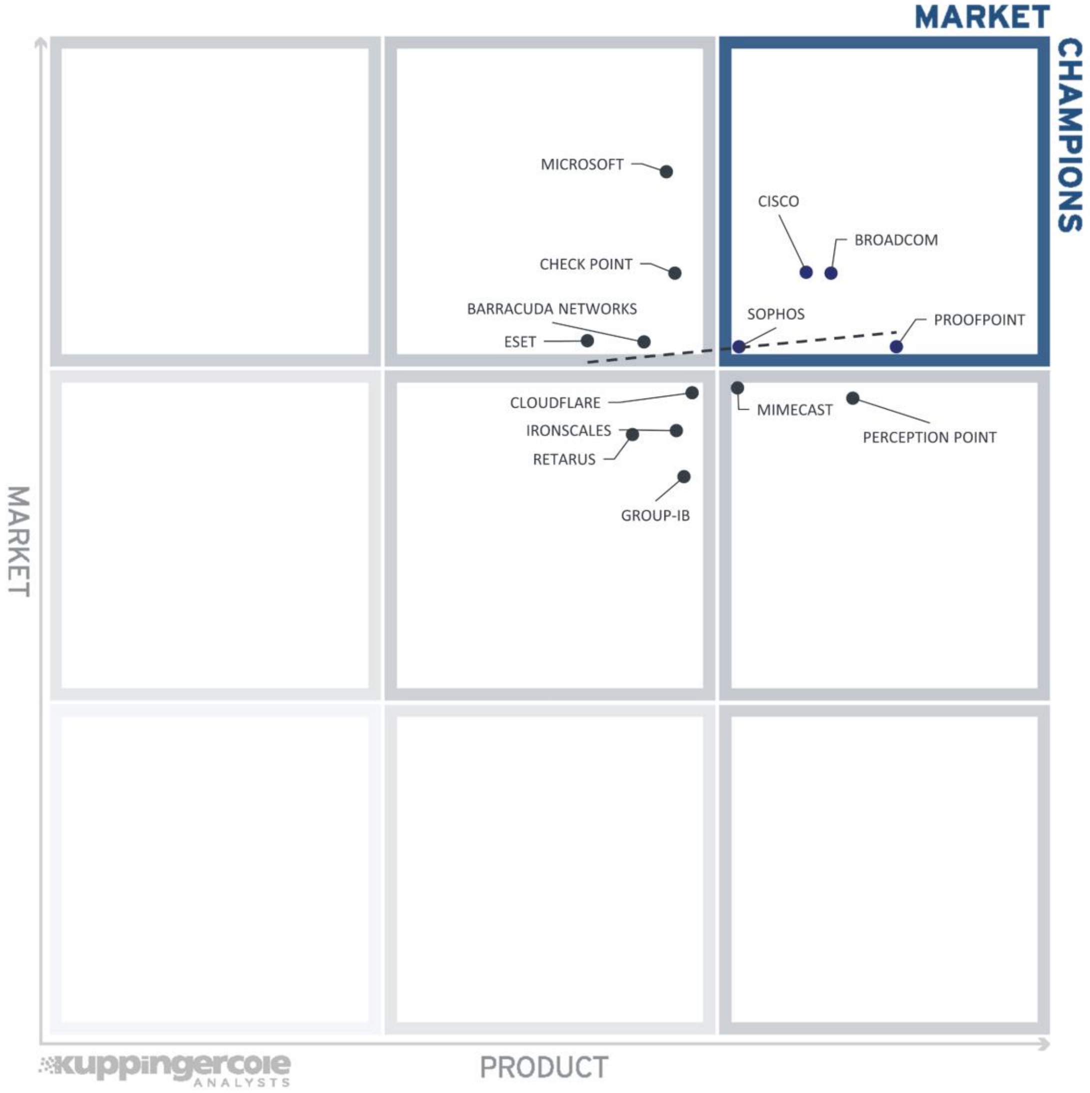


Figure 5: The Market / Product analysis, indicating the relative market strength compared to product rating.

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are to some extent “overperformers” when comparing Market Leadership and Product Leadership.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

In the upper right corner, the “Market Champions,” we find four vendors, Broadcom, Cisco, Sophos, and Proofpoint. This is a somewhat uncommon picture; however, several of the leading players have not been rated as Market Leaders, and many of the other large players have not reached a Product Leader rating.

Thus, the segment to the upper centre is crowded, with four vendors scoring stronger in their Market Leadership rating than for Product Leadership. All these vendors have strong offerings, though.

Perception Point and Mimecast are positioned to the centre right, indicating their technological strength, which gives them strong potential for increasing their position in the market.

In the centre segment, we find four other vendors that show, based on their technology rating being above their market rating, good potential for growth.

The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a rather good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

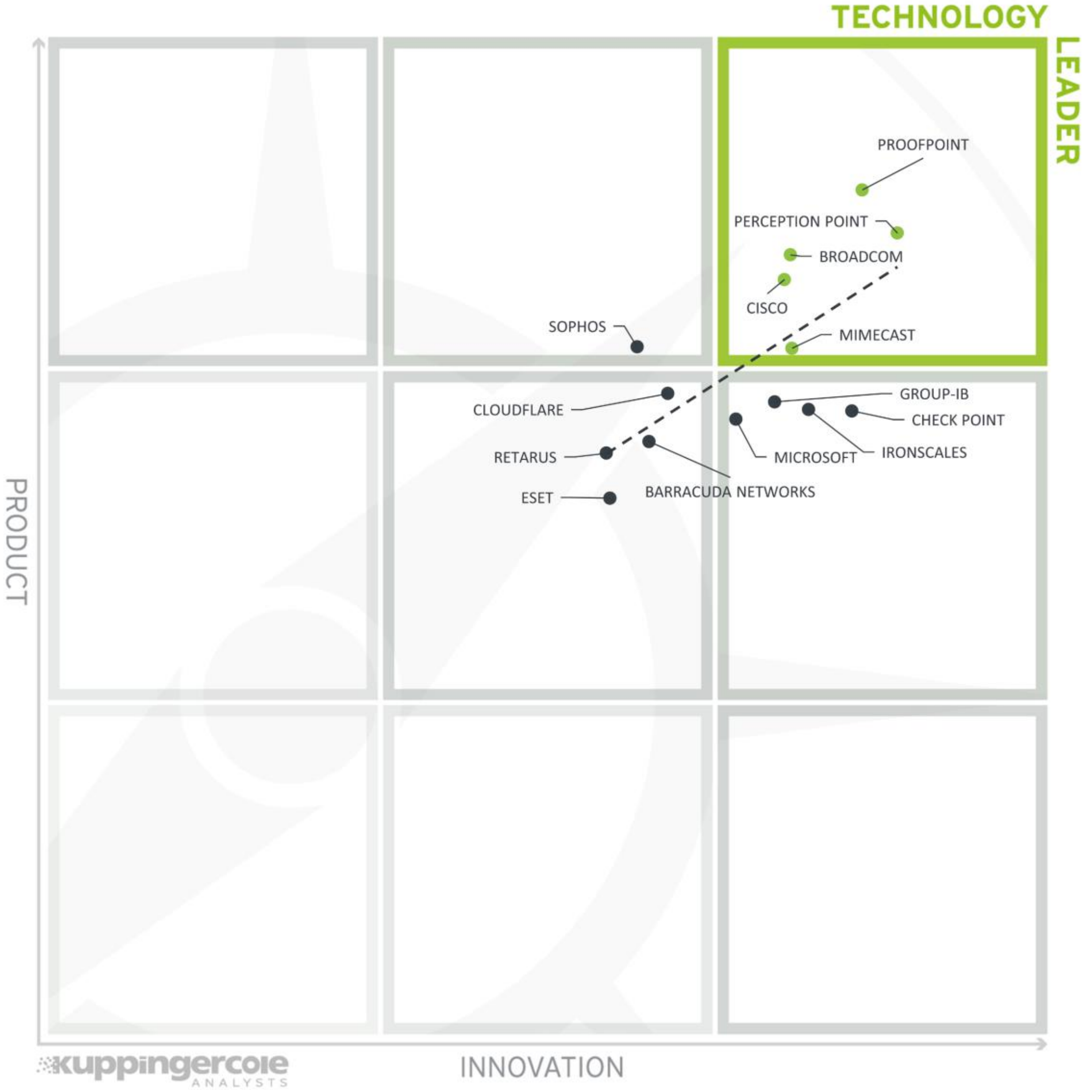


Figure 6: The Innovation / Product rating, relating innovative strength to the current product capabilities.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Overall, there is a good correlation between the level of innovation and the technical strength. Some of the vendors with mature solutions stand out as “Technology Leaders” in the upper right segment, including Proofpoint, Perception Point, Broadcom, Cisco, and Mimecast.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk on their market position in the future, however it depends on how they improve their Innovation Leadership position. Vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

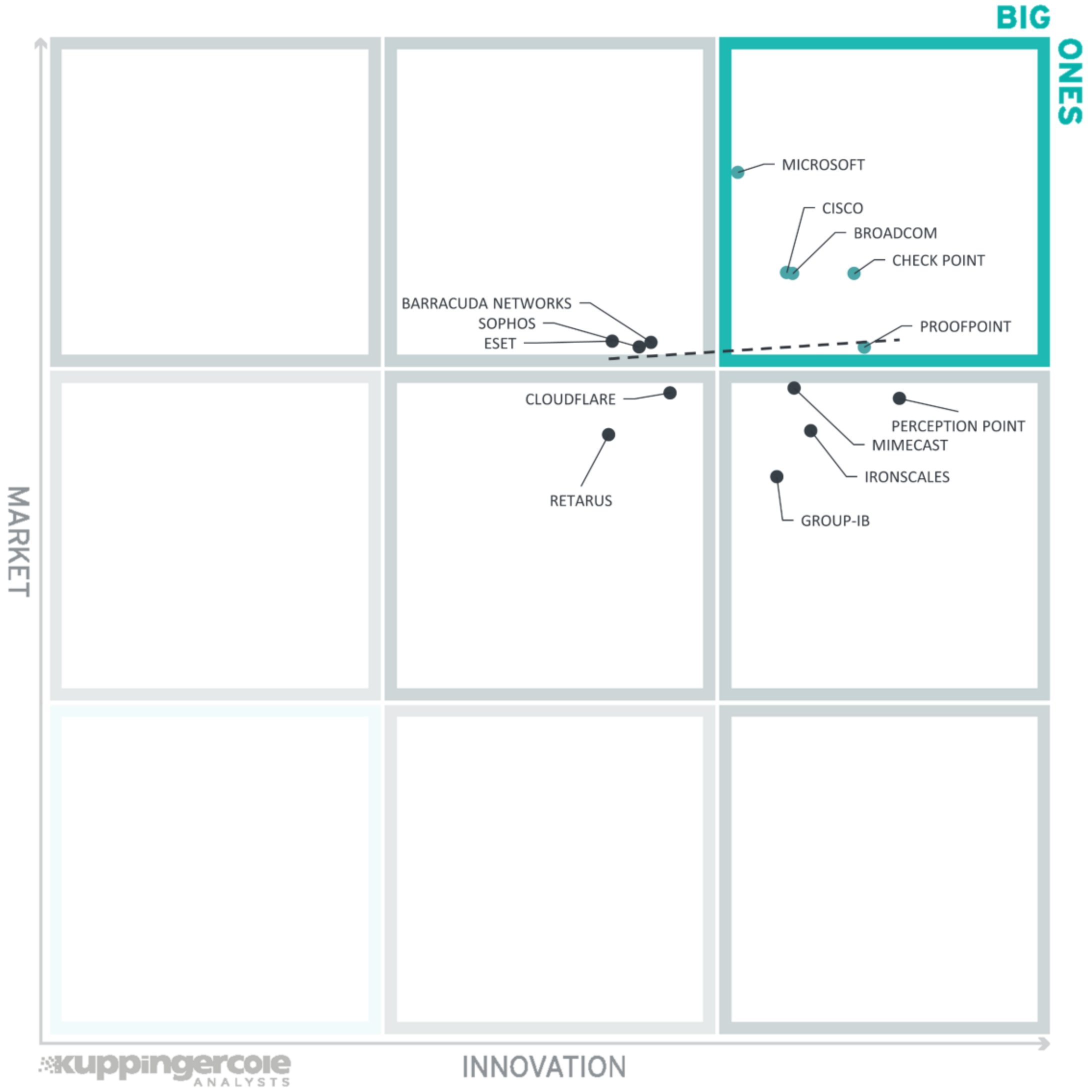


Figure 7: The Innovation / Market matrix, relating innovation to market presence.

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus have the biggest potential for improving their market position.

The correlation between these two ratings is low for this Leadership Compass, with some established vendors standing out with their market presence, while several vendors excel with innovation, but not seeing this being fully reflected in their market position. The “Big Ones,” not surprisingly, include Microsoft, Cisco, Broadcom, Check Point, and Proofpoint, all with a strong market presence and significant investment into further innovation.

Products and Vendors at a Glance

This section provides an overview of the various products we have analysed within this KuppingerCole Leadership Compass on Email Security Solutions. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative, but specialized vendors or local players that provide strong product features, but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
BARRACUDA NETWORKS	Strong Positive	Positive	Positive	Positive	Positive
BROADCOM / SYMANTEC	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
CHECK POINT	Strong Positive	Positive	Positive	Positive	Positive
CISCO	Positive	Strong Positive	Strong Positive	Strong Positive	Positive
CLOUDFLARE	Strong Positive	Positive	Strong Positive	Positive	Positive
ESET	Positive	Positive	Strong Positive	Positive	Positive
GROUP-IB	Positive	Positive	Strong Positive	Positive	Positive
IRONSCALES	Positive	Positive	Positive	Positive	Positive
MICROSOFT	Strong Positive	Positive	Strong Positive	Positive	Positive
MIMECAST	Positive	Positive	Strong Positive	Strong Positive	Positive
PERCEPTION POINT	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
PROOFPOINT	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
RETARUS	Positive	Positive	Positive	Positive	Positive
SOPHOS	Positive	Positive	Strong Positive	Strong Positive	Strong Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem

BARRACUDA NETWORKS	Positive	Positive	Strong positive	Positive
BROADCOM / SYMANTEC	Positive	Strong positive	Strong positive	Strong positive
CHECK POINT	Strong positive	Strong positive	Strong positive	Strong positive
CISCO	Positive	Strong positive	Strong positive	Strong positive
CLOUDFLARE	Positive	Positive	Positive	Strong positive
ESET	Neutral	Positive	Positive	Strong positive
GROUP-IB	Positive	Neutral	Neutral	Positive
IRONSCALES	Strong positive	Neutral	Neutral	Positive
MICROSOFT	Positive	Strong positive	Strong positive	Strong positive
MIMECAST	Positive	Positive	Strong positive	Positive
PERCEPTION POINT	Strong positive	Positive	Positive	Positive
PROOFPOINT	Positive	Positive	Strong Positive	Strong positive
RETARUS	Neutral	Neutral	Positive	Neutral
SOPHOS	Positive	Positive	Positive	Strong positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC Email Security, we look at the following eight categories:

- Analytics Engine: In this category, we rate the specific capabilities for analysing emails and implementing email security measures. This category focuses on the entire breadth of email security and indicates the overall email security posture of the solution. We further look specifically at email content analysis and attachment analysis and security, for instance the ability to identify malicious attachments and protecting against related attacks. Also, we rate the ability to protect other types of interaction and content, beyond emails, such as Microsoft Teams or Slack.
- BEC Protection: With BEC having become one of the most relevant and critical types of attacks, we rate the capabilities in this area, specifically the ability of identifying malicious BEC content and identifying malicious senders, separately.
- Email Management: While Email Security is mostly focused on protecting against attacks via incoming emails, the ability to back up emails, restore, archiving, and manage bouncing is also essential to many customers. This category rates these features.
- DLP: Here, we rate the support for protecting not only from incoming threats, but also analysing outgoing mails through means of DLP (Data Leakage Prevention) to prevent escapes of financial information, Personally Identifiable Information (PII), and sensitive intellectual property.
- Architecture: The flexibility in deployment with support for multiple deployment modes and for different types of email systems and clients as well as hybrid deployments is rated here. Integration with Microsoft 365, Google, and other email platforms is considered. The availability of plug-ins for a variety of clients and browsers is preferred.
- AI / ML: Finally, we look at the level and sophistication of integrated AI / ML capabilities, which play an increasingly significant role in protecting against email-based attacks by improving detection capabilities while keeping false positive rates low.

Barracuda Networks – Barracuda Email Protection

Barracuda Networks counts amongst the pioneers in the Email Security market. The company has extended their portfolio into adjacent areas such as application protection, network security, and backup. They provide software, also in form of appliances, with a shift from hardware-based appliances to cloud-based appliances, as well as solutions for MSPs (Managed Service Providers). Their integrated suite of Email Security solutions is Barracuda Email Protection.

The solution supports two conceptual approaches. One is the gateway deployment, where incoming mails are analysed, focusing on spam, malware, and zero-day attacks. The other is the API-based, integrated cloud Email Security inbox defence, currently supported for Microsoft 365. Barracuda plans to extend this to other platforms. The inbox defence focuses on additional attack vectors, including BEC attacks, ATO (Account Take Over) attacks, and lateral phishing attacks. Customers can deploy both solutions in combination for Microsoft 365 or rely on the gateway for other Email solutions.

Barracuda Email Protection covers three pillars of functionality. Threat Prevention is the main area, focusing on the core capabilities we expect to see in Email Security solutions, but also delivers web security and ZTA (Zero Trust Access) for Microsoft 365 as extended features. Detection and Response as the second area adds incident response and security awareness training. The third pillar, Data Protection and Compliance, adds email encryption, backup, and archiving, but also the Data Inspector, a solution that can analyse information held on on-premises and cloud storage such as Microsoft SharePoint and Microsoft OneDrive. With this approach, Barracuda takes a broader approach beyond Email Security.

They also offer integration with their own XDR (eXtended Detection and Response) solution as well as with other vendor’s XDR, SOAR, and SIEM solutions, and with the broader Barracuda portfolio. This is of particular interest to customers that either already have deployed other Barracuda products, or that look for a comprehensive Enterprise Protection Platform approach, spanning the different channels for incoming and outgoing data such as email and web. Barracuda Email Protection can filter on predefined data types in outgoing email to look for and prevent the escape of sensitive information such as credit card numbers, SSNs, dates of birth, addresses, phone numbers, and health care records. It does not integrate with third-party tools. E-discovery and litigation hold functionality is provided.

Due to the history of the solution, with the established gateway product and the newer API-based solution, the administrative user interface (UI) varies. Integration and unification of the UIs would be appreciated. The solution provides dashboards for a rapid overview of the security and incident status.

There are a wide range of configuration options available. Default settings are based on best practices, allowing customers to quick start email protection. Based on AI capabilities, the solution can support customers in auto-tuning settings and rapidly implementing their custom settings. This reduces complexity compared to rule-based approaches.

Barracuda Email Protection provides detailed insight to the users, by providing comprehensive log data as well as insight into the classifiers used. These are auto-tuned and can be extended to consumer additional threat signals from a wide range of sources. Feedback about false positives is consumed and used to retrain classifiers almost real-time.

The solution is powerful and feature rich. It is, at this point, an option for environments that require a traditional email security gateway, for instance when using on-premises email systems, or for customers using Microsoft 365 who are looking for a solution that complements this by adding an additional layer of protection, as well as having backup and recovery capabilities and integration to a broader set of capabilities which protect incoming and outgoing communication channels.

Security	Strong positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Barracuda®

Table 3: Barracuda Email Protection's rating

Strengths

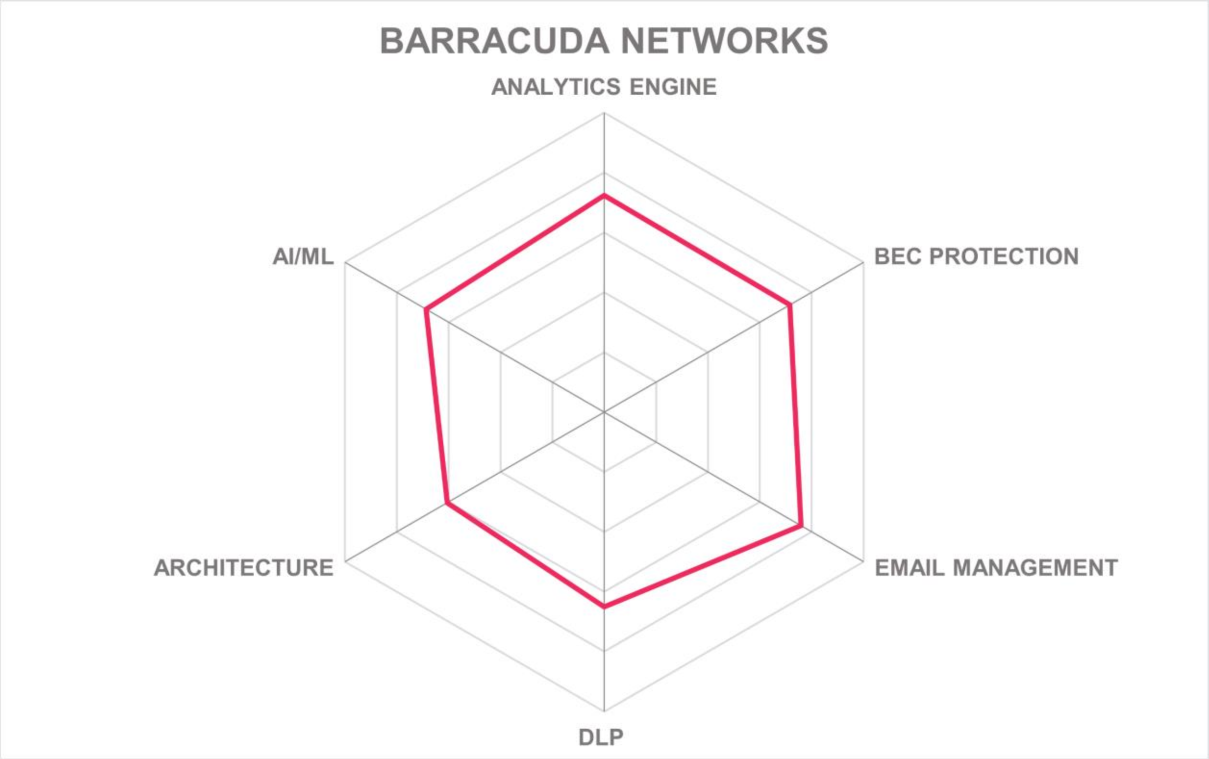
- Established, proven solution with a long history
- Broad set of coverage of email threat vectors specifically by API-based solution
- Integration between gateway and API-based components
- AI capabilities, including support for auto-tuning
- Best practices-based standard configuration allowing for rapid deployment
- Feedback loops for continuous optimization of classifiers
- Option for adding further external threat signals
- Integration to the broader Barracuda ecosystem
- Email backup and archival capabilities
- Built-in rules-based DLP filtering capabilities
- E-discovery and litigation support
- Strong global partner ecosystem

Challenges

- User interface of gateway and API-based solution not yet integrated
- API-based solution currently targeted on Microsoft 365 only, but plans to expand beyond this
- Auto-tuning features deserve further improvements regarding explainability

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


BARRACUDA NETWORKS
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Broadcom – Symantec Email Security

Broadcom is one of the leading software vendors, following their acquisitions of CA Technologies, the enterprise security portfolio of Symantec, amongst others. The company is very R&D driven and well-established in large enterprises and governmental organizations, as well as other industries, in particularly highly regulated ones. Their Email Security approach differs from other vendors in that it is a true Managed Services solution, where Symantec continuously supports the customer in analysing the status and optimizing the service, for example, with respect to false positives.

The solution consists of a combination of a traditional Email Security gateway (SaaS, virtual and physical appliance) plus inline protection, as well as other services such as log analytics. Symantec in part relies on partners that provide, for example, log analysis and SIEM (Security Information and Event Management) capabilities or enterprise-grade DMARC authentication and combines them into a unified solution. The inline protection capabilities support both Microsoft 365 and Google. They deliver added features such as threat isolation, browser isolation, BEC analysis, and more. Based on the gateway component and downstream email systems, such as Microsoft Exchange on-premises/hybrid or Lotus Notes, are supported. Symantec has a plug-in for Outlook, but not for any other email clients.

As with some of the other players in the market, Symantec takes an approach that goes beyond pure email protection of Microsoft Exchange, Google Workspace, and Microsoft Office 365 (including inbox protection) and covers multiple inbound and outbound communication channels including email, web, and collaboration channels on the endpoint such as Microsoft Teams. This reflects the diversity of communication and collaboration, but also the need for protecting against new types of attacks which do not solely rely on email.

The antivirus-/antimalware features of the solution are strong and proven, relying on the Symantec technology. Symantec supports adding controls for outgoing traffic by integrating with their own DLP (Data Leakage Prevention) layer. They also provide UBA (User Behaviour Analysis) controls across various channels, beyond just email-based analytics. Other integrations are to their CASB (Cloud Access Security Broker) solution.

For Microsoft 365 and Google Workspace customers, Symantec delivers a comprehensive, layered approach, involving the Symantec gateway and integrated, API-based solutions plus Microsoft Defender.

Symantec follows a policy-based approach when configuring the solution. Policies span multiple channels. While this approach is consistent with different parts of the solutions, the administrative consoles for example for Email Security and DLP are not yet fully integrated. However, once the DLP policy has been configured (by the DLP specialist team), that policy is automatically applied to the Email channel, ensuring consistency of detection and control across the organization, without the risk that the Email security team create DLP policies that conflict with the wider DLP posture. The Email Security console is feature rich, delivering a high density of information and hinting on related tasks that administrators may need to take. Due to the managed services approach, Symantec experts support customers on a regular basis in optimizing their environments, providing best practice experiences from other customers.

In contrast to several other vendors, Symantec does not support auto-tuning capabilities. However, with their focus on customers in highly regulated industries, this is adequate to ensure that there is always control and governance within the configurations.

The Symantec solution is a feature rich and powerful solution for Email Security and beyond. It is targeted at customers that are looking for a layered approach, supporting a range of email solutions, and backed by managed services. This is in line with the Broadcom focus on highly regulated industries.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Symantec™
A Division of Broadcom

Table 4: Broadcom Security Email Security's rating

Strengths

- Proven solution with a long track record
- Integrates controls across email, web, and collaboration channels
- Integrates with DLP, CASB, and SIEM solutions
- Strong antivirus/antimalware features
- Support for Microsoft 365 and Google
- Support for legacy/hybrid email environments
- Email configuration health check service
- Broadcom supporting customers in optimizing their environments in regular intervals
- Feature-rich solution
- Targeted at highly regulated industries
- Supports multi-layered approaches with gateway, Microsoft 365, Google Workspace and additional API-based inline protection

Challenges

- Managed services approach comes at a cost
- Administrative consoles not yet fully integrated across channels, but DLP policies are
- No auto-tuning capabilities
- Relies on Broadcom services, not an external partner ecosystem
- No email backup/archive functions
- Does not have e-discovery and litigation hold features

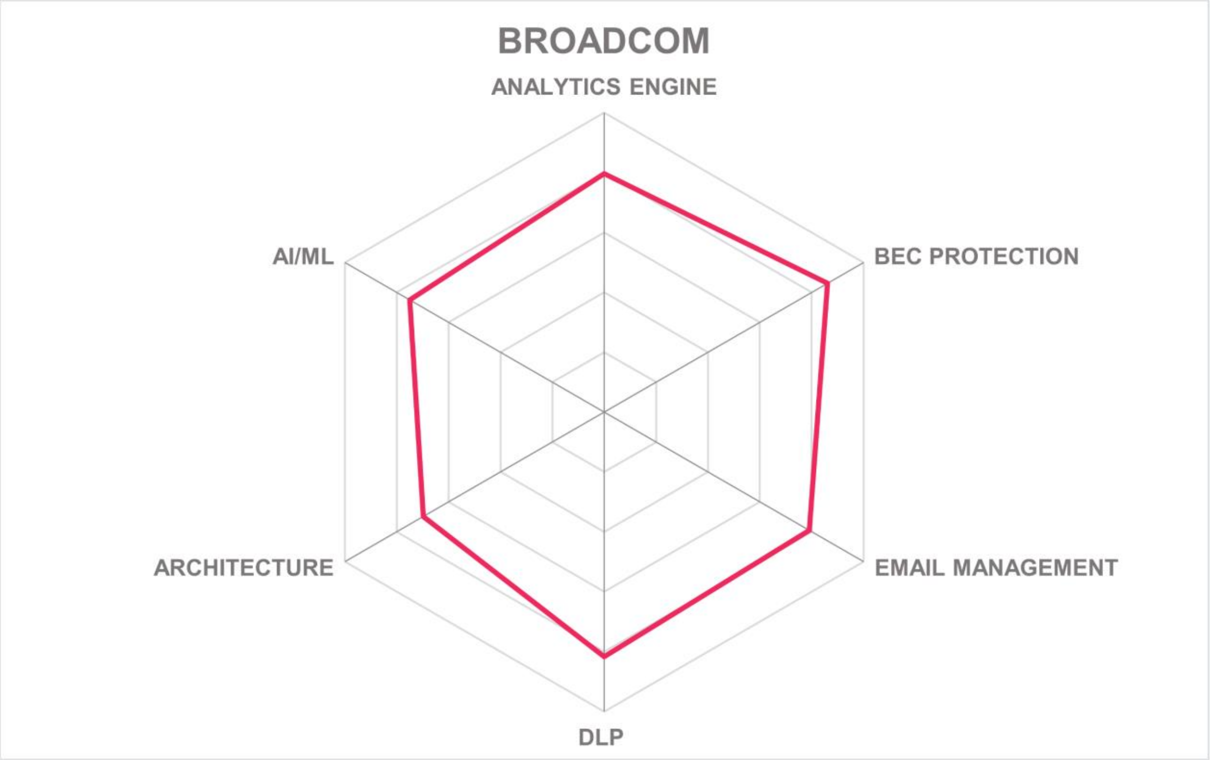
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


BROADCOM
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Check Point – Harmony Email & Collaboration

Check Point, founded 1993 in Israel, is a leading vendor of cybersecurity solutions. They started as a firewall vendor and expanded beyond network security to cloud security, endpoint and email security, and MDR/XDR (Managed / Extended Detection & Response) solutions. Harmony Email & Collaboration (formerly Avanan) is their solution for Email Security and collaboration security, focusing on Microsoft 365, Google Workspace, and collaboration solutions such as Slack, Teams, or Microsoft OneDrive.

In contrast to many other vendors, Check Point focuses on API-based Email security. Hybrid cloud and on-premises scenarios are supported if the email first flows through the cloud instance. Check Point also continues supporting Email Security MTA as an appliance-based security layer for customers with on-premises email solution both permanently or in the process of moving to cloud email. They focus on identifying malicious emails ahead of reaching the inbox, as well as providing post-delivery protection. Harmony Email & Collaboration can be used with or without existing SEGs as an additional layer of defence, depending on the security architecture and specific needs of enterprises. It features browser isolation and Content Disarm and Reconstruction as additional methods for attachment handling. It integrates neatly with the other security solutions of Check Point, benefiting from the large installed base of Check Point solutions. Harmony Email & Collaboration, in Microsoft environments, could either be combined with Microsoft Defender as a further layer of defence, or, more commonly, replaces Microsoft Defender.

In contrast to many API-based solutions, Check Point combines inline protection with API-based protection in a unified approach. Inline protection is about email security solutions analysing and protecting ahead of emails reaching the inbox, while several API-based solutions only begin their analysis when emails reach the (cloud-based) inboxes. Check Point hooks into the delivery ahead of the Email being put into the user’s inboxes. This also allows implementing a wide variety of analytical and protective measures against a variety of threats, including BEC (Business Email Compromise) and many others.

Analysis is backed by the Check Point Threat Cloud, which Check Point claims is the largest threat intelligence network available globally. Check Point has a vast number of signals around threat intelligence on hand which can be used for threat analytics on incoming emails.

Implementation of the cloud-based Harmony Email & Collaboration solution is fast. For Microsoft 365, Check Point builds on a patented approach for automatically creating rules in Microsoft 365. This avoids manual configuration of the target environment and allows customers to set up the solution with very few steps and within minutes.

The solution comes with a modern UI and provides a range of dashboards, providing insight into the current threat status. It supports drilling down into further details directly from the dashboards. They provide a wide variety of details on suspicious emails, including background information. However, analysing the details requires a good level of expertise.

Notifications about malicious emails can be fully customized in plain text, and do not require HTML or other specific knowledge. Quarantine messages can be integrated with those provided by Microsoft Defender, delivering a unified experience to the users. It can be integrated with Microsoft Defender.

Other important capabilities of the solution include integration with DLP (Data Leakage Prevention), URL sandboxing, and support for analysing not only emails, but also collaboration solutions such as Microsoft Teams and Slack.

Check Point Harmony is a powerful, cloud-based solution that integrates well with the suites of Microsoft and Google, adding additional layers of defence to these as well as common collaboration tools. This makes the solution specifically interesting to organizations that run their email solutions already fully cloud-native.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 5: Check Point Harmony Email and Collaboration’s rating

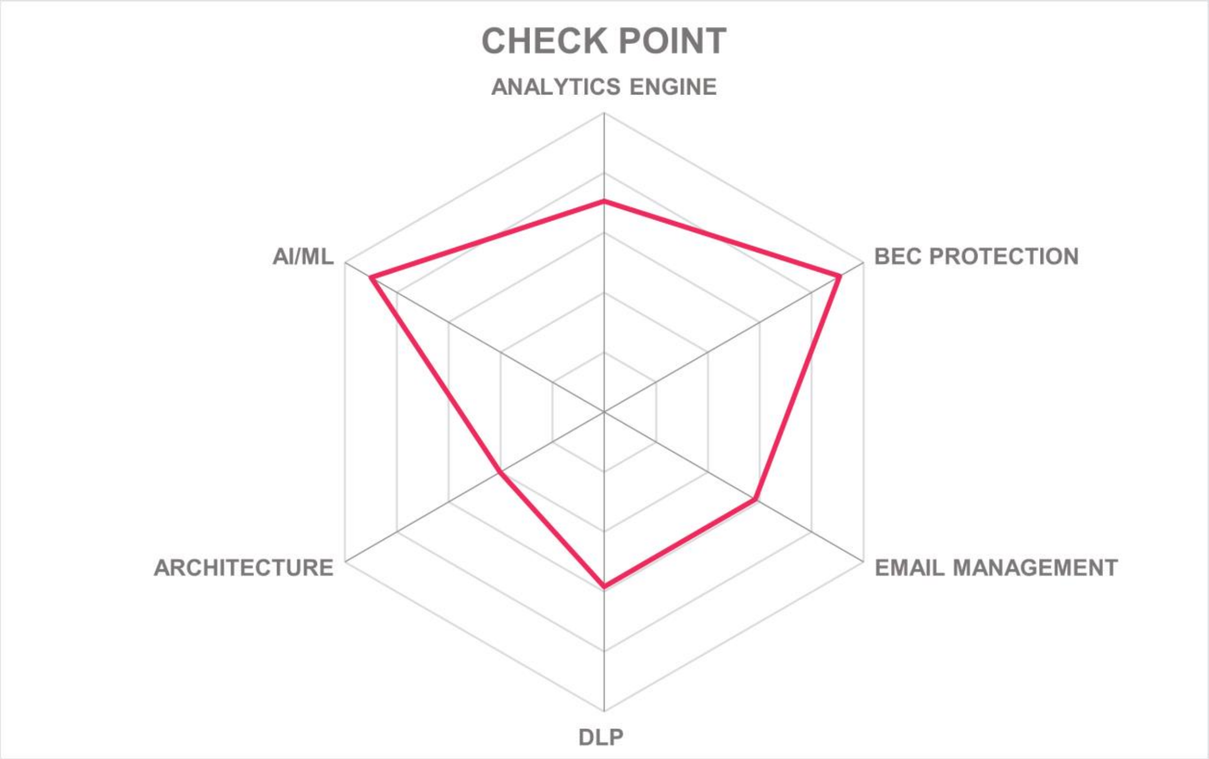
Strengths

- Close integration to Microsoft 365 and Google Workspace
- Combines inline and API-based integration without the need for a SEG (Secure Email Gateway)
- Modern UI and powerful dashboards, including support for drill-down into details
- Rapid deployment due to close integration with Microsoft 365 and patented auto-configuration of rules
- Also supports collaboration environments such as Microsoft Teams and Slack
- Close integration with Microsoft Defender, with Harmony acting as an additional and upstream layer of defence
- Unifies information about malicious and blocked mails with Microsoft Defender quarantine messages
- Browser isolation and CDR for attachment handling
- High degree of customization

Challenges

- Focused on cloud-native email solutions from Microsoft and Google, not on heterogeneous email environments containing legacy solutions
- Analysis of malicious emails is powerful, but requires some level of expertise
- Integrated archiving does not support archiving keys for S/MIME encrypted mails

Leader in OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER


CHECK POINT
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Cisco – Secure Email Threat Defense

Cisco Systems is one of the global leading solutions for networking and telecommunications solutions and has expanded into adjacent areas, in particular security. Security is a strategic field to Cisco Systems. The company has been active for many years with an own Email Security solution. That solution, Cisco Secure Email, a traditional SEG (Secure Email Gateway) approach, more recently has been complemented by their API-based Email Security solution Secure Email Threat Defense, which now is the core product in Cisco's Email Security strategy.

Cisco Secure Email Threat Defense can be used with Cisco Secure Email in a combined solution, with Cisco Secure Email being the traditional SEG (Secure Email Gateway) product of Cisco. This also provides strong support for mixed environments where both legacy email products and modern, cloud-based services such as Microsoft 365 are in place.

While Secure Email Threat Defense utilizes proven capabilities such as the Cisco CASE (Contextual Anti Spamming Engine) technology, it builds extensively on the use of Machine Learning and Large Language Models to detect advanced threats. Their focus for the solution is on detecting new threats such as brand and user impersonation, ATO (account-take-over) attacks, and others such as BEC (Business Email Compromise).

While Cisco has removed dependence on third-party solutions for certain capabilities, it integrates closely with a range of other solutions provided by Cisco. This includes Cisco Talos, the Cisco solution for threat intelligence and backed by the Cisco Threat Intelligence team, which is both a provider to and consumer of signals from Cisco Secure Email Threat Défense.

Cisco Secure Email Threat Defense also integrates and utilizes Cisco Vulnerability Management (formerly Kenna Security), Cisco XDR (eXtended Detection & Response), and Cisco Secure Endpoint. Given that email is a primary vector for attacks, email security is a central element of the overall Cisco security and XDR strategy.

With many organizations shifting to Microsoft 365, Cisco Secure Email Threat Defense provides close integration features to Microsoft 365, adding to Microsoft Defender and expanding the capabilities of the standard / built-in solution provided by Microsoft. It also integrates with Microsoft Sentinel for consuming and providing back signals.

Currently, the cloud-based version of Cisco Secure Email and Secure Email Threat Defense are separate cloud services and have distinct user interfaces. It does not come as a surprise that Cisco Secure Email Threat Défense as the newer solution has a more modern UI, based on dashboards which allow for quick and flexible configuration. Cisco plans for closer integration here to support customers that use both platforms in heterogeneous email systems environments.

Cisco offers a range of very flexible licensing options, including different types and lengths of subscriptions as well as integration into larger Cisco buying programs for Security Suites and Enterprise Agreements.

Cisco provides a powerful Email Security solution that can both extend existing Cisco Secure Email environments and support heterogeneous environments as it can expand the level of email threat defence in Microsoft 365 environments. With its integration into the broader Cisco security solutions, it is well-targeted at enterprise buyer’s that already have a range of Cisco solutions in place or are strategically looking to bolster their security posture.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Cisco Security

Table 6: Cisco's Secure Email Threat Defense's rating

Strengths

- Modern API-based solution for email security
- Close integration with Microsoft 365, Microsoft Defender, and Microsoft Sentinel
- Close integration into the broader Cisco security portfolio, including Cisco XDR and Cisco Talos Threat Intelligence
- Can be used in combination with Cisco Secure Email for combined solution including a SEG (Secure Email Gateway), thus providing strong support for mixed / heterogeneous email environments
- Good set of email security features for a wide range of threats
- Ambitious roadmap for further expanding the feature set
- Well-suited for existing Cisco customers due to integrations and licensing options
- Flexible licensing options

Challenges

- API-based solution focuses on email inbox analysis, but does not intercept emails ahead of reaching the inbox
- Cloud services and user interface of SEC and API-based solution not yet integrated
- No specific support for Google Workspace
- No email archiving supported

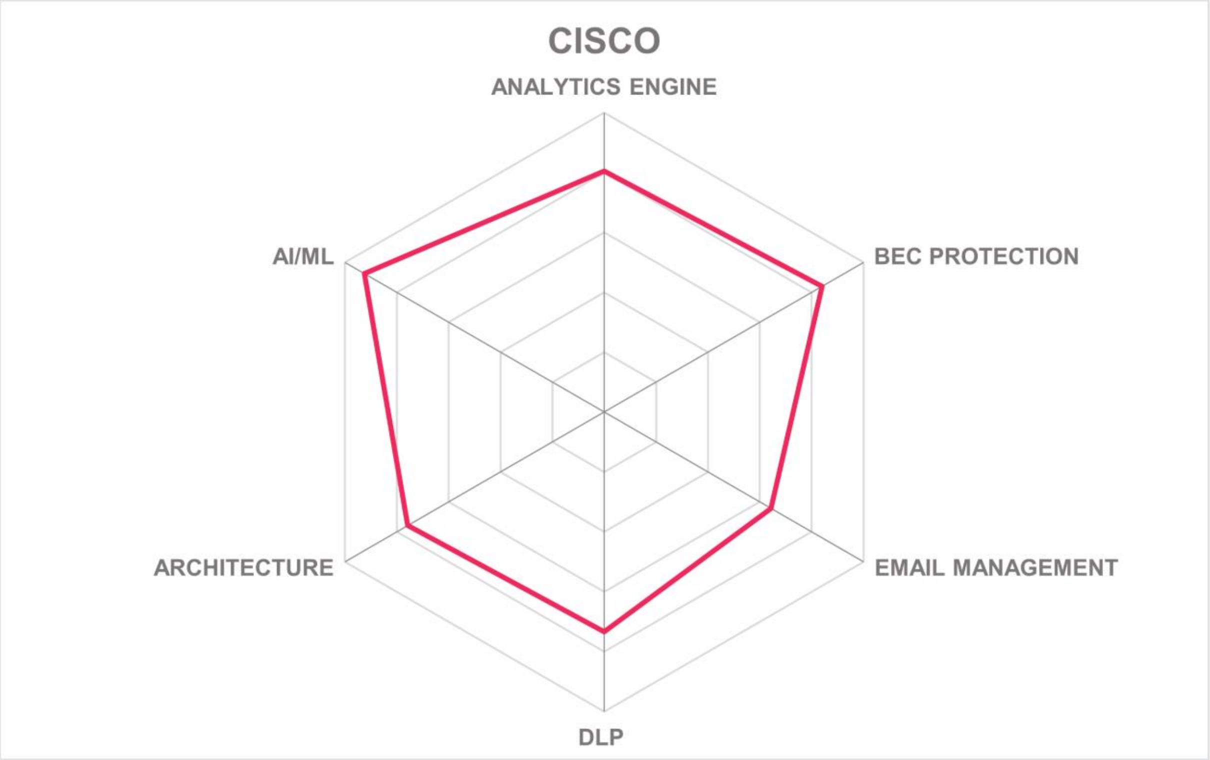
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


CISCO
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Cloudflare – Area 1 Email Security

Cloudflare, a US based company, provides a range of services from its global cloud network including CDN, WAAP, DDoS protection, SSE, Single-Vendor SASE, and developer services. Beyond protecting public-facing internet services and websites, Cloudflare has expanded into also protecting other services. This expansion was based on a series of acquisitions, including Area 1 Security, which brought Email Security to the Cloudflare portfolio.

The core offering of Cloudflare, Cloudflare One, is positioned as a highly secure, agile, and composable business wide networking fabric, spanning a range of services from application security services, developer services, Zero Trust services, and network services. Cloudflare One is positioned to deliver a full stack SASE (Secure Access Service Edge) platform.

Within Cloudflare One, Email Security is one of the services provided as part of their Secure Web Gateway services. Cloudflare Area 1 Email Security, despite its relation to the SWG (with “gateway” in the name) is a combination of inline and API-based deployment, with the inline deployment provided as part of the Cloudflare One network and the ability to analyse network traffic including emails. This means incoming mail can be routed through the Area 1 Email Security solution. The solution can analyse incoming mails in both Microsoft 365 and Google Workspace inboxes.

This approach allows Cloudflare to support both modern, cloud-based email environments as also heterogeneous and legacy environments where still on-premises email systems are in use.

Cloudflare builds on a layered approach for analysing incoming email traffic, utilizing a range of modern technologies such as NLU (Natural Language Understanding) that are essential for tackling today’s threats such as BEC (Business Email Compromise) and Social Graph Analysis, which looks at common patterns as well as outliers in email communication.

Following a structural analysis of emails including header, body, graphics, links, and payload, the solution analyses the content based on NLU. Additionally, Area 1 Email Security uses sentiment analysis, industry-focused analysis and modelling and social graphs to gain insight into the content and whether this is potentially malicious. This adds to other features such as anti-malware protection and advanced threat defence in combination with the signals the Cloudflare One ecosystem can provide. It also supports integration to various SIEM (Security Information and Event Management) solutions via APIs to correlate own detections to other security events from a variety of sources.

Cloudflare targets replacements of existing SEG environments and the expansion of Microsoft 365 Email Security as their primary use cases.

With its dependence on other Cloudflare services, Cloudflare Area 1 Email Security is primarily of relevance to customers that are also using other Cloudflare services and that are looking for a comprehensive cloud security and SASE approach including Email Security and, potentially, adding another layer of security to Microsoft 365 or Google Workspace.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

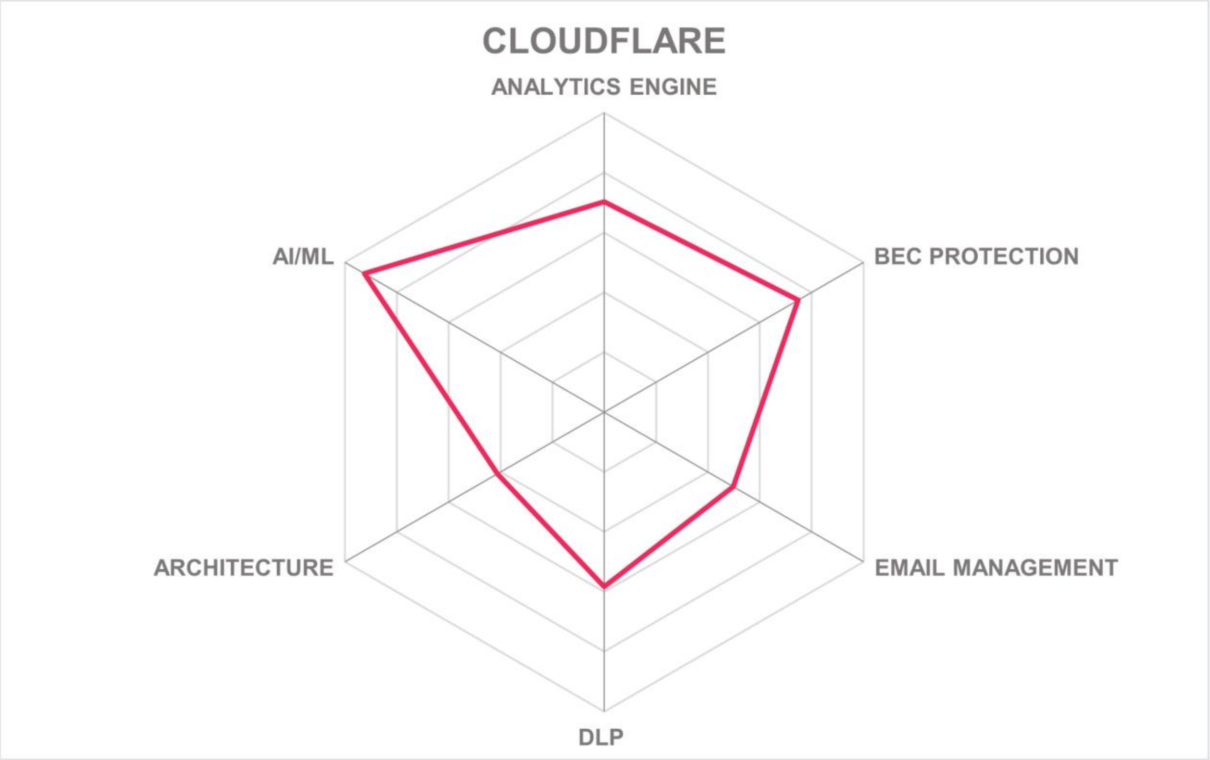
Table 7: Cloudflare Area 1 Email Security's rating

Strengths

- Cloud-based solution, not requiring on-premises components
- Supports deployment inline and API-based
- Supports both Microsoft 365 and Google Workspace
- Close integration with other Cloudflare services
- Modern user interface
- Strong set of APIs for integration with other solutions
- Modern analytics for content analysis of emails

Challenges

- Best value provided in combination with the overall Cloudflare One solution portfolio
- No email backup and archiving capabilities
- No integrated support for additional channels such as Microsoft Teams or Slack
- API-based integration to SIEM solutions requires additional customization


CLOUDFLARE
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

ESET – Mail Security / Cloud Office Security

ESET is a privately held software company headquartered in Slovakia. Their roots are in the anti-malware, from where ESET expanded into adjacent areas of cybersecurity. ESET is currently recognized as Europe's largest privately held cybersecurity company. ESET provides services for both the SMB and the enterprise market segments as well as to MSPs (Managed Service Providers). Their go-to-market approach is channel-focused.

The product portfolio of ESET is centred around their ESET PROTECT Platform and the XDR-enabling (Extended Detection & Response) component ESET INSPECT. This platform covers a range of services, including Advanced Threat Defence based on ESET LiveGuard Advanced, which is used for proactive monitoring, cloud sandboxing, and behavioural analysis, extending the feature set of ESET Mail Security. The platform also includes a range of different specialized security solutions, including Endpoint Security, Mobile Device Security, and – finally – Email Security.

The Email Security solutions provided by ESET are split into two separate solutions. ESET Mail Security is a traditional on-premises SEG (Secure Email Gateway) integrated with Microsoft Exchange, and ESET Cloud Office Security is an API-based Email Security solution for Microsoft 365 and Google Workspace environments. It accesses these environments via a Graph API and Google APIs respectively, focusing on the post-delivery analysis of emails in contrast to an inline deployment where mails are analysed immediately after they appear in the user's inbox. The emails remain hidden during inspection.

While not being fully integrated products, both can be managed via the ESET PROTECT console, a unified interface for managing various ESET security solutions in an integrated manner. This console comes with powerful dashboards, providing insight into the details of the various connected solutions.

Being part of a broader XDR and cybersecurity tools portfolio including a managed services / MDR (Managed Detection & Response) solution, the ESET solutions for Email Security also benefit from managed services as well as shared signals from the XDR platform.

ESET Mail Security runs on Windows Servers and can support Microsoft Exchange Server and IBM / HCL Domino servers as well as hybrid Microsoft Exchange setups integrating with Microsoft 365. It provides a rich feature set covering anti-spam, anti-malware, anti-phishing, web-based email quarantine, as well as rule-based filtering and actions. The endpoint security product can integrate directly with Microsoft Outlook, although Mail security does not, securing the Microsoft Exchange Server side. No plug-ins are available for other email clients.

ESET Cloud Office Security adds the integration to ESET LiveGuard Advanced. It also comes with the option for automatic protection, where all Microsoft 365 and Gmail mailboxes are automatically added to the protection provided by the solution. As the name indicates, ESET Cloud Office Security goes beyond Email Security and adds protection for Microsoft OneDrive, Microsoft Teams, and Microsoft SharePoint Online and Google Drive.

Administrators also can submit false positive and false negative spam, phishing, and malware samples for further analysis, helping to improve the reliability of detection of malicious emails.

ESET are of particular interest to EU headquartered and governmental organizations, which may prefer building on a European solution for cybersecurity since ESET is one of the few European providers of Email Security and other cybersecurity solutions.

Security	Positive
Functionality	Positive
Deployment	Strong positive
Interoperability	Positive
Usability	Positive

Table 8: ESET Mail Security/Cloud Office Security’s rating

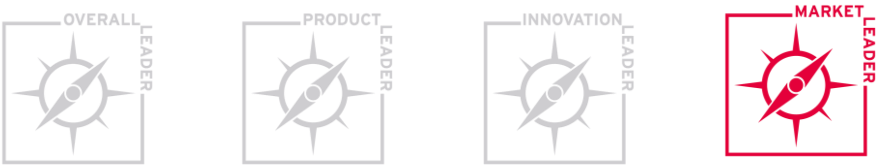
Strengths

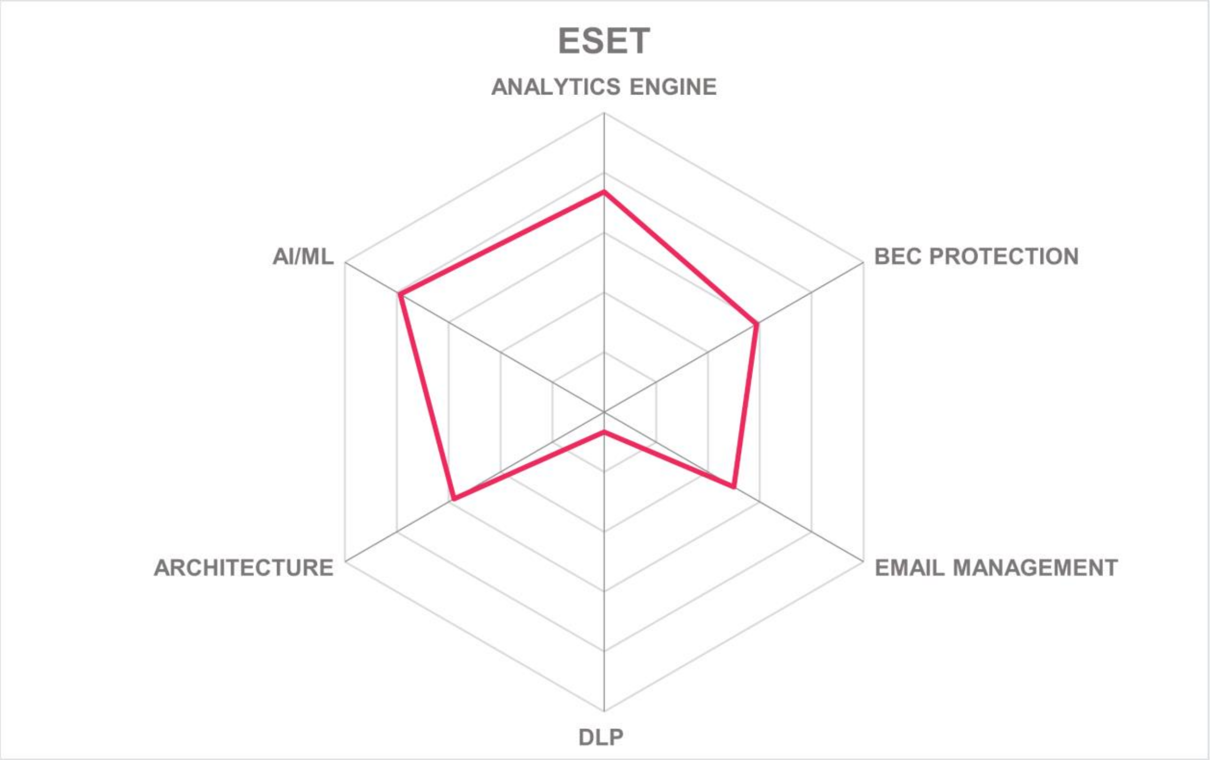
- Supports both API-based and on-premises deployments
- Unified user interface based on ESET PROTECT console
- Modern user interface with good dashboards
- Integrates into the broader ESET cybersecurity portfolio and XDR approach
- Leading-edge anti-spam, anti-phishing, and anti-malware support
- Supports quarantining malicious emails
- Also supports other Microsoft 365 solutions such as Microsoft Teams
- Google Workspace support for Gmail and Google Drive
- European software solution that can be deployed from an EU data centre
- Native multi-tenancy for MSPs

Challenges

- No support for inline deployments with Microsoft 365, only API-based analysis of mails after arriving in inbox
- On-premises support limited to Microsoft Exchange Server and Lotus / HCL Domino
- No specific BEC (Business Email Compromise) detection features
- No auto-tuning capabilities
- No email backup functions
- Does not have DLP features

Leader in




ESET
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Group-IB – Business Email Protection

Group-IB is a company delivering cybersecurity solutions. It is headquartered in Singapore, having fully split from their former Russian business. Their current European headquarters are based in Amsterdam, Netherlands. The company employees more than 250 people, is active in sixty countries and holds / has applied for more than 120 patents. It has a close partnership with both Interpol and Europol, as well as various national criminal police offices across Europe.

The company started in DFIR (Digital Forensics and Incident Response), before launching their first own software solutions back in 2013. At the core of their product portfolio is the Unified Risk Platform, which is centred around their Managed XDR (Extended Detection and Response) capabilities. This platform is a combination of technology and services. Part of it is the Business Email Protection (BEP). It is developed completely by Group-IB, also due to their specific focus on DFIR.

Group-IB has added DFIR to their portfolio, protecting Microsoft 365 as well as Microsoft Office 365 and Google Cloud. This is because most attacks utilize emails as part of the attack chain and that attackers tend to test their attacks against the Microsoft environment first, as this is used by most organizations.

In contrast to many other solutions, Group-IB Business Email Protection follows a SEG (Secure Email Gateway) approach that can be delivered as SaaS, in private cloud environments, on-premises, and commonly sitting in front of an existing mail gateways. This form of inline protection helps in analysing mails and their content ahead of hitting the user's mailboxes. Group-IB is expanding API-based integration and already is using this for the Google integration. It does not directly integrate with email clients, although it can be configured for IMAP/POP3 compliant interfaces.

The feature areas of Business Email Protection include the analysis of attachment and links and supports more than 290 different file formats. It can run detonate payloads in isolated environments, including technologies, which help in protecting against advanced types of attacks. There is support for anti-spam and anti-phishing. The solution uses Machine Learning techniques for identifying BEC (Business Email Compromise), as well as other features such as failed DKIM /SPF and DMARC policy checks.

The solution comes with a powerful interface for administrators and cybersecurity analysts, allowing them to drill-down into the details of suspicious mails. Due to the integration with (managed) XDR, the analysis can be done in the context of a broader range of threat information and can be supported by the managed services teams of Group-IB. The user interface is modern and delivers a large quantity of information, being extremely focused on the detailed investigation of email-based attacks. For each malicious file, Group-IB can automatically build a MITRE matrix, indicating the type of attack. Group-IB BEP solution also provides detailed detonation reports with process details, behavioural markers, scorings, network connections, and further information.

To minimize the impact of a gateway-based approach as well as for rapid evolution of the solution, the analytical capabilities are split across multiple integrated engines that all work simultaneously on the mails.

Configuration of the solution is very flexible but requires significant administrative knowledge and lacks in auto-tuning capabilities. This, together with the deployment approach and the strength in investigation, makes Group-IB Business Email Security a solution that is of specific interest for high-risk customers such as governmental agencies. It can also extend other vendor's Email Security solutions with an added level of security and managed services. Due to the cost involved, this, as stated, is primarily of interest to organizations with a very high-risk exposure.

Security	Positive
Functionality	Positive
Deployment	Strong positive
Interoperability	Positive
Usability	Positive

Table 9: Group-IB Business Email Protection's rating

Strengths

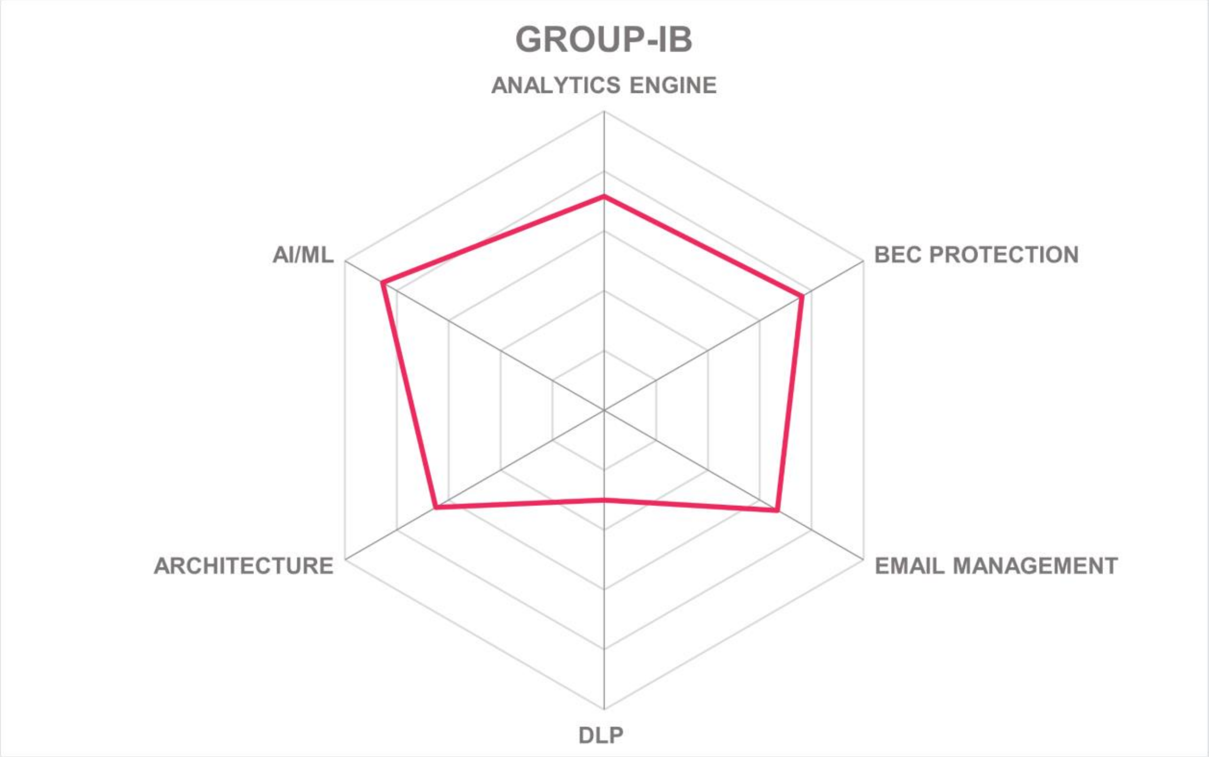
- Solution can be deployed in front of any email server and in front of other email Security solutions
- Flexible deployment options from on-premises deployments to SaaS
- Integrated with other security solutions as part of the Group-IB managed XDR portfolio
- Excellent capabilities for investigation of malicious emails
- Supports ML-based BEC (Business Email Compromise) analytics
- Good performance due to parallel execution of analytics engines
- Additional security layer for high-risk organizations

Challenges

- Not yet a fully integrated email security approach, but increased API-based integration
- No plug-ins for standard email clients
- Powerful, but rather complex configuration, lacking auto-tuning capabilities; comes with out-of-the-box default settings for simplifying roll-out
- Managed services provided, delivering expertise to the customers, but at a cost
- Limited scalability of services
- No built-in DLP functions

Leader in

OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


GROUP-IB
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

IRONSCALES – Email Security Platform

IRONSCALES is a mid-stage startup founded in 2014 and headquartered in Atlanta, Georgia, US. IRONSCALES specializes in email security. Their platform is an API-based integrated cloud email security solution that supports the Microsoft 365 and GWS cloud-based email platforms, as well as Microsoft Exchange 2007+ servers. It runs in either Amazon AWS or Microsoft Azure. It integrates with Microsoft Outlook, Outlook mobile app, and Outlook Web Access. Pricing is per-mailbox with two options. They also offer a starter package for free.

IRONSCALES scans emails using pre-configured rules and applies unsupervised and supervised ML and Deep Learning algorithmic detection models. These models are trained on customer data and use Reinforcement Learning from Human Feedback (RLHF). IRONSCALES understand dozens of the most used languages. It can detect spam, phishing, spear phishing, malware, and BEC, as well as many specific attack types including, backscatter, directory harvest attacks (DHAs), DDoS, and MIME-FROM. Bounce management and outbound email keyword filtering are not supported.

Their Email Security Platform scans and can block attachments. It does not identify nested or password-protected archive files, nor does it perform Content Disarm and Reconstruction (CDR). IRONSCALES leverages nearly 80 third-party malware scanners, covering signatures, sandboxing, heuristics analysis, and exploit detection methods. IRONSCALES takes in cyber threat intelligence (CTI) from most major open and commercial sources. It uses CrowdStrike Falcon for sandboxing. When malicious emails are discovered, it can quarantine them and alert both users and administrators or add customizable disclaimers to the email. It also fingerprints incoming messages and continues to test links after delivery to see if they become malicious, and if so, it can remove those from users' mailboxes.

IRONSCALES emphasizes the prevention of BEC with its AI assisted detection routines. It can identify and looks out for Very Attacked Persons (VAPs), such as executives. It integrates with KnowBe4, Mimecast, Microsoft, and Proofpoint for reporting phishing and phishing testing. Integration with supply chain risk management systems is supported by RESTful APIs. Users can report spam as well as phishing, and the platform adjusts based on RLHF.

IRONSCALES supports SPF, DKIM, and DMARC authentication and reputation management for inbound mail. It does not perform directory checking, querying, or synchronization for outbound email. Email signing and encryption are not supported.

The platform has some built-in DLP functions in the Accidental Data Exposure feature, which uses AI/ML natural language processing to detect sensitive data in the subjects, bodies, or attachment names. It does not integrate with other DLP tools, and as an API-based service, it does not provide eDiscovery/litigation hold capabilities.

IRONSCALES does not provide email backup services as customers generally use those offered by the customers' email service provider. There are out-of-the-box integrations with major SIEM, SOAR, and XDR systems. Customers can build API connectors for CASB if needed. Executive and administrative dashboards are available. The admin console allows for drilling down into forensic details for analysis into attack flows, content, and types of attacks. Playbooks are available for quick response handling. The admin interface also allows controls to be defined based on risks associated with particular email types, users, and groups of users. Standard report types are available, but neither the report content nor admin interface are customizable without coding.

IRONSCALES’ Realtime Learning from Human Feedback feature trains detection models continuously for better accuracy. IRONSCALES is ISO 27001 and SOC 2 Type 2 certified. Outbound authentication, CDR, and integration with external DLP tools would strengthen the offering. As an integrated cloud email security platform, IRONSCALES is best suited for organizations with extensible email service platforms that are looking for ML-enhanced multi-engine malware scanners.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

IRONSCALES SAFER TOGETHER

Table 10: IRONSCALES Email Security Platform's rating

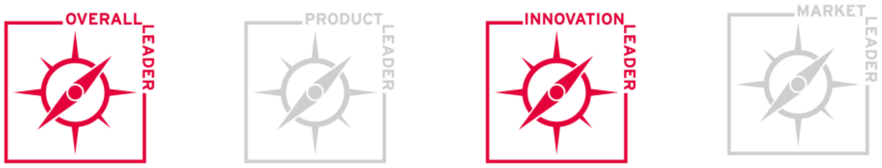
Strengths

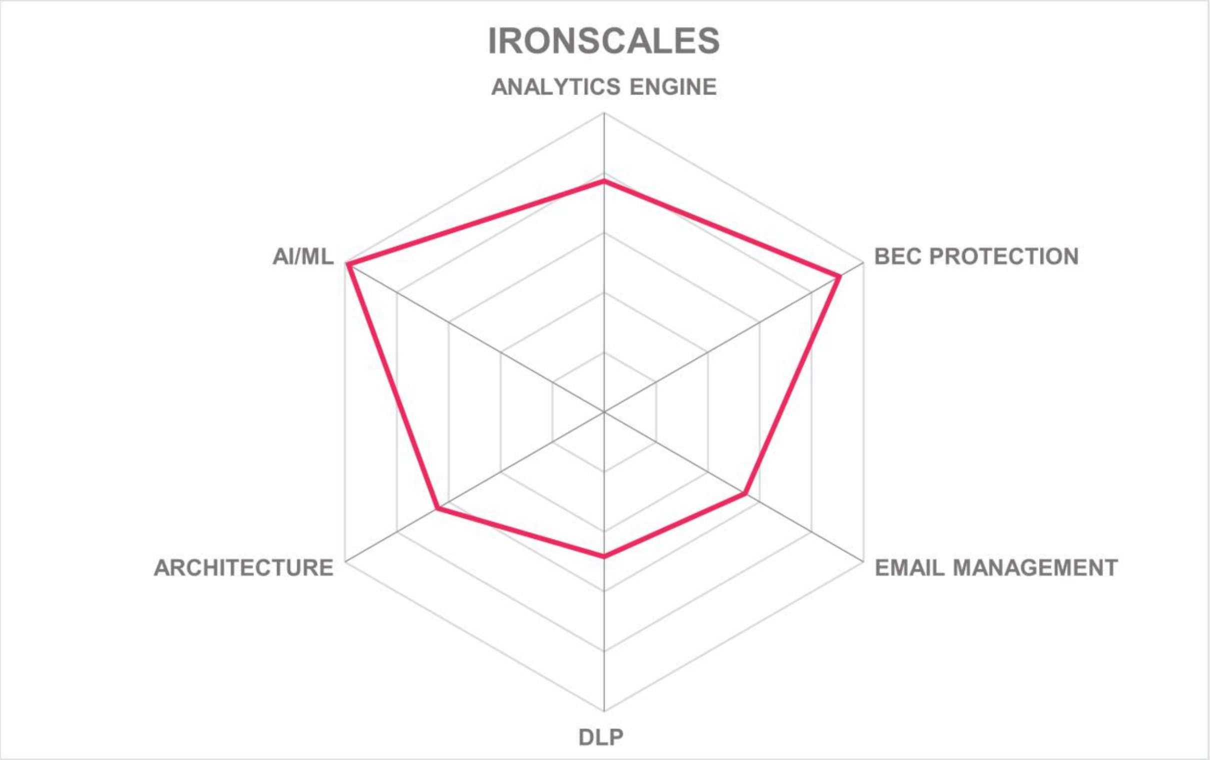
- Uses advanced ML, DL, and Generative AI with Reinforcement Learning from Human Feedback
- VAP identification and monitoring
- Uses dozens of malware scanners and CTI sources
- Post-delivery protection for client inboxes
- Accidental Data Exposure prevention looks at subjects, body text, and attachment names
- Connectors for SIEM and SOAR
- Free IRONSCALES starter package
- Provides a mobile app for administrators
- Integrated PST (Phishing Simulation Training) and SAT (Security Awareness Training)

Challenges

- Scanning rules are not customer configurable
- Does not do bounce management or keyword filtering on outbound email
- Does not perform CDR
- No certificate or key-based encryption
- Does not integrate with third-party DLP tools
- Admin interface and reports are not easily customized

Leader in




IRONSCALES
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Microsoft – Defender for Office 365

Microsoft is the world's largest software manufacturer. Over the years, Microsoft has heavily invested into identity and cybersecurity solutions, which are neatly integrated with their Microsoft 365 and other solutions. These come in the form of both integrated solutions and add-on services that are commonly acquired via different forms of packaged licenses.

Microsoft Defender for Office 365 is the Email Security solution of Microsoft. The product comes in two different plans, a baseline plan covering common Email Security functionality, and an extended plan that adds threat investigation, automated investigation and response, attack simulation training, and cross-domain (beyond email) XDR (Extended Detection and Response) capabilities for correlation of security incidents and advanced analysis and forensics of security-related incidents.

Microsoft Defender for Office 365 is one of several related solutions and can work with Microsoft Sentinel (SIEM, Security Information and Event Management), Microsoft Defender and Microsoft Defender for Cloud (XDR solutions) for increasing the cybersecurity posture with a set of integrated solutions.

Microsoft Defender for Office 365 should not be confused with the integrated Email Security features of Microsoft 365. The baseline protection of Microsoft 365 already provides capabilities such as antimalware analysis, phishing detection, and URL scanning in the Premium Edition of Microsoft 365. Microsoft Defender for Office 365 adds to these capabilities with the two different plans.

The solution covers various areas from prevention and detection to investigation and hunting, response and remediation, and awareness training plus the above-mentioned XDR integration. It works with a layered defence-in-depth approach starting at the edge and covering a wide range of features including sender analysis, content filtering, and post-delivery protection. Thus, it starts protecting ahead of emails reaching the in-box of users, but also supports post-delivery protection. Other capabilities include processing email attachments in sandboxed environments.

Microsoft benefits from a vast number of signals across their tenants, claiming to analyse around 470 billion (and growing) emails per month. Based on these signals and their automated processing, Microsoft Defender for Office 365 comes with a high degree of auto-tuning capabilities. It applies machine learning models to form contact graphs of users, for instance, in the context of BEC (Business Email Compromise) identification.

Microsoft Defender for Office 365 spans additional areas, beyond email, such as identifying anomalies in collaboration activities on Microsoft Teams. It can deliver detailed alerts via dashboards, enabling administrators to drill-down into the details.

Not surprisingly, Microsoft Defender for Office 365 is targeted at the Microsoft 365 environment. While Microsoft also offers a separate, functionally limited Email Security solution for Exchange Server environments, the current focus is on the Microsoft 365 environments only. Microsoft offers APIs for integrating with other email solutions and thus supporting organizations that have mixed or legacy email environments.

Security	Strong Positive
Functionality	Positive
Deployment	Strong positive
Interoperability	Positive
Usability	Positive

Microsoft

Table 11: Microsoft

Strengths

- Comprehensive coverage of Email Security capabilities
- Backed by a vast number of signals from processing emails on Microsoft 365
- Common user experience with other Microsoft 365 solutions
- Advanced Plan 2 supports additional features such as XDR integration and training
- Close integration to other Microsoft Defender solutions as well as to Microsoft Sentinel
- Integrated deployment in Microsoft 365 environments
- Supports multi-layered defence, starting at the edge and analysing mails ahead of hitting the user’s inbox
- Supports post-delivery security functions
- Modern UI and dashboards

Challenges

- Targeted at Microsoft 365 / Office 365 environments only, limited support for hybrid / legacy environments by API-based integration
- Complex licensing structure in the context of other Microsoft 365 offerings
- Further analysis and security integration targeted at Microsoft solutions, lesser other vendor’s SIEM and XDR

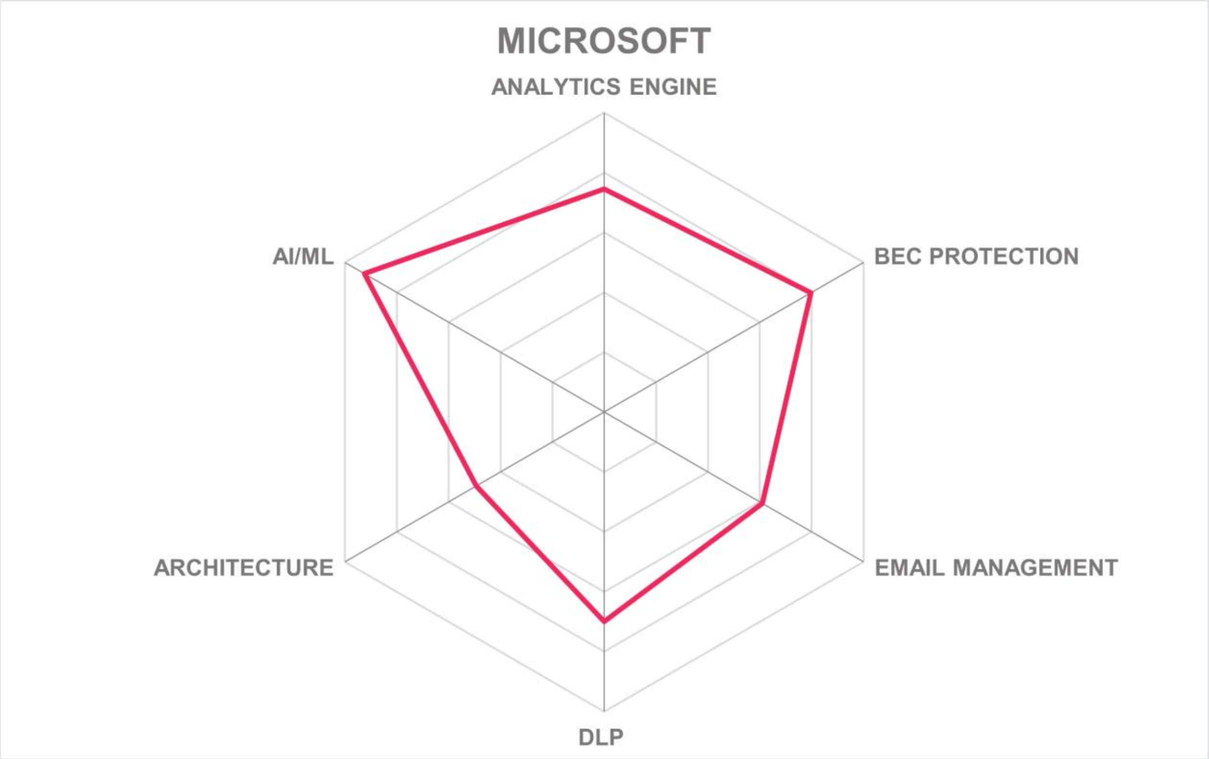
Leader in

OVERALL
LEADER

PRODUCT
LEADER

INNOVATION
LEADER

MARKET
LEADER


MICROSOFT
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Mimecast – Email Security

Mimecast was founded in 2003 and then acquired by Permira, a private equity firm in 2022. They are headquartered in Boston, MA. Mimecast is an email security and management specialist, with additional solutions for data retention and compliance, and security awareness training. Mimecast Email Security is a SaaS hosted in their own data centres and multiple cloud service providers. It can integrate with Microsoft Outlook. Subscription plans are per-user per-service.

Mimecast leverages complex rules and AI-/ML-based detection models. Mimecast makes extensive use of supervised ML and DL algorithms for phishing site detection, URL analysis, natural language processing, identity graphs, brand impersonation detection, BEC detection, spam detection, and detecting NSFW images and GIFs in email. Detection models are regularly retrained on customer data. Language analysis is limited to English and German. Mimecast protects against attacks such as backscatter, DHA, and DDoS. It provides bounce management, policy-based email throttling, and outgoing email scanning.

For attachment handling, Mimecast examines the relevant file types for malware detection and content analysis. Additional file types can be added. For malware detection, Mimecast uses multiple scanning engines that employ signature, sandboxing, heuristic analysis, and exploit detection methods. Multiple commercial sandboxes are leveraged for malware analysis. Malicious files can be deleted, quarantined, or scrubbed using CDR and rendered into safe, read-only versions. URLs are rewritten after examination. Recipients and admins are alerted when actions are taken. Neither incoming nor outgoing messages are fingerprinted, but Mimecast provides powerful search capabilities for mails as well as automated remediation. Mimecast performs post-delivery URL checking for latent malware activation and automated malware remediation but does not automatically delete it from users' inboxes. Mimecast also has browser isolation for additional layer of protection for attachment processing.

Mimecast generates lists of VAPs, and customers can manually add to the list. Supply chain risk management integration is not available, but various capabilities including DMARC management support the respective use cases. Security awareness training and testing are add-on solutions.

Their platform supports SPF, DKIM, and DMARC management and validation. Mimecast adds sophisticated sender reputation analysis beyond the standards. Mimecast supports outbound authentication, directory queries and synchronization with Google Workspace, Lotus Notes/Domino, Microsoft Exchange and Office365, and any LDAP compatible user database. Mimecast supports SSL/TLS and STARTTLS encryption, but not x.509 certificates.

Configurable banners, based on rules, ML, and an identity graph, warn users of external origins, untrusted (low reputation) senders, potential phishing or malware, and encryption status. Outlook integration enables one-click reporting of spam, junk, or suspected phishing emails.

Mimecast has a DLP content inspection engine with reference dictionaries covering major industries such as finance and health care. Customers can extend content inspection with regular expressions as needed. It also supports litigation / e-discovery holds. A connector is available for Netskope CASB. Their platform integrates with many EPDR, XDR, SIEM, SOAR, and ITSM tools. Dashboards and reports are available and can be customized. The administrative interface is easy to use. A mobile app for management is available.

Mimecast has obtained ISO 27001, ISO 27701, HIPAA, SOC 2 Privacy Trust Principle, and SOC 2 Type 2 certifications. The roadmap includes extending protection to Microsoft SharePoint and Teams and Slack. Backup and archive options are present. Organizations looking for additional protection for the email systems should have Mimecast on their shortlist for consideration.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

mimecast®

Table 12: Mimecast Security Cloud's rating

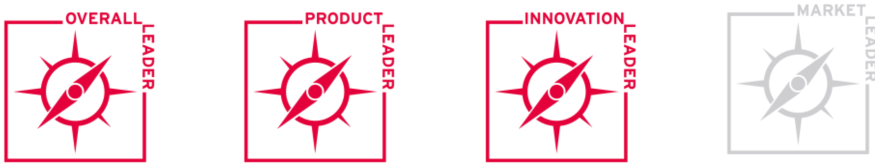
Strengths

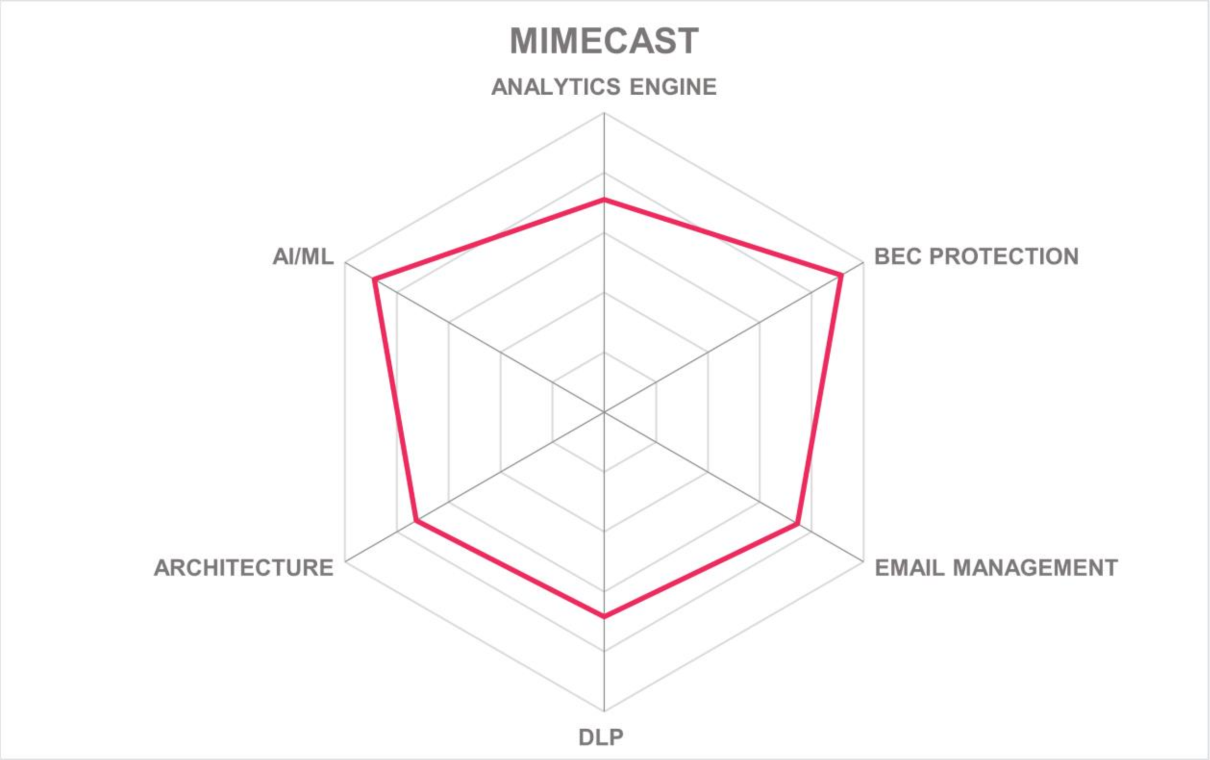
- Extensive use of ML for spam, phishing, URL, and malware detection and user behavioural analysis
- Content Disarm and Reconstruction for malicious content
- Browser isolation
- Can remove NSFW images and videos
- Multiple security and privacy certifications
- TLS encryption
- Multiple integrations for popular security and IT management tools
- DLP content inspection with common dictionaries is available and is extensible via RegExp
- Support for e-discovery and litigation holds

Challenges

- Post-delivery scanning and automated remediation of malware, but no automatic deletion of infected mails
- Limited language support
- No supply chain risk management

Leader in




MIMECAST
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Perception Point – Advanced Email Security

Perception Point was founded in 2015 in Israel. They are a mid-stage venture-backed company. In addition to email security, Perception Point also has products for web browser and cloud collaboration security. Their solution is primarily API-based, but has multiple deployment options, such as out-of-band message copying and acting as a SEG. It is SaaS, hosted in public IaaS. It can integrate with Google Workspace and Microsoft Outlook via routing/compliance rules. Pricing is based on the numbers of users per month, although fixed price and other options are available.

Perception Point uses complex rules and sophisticated, internally developed unsupervised and supervised ML and DL detection models to power their solutions. The models are continuously trained on data from all customers. Perception Point detects spam, phishing, BEC, CEO fraud, key personnel and brand impersonation, fake invoices and other fraud types, backscatter, DHA, DDoS, and MIME-FROM attacks. The solution does not address bounce management. It scans outgoing mail as well for keywords and content.

For attachment handling, Perception Point scans all files dynamically and can block over 230 types based on attributes, password protection, etc. It can scan and manage nested and password-protected archive files. Perception Point integrates several commercial CTI sources and anti-virus scanning engines with its in-house tools, which address all the major A/V techniques including signature-based, heuristic analysis, and exploit prevention. Their platform does not provide CDR, but instead it leverages their HAP™ (Hardware-Assisted Platform, a “next-gen” dynamic sandbox) for thorough analysis. Handling options include quarantine, delete, move to other folders, reject, add to allow/deny lists, and add warning banners. It fingerprints items and can remove malicious content and links even after delivery.

The Advanced Email Security product can identify VAPs for additional monitoring, and customers can add users to the list. At present there are no integrations for passing this information to other systems. There are also no integrations with supply chain risk management solutions. Perception Point has a connector for KnowBe4 email security awareness training, and others could be configured via APIs if needed.

The company offers Incident Response services as an integral part of its solution with no extra charge. The Incident Response service includes engine optimizations on a customer-basis, detection enhancements, fraud prevention management, cyber intelligence, and support for security teams.

This solution uses SPF, DKIM, and DMARC authentication and both external and in-house intelligence for sender reputation determinations. Perception Point also performs authentication for outbound connections. Directory synchronization is possible with Microsoft Exchange and Office 365, Lotus Notes/Domino, or any LDAP type database. Directory queries are not supported. Perception Point is exploring partnerships for email encryption, but it is not currently offered.

DLP features are limited to detecting potential violations and alerting customer administrators. Additional functionality is planned for future development. Integrations with third-party DLP systems is possible via API, but no connectors have been built. Connectors are available for CrowdStrike, Cynet, and Sentinel One XDR products. E-discovery and litigation hold capabilities are not present. Their primary dashboard, called X-Ray, contains views for management and security analysts. It shows high-level trends and allows for easy policy management and deep forensic analysis. Widgets are configurable. Mobile access is available for on-the-go reporting and management.

Perception Point is ISO 27001, SOC 2, and HIPAA certified. It is also GDPR compliant. It can store emails and attempt redelivery if clients' email services are down temporarily, but it does not offer email archiving. Perception Point is missing some features and has interoperability limitations, but it has multiple deployment options and advanced sandboxing and analysis capabilities. Perception Point can be extended to protect Microsoft OneDrive, SharePoint, and Teams, as well as Salesforce, Slack, and Google Workspace apps. Organizations that need those leading-edge threat detection capabilities and have other solutions for encryption and backup should consider Perception Point.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 13: Perception Point Advanced Email Security's rating

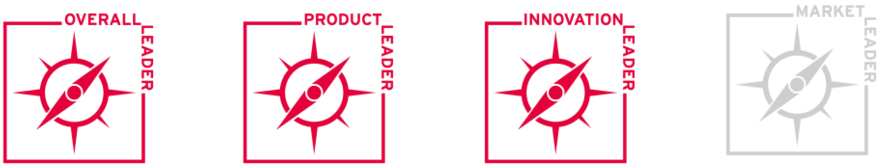
Strengths

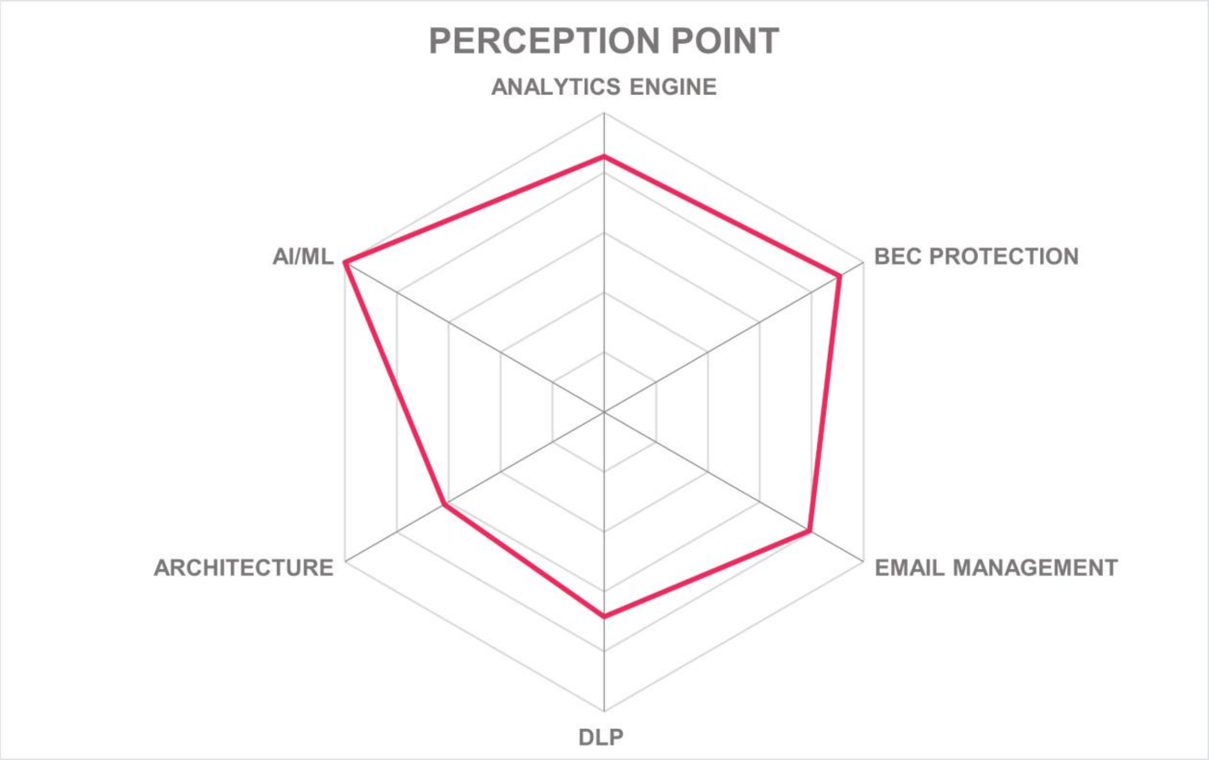
- Flexible pricing and deployment models
- Advanced use of ML and DL detection algorithms across all products
- Broad range of file types understood, include nested and secured archives
- Message fingerprinting and post-delivery removal if later detected to be malicious
- Next-generation sandbox included for email analysis
- Integrated, free-of-charge incident response service
- Protection for Microsoft OneDrive, SharePoint, and Teams, Google Workspace apps, Salesforce, and Slack

Challenges

- Does not perform CDR
- No email encryption (in roadmap for partnership) or archiving
- DLP limited to identifying and alerting on violations of outbound mail policies
- No connectors for third-party DLP systems, but API integration is possible
- Does not have e-discovery or litigation hold capabilities
- Does not have supply chain risk management integrations
- Limited out-of-the-box connectors for other security solutions

Leader in




PERCEPTION POINT
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Proofpoint – Aegis Threat Protection Platform

Proofpoint launched in 2002 and is headquartered in Sunnyvale, CA. They have offices and partners around the world. In 2022, private equity firm Thoma Bravo acquired the company. Proofpoint offers archive and compliance, data classification, DLP, Insider Risk Management, ITDR (Identity Threat Detection and Response), digital risk protection, security awareness, and managed services in addition to email security. The solution has on-premises software and appliance deployment options as well as SaaS and fully managed instances. The SaaS offering is hosted in their own facilities and in public IaaS. The solution can function as an integrated cloud email security system or as a SEG. Microsoft Outlook plug-ins are available. Licensing is per-user per-service with multiple tiers of support.

Proofpoint uses complex rules with built-in and customizable dictionaries and RegExp as well as supervised ML and DL algorithmic detection models. The models are continuously trained on live data across all customer environments and human feedback. Customers can edit allow/deny lists as required. Proofpoint analyses email in the ten or so most popular languages. Aegis can discover and prevent spam, phishing, BEC, backscatter, DHA, DDoS, malware, ransomware, and MIME-FROM attacks. It handles bounce management and scans outgoing email for keywords.

Proofpoint examines multiple file types as attachments, including nested and password-protected archives, by attempting to unlock them. Office documents with macros are not blocked by default, but instead scanned for malicious code. Standard actions such as block, quarantine, delete, and alert are available in customer configurable policies. It does not perform CDR because Proofpoint believes it leads to poor user experiences. The platform has its own malware detection engine and is augmented by two other commercial engines. These leverage all available malware identification methods including signature-based, heuristic analysis, ML analysis, sandboxing, browser isolation, and exploit prevention. Proofpoint incorporates CTI from a few third-party sources in addition to their own. When an infected email arrives, policy-based actions include, flagging it as suspicious, adding warning banners, quarantining, and alerting admins. Aegis fingerprints emails and can detect if malicious links are activated after delivery and can remove those emails from user mailboxes.

Proofpoint's Very Attacked People (VAP) is an Attack Index that reflects the risk of a given threat, or set of threats, to an individual or groups, and is an auto-generated list that can be manually edited by customers. VAP information can also be shared with Okta and SailPoint and more partners over API. Proofpoint also integrates with supply chain risk management solutions. Proofpoint has built-in user training enhanced via its 2018 acquisition of Wombat and its 2020 acquisition of The Defence Works, so it does not have connectors for external training services. Aegis Threat Protection Platform uses SPF, DKIM, and DMARC for sender validation and its proprietary Reputation Block Lists (RBL) for sender reputation analysis. Aegis can query and synchronize with Microsoft Exchange and Office365, Azure Active Directory, Lotus Notes/Domino, Google Workspace, and any LDAP compliant user database. Proofpoint provides encryption and it supports S/MIME gateway to gateway/client encryption.

Aegis Threat Protection Platform has extensive DLP capabilities including keyword matching, RegExp, data dictionaries, smart identifiers, and exact data matching. It is compatible with Microsoft AIP and Boldon James labels and can be configured to work with any solution that tags data objects with metadata. Proofpoint Discover (separate service) can provide full e-discovery and litigation hold features, with case management, data tracking, conversation threading, and ML assisted identification.

Proofpoint can integrate with several SIEM systems, and SOAR integration is possible via API. Aegis has executive and administrative dashboards which show types and flows of attacks, as well as status of VAPs. The solution provides many granular reports. Analysts can drill down into forensic investigations directly from the dashboard.

Proofpoint has entered into a definitive agreement to acquire Tessian, adding AI-backed capabilities for automatically detecting and guarding against both accidental data loss and evolving email threats. Proofpoint Archive offers thorough and secure backups using their DoubleBlind Key Architecture. Proofpoint's SLAs provide remediation if service uptime is less than 99.999%, virus detection is less than 100%, and spam detection is less than 99%. Their solution is SOC 2 Type 2 certified and aligns with, but is not certified with, ISO 27001 and NIST 800-53. Proofpoint provides an extensive list of standard features which address most of the requirements for SEGs and API-based email security services. Any organization looking for email security enhancements should have Aegis Threat Protection Platform on their shortlist for evaluation.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 14: Proofpoint Aegis Threat Protection Platform’s rating

Strengths

- Email encryption and DLP functions in the platform
- Bounce management
- Deep analysis of archive files
- Excellent SLAs with customer credit guarantees
- Post-delivery removal of latent malicious email
- VAP threat intelligence sharing
- Supply chain risk management integration
- Excellent and extensible DLP functions

Challenges

- Does not perform CDR
- Additional language support would be beneficial
- No connectors for third-party security training services
- Additional external CTI sources could be utilized
- Not ISO 27001 certified

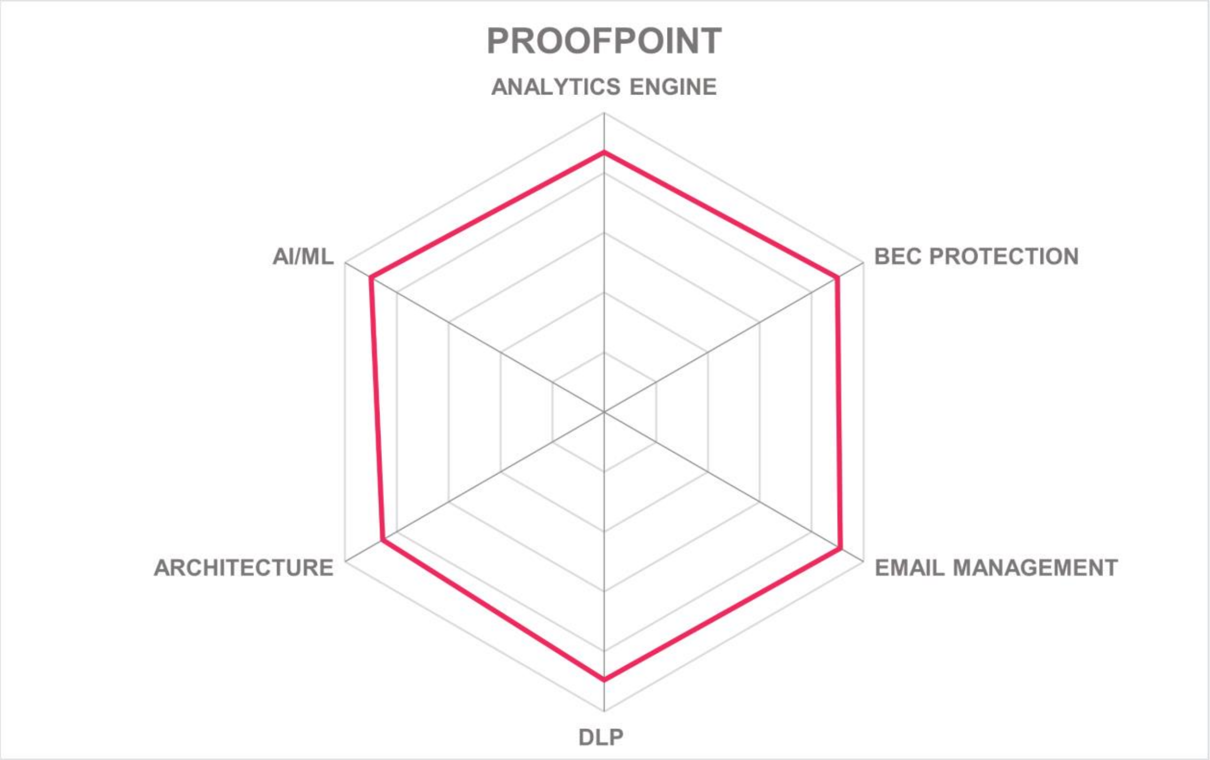
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


PROOFPOINT
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Retarus – Secure Email Platform

Retarus was founded in 1992 and is a privately held corporation headquartered in Munich, Germany. In addition to Secure Email Platform, they offer full enterprise messaging solutions (including SMS), cloud EDI, intelligent document capture and processing, and e-invoicing. Secure Email Platform is an API-based SaaS with Integrated Cloud Email Security (ICES) and application email delivery hosted in their own data centers' facilities within Europe.

Retarus offers a patented solution for post-delivery protection (Retarus Patient Zero Detection®), email encryption, email archive, email continuity (fallback service) and data loss protection. Retarus platform also protects customer domain sender reputation through splitting application traffic from business traffic (Retarus Transactional Email).

Retarus Email Delivery Service enables customers to send 10+ million emails from their applications per hour at peak times and includes Bounce Management. Retarus OEM's multiple major security solutions under their service.

Plug-ins are available for Microsoft Outlook. Subscription pricing is determined by numbers of mailboxes and add-on services per month. Retarus Secure Email Platform leverages configurable static rules for email analysis. OEM products use ML-based detection models, while Retarus is in the process of adding such capabilities to their products. A wide range of languages can be examined. The solution looks for spam, impostor, phishing, BEC, and emails containing malware, as well as backscatter, DHA, DDoS, and MIME-FROM attacks. For BEC prevention, Retarus considers senders' IPs and reputations, but does not employ other common methods. However, it can identify the sender's geo-location. Retarus handles bounce management.

Retarus blocks archive files, unknown MIME types, and password-protected files by default. Customer admins can apply policies that allow quarantining and release of files if desired. Content Disarm and Reconstruction is not available, but alternative security mechanisms help in protecting from malicious attachments and URLs. Retarus uses four different commercial anti-malware engines that employ signature-based, heuristic analysis, ML detection, sandboxing, and exploit prevention technologies. Infected emails can be deleted, including post-delivery, and users informed. Retarus uses five external CTI sources. Secure Email Platform fingerprints incoming email and can remove latent malicious content when discovered. It does not fingerprint and notify recipient domains about malicious email after sending, however.

Secure Email Platform does not provide specific protection for VAPs or provisions for supply chain risk management for email threats. It does have integrations with email security awareness training systems.

Secure Email Platform does SPF, DKIM, and DMARC sender validation. Additional sender reputation analysis comes from Spamhaus. Retarus authenticates outbound senders for downstream protection. Directory queries are not supported, but directory synchronization is available for Microsoft Exchange and Office365, Azure Active Directory, Lotus Notes/Domino, and Google Workspace. S/MIME, PGP, OpenPGP, and x.509 certificate encryption is supported. SwissSign is leveraged for certificate management.

Retarus has some limited DLP features, such as policy-based evaluation of manually defined senders/recipients per mailbox, attachment blocking, pattern recognition of credit card numbers and bank account information. Integration with third-party DLP tools is not available. E-discovery and litigation hold functionality is not present.

Email backup functions are available in a separately licensed service. Retarus can integrate with all major SIEMs using JSON formatted messages. There are no connectors for SOAR systems. Secure Email Platform has both executive and administrative dashboards. Dashboards are not configurable by users. Analysts can launch forensic investigations from the admin interface. Controls can only be implemented for risky email types, not by users or groups. Basic reports are available and additional report types can be customized by users.

Retarus has multiple security certifications including ISO 27001, SOC Type 1 and 2, PCI-DSS, HIPAA, and TISAX. Organizations in Europe looking for a regionally-hosted email security service should consider Retarus when conducting RFPs.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

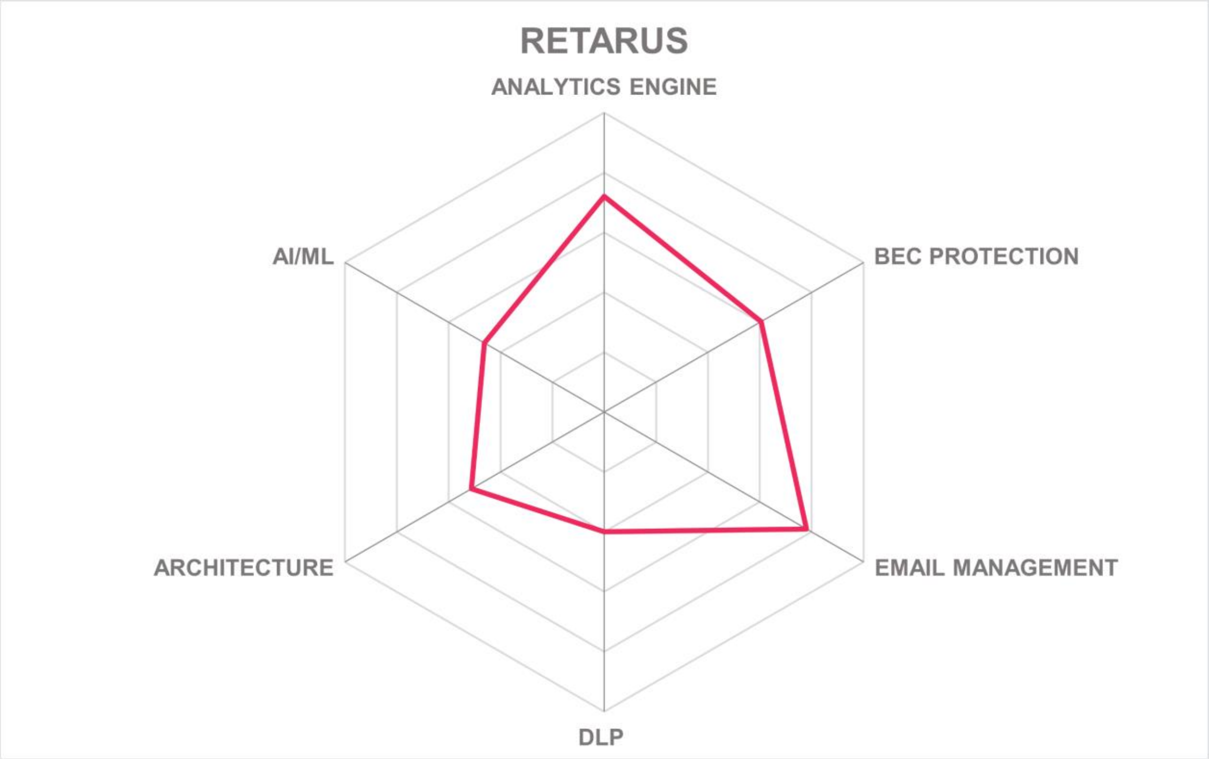
Table 15: Retarus Secure Email Platform’s rating

Strengths

- Offers inbound and outbound Email Security
- Offers email delivery for customers requiring timely delivery of high-volume, business-critical emails, including bounce management
- Support for most common languages
- Can detect and remove messages with latent malicious links
- Supports post-delivery protection
- Supports email encryption
- Supports email archiving
- Own infrastructure and data centers
- Multiple security certifications

Challenges

- Static rule-based detections, little usage of ML detection models
- Extensive use of OEM’d security tools
- Basic DLP functions
- No e-discovery or litigation hold capabilities
- No supply chain risk management for email


RETARUS
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Sophos – Email

Sophos was founded in Abingdon, UK in 1985 and acquired by Thoma Bravo in 2020. Sophos is a pureplay cybersecurity solution. Sophos also offers solutions for endpoint security (Endpoint Protection, Detection and Response), encryption, unified threat management, cloud security, firewalls, secure web gateways, and Zero Trust Network Access. Sophos offers full managed detection and response services. Sophos Email can function as either a Secure Email Gateway or an Integrated Cloud Email Security service run from their own data centres. It works with any SMTP-compliant mail system. It can integrate with Apple Mail, Thunderbird, and any MIME-compliant client. Pricing is per mailbox per month or per year(s).

Sophos uses both complex static rules and advanced ML and DL detection algorithms, developed by their dedicated team of AI researchers. These models are trained regularly in-house and updated quarterly. Sophos understands all the most common languages and its heuristics are language agnostic. Their solution protects against BEC, backscatter, DHA, DDoS, and MIME-FROM attacks. It provides bounce management. They provide and customers can augment keyword lists for outbound email scanning.

Sophos Email can block, quarantine, or remove file types used for attacks such as archives, executables, and Office macros. Nested and password-protected archives can also be examined. Other types are referred to their Intelix service for sandboxing and analysis. Customers can also choose to connect third-party sandboxes if desired. Customizable banners can be appended to emails in inboxes. Customer admins are alerted when actions are taken. Sophos does not use Content Disarm and Reconstruction techniques. Sophos leverages its industry-leading anti-malware engine for detecting malicious code in emails. It fingerprints and can remove emails with latent malicious URLs. However, it does not fingerprint and notify external recipients if malicious links are discovered later.

Sophos generates lists of Very Attacked Persons based on their own analysis, and customers can manually add users to those lists. There are no integrations with supply chain risk management solutions at present. Sophos Phish Threat educates and tests an organization’s end users through security awareness training, automated attack simulations, and actionable reporting metrics. It does not integrate with third-party phishing and security awareness training services.

SPF, DKIM, and DMARC are supported for sender authentication. Inbound scanning includes domain reputation and age as well as sender conversation historical analysis. Directory synchronization to Microsoft Azure Active Directory, Exchange, Office365, and Google Workspace are supported, but directory queries are not. Generic LDAP synchronization is not available. Sophos has built-in encryption options including TLS and S/MIME, which can be applied based on policies for sensitive data, senders, recipients, domains, message content, attachments, and headers.

Sophos Email has fine-grained DLP features which allow customers to set policies based on sender email IDs, sender domains, recipient sender IDs, recipient domains, groups, IP addresses, message subjects, body text, headers, attachment types and content and URLs. Dictionaries cover HIPAA, PCI, and PII. Actions available within policies include modify headers, bounce, rewrite addresses, delete, encrypt, and log. Sophos does not have e-discovery and litigation hold features. There are no email backup and archive capabilities.

Sophos Email can integrate with third-party SIEMs and SOARs via APIs. Executive and administrative dashboards are present. Analysts can instigate forensic investigations directly from the console. Multiple report types are available, but customers cannot define their own.

Sophos is HIPAA, PCI-DSS, and AICPA SOC 2 Type 2 certified. It has not been ISO 27001 certified yet. Their solution has the standard features one would expect, but lacks backup/archive, legal discovery, report customization, and CDR. Language support is above average, and its analysis capabilities are language agnostic. It has excellent DLP functions with fine-grained controls. Phishing awareness and training options are available. Organizations that have separate email backup and legal discovery functions should consider Sophos Email when conducting RFPs for email security solutions.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 16: Sophos Email's rating

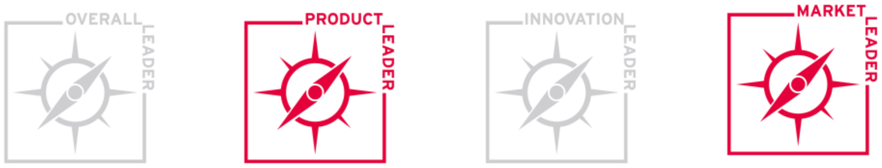
Strengths

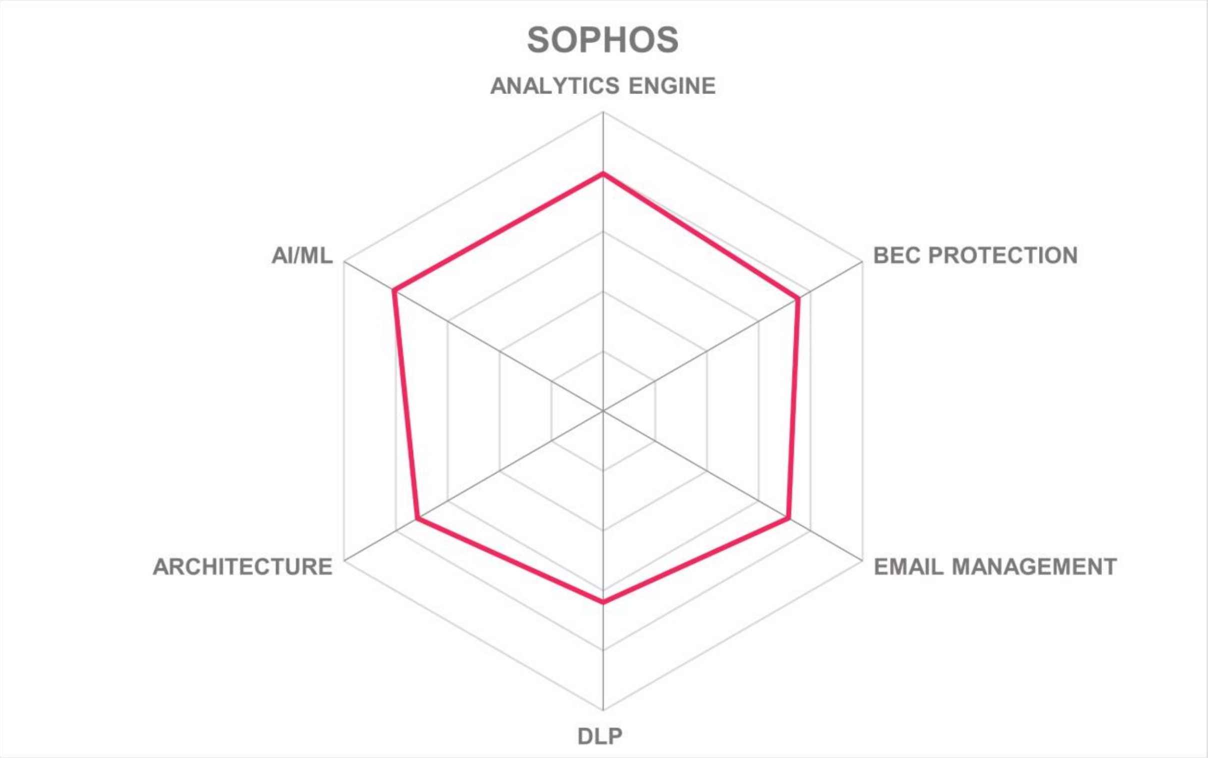
- Deep sender reputation analysis capabilities
- Bounce management
- In-house AI research team
- Strong AI capabilities
- Post-delivery removal of latent malicious content
- Sophos Phish Threat for security awareness training and testing
- Excellent language coverage
- Built-in, granular policy-based encryption options are present

Challenges

- Does not do CDR
- Does not notify external recipients of latent malicious content
- No integrations for supply chain risk management
- No connectors for LDAP directories
- Lacks e-discovery and litigation hold features
- No backup/archive functions
- Reports are not customizable

Leader in




SOPHOS
ANALYTICS ENGINE
BEC PROTECTION
EMAIL MANAGEMENT
DLP
ARCHITECTURE
AI/ML

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

Abnormal Security

Abnormal Security provides an Email Security solution based on a cloud-native, API-based architecture that integrates neatly with Microsoft 365, but also a range of other security solutions for gathering data for security analytics. Focus is on AI-based behavioral anomaly detection and protection across multiple channels, including Teams, Slack, and Zoom.

Why worth watching: Deep integration into Microsoft 365, multi-channel protection, and strong AI capabilities.

Coro

Coro provides Email Security as part of their modular cybersecurity platform, consisting of 14 different modules. This makes them interesting for mid-sized and mid-market companies looking for a comprehensive, integrated cybersecurity approach spanning multiple areas.

Why worth watching: One-stop shopping for a wide range of cybersecurity capabilities.

Data443-Cyren

Cyren by Data443 is a provider of anti-malware and Email Security solutions, including a product for supporting inbox security for Microsoft 365. The focus is on social engineering attacks on mailboxes, supporting deletion or hiding mails that are supposed to be security threats.

Why worth watching: Add-on solution for increasing the cybersecurity posture for Microsoft 365.

Darktrace

Darktrace is a provider of cloud-native security solutions covering a wide range of areas. The portfolio includes an Email Security solution that integrates natively with Google Workspace, Microsoft 365, and Microsoft Exchange. It analyzes emails for a range of threats and supports direct actions as well as gathering end user feedback to improve the analysis.

Why worth watching: Part of a broader cloud security platform, strong ML capabilities.

Echoworx

Echoworx is a specialized provider focusing on email encryption. They don’t provide full Email Security capabilities as asked for in this Leadership Compass but can be complimentary to most solutions that have been analyzed here. They support a wide range of delivery options for secured, encrypted email.

Why worth watching: Specialized provider for email encryption, can complement other Email Security solutions.

Egress Security

Egress Security is an established vendor of solutions for Email Security and secure collaboration. Their Intelligent Email Security Suite covers a range of capabilities in a cloud-native delivery model. Egress focuses on an adaptive, graph-based security model, dynamically adapting security policies.

Why worth watching: Modern Email Security platform with adaptive policies, complemented by a secure collaboration solution.

Forcepoint

Forcepoint sits on the outgoing channel of Email Security, offering Data Loss Protection (DLP) for Cloud Email. Based on that solution, outgoing mails can be analyzed for sensitive information. Additionally, several features for incoming email such as anti-malware, content filtering, and URL sandboxing are supported as well.

Why worth watching: Strong capabilities in DLP combined with Email Security features.

Fortinet

Powerful Email Security offering with multi-layer protection, combined with Fortinet’s SIEM and SOAR solutions into a broader cybersecurity solution. Includes advanced capabilities such as sandbox file analysis and others.

Why worth watching: Good Email Security solution with close integration to other security solutions by Fortinet.

Fortra / Agari

Agari is a provider of a comprehensive set of Email Security solutions including Cloud Email Protection and a Security Email Gateway, but also specialized DMARC protection and Security Awareness Training. They integrate with Microsoft 365, Google Workspace, and Microsoft Exchange Server.

Why worth watching: Feature-rich Email Security solution provided by Fortra, a leading provider of cybersecurity solutions.

FTAPI

Specialized provider of email and data encryption and secure transfers. No focus on the broader Email Security market that is focus of this Leadership Compass. Also providing secure data rooms and secure data transfers.

Why worth watching: Add-on to Email Security for encryption and secure information sharing.

GreatHorn

Provides a cloud-native Email Security solution for Microsoft 365. Supports multiple layers of protection, supporting content analysis, user education, account takeover protection, and various other capabilities.

Why worth watching: Focused solution with simple deployment, also targeting SMB customers.

Heimdal Security

Heimdal Security is a provider of an integrated set of cybersecurity solutions and services, including Email Security. They provide a SEC (Secure Email Gateway) that helps customers protecting against phishing, ransomware, and other types of attacks.

Why worth watching: Provider of an integrated portfolio of cybersecurity solutions targeting mid-sized to mid-market organizations, including Email Security.

Hornet Security

Integrated solution for Microsoft 365 security, including security hardening, backup, compliance services and others specifically for Microsoft 365. This includes Email Security services including spam and malware protection, advanced threat protection, and email protection, but also email archiving.

Why worth watching: Deep integration into Microsoft 365 and comprehensive set of security services beyond Email Security.

Inky

Inky provides what they call a behavioral Email Security platform, covering a range of different capabilities for Email Security. This includes both inbound and outbound email protection. It also covers security awareness training and email encryption.

Why worth watching: Integrated solution covering a wide range of Email Security features.

Libraesva

Provider of an Email Security solution that supports a wide range of detection capabilities for email-based threats. It can be complemented by a phishing simulator and comprehensive DMARC protection. Libraesva also supports email archiving.

Why worth watching: Email Security solution that can be integrated with email archiving.

Menlo Security

Menlo Security is a provider of a wide range of cybersecurity solutions. Their primary focus is browser security for preventing phishing and malware attacks. Part of the product portfolio is email isolation, allowing to deliver only safe content to endpoints.

Why worth watching: Interesting for organizations with very high security requirements, specifically when looking for a wider range of cybersecurity solutions.

OpenText / AppRiver

AppRiver by OpenText is an Email Security solution focused on protection Microsoft 365 environments, but also supporting additional capabilities such as email backup, email encryption, and secure file sharing.

Why worth watching: Part of the broad cybersecurity portfolio of OpenText, wide range of capabilities beyond pure Email Security.

Proton

Provider of secure email services with end-to-end encryption. Does not provide an additional layer of Email Security to other email solutions.

Why worth watching: Highly secure email service with end-to-end encryption.

Red Sift

Red Sift is a provider of advanced security analytics and capabilities such as ASM (Attack Surface Management). Part of their portfolio is OnDMARC for protection against phishing and BEC attacks. The solution also supports SPF, DKIM, and MTA-STS.

Why worth watching: Specialized add-on with focus on DMARC protection and related capabilities, complimentary to many Email Security solutions.

SlashNext

Cloud-native Email Security solution covering a range of threats, backed by AI/ML capabilities. API-based integration into Microsoft 365. Works with relationship graphs. Modern and extensible architecture with layered protection.

Why worth watching: Modern solution, cloud-based, targeting Microsoft 365 environments.

SpamTitan

Email Security solution with a wide range of capabilities, from AI-backed phishing protection, anti-malware, and whitelisting / blacklisting to DLP features, outbound scanning, sandboxing, and a range of other capabilities. Integrates neatly with Microsoft 365. Supports multi-tenancy for MSPs. Attractive pricing model.

Why worth watching: Feature-rich solution with interesting features for MSPs (Managed Service Providers).

Tessian

Provider of AI-based Email Security, delivered from the cloud. Focused on behavioral analysis, content analysis, and threat network analysis. Strong dashboards and investigation support.

Why worth watching: Modern Email Security solution focusing on AI-based analysis.

Trellix

Email Security solution with a multi-layered, adaptive approach on Email Security, including URL protection, attachment isolation, and detection of deferred phishing attacks. Supports investigation and automated filtering of malicious emails. Supports both SEG and ICES deployments. Integration with Trellix XDR.

Why worth watching: Modern Email Security solution that integrates with an own XDR solution.

Trend Micro

Email Security solution covering a range of capabilities, provided as a service. Offers layered protection, DLP capabilities, DMARC support, integration into the Trend Micro Threat Intelligence network, email encryption, and many other advanced features. Works with a wide variety of email services.

Why worth watching: Feature-rich Email Security solution with strong support for heterogeneous email environments and integration into the broader Trend Micro cybersecurity portfolio.

Trustifi

Trustifi is an email security specialist startup, founded in 2017. They are based in Las Vegas, Nevada, US. Trustifi provides inbound and outbound protection, encryption, and archiving solutions. It can function as a Secure Email Gateway or as an Integrated Cloud Email Security tool.

Why worth watching: Several innovative capabilities including AI/ML-powered email analytics.

Vade Security

Integrated Email Security solution for Microsoft 365, backed by AI. Protects against a variety of attack types including spear phishing, malware, and ransomware. Cloud-delivered, easy to deploy.

Why worth watching: Email Security solution with a good set of features and lean deployment.

Vipre

Proven Email Security solutions that can be deployed in integrated packages covering a wide range of cybersecurity features, including cloud and endpoint protection. Good reporting capabilities.

Why worth watching: Various packaged offerings for comprehensive cybersecurity.

Virtru

Virtru is a mid-stage, venture-backed security specialist firm. Virtru was established in 2012, and they are based in Washington, DC. Virtru offers secure collaboration, encryption, and data flow protection in addition to some email security functionality.

Why worth watching: Virtru focuses on data security and collaboration workflows, including within SaaS apps and some email systems, for highly regulated industries.

Zivver

Solution focused on secure email delivery, including sending encrypted email, supporting email recalls, proof of delivery, and a range of other features. Complimentary to many of the specialized Email Security solutions.

Why worth watching: Add-on solution focusing on securing sensitive emails and files, specifically for outgoing information.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report does not provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements, but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security

- Functionality
- Deployment
- Interoperability
- Usability

Security is primarily a measure of the degree of security within the product/service. This is a key requirement. We look for evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer, including authentication measures, access controls, and use of encryption. The rating includes our assessment of security vulnerabilities, the way the vendor deals with them, and some selected security features of the product/service.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment does not lead to a very low overall rating. This factor considers the vendor’s presence in major markets.

Financial strength even while KuppingerCole does not consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to function as a “good citizen” in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are:

Strong positive — Outstanding support for the subject area, e.g., product functionality, or outstanding position of the company for financial stability.

Positive — Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a small number of partners.

Neutral Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for are not met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which do not appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which do not provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

Leadership Compass: Unified Endpoint Management

Market Compass: Cloud-Delivered Security

Leadership Compass: Security Orchestration Automation and Response

Leadership Compass: Endpoint Protection Detection and Response

Leadership Compass: Managed Detection and Response

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.