KUPPINGERCOLE ANALYSTS

Email Security

Martin Kuppinger

September 18, 2025

LEADERSHIP COMPASS 2025

This report provides an overview of the Email Security market and a compass to help you find a solution that best meets your needs. It examines solutions that support analysis of incoming emails and their attachments for identifying malware in attachments, malicious links, Business Email Compromise (BEC), and other forms of attacks. It also looks at advanced capabilities such as email backup and archiving. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and manage these risks.

Contents

Executive Summary 5
Key Findings 6
Market Analysis 6
Delivery Models 8
Required Capabilities 11
Trends and Evolution 12
Leadership 14
Overall Leadership 14
Product Leadership 16
Innovation Leadership 18
Market Leadership 20
Product/Vendor evaluation 22
Spider graphs 22
Broadcom – Symantec Email Security.cloud 23
Check Point – Harmony Email & Collaboration 26
Cisco Systems – Email Threat Defense 28
Cloudflare – Email Security 31
Coro – Email Protection Suite 33
IRONSCALES – Email Security Platform 35
Mailinblack – Protect 38
Microsoft – Defender 40
Mimecast – Email Security 42
OpenText – Core Email Threat Protection 45
Proofpoint – Prime Threat Protection 47
Sophos – Sophos Email 50
Trellix – Security Platform 52

xorlab – Email Security 54
Vendors to Watch 56
Abnormal Security 56
Arkose Labs 56
Barracuda Networks 56
Darktrace 56
Echoworx 57
Egress Security 57
eleven cyber security 57
ESET 57
Forcepoint 58
Fortinet (includes Perception Point) 58
Fortra (includes Agari & Titus) 58
FTAPI 58
Google 58
GoSecure 59
GreatHorn 59
Group-IB 59
Heimdal Security 59
INKY 59
Libraesva 60
Mailprotector 60
Menlo Security 60
Pointsharp 60
Proton 60
Retarus 61
Securepoint 61
SonicWall 61
SSH Communications 61
Tessian 61
TitanHQ (SpamTitan) 62
Trend Micro 62
Trustifi 62

Virtru 62
Xcitium 62
ZeroBounce 63
Zivver 63

Executive Summary

Email security, an important component of every cybersecurity infrastructure, is constantly evolving to address ongoing and emerging threats. As the predominant channel for business communication, email remains a primary vector for cyberattacks targeting enterprises of all sizes. The market for email security software is driven by the increasing complexity and volume of threats, notably phishing, malware dissemination, and Business Email Compromise (BEC). These dangers necessitate advanced protective measures beyond those provided by built-in features of leading email systems like Microsoft's and Google's.

The demand for enhanced email security solutions is fueled by the limitations of legacy email security solutions, which struggle to manage the sophisticated and polymorphic nature of today's threats that are commonly powered by advances in AI. Generative AI, in particular, is being leveraged by cybercriminals to produce highly deceptive phishing schemes with enhanced automation, creating a scenario where traditional filters and heuristics might fail. Consequently, businesses are under pressure to adopt solutions incorporating robust AI-driven threat detection and behavior analysis to stay ahead of potential breaches.

The primary business need for these solutions centers on maintaining the integrity and confidentiality of communications, preventing data theft, and ensuring business continuity. As organizations shift towards increasingly remote and hybrid work environments, the attack surface expands, heightening the need for comprehensive email protection. Major use cases include the detection and mitigation of phishing attempts, identifying and blocking malware within attachments and URLs, and securing sensitive corporate data through encryption and DLP strategies.

Moreover, vendors are addressing the challenge of email-related threats by exploring multi-channel support that extends protection to other communication and collaboration platforms such as Slack, Teams, and Zoom. This trend reflects a holistic approach towards Email and Messaging Platform Security for securing an organization's entire digital communication landscape, not just traditional email.

Additionally, solutions are advancing to automatically disarm suspicious emails and intelligently manage the flow of email traffic, while maintaining minimal latency in analyzing and delivering email content. Integration with security orchestration systems like SOAR and XDR is becoming a commonplace requirement to enhance incident response capabilities and streamline security operations.

From an investment perspective, organizations should look toward vendors offering flexible deployment models that fit to their existing and future email (and communication) system/channel landscape, be it API-based pre- and post-delivery analysis or integrated solutions that complement existing platforms. Email security vendors are working on effectively balancing intrusion detection, minimizing false positives, and user transparency without impeding business processes. This balance is a key decision criterion.

As the market continues to grow, driven by the evolving nature of cyber threats, we anticipate further innovation and consolidation. New entrants are introducing pioneering

techniques, and established players are likely to engage in strategic acquisitions to enhance their portfolios. Regardless, the focus remains clear: providing comprehensive and adaptive email security that protects against an array of sophisticated threats while facilitating safe and efficient communication.

Key Findings

- Growing complexity in email threats pushes demand for advanced email security solutions utilizing AI and machine learning technologies.
- Business Email Compromise (BEC) remains a primary concern, necessitating sophisticated detection methods combining behavior analysis and AI.
- Market trends show a shift towards multi-channel security, extending email protection to platforms like Teams and Slack.
- Integration of Data Leakage Prevention (DLP) into email security solutions enhances protection of outgoing communications.
- Emergence of API-based and hybrid deployment models improves adaptability and scalability of email security solutions.
- Vendors are increasingly focusing on seamless integration with leading email systems like Microsoft 365 for pre-delivery analysis.
- Investment in AI-driven solutions continues rapidly as vendors aim to provide more nuanced threat detection and user security.
- 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.
- Consolidation of the market is anticipated, with new entrants innovating and traditional players acquiring newer technologies.

Market Analysis

Email security is an essential domain within cybersecurity, addressing the persistent issue of malicious attacks on this indispensable communication medium. This segment encompasses a range of solutions designed to ensure the security and integrity of email communications, protect sensitive information, and safeguard organizations from threats such as phishing, malware, and Business Email Compromise (BEC). As cyber threats continue to evolve, email security solutions must provide advanced protection features and adapt to new communication modes. They must protect against a wide range of different attack vectors. Thus, a key criterion in selecting such solutions is the breadth and currentness in tackling email-based cyberattacks.

Common Email Attack Vectors

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 Multi Factor Authentication (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.

Market Segment Structure

The market is composed of

- Secure Email Gateways (SEGs): Deployed at the network perimeter, SEGs intercept and scrutinize incoming and outgoing email traffic, identifying threats and ensuring only secure messages are delivered to users.
- Integrated Cloud Email Security: These solutions operate via APIs, allowing seamless integration with existing email platforms. They serve as a modern counterpart to SEGs, offering real-time threat detection without disrupting email flows.
- Built-in Email System Security: Leveraging security extensions in existing platforms like Microsoft 365 or Google Workspace, these solutions enhance native email security features, often incorporating MFA and DLP.
- Supplementary Email Security Services: Additional services such as encryption, sandboxing, and browser isolation complement core email security capabilities, providing comprehensive protection across various vectors of cyber threats.

The solutions in this significantly enhance the resilience of organizations against dynamic email threats, focusing on extended capabilities such as AI-driven threat detection and multi-channel security integration.

Delivery Models

The delivery models for email security solutions are critical for meeting diverse organizational requirements and enhancing email protection capabilities. Three primary models dominate the landscape: SEGs, API-based solutions, and integrated email security within existing platforms. Each model offers unique advantages, depending on deployment preferences and security needs.

SEGs are standalone solutions strategically placed at the perimeter of an organization’s network. These gateways provide a robust line of defense by filtering incoming and outgoing email messages to detect threats such as phishing, malware, and spam. SEGs rely on content filtering, URL rewriting, and anti-malware scanning techniques to protect users before email reaches their inboxes. Typically, companies with complex network infrastructures benefit from SEG installations for their comprehensive, hardware-based protection capabilities.

A **SEG** is deployed in front of an organization’s actual email servers by changing the MX (mail exchanger) DNS record. It serves 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 analyzing the email 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 behaviors 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 analyze 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 analyze code to detect zero-day threats. This can keep 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. As of February 2024, Google and Yahoo started requiring senders of 5,000 or more messages to authenticate using these methods and requiring 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 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, also named **Integrated Cloud Email Security** (ICES) systems, offer flexibility by interfacing directly with existing email platforms through secure APIs. This model is well-suited for cloud email systems like Microsoft 365 and Google Workspace, enabling them to execute advanced security functions such as threat detection, email quarantine, and automated remediation without interrupting service. Due to their integration ability and cloud-native flexibility, these solutions are also effective in handling BEC attacks and enhancing compliance with security policies via seamless updates.

ICES systems are API-based email security solutions that allow organizations to use their preferred email platforms, whether on-premises, cloud-hosted, or in many cases, those delivered as SaaS. However, they require API-based integrations to these email platforms and thus are commonly limited to one or few email platforms. This is a limitation for organizations using many email platforms, including legacy email systems.

The email platforms are interfaced 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 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 analyzed via API-based access before hitting the inbox of the users
- API-based post-delivery analysis, where incoming mails are analyzed 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.

Lastly, integrated security within email platforms extends the built-in features of email services such as Microsoft and Google's offerings. These solutions incorporate modern security practices, including MFA and real-time analysis, often suitable for organizations already using these major platforms for streamlined management and cost efficiency.

The third architectural option for email security is leveraging the built-in (or optional add-on) capabilities within. Many organizations use major email service platforms such as Google’s Gmail and Microsoft Outlook 365 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 MFA for users and have DLP functions that can help prevent exfiltration (either intended or unintended) of sensitive data and intellectual property.

Together, these delivery models cater to a wide range of operational needs, illustrating the importance of selecting the appropriate model based on an organization’s infrastructure, security requirements, and desired integration capabilities. The ability to adapt these models to evolving threats and interoperability with other security solutions remains a core focus for vendors in the email security domain.

Required Capabilities

Email security solutions must encompass a broad range of capabilities to address the intricate and evolving threats that target email infrastructures. The sophistication required in these solutions calls for comprehensive protection, detection, response, recovery, and governance measures as defined by the NIST Cybersecurity Framework.

Common Capabilities

- Spam Detection and Blocking: Identifies and blocks unsolicited emails using content scanning and domain reputation.
- Malware Detection: Encompasses the identification and isolation of malicious attachments and links.
- Phishing Protection: Detects attempts at credential theft and spoofing through sender and content analysis.
- BEC Protection: Detects impersonation and fraud attempts using domain intelligence and behavior analysis.
- CDR: Strips malicious content from attachments to provide sanitized copies.
- DLP: Applies corporate policy to outgoing emails to prevent sensitive data exfiltration.
- Email Encryption and Digital Signatures: Ensures message integrity and origin authenticity.
- Backup and Archiving: Supports business continuity and compliance through data retention.
- Email Quarantine and Sandboxing: Isolates suspicious emails for further analysis.
- Monitoring and Analytics: Offers detailed insights into email flows for proactive security management.
- AI/ML-based Threat Detection: Leverages advanced analytics to identify and respond to novel threats.
- Integrated Security Awareness Training: Enhances user education against phishing and other social engineering tactics.
- Traffic Routing and Filtering: Manages email traffic at the network's perimeter, preferring trusted sources.
- Authentication Checks and Protocols: Utilizes DMARC, DKIM, and SPF for sender validation.
- Robust Policy Enforcement: Automates and defines security policies to streamline management.
- Detailed Reporting and SIEM Integration: Enhances threat intelligence and actionable insights.
- Real-time Monitoring and Automation: Delivers seamless threat updates and automated responses.
- Flexible and Scalable Integration: Ensures easy mode of operation across various cloud environments and platforms.
- Pre- and Post-Delivery Analysis: Executes in-depth security checks without disrupting operational efficiency.
- Native Integration with Email Services: Leverages built-in security functions of major platforms.

These capabilities must align effectively across various models, ensuring comprehensive protection and adaptability to the evolving security landscape. The ability to integrate with existing systems and adapt to multi-channel environments remains a core consideration as email-based threats continue to escalate.

For information about the Leadership Compass process, see our KuppingerCole Leadership Compass Methodology.

Trends and Evolution

The email security market is undergoing significant transformation driven by evolving threat landscapes and advancements in technology. As email persists as a primary communication tool within enterprises, its security continues to be a critical focal point for organizations looking to safeguard sensitive information and maintain operational integrity.

Among the notable trends is the increasing reliance on AI and ML within email security solutions. Vendors are integrating AI to enhance threat detection, enabling more precise identification of phishing and BEC attacks. This trend reflects the necessity for solutions capable of analyzing vast volumes of data to distinguish between benign and harmful communications efficiently.

Simultaneously, the challenge of balancing detection accuracy and false positives persists. While AI enhances detection capabilities, avoiding excessive reliance on automated decision-making is crucial to ensure genuine threats are addressed without disrupting business operations. Vendors are implementing strategies to integrate AI judiciously, combining it with human oversight and layered security measures for more effective defenses.

There is also a marked shift towards multi-channel security solutions. As businesses diversify their communication tools to include platforms such as Microsoft Teams, Slack, and Zoom, email security vendors are expanding their protection scope to encompass these applications. By utilizing existing detection engines across various communication channels, organizations are better positioned to mitigate risks associated with real-time collaboration tools.

DLP integration within email security is gaining traction as businesses seek to prevent unauthorized leakage of sensitive data. Solutions are actively evolving to incorporate DLP features, allowing organizations to enforce corporate policies on data handling and distribution, thereby reducing opportunities for data exfiltration via emails.

The deployment landscape is characterized by increased flexibility and integration. Vendors are enhancing solutions to support not just SEGs, but also API-based protection and native security capabilities within email platforms, notably Microsoft 365 and Google Workspace. This approach appeals to organizations seeking diverse deployment models tailored to their infrastructure and risk posture.

Market dynamics reveal a steadily growing demand for email security solutions, driven by the escalation in email-based attacks. This demand attracts new entrants, fostering innovation and contributing to market competition. With cyber threats evolving at a rapid pace, organizations are recognizing the value of advanced and adaptable security measures to maintain their cybersecurity posture.

As we look ahead, strong investments in bespoke AI solutions are expected to continue, further refining threat intelligence and response mechanisms. Organizations should anticipate a continued expansion of capabilities, reinforcing email security's integral role in modern cybersecurity strategies. These trends collectively signify an era where email security solutions are no longer standalone products but part of a comprehensive cybersecurity framework that spans multiple communication and collaboration tools.

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 identify vendors that shall 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 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 in the Email Security market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

The Email Security market proofs being a mature market with a significant number of vendors. All vendors in the rating deliver proven solutions that help customers in addressing the challenges they are facing with email-based cyberattacks. The solutions differ in breadth and depth of capabilities and integrations but are all solid offerings.

Among the Overall Leaders, we see Proofpoint in front. Former head-to-head competitor Perception Point has become acquired by Fortinet and declined participation in this edition of the Leadership Compass on Email Security. Following Proofpoint, we find Cisco Systems, Microsoft, Check Point, and Trellix, all having a strong presence in the market and mature, feature-rich products. Microsoft also benefits from its dominance in the market. Further vendors in the Overall Leader section include (in alphabetical order) IRONSCALES, Mimecast, Sophos, and Broadcom, also with proven solutions and a significant market share.

Among the Challengers, we find Cloudflare close to the Leaders segment. Following them is OpenText. Further vendors include Coro and the two European Email Security providers Mailinblack from France and xorlab from Switzerland. All these vendors deliver very solid Email Security solutions with a good feature set and established customers.

There are no Followers in this overall leadership rating.

Overall Leaders are (in alphabetical order):

- Broadcom
- Check Point
- Cisco Systems
- IRONSCALES
- Mimecast
- Microsoft
- Proofpoint
- Sophos
- Trellix

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

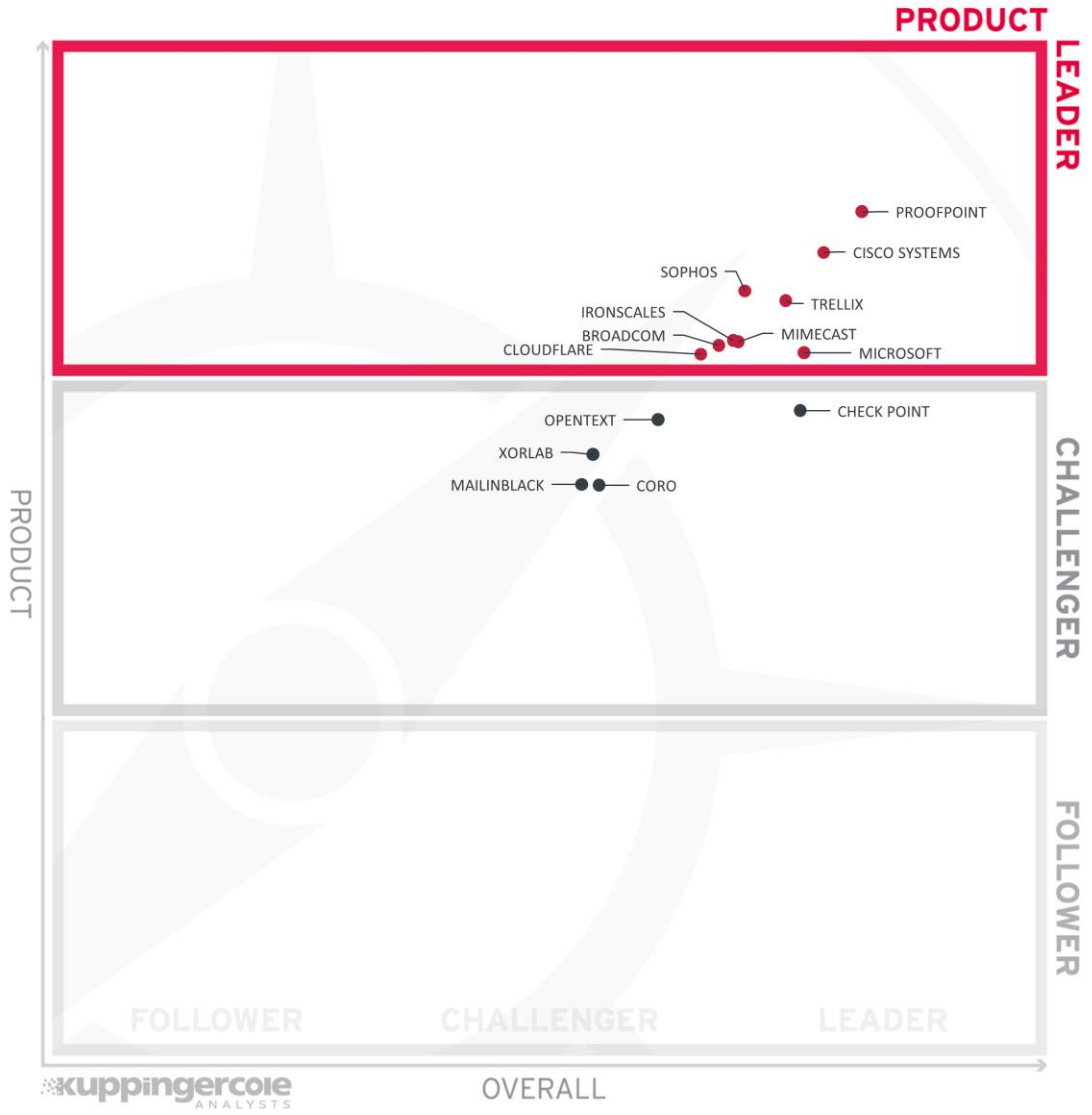


Figure 2: Product Leadership in the Email Security market

The Product Leadership rating again verifies that the Email Security market is a mature cybersecurity market segment, even while leaving room for further improvement of the solutions. We see many vendors in the Leader segment, but also all vendors in the

Challenger segment are positioned in the upper area of that segment, indicating their good set of capabilities and potential for further development as well as their full competitiveness.

We again see Proofpoint in the leading position, followed by Cisco Systems. Sophos and Trellix are following closely. Also in the Leader segment, we find (in alphabetical order) Broadcom, Cloudflare, IRONSCALES, Mimecast, and Microsoft. Their approaches vary significantly, from strong human involvement to mostly AI-based, automated solutions. Thus, as indicated above, we strongly recommend going into a more detailed analysis based also on the vendor-specific information provided in this Leadership Compass.

As mentioned, all vendors in the Challenger segment also are placed well, all in the upper part of this segment. On top, we see a group of (in alphabetical order) Check Point, and OpenText, followed by the smaller players (again alphabetically) Coro, Mailinblack, and Xorlab. Mailinblack and Xorlab, being headquartered in Europe, are of specific interest for organizations looking for cybersecurity sovereignty.

Product Leaders (in alphabetical order):

- Broadcom
- Cisco Systems
- Cloudflare
- IRONSCALES
- Microsoft
- Mimecast
- Proofpoint
- Sophos
- Trellix

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.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

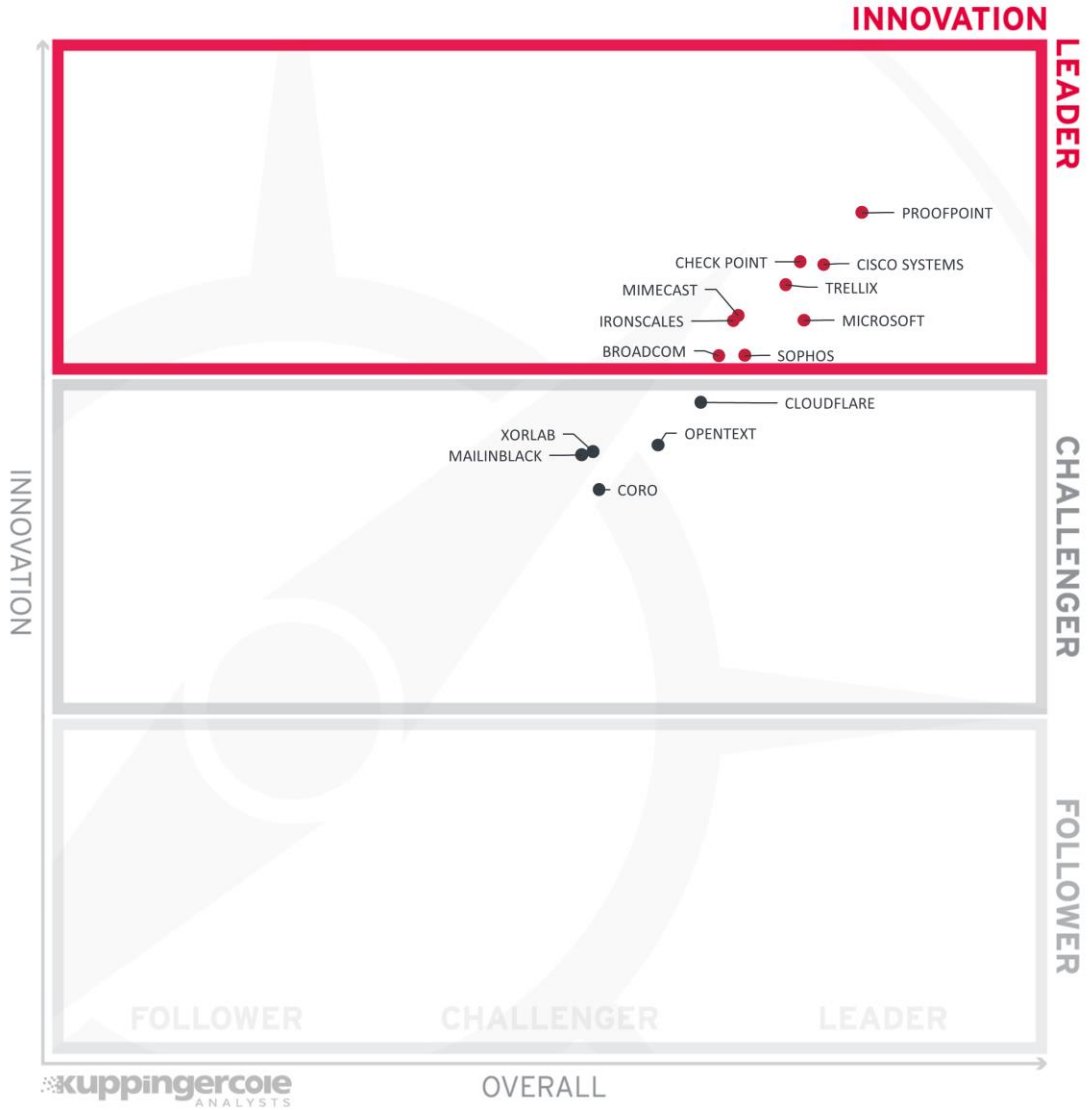


Figure 3: Innovation Leadership in the Email Security market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

All vendors in the market deliver a significant level of innovation. This is indicated by the fact that all are situated rather close to each other, either already in the Leaders segment or in the upper area of the Challenger section. A lot of innovation is coming from using AI to support the identification of malicious emails. We also have seen many vendors adding additional detections based on specialized modules or engines that focus on newer types of attack vectors.

In the Leader segment, we see again Proofpoint on top, followed by Check Point, Cisco Systems, and Trellix. Another group including (in alphabetical order) Broadcom, IRONSCALES, Mimecast, Microsoft, and Sophos are close to them.

In the Challenger segment, we find the other vendors, all positioned well and demonstrating significant investments in innovation. Cloudflare, OpenText, Mailinblack, Xorlab, and Coro are all placed close to each other.

Innovation Leaders (in alphabetical order):

- Broadcom
- Check Point
- Cisco Systems
- IRONSCALES
- Mimecast
- Microsoft
- Proofpoint
- Sophos
- Trellix

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the ratio between customers and managed mailboxes, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

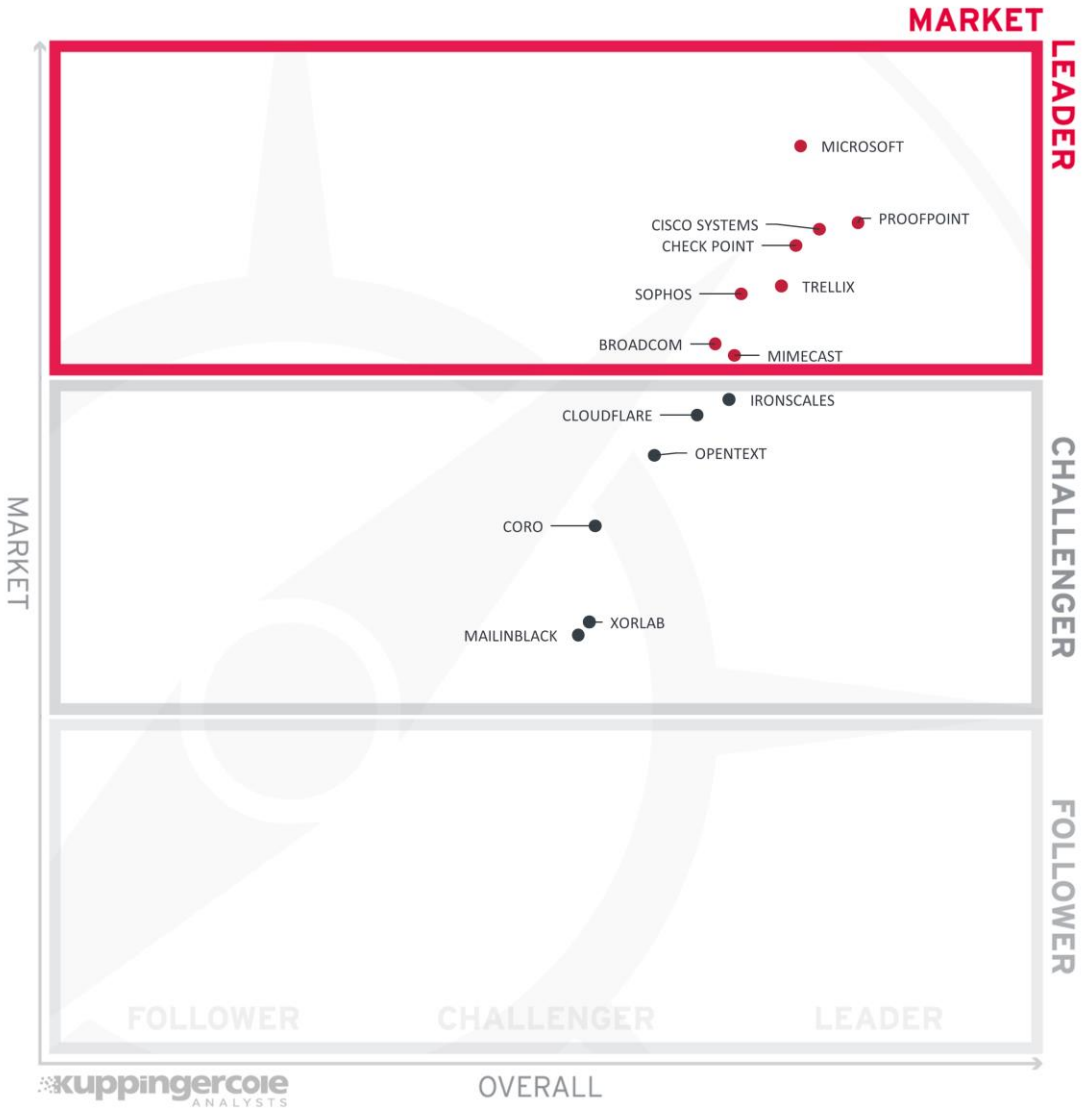


Figure 4: Market Leaders in the Email Security Market

In this area, we see the largest spread of vendor ratings, but again all vendors are placed either in the Leader segment or the Challenger segment. Microsoft is leading in this rating, having a huge number of customers for both the standard, integrated capabilities of Email Security and advanced solutions. Proofpoint takes a strong position specifically for the Email Security market, while both Cisco Systems and Check Point also benefit from their overall market position in the cybersecurity market. Trellix and Sophos, also with large numbers of customers and a global presence, are following closely. Broadcom as well as Mimecast are also placed in the Leader segment.

Amongst the challengers, we find IRONSCALES and Cloudflare at the top, close to entering the Leaders segment. OpenText also takes a strong position. The smaller vendors such as Coro, Xorlab, and Mailinblack are positioned a bit further down, but all showing a strong growth potential due to their good position in both product and innovation rating.

Market Leaders (in alphabetical order):

- Broadcom
- Check Point
- Cisco Systems
- Mimecast
- Microsoft
- Proofpoint
- Sophos
- Trellix

Product/Vendor evaluation

This section contains a quick rating for every product/service we've 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 this market segment, we look at the following categories:

Email Analysis & Security: In this category, we rate the specific capabilities for analysing emails and implementing email security measures. This category focuses specifically on how emails are analyzed and capabilities such as protection against malicious URLs and other essential features.

Attachment & Content Security: 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.

Antivirus & Antimalware: A specific focus also is on the integrated support for antivirus and antimalware capabilities that help in identifying various types of malware, including advanced attacks such as polymorphic ransomware.

Business Email Compromise Prevention: 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.

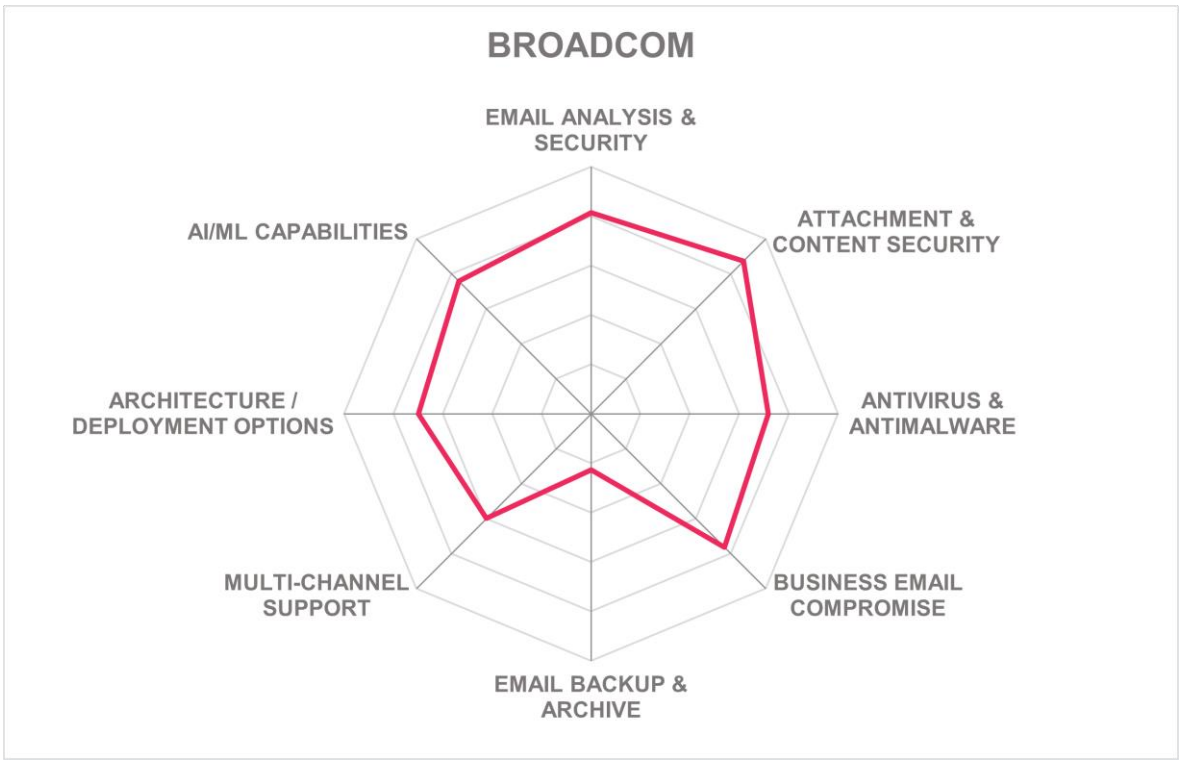
Email Backup & Archive: While Email Security is mostly focused on protecting against attacks via incoming emails, the ability to back up emails, restore, archiving, and manage bouncing is also essential to many customers. This category rates these features.

Multi-Channel Support: Here, we rate the ability to protect other types of interaction and content, beyond emails, such as Microsoft Teams or Slack.

Architecture / Deployment Options: 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 Capabilities: 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.

Broadcom – Symantec Email Security.cloud



Leader in

Broadcom, established in 1991 and headquartered in San Jose, California, is a key player in the Email Security arena. Its products, Symantec Email Security.cloud and Symantec Messaging Gateway, form the core of its offerings under the IMS Division's Cybersecurity & IT Management section. The company's solutions cater to diverse organizational needs, offering deployment in on-premises, cloud, and appliance forms. Broadcom's experience in cybersecurity makes its email security solutions well-suited for environments requiring robust data protection and threat mitigation strategies.

The Email Security solutions by Broadcom leverage advanced AI and ML technologies to handle risky user behaviors and securely authenticate emails, preventing spoofing and impersonation as well as BEC attacks effectively. Their robust security framework includes comprehensive antivirus and antimalware scanning, coupled with in-depth AI-driven email content analysis. Supporting key standards like SPF, DKIM, and DMARC, Broadcom's solutions meet various industry certifications, providing clients with trusted email security capabilities across their communications.

Broadcom stands out by incorporating a strong human intelligence element alongside ML, delivering advanced email analytics and customizable policy frameworks. Its distinctive features include click-time URL protection that analyzes links dynamically, making it effective against cutting-edge threats. Nevertheless, challenges such as non-integrated administrative consoles and the absence of auto-tuning abilities present areas for improvement. Broadcom's focus on premium service offerings is particularly advantageous for larger enterprises but may deter smaller organizations due to the associated complexity and cost.

Broadcom’s Email Security solutions offer an array of deployment models, reflecting the flexibility required in modern enterprise environments. With its Symantec Email Security.cloud and Symantec Messaging Gateway, organizations can choose between cloud-based, on-premises, or hybrid deployments, allowing them to align their security infrastructure with their operational and compliance needs. This flexibility is further enhanced by Broadcom’s support for deployment across SaaS and on-premises environments.

The integration capabilities of Broadcom’s solutions extend into critical cybersecurity ecosystems, such as SIEM, SOAR, and XDR platforms, and ensure seamless interoperability with various email systems including Microsoft 365 and Google Workspace. Moreover, Built-in security controls are complemented by detailed logging and monitoring capabilities, offering comprehensive oversight of email threats. Broadcom’s suite delivers not only adaptive threat detection and response but also a structured approach to policy management and regulatory compliance.

Broadcom's Email Security solutions are aimed primarily at large enterprises and heavily regulated sectors across North America and Europe, offering specialized use cases for industries that demand rigorous data compliance, such as finance and government. These offerings are particularly beneficial for organizations needing comprehensive, multi-layered email security strategies to protect sensitive information and counter sophisticated threats.

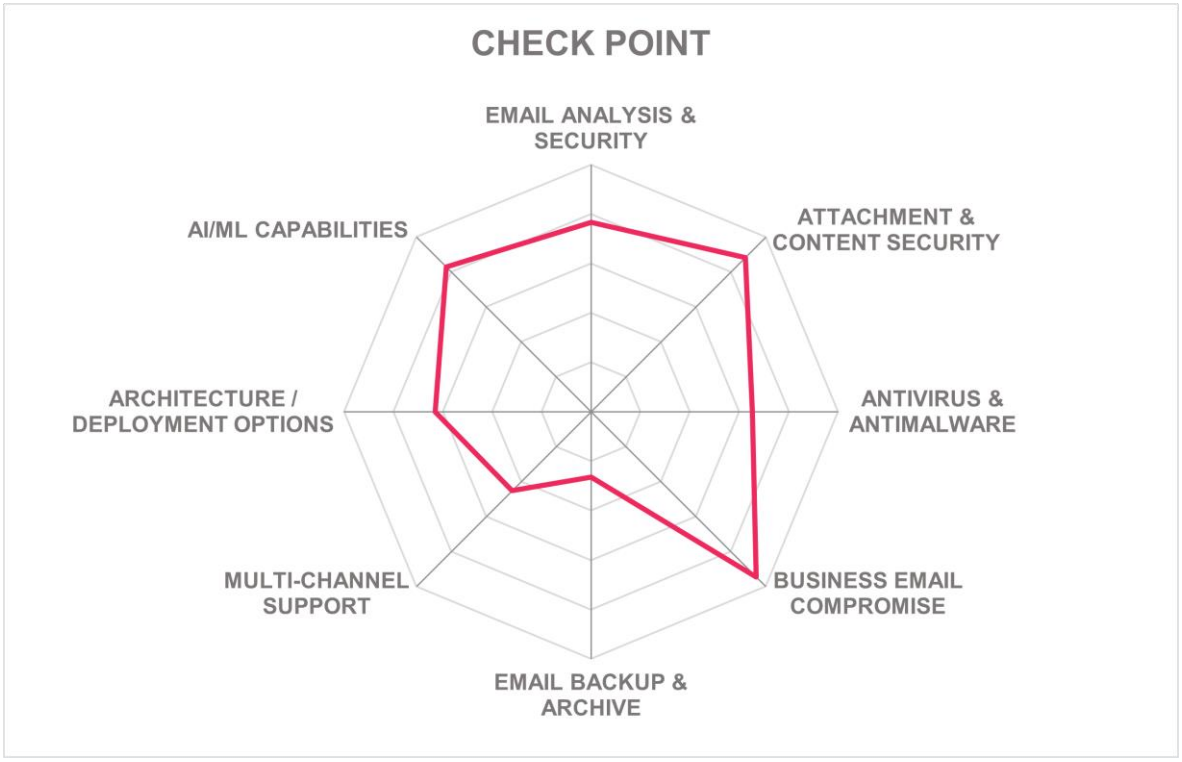
Strengths

- Proven solution with a long track record.
- Integrates controls across email, web, and collaboration channels.
- Strong antivirus/antimalware features.
- Supports multi-layered approaches with gateway, Microsoft 365, and Google Workspace.
- Broad use of AI/ML for enhanced threat detection.
- Integrates with DLP, CASB, and SIEM solutions.
- Multi-channel support for other communication channels via integration to Symantec CASB.
- Supports targeted administrative consoles for both internal administrators and MSPs.
- Feature-rich solution targeting regulated industries.
- Regular customer environment optimization assistance.

Challenges

- Human oversight of AI by internal threat analysts comes at a cost.
- No built-in email backup/archive functions, but partnerships with third-party vendors.
- Does not have e-discovery and litigation hold features.

Check Point – Harmony Email & Collaboration



Leader in

Check Point, founded in 1993 and headquartered in Israel, has established itself as a leader in cybersecurity, extending its initial firewall offerings to a full spectrum of security solutions. Their email security product, Harmony Email & Collaboration, builds on the acquisition of Avanan, targeting API-driven email security for platforms like Microsoft 365 and Google Workspace, as well as collaborating tools such as Slack and Microsoft Teams. The solution builds on cloud-native deployment models to adapt to rapid enterprise needs in the current API segment of the market.

Key capabilities of Harmony Email & Collaboration include its proficiency in handling risky users and comprehensive email authentication, aligning with standards like SPF, DKIM, and DMARC. The platform employs Check Point's proprietary ThreatCloud for antivirus/antimalware detection, offering a spyware and zero-day attack defense with reputed 99.8% malware catch rates. Enhanced BEC protection leverages AI to analyze emails based on a plethora of risk factors and indicators. The system's multifaceted email content analysis, including AI/ML to detect phishing, showcases its capability across various

threat vectors. It is supported by significant industry certifications, including ISO/IEC 27001 and SOC 2 Type 2, which underscore its commitment to best practices in security integrations.

Notably, the product differentiates itself through several unique innovations, including consistent use of advanced AI technologies, a patented inline and API-based scanning approach that enhances email threat protection before reaching user inboxes, and the integration of threat intelligence beyond email, into realms such as dark web scanning. Nevertheless, areas such as further integration with non-cloud-native environments and simplifying user configurations can be seen as potential improvement points to enhance user adaptability and interface efficiency, particularly as demand evolves.

Deploying predominantly as a SaaS, it complements environments relying on cloud services by integrating seamlessly with Microsoft 365 and Google Workspace without traditional on-premises setups. The product's interoperability is evidenced by its integrations with technologies such as SIEM and XDR, broadening the security landscape by enabling enhanced threat intelligence sharing and comprehensive security monitoring. Built-in security features include integration to Check Point's ThreatCloud platform, delivering real-time threat intelligence and response capabilities backed by big data insights.

Check Point caters to a wide range of enterprise clients globally, with significant traction in North America, EMEA, and APAC regions, enabled by its partner-driven distribution strategy. The product is particularly suited for organizations adopting cloud-first strategies within their IT infrastructure, making it a compelling choice for those using platforms like Microsoft 365 and Google Workspace and require a scalable solution that addresses not just emails but broader collaboration security requirements. The focus on API-based solutions and advanced AI integration makes it highly applicable to entities aiming to enhance their security postures with a modern, dynamic, and integrated approach.

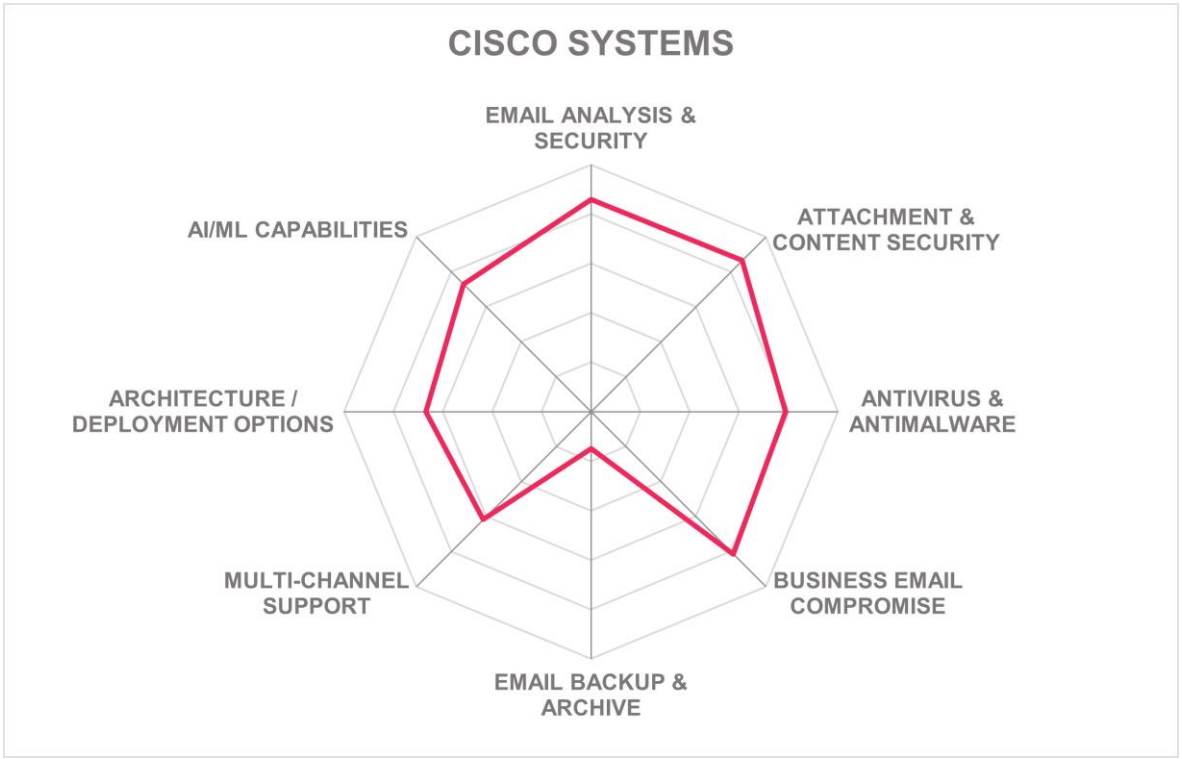
Strengths

- Seamless integration with Microsoft 365 and Google Workspace.
- Combines inline and API-based security without a secure email gateway.
- Advanced AI-backed threat detection and alert systems.
- Unified email security and threat intelligence enhancing existing security measures.
- Modern UI and dashboard.
- High malware and phishing block rates.
- Patented tight security for pre-inbox protection.
- Strong certifications, including ISO/IEC 27001 and SOC 2 Type 2.
- Supports significant third-party integrations for holistic protection.

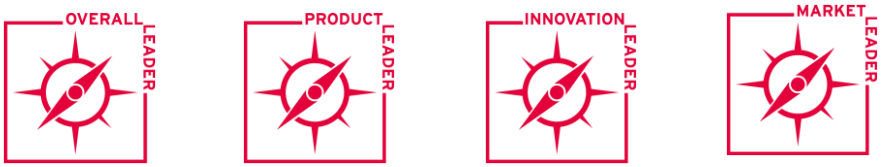
Challenges

- Requires technical expertise for detailed analysis of malicious emails.
- Limited support for heterogeneous, legacy email environments.
- Integrated archiving not supporting S/MIME encrypted email keys.
- Some options for further automation and self-configuration remain.

Cisco Systems – Email Threat Defense



Leader in



Cisco Systems, established in 1984 and headquartered in San Jose, California, has been a prominent force in networking and telecommunications. With a strategic extension into the security domain, Cisco has significantly invested over $50 million in email security solutions over the past five years. This includes the development of their Secure Email Gateway and the now core product, Email Threat Defense. These offerings can be deployed on-premises or through Cisco-hosted cloud instances, addressing the needs of both traditional and modern cloud-based infrastructures such as Microsoft 365.

Key strengths of Cisco's email security include advanced AI-powered detection, leveraging over 200 new detectors for threats like phishing and BEC. The company employs a threat-centric approach facilitated through sophisticated machine learning and deep learning models, enhancing the efficacy of email authentication and content analysis. Cisco's solutions support recognized standards like SPF, DKIM, and DMARC for email authentication, ensuring resilience against spoofing and unauthorized email access attempts. The integration with Talos provides robust antivirus and antimalware defenses, incorporating sandboxing and heuristic techniques. These cohesive capabilities position Cisco strongly in the market.

Cisco excels through its innovative use of generative AI, focusing on threat interpretation and reasoning, thereby augmenting human analyst capabilities. The ambitious roadmap underscores plans for further platform enhancements and AI-integration, demonstrating commitment to leading industry innovation. However, challenges remain, such as the need for UI integration across products and full interoperability with Google Workspace. Their roadmap, while promising, outlines a journey towards more cohesive interfaces and expanded global reach.

Cisco's email security solutions are characterized by their versatile deployment models, which include the Secure Email Gateway (SEG) and the SaaS-based Secure Email Threat Defense (ETD), supporting operations in on-premises, virtual, or cloud environments. This flexibility allows businesses to tailor their email security to specific infrastructure needs, delivering a seamless integration experience with major email systems.

Cisco’s offerings are enhanced by connectivity to a wide range of cybersecurity solutions, including SIEM, SOAR, and its own Cisco XDR, leveraging threat intelligence from Cisco Talos. Built-in security capabilities bolster this integration further, including robust API authentication and internal API usage monitoring.

Cisco’s email security solutions target large enterprises and governmental sectors, with coverage expanding into regions like Canada, Singapore, and the Middle East. These products are particularly advantageous for organizations already invested in Microsoft environments, seeking robust email threat defenses and layered security measures. The comprehensive integration across Cisco’s security suite supports strategic initiatives for enterprises aiming to bolster their overall security posture.

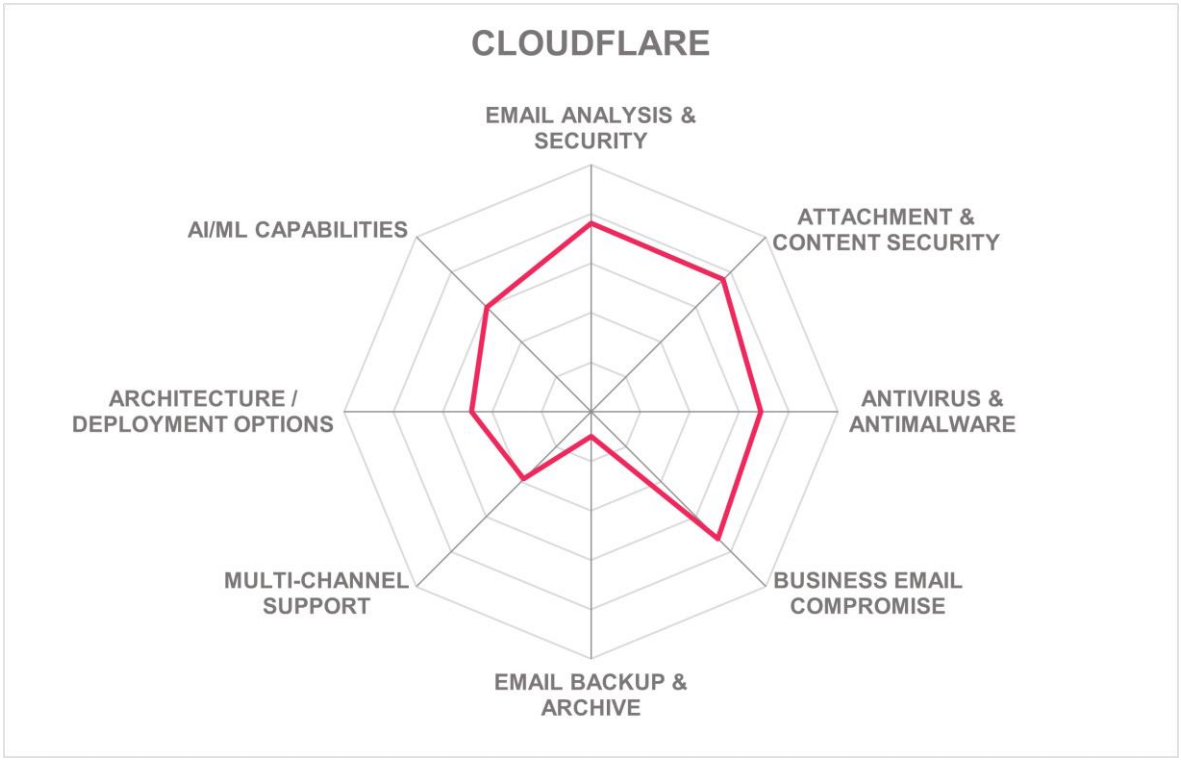
Strengths

- Advanced AI models for robust threat detection.
- Seamless integration with Microsoft ecosystems.
- Extensive deployment flexibility on-premises and cloud.
- Comprehensive email authentication standards support.
- Strong connection with Cisco Talos for threat intelligence.
- Integration with Cisco XDR and Cisco Talos.
- Extensive global expansion supporting diverse enterprises.

Challenges

- UI unification across products remains incomplete.
- Limited interoperability with Google Workspace.
- Need for improved integration of separate cloud services.
- Organic email archiving solutions could enhance the offering.

Cloudflare – Email Security



Leader in

Cloudflare, founded in 2010 and based in San Francisco, delivers a wide array of cloud security solutions including CDN, WAAP, and Secure Access Service Edge (SASE), with Email Security crafted into its platform post its acquisition of Area 1 Security. As part of Cloudflare One, their solution is designed for robust email protection suitable for both cloud and hybrid environments, supporting major platforms like Microsoft 365 and Google Workspace. The offering supports a variety of integration approaches, including MX record-based inline integration, API-based integration, and journaling, facilitating integration across diverse architectures and aiding businesses in enhancing their cybersecurity framework.

Key capabilities of Cloudflare's Email Security focus on comprehensive threat detection using advanced AI and ML, which includes Natural Language Understanding (NLU), sentiment analysis, and social graph analytics. These features allow for effective mitigation of threats like BEC and phishing attacks. The platform supports email authentication standards such as SPF, DKIM, and DMARC alongside antivirus/antimalware detection

protocols. Its integration with various SIEM systems enhances incident response by correlating email security events with broader organizational cybersecurity measures.

The standout differentiator for Cloudflare's solution is its integration within Cloudflare One, providing cohesion and strength to security orchestration across the organization's infrastructure. Innovations like AI-driven threat detection and interoperability enhance its effectiveness significantly. However, areas such as email backup and archiving remain unaddressed, alongside minimal built-in support for other channels like Microsoft Teams. The overall value tends to expand considerably when integrated with Cloudflare's broader services.

The service can be deployed as part of an ICES approach within the Cloudflare One platform, supporting flexible configurations to meet diverse enterprise requirements. It offers a cloud-native SaaS model, optimized for rapid deployment without the need for complex on-premises infrastructure.

This flexibility supports interoperability across multiple cybersecurity frameworks; integration capabilities extend to SIEM and SOAR solutions, complementing broader incident response mechanisms. Furthermore, the service connects seamlessly with Cloudflare’s infrastructure, enhancing its suite-based approach alongside standalone functionalities. Supported email environments include Microsoft 365 and Google Workspace, while coverage expands to various legacy systems, facilitating migration pathways for different organizational setups.

Cloudflare primarily targets enterprises using Microsoft 365 and Google Workspace, looking to extend beyond their basic security measures. With a global reach in over 125 countries, Cloudflare caters to customers within industries such as finance and tech, which require a heightened security posture. It is particularly advantageous for organizations already involved with Cloudflare services, allowing for a more comprehensive threat management approach.

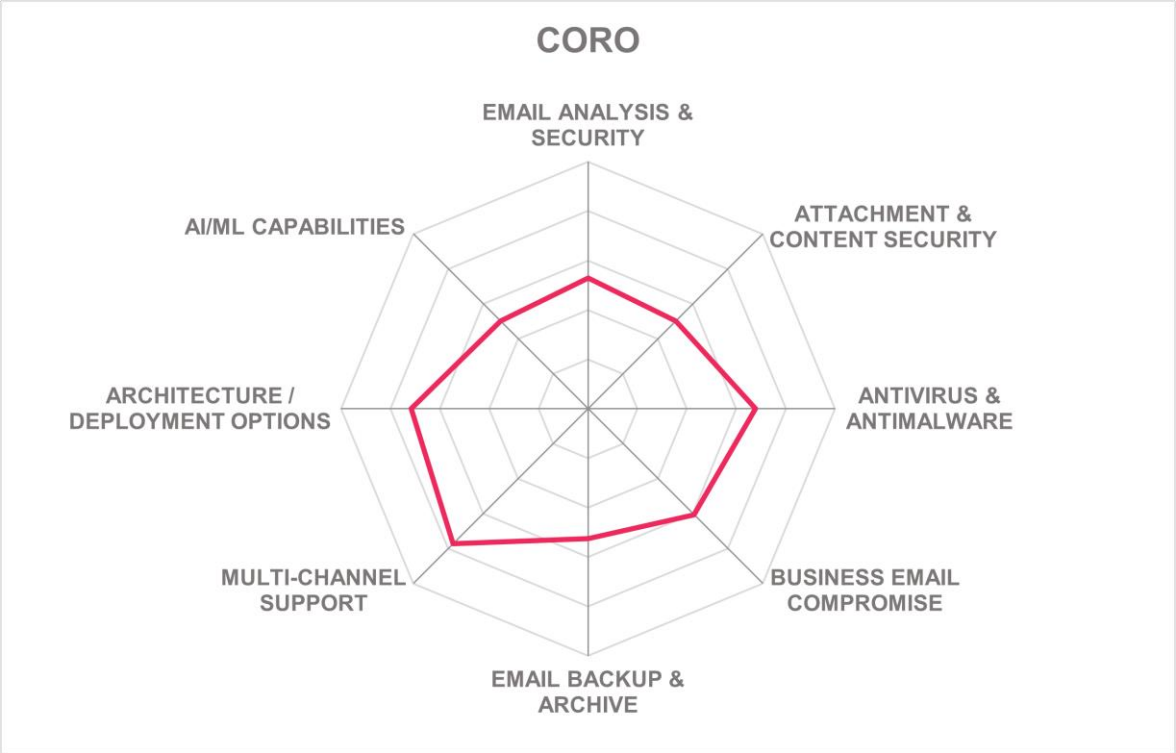
Strengths

- Cloud-based service ensures easy deployment.
- Supports both inline and API-based deployments.
- Solid AI-driven threat detection.
- Seamless integration with Cloudflare’s ecosystem, simplifying delivery especially for existing Cloudflare customers.
- Global reach with vast network capacity.
- Strong standards support for email authentication.
- All Cloudflare services such as DLP and isolated browsing that are needed for Email Security are included in the offering.

Challenges

- Lacks intrinsic email backup and archiving solutions.
- Limited native support for platforms like Microsoft Teams.

Coro – Email Protection Suite



Coro, established in 2014 and headquartered in Chicago, is a cybersecurity vendor specializing in providing affordable and effective solutions primarily for small to mid-sized businesses. Their Email Protection Suite integrates seamlessly with broader offerings in cloud security and endpoint data governance, encapsulated under their modular cybersecurity platform. Leveraging API-based cloud technology, the suite prides itself on ease of deployment without any hardware requirements. Catering to businesses needing streamlined solutions, Coro's emphasis is on simplicity and reliability, evident in the unified interface that employs a single endpoint agent across various modules.

Coro's Email Protection Suite showcases a range of essential capabilities, including the automatic detection and handling of threats like spam, phishing, and ransomware. Notably, the platform integrates advanced threat intelligence driven by Large Language Models (LLMs) to elevate its threat detection accuracy. The suite supports both gateway and native API approaches, augmenting its versatility across multiple email platforms, such as Microsoft 365 and Google Workspace. Standards like SPF, DKIM, and DMARC underpin its authentication processes, while it ensures compliance through alignment with regulations

like GDPR, HIPAA, and PCI DSS. The platform's adaptive security awareness training further enables user empowerment in threat recognition and mitigation.

Coro's differentiated strength lies in its user-centric design that aims to minimize complexity while maximizing security. Its intuitive interface caters specifically to IT teams without dedicated cybersecurity specialists, ensuring minimal configuration errors. Coro's commitment to a simplified user experience is particularly beneficial for its target client base, reducing overhead and misconfigurations. However, improvements could be directed towards expanded integration with third-party DLP tools and more robust archival functionalities to enhance comprehensive data governance capabilities. Such enhancements could fortify their offering in more complex, regulated environments.

Coro's Email Protection Suite offers flexible deployment models, encompassing both gateway and API-based options, allowing it to pair flexibly with a broad range of email systems beyond Microsoft 365 and Google Workspace. The solution is SaaS. This cloud-centric approach pairs with Coro's unified platform, maintaining simplicity while supporting extensive API-based integration capabilities with external cybersecurity solutions including SIEM systems, enhancing operational efficiency and threat management.

The platform's design is particularly suited for small and mid-sized enterprises, who can benefit from its cost-effective, email security solution managed through an easily navigable dashboard. The worldwide availability of Coro's services makes it an attractive option for companies seeking regionally-supported email security solutions. The adaptive nature of the integrated security awareness training offers significant appeal to organizations looking for practical, real-time educative tools. Organizations prioritizing straightforward implementation and operation, along with the flexibility to handle various security postures across e-devices and cloud applications, should consider evaluating Coro's Email Protection Suite.

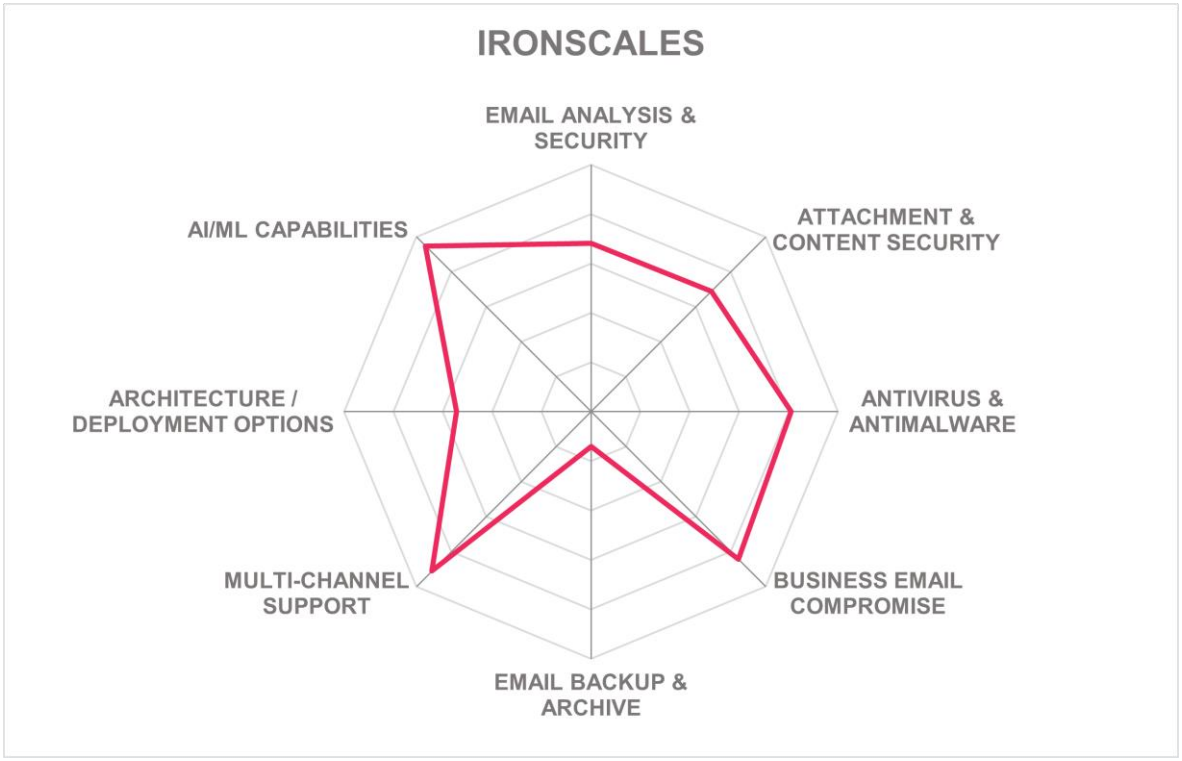
Strengths

- Simplified, user-centric interface.
- Seamless integration with Microsoft 365 and Google Workspace.
- Compliance with GDPR, HIPAA, and PCI-DSS standards.
- High accuracy threat detection using LLMs.
- Minimal configuration required for deployment.
- Adaptive security awareness training.
- Fast deployment without hardware requirements.
- Unified platform with single endpoint usage for various modules.

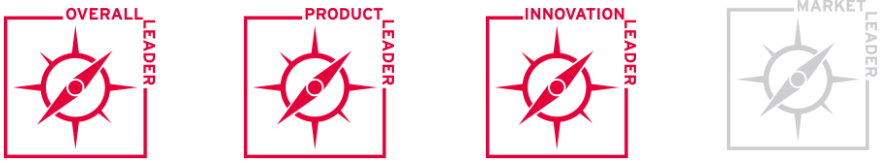
Challenges

- Email archival capabilities need enhancement.
- Dependence on manual processes for some functions.
- Lack of auto-tuning capabilities for system configurations.
- Limited post-delivery threat mitigation options.

IRONSCALES – Email Security Platform



Leader in



IRONSCALES, established in 2014 and based in Atlanta, Georgia, is recognized for its advanced AI-powered email security solutions. The company focuses on providing a security platform that integrates with existing email systems like Microsoft 365 and Google Workspace. Primarily deployed via public cloud infrastructures such as Amazon AWS and Microsoft Azure, IRONSCALES targets mid-sized enterprises and the Managed Service Provider (MSP) and Managed Security Service Provider (MSSP) markets. With thousands of customers worldwide, IRONSCALES has developed a robust platform that addresses increasing threats in email security, focusing on both threat detection and human risk management.

The IRONSCALES platform is notable for its capabilities in real-time email analysis, detecting threats such as phishing, BEC, and deepfake content. It employs a complex matrix of AI and ML algorithms for enhanced threat detection, featuring autonomous email

remediation and integration with services like CrowdStrike. The platform supports essential standards like SPF, DKIM, and DMARC for sender authentication and integrates with corporate environments via APIs, providing risk management tools tailored towards high-risk users and integrating security training for improved user awareness.

IRONSCALES offers some unique functionality such as VAP (Very Attacked Persons) identification and multi-language support for phishing simulations. The adaptive AI models for identifying emerging threats are a key strength. However, areas remain for enhancement, including improved outbound email filtering and expanded integration with third-party DLP tools, which are currently limited. The customizable nature of the administrative interface and the dashboard could see further refinements for enhanced user experiences.

IRONSCALES' deployment model is focused on cloud-based delivery, mainly utilizing public cloud infrastructures such as Amazon AWS and Microsoft Azure. The solution is an ICES platform, not reliant on traditional SEGs, thus making it highly suitable for enterprises aiming for swift deployment without the complexity of on-premises infrastructure. This SaaS approach facilitates rapid scaling and integration within Microsoft 365, Google Workspace, and a growing list of collaboration tools like Microsoft Teams.

Regarding interoperability, the platform boasts integrations with advanced cybersecurity solutions, including SIEM and XDR systems, enhancing multi-channel threat visibility and management. Built-in security capabilities are robust, featuring support for encryption standards such as AES and comprehensive authentication methods, including Microsoft and Google Authenticator apps. Moreover, IRONSCALES supports API authentication through JWT and key exchange.

IRONSCALES has a broad customer base, with significant presence in North America, EMEA, and APAC regions. The platform is particularly favorable for mid-market and medium-sized businesses seeking to enhance their email security frameworks while benefiting from AI-driven analytics and threat protection. Its strong foothold in the MSP/MSSP sector makes it an attractive partner for organizations looking to deliver advanced security solutions to their clients. Furthermore, the platform's integration of security awareness training with technological solutions marks its appeal to organizations emphasizing comprehensive cybersecurity measures.

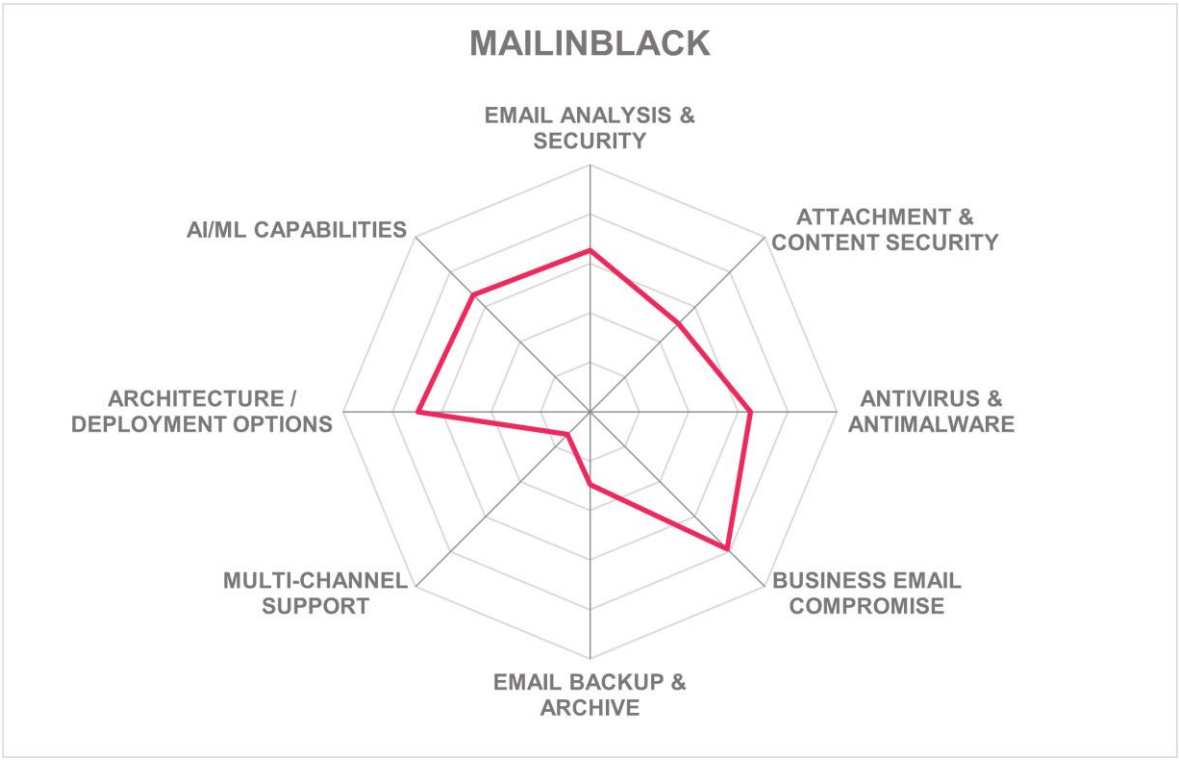
Strengths

- Uses advanced ML, DL, and AI for threat detection.
- VAP identification and monitoring are distinguishable features.
- Integration with multiple third-party malware scanners.
- Effectively combines post-delivery protection and real-time remediation.
- Integrations with platforms such as Microsoft Teams.
- Continuous development with integrated user feedback loops.
- Strong presence in the MSP and MSSP market.
- Extensive user support options across multiple languages.
- Integrated security training for users.

Challenges

- Does not integrate with third-party DLP tools.
- Admin interface customization could be further improved.
- Lacks keyword filtering for outbound emails.
- Lack of email backup and archiving support.

Mailinblack – Protect



Mailinblack, headquartered in France and founded in 2003, specializes in advanced email security solutions that cater to the stringent security requirements of modern enterprises. Their Protect Advanced solution operates by integrating with email MX records, ensuring that emails are filtered before reaching user inboxes.

Protect Advanced offers multi-layered email protection, including AI-enhanced spam filtering, virus detection through Clam AV and Bitdefender, and defense against polymorphic malware. The solution uses behavioral analysis and sender reputation checks for effective BEC mitigation. It also integrates with SIEM systems. The Secure Link technology further distinguishes Mailinblack, rewriting and encrypting links within emails to guard against phishing attacks during user interaction.

Mailinblack's further differentiators include its proprietary AI models that ensure high-precision spam and threat detection. While innovative, the product does not yet support automatic removal of harmful emails post-detection or provide direct user capabilities for reporting suspicious emails, indicating areas for potential enhancement. Planned

improvements in content analysis and API integration, particularly with Microsoft 365, are on the product roadmap.

Mailinblack offers cloud-based and on-premises solutions. The Protect Advanced solution is primarily offered as a cloud service, though it supports hybrid configurations suitable for diversified IT environments.

Mailinblack integrates with SIEM systems. The platform is currently working towards deeper interoperability, particularly targeting integration with Microsoft 365 through forthcoming dedicated APIs that bypass traditional redirection techniques.

Mailinblack primarily serves European organizations that value strict data residency and compliance with GDPR but also serving growing customer demand for sovereign solutions. The solution is particularly beneficial for industries with high-security needs, offering customizable user settings and advanced delegation management for shared inboxes. It supports flexible scaling within enterprise environments, making it suitable for businesses aiming to integrate advanced email protection while maintaining stringent control over their communication channels.

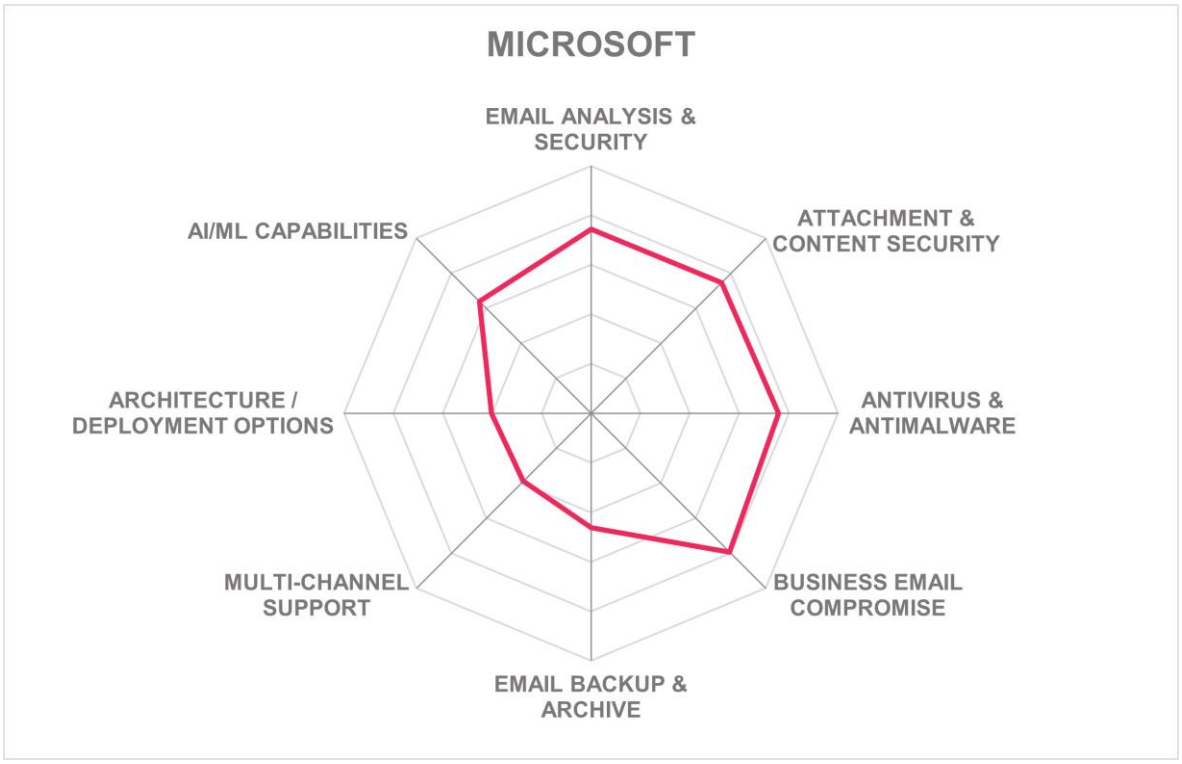
Strengths

- Provides robust spam and threat detection.
- Integrates with Clam AV and Bitdefender for antivirus protection.
- Offers proprietary AI for high-precision filtering.
- Delivers strong Business Email Compromise mitigation.
- Secure Link technology for real-time URL protection.
- Compliance with European residency and regulatory demands.

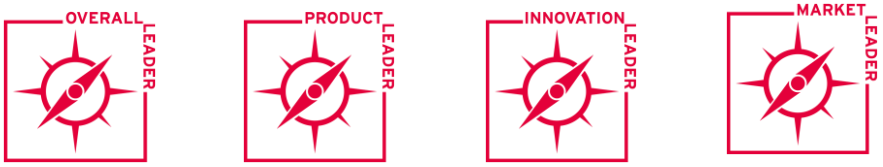
Challenges

- Lacks automatic removal of harmful emails post-detection.
- Limited user capabilities for direct email threat reporting.
- Improvement needed in email content analysis features.
- Enhanced API integration, particularly for Microsoft 365, is required.
- Some limitations in user customization of dashboard features.

Microsoft – Defender



Leader in



Microsoft, established in 1975 and headquartered in Redmond, Washington, is a leading giant in the software market, having expanded significantly into cybersecurity and identity solutions over the years. Microsoft Defender for Office 365 is a key component of Microsoft's expansive security suite, specifically targeting email security. This solution is integrated within the Microsoft 365 ecosystem to provide enhanced security capabilities that extend beyond the default protections offered. Through its multifaceted deployment options, Microsoft Defender for Office 365 serves as a critical tool for organizations leveraging Microsoft's broad software ecosystem, enhancing the robustness of enterprise email security.

Microsoft Defender for Office 365 maximizes its capabilities by integrating advanced ML algorithms to anticipate and thwart email threats, including BEC and phishing attempts. The BEC capabilities are closely integrated with Microsoft's XDR. It fortifies email security through sophisticated risky user analytics and AI-based threat detection that proactively manages potential compromises. Its multi-layered defense employs baseline features like

SPF, DKIM, and DMARC authentication and protection against spoofing. Enhanced capabilities include antivirus and antimalware defense through real-time sandboxing and heuristic analysis. Defender’s formidable scanning and filtering capabilities process and analyze vast email data, providing administrators with actionable insights.

One of Microsoft's unique strengths lies in its exhaustive signal intelligence, obtained from processing millions of emails across its vast network, which enhances Microsoft's capability to predict and neutralize emerging threats efficiently. It seamlessly integrates with Microsoft Sentinel and the broader Microsoft Defender suite. Despite its strengths, Microsoft's primary focus on Microsoft 365 environments presents challenges for organizations needing extensive support for hybrid or non-Microsoft email systems. Improvements in interoperability and licensing clarity could enhance the adoption of its advanced security layers across a broader range of deployment environments.

Microsoft delivers its Defender for Office 365 only in a SaaS deployment model, as is common for their product portfolio. The suite's interoperability extends beyond Microsoft Exchange, supporting integration with other email systems through API-based connectors. Microsoft supports integrations with SIEM solutions such as Microsoft Sentinel.

Microsoft Defender for Office 365 is tailored for organizations deeply embedded in the Microsoft 365 environment, with strong coverage across all global regions. Enterprises that rely heavily on Microsoft’s suite for their IT infrastructure will find Defender an essential component in fortifying their cybersecurity posture, especially those in regulated industries requiring rigorous compliance standards. The solution’s integration within a familiar Microsoft user experience makes it practical for organizations seeking to streamline their security management across multiple domains. However, businesses with non-Microsoft email infrastructures should consider supplemental solutions for complete coverage.

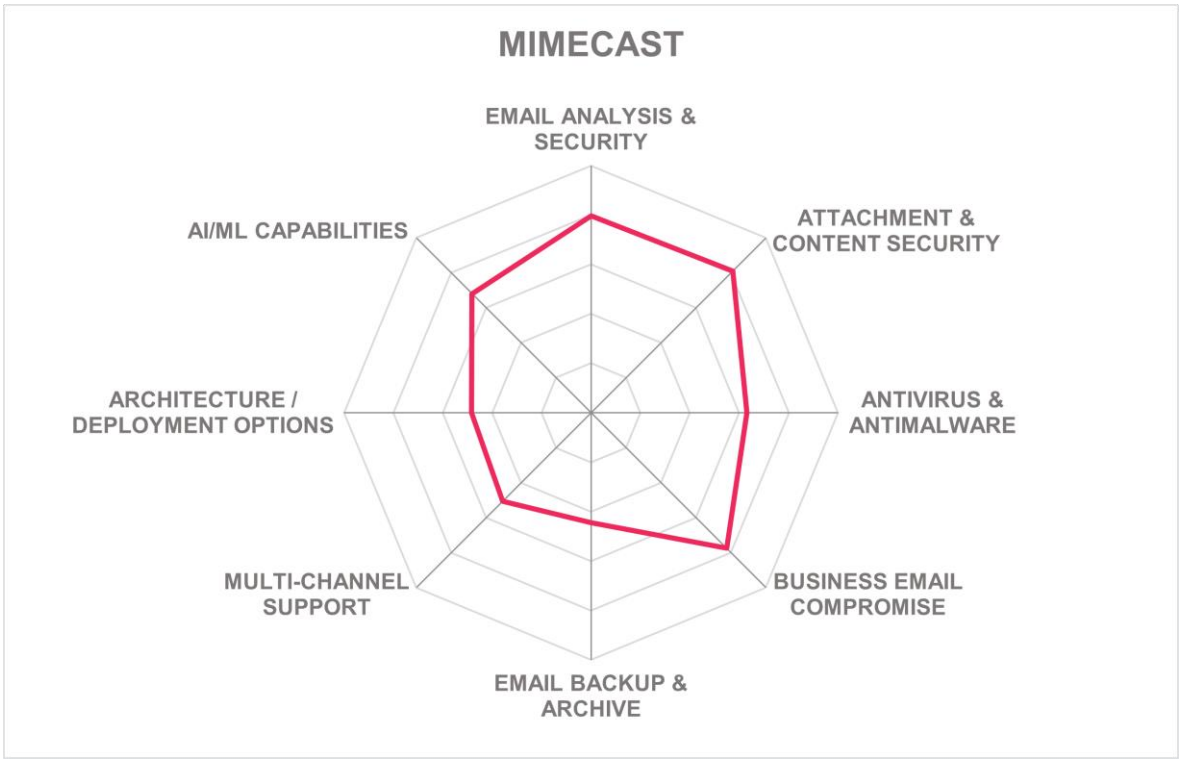
Strengths

- Comprehensive email security features.
- Robust integration with Microsoft 365 and Defender suite.
- High signal intelligence from global email data.
- Advanced AI/ML capabilities for threat detection.
- Multi-layered email protection including post-delivery.
- Supports extended SIEM functionality via Microsoft Sentinel.
- Integrated with Microsoft Defender XDR capabilities.
- Support for Microsoft Teams is a newly added capability

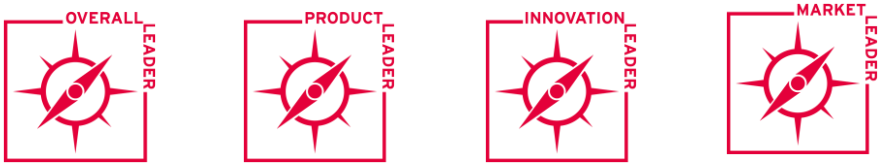
Challenges

- Focused mainly on Microsoft 365 environments.
- Limited interoperability with non-Microsoft systems.
- Need for broader support beyond API integration for hybrid setups.

Mimecast – Email Security



Leader in



Mimecast, established in 2003, is an influential player in the email security domain, headquartered in Boston, MA. Acquired by Permira, a private equity firm, in 2022, Mimecast's core specialization lies in email security and management, encompassing data retention and compliance solutions along with security awareness training. In addition to email, Mimecast scans and remediates content in Microsoft Teams, SharePoint, and OneDrive, and applies policies to sensitive content, not only threats. The Mimecast Email Security service is delivered through a SaaS model hosted at their own data centers and various cloud providers. Designed for integration with popular email clients such as Microsoft Outlook, Mimecast adopts a subscription model based on per-user, per-service fees, offering flexible deployment models accommodating diverse business needs.

The flagship solution enhances security through sophisticated techniques, integrating AI and ML models to combat phishing, spear-phishing, and other email-borne threats. Mimecast employs advanced DNS authentication mechanisms like SPF, DKIM, and DMARC, closely monitoring email authenticity and integrity. The system also supports multiple antivirus and

antimalware engines, leveraging signature and heuristic technologies alongside an automated sandbox for thorough threat identification. Their email content analysis uses contextual understanding and identity graph analysis to detect anomalies like BEC, spam, and offensive content.

Mimecast's standout features include leveraging supervised ML for dynamic threat detection to mitigate risks from sophisticated phishing attacks and identity theft. Unique offerings such as brand impersonation detection and post-delivery threat mitigation set Mimecast aside as leaders in innovation. Additionally, capabilities like browser isolation and Content Disarm and Reconstruction (CDR) further enhance user safety. While the platform excels in detection and protection, advanced reporting features are areas for potential growth.

Mimecast's email security solutions offer two deployment models, cloud gateway (MX-based) and cloud-integrated (API-based). Both use the same detection engines and protection. The solution is delivered as cloud-based, SaaS, operated by Mimecast in own data centers and select cloud infrastructure.

Mimecast integrates with leading email systems such as Microsoft 365, Google Workspace, and SMTP-based systems. For interoperability, it supports integrations with a wide range of systems including Microsoft Azure Sentinel, Exabeam, FireEye Helix, Fortinet FortiSIEM, Rapid7, and Splunk. Mimecast excels with a high number of out-of-the-box connectors and integrations.

Mimecast predominantly serves a global customer base, catering to industries with rigorous compliance demands, including finance, healthcare, and telecommunications. Designed to fulfill the needs of organizations ranging from SMBs to large enterprises, the service is particularly significant for those seeking robust email defense mechanisms coupled with flexible integration into existing IT frameworks. Mimecast’s ability to integrate with prominent SIEM, SOAR, and ITSM tools is particularly advantageous for customers aiming to augment operational security intelligence across their IT infrastructure. Mimecast remains a compelling choice for enterprises prioritizing comprehensive email security solutions with significant integration capabilities and advanced threat mitigation strategies.

Strengths

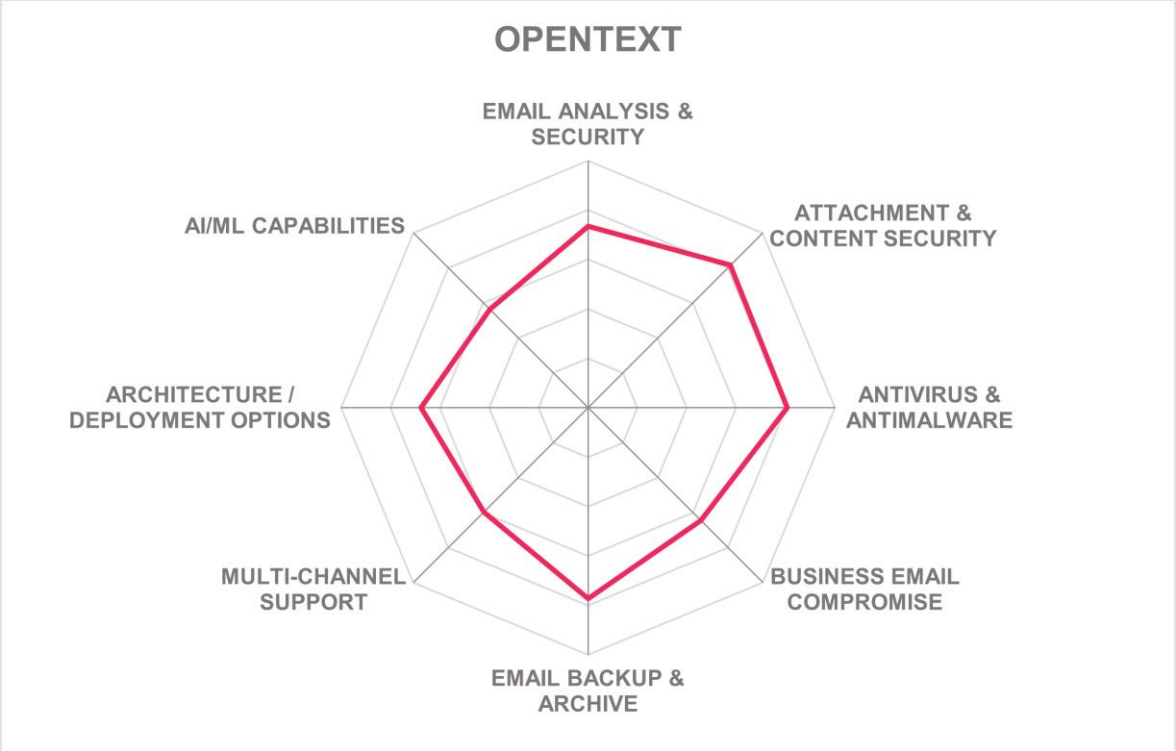
- Extensive use of machine learning for email threat detection.
- Advanced risk management via DNS authentication protocols (SPF, DKIM, DMARC).
- Sophisticated sender reputation analyses leveraging AI.
- Versatile integrations with prominent IT and security tools.
- Robust antivirus engines coupled with sandboxing capabilities.
- Detailed exploration features for e-discovery and litigation holds.
- Certifications in key security and privacy standards (ISO 27001, HIPAA).
- Enriched user protection through browser isolation and CDR.
- Service flexibility with diverse deployment models (SaaS-based).
- AI-driven anomaly detection and brand impersonation safeguards.

Challenges

- Supports standard 3rd party risk profiles, but no out-of-the-box integration to supply chain risk management solutions.
- Broader language integration is desired.
- Enhanced reporting and customization features needed.

OpenText – Core Email Threat Protection

opentext™
Cybersecurity



OpenText, established in 1991 and headquartered in Waterloo, Canada, offers a robust cybersecurity portfolio with a focus on email security. Their offerings, which include OpenText Core Email Threat Protection, Email Encryption, Security Awareness Training, Business Communication Archive, Cloud-to-Cloud Backup, and Email Continuity, are unified under their sophisticated cloud-based platform. This integration leverages their extensive expertise in Microsoft technologies, underpinning a cloud-first approach enriched with artificial intelligence capabilities aimed at enhancing security outcomes.

The OpenText Email Security solution boasts many capabilities, such as multilayered filtering against ransomware, phishing, and spam threats. It includes six antivirus/antimalware engines, with four being third-party, enabling robust defenses. The product's supports standards like SPF, DKIM, and DMARC, ensuring effective email sender authentication. Additionally, it integrates smoothly with directories like Microsoft Exchange and Google Workplace, supported by real-time threat analysis and machine learning to adaptively protect organizational communications.

Key differentiators for OpenText's Email Security are its expansive threat intelligence processing and product suite integration, which help to ensure high efficacy with minimal false positives. Its user interface is crafted for simplicity and efficiency, streamlining security policy management.

While primarily a cloud-delivered service, OpenText’s email security solutions, including Core Email Threat Protection and Email Encryption, can also be deployed on-premises appliances. Managed services are also available.

Internal security is based on RBAC and extensive monitoring and logging, ensuring that administrative activities and data exchanges are securely handled and auditable.

OpenText's Email Security is ideally suited for organizations in North America and EMEA, particularly those in regulated sectors like healthcare and financial services. Its integration with Microsoft environments makes it highly appealing to firms within these ecosystems, offering a cohesive security package. The platform is particularly attractive to small to mid-sized companies and managed service providers (MSPs) seeking rapid deployment and a consistent user experience across their cybersecurity infrastructure.

Strengths

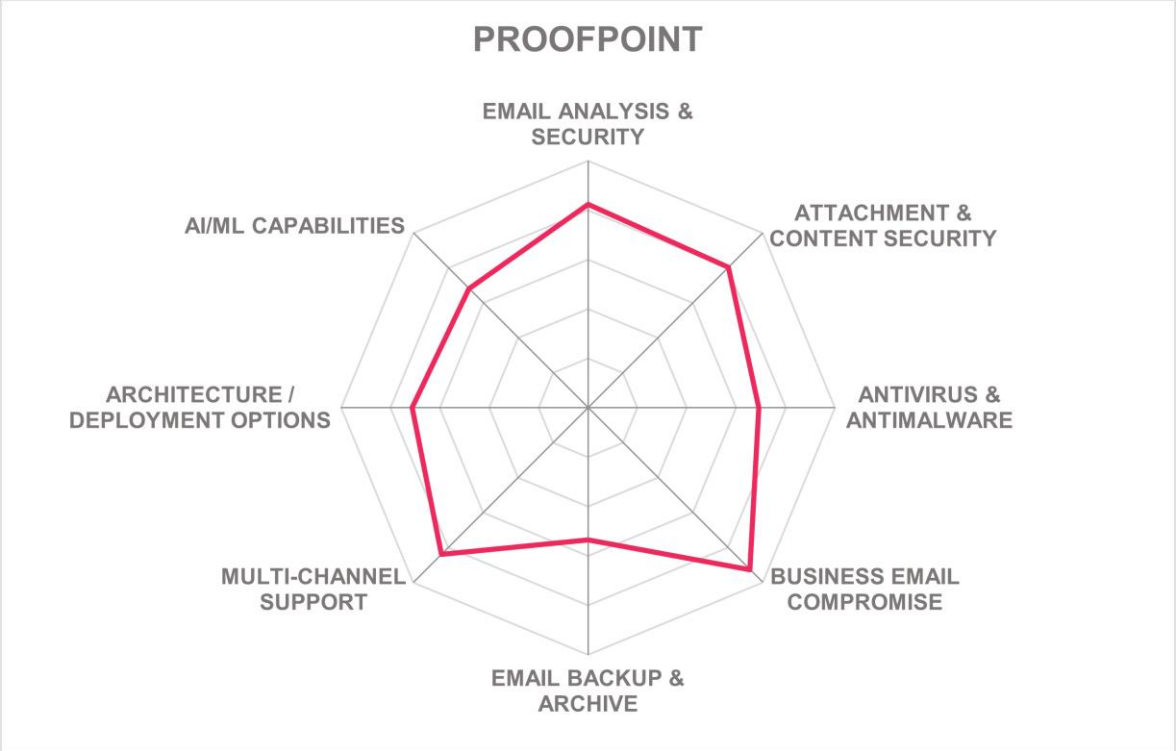
- Multilayered filtering against diverse email threats.
- Seamless integration with Microsoft 365 and Google Workplace.
- Unified cloud-based platform for security management.
- Six-engine antivirus/antimalware system.
- Advanced machine learning threat analysis.
- Effective sender authentication with SPF, DKIM, and DMARC.
- User-friendly, modern interface for easy administration.
- Excellent threat intelligence capabilities.
- Offers robust data encryption and backup.
- Security awareness training present.

Challenges

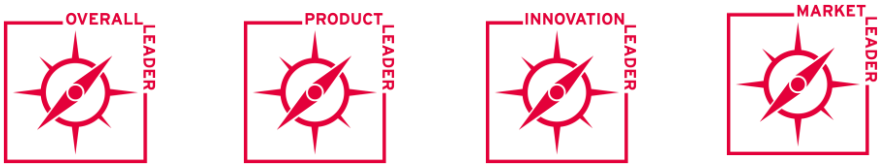
- Internal policy optimization tools are lacking.
- Limited to North America and EMEA primarily.
- Some directory integration features need improvement.
- No auto-enroll for X.509 certificates.
- Lack of multi-channel support for environments such as Teams and Slack.

Proofpoint – Prime Threat Protection

proofpoint.



Leader in



Proofpoint, established in 2002 and headquartered in Sunnyvale, California, is a leader in the email security sector. Under private equity firm Thoma Bravo, Proofpoint offers a diverse portfolio spanning threat protection, data security, data governance, and compliance. They have acquired other vendors, including Tessian and at the time of this report, announced their intention to acquire Hornet Security. Proofpoint has extensive deployment options, including on-premises, SaaS, and fully managed services. Proofpoint supports millions of customers globally, including a significant portion of the Fortune 100. This wide distribution of service models ensures Proofpoint meets the varied needs of both large enterprises and smaller businesses across industries.

Proofpoint's product capabilities are marked by its advanced threat detection and preemptive defense mechanisms, powered by AI/ML. The platform provides robust protection against phishing and BEC with tools like Semantic Analysis for understanding threat context and intent. Their security framework supports standards such as SPF, DKIM, and DMARC for stringent email authentication, and uses third-party integrations like WithSecure and Trellix

for antivirus protection. Capabilities are further strengthened by Proofpoint Nexus, which employs AI-driven multilayered detection engines to identify emerging threats, ensuring high protection efficacy.

Proofpoint distinguishes itself with its innovative use of AI and ML, particularly through semantic analysis in threat detection and preemptive blocking of malicious URLs. Recent advancements include the introduction of the Enhanced TOAD Detection model and the Collab Protection feature, extending security beyond email to other collaborative platforms such as Teams, Slack, or Zoom, but also traditional methods such as fax. However, the product's complexity due to rule-based configurations could benefit from simplification to ease integration. While the focus on internal security awareness training is strong, there is room to expand interoperability with external security training solutions. Additionally, the need for integrating Hornet Security's offerings (post-acquisition) poses a potential business challenge.

Proofpoint's deployment flexibility is a standout feature, offering SEG, ICES, and hybrid deployment models that cater to different customer needs. Many customers use SEG and ICES deployment option in tandem to support a multi-tier, defense in depth architecture. The platform is available as an on-premises solution, SaaS, or a fully managed service.

In terms of interoperability, Proofpoint excels with broad compatibility across various email systems, including Microsoft Exchange, Google Workspace, and legacy systems such as Lotus Notes/Domino. The solution integrates with leading enterprise cybersecurity solutions such as SIEM, SOAR, and XDR platforms.

Proofpoint serves multinational enterprises across North America, EMEA, APAC, and LATAM regions, catering especially to sectors requiring high security. Its robust set of features makes it particularly appealing for organizations facing frequent threats and who value extensive threat intelligence integration. Proofpoint's adaptability in deployment and user-friendly reporting tools aid administrators in managing complex security environments. The solution's extensive support network and its track record in industries such as finance, healthcare, and government underscore its suitability for organizations that prioritize high-standard security and compliance in email communication.

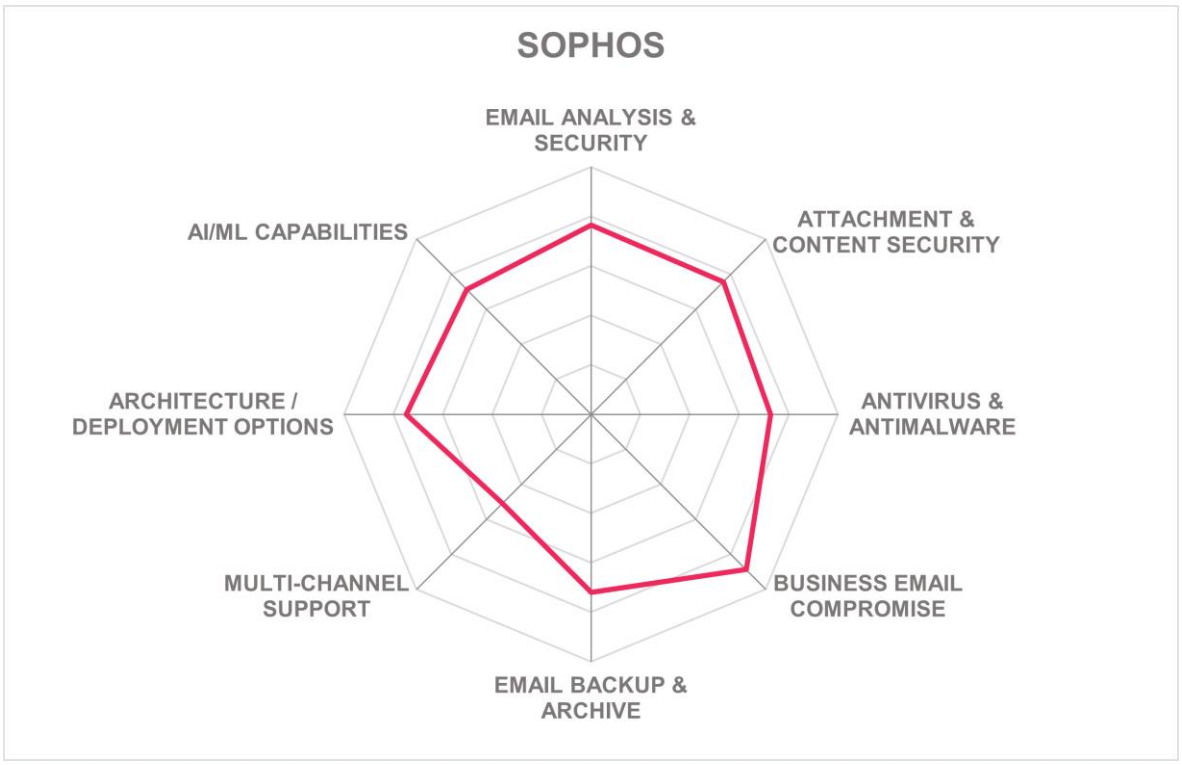
Strengths

- Leading detection efficacy, leveraging advanced AI and ML capabilities.
- Very comprehensive set of email security and workspace protection capabilities.
- Comprehensive threat intelligence integration via Nexus platform.
- Flexible deployment options.
- Support for standards like SPF, DKIM, and DMARC.
- High adaptability across deployment models.
- Extensive cybersecurity certifications, including SOC 2 Type 2.
- Robust user training integration enhancing security culture.
- Predictive and pre-delivery sandboxing for threat prevention.
- Excellent multi-channel support including Teams, Slack, and Zoom.

Challenges

- Policies require advanced understanding to deploy and tune effectively.
- Limited support for third-party security training integration, but own solution is available.
- Post-acquisition integration of Hornet Security remains under evaluation.
- Email backup and archiving capabilities are sold separately.

Sophos – Sophos Email



Leader in

Sophos, founded in Abingdon, UK in 1985, is a well-regarded leader in cybersecurity, servicing hundreds of thousands of customers globally. The company specializes in endpoint security, network security, and email security among other offerings. Their Sophos Email solution, built on the Sophos Central platform, integrates with Microsoft solutions and various email clients, lending itself to deployment as a Secure Email Gateway or as an Integrated Cloud Email Security measure. Known for robust AI and ML defenses, it effectively guards against threats like BEC and phishing attacks.

Key capabilities of Sophos Email include its ability to effectively handle risky users in BEC protection, and provide granular email authentication, with support for SPF, DKIM, and DMARC standards. The solution incorporates its proprietary anti-malware technologies, featuring dynamic and static analysis through SophosLabs Intelix. ML detection models actively monitor and enable responses to cyber threats, with multiple policy-based options available for managing sensitive data and communication. Additional tools such as Time of Click protection for instant analysis of potentially malicious links in emails further bolster its threat detection and mitigation capabilities.

The standout aspect of Sophos Email lies in its integration with Sophos MDR, enabling superior security outcomes through real-time threat response. This includes manual message clawback and the ability to adjust configurations dynamically during an active threat. The innovative AI-powered natural language processing enhances the system's ability to thwart social engineering attacks, making it particularly effective against BEC. Noteworthy challenges include the absence of integrated backup and archival functions, as well as provisions for e-discovery and litigation holds. These areas, however, are under active development, aiming for near-future enhancement.

Sophos Email provides both SEG and ICES solutions. This flexibility enables enterprises to deploy the solution in different environments such as on-premises, cloud, or hybrid setups.

Sophos Email integrates with a range of cyber defense solutions, including Sophos XDR and MDR, as well as third-party SIEM and SOAR systems. The platform also supports Microsoft Exchange, Google Workspace, but also other email systems via the MIME standard, thus ensuring wide interoperability.

From a built-in security perspective, Sophos Email leverages modern authentication models including FIDO2 passkeys, which facilitates enhanced security without compromising the user experience.

Sophos's key customer base spans many sectors, with a significant stronghold in North American and European markets. The solution is particularly well-suited for organizations operating on Microsoft 365, where its ability to layer additional security measures is highly beneficial. Its straightforward user interface and ease of policy management are advantageous for enterprises seeking a robust, integrated approach to email security and wider cybersecurity measures. Prospective clients are encouraged to consider Sophos Email for its comprehensive security capabilities that cater to intricate operational needs.

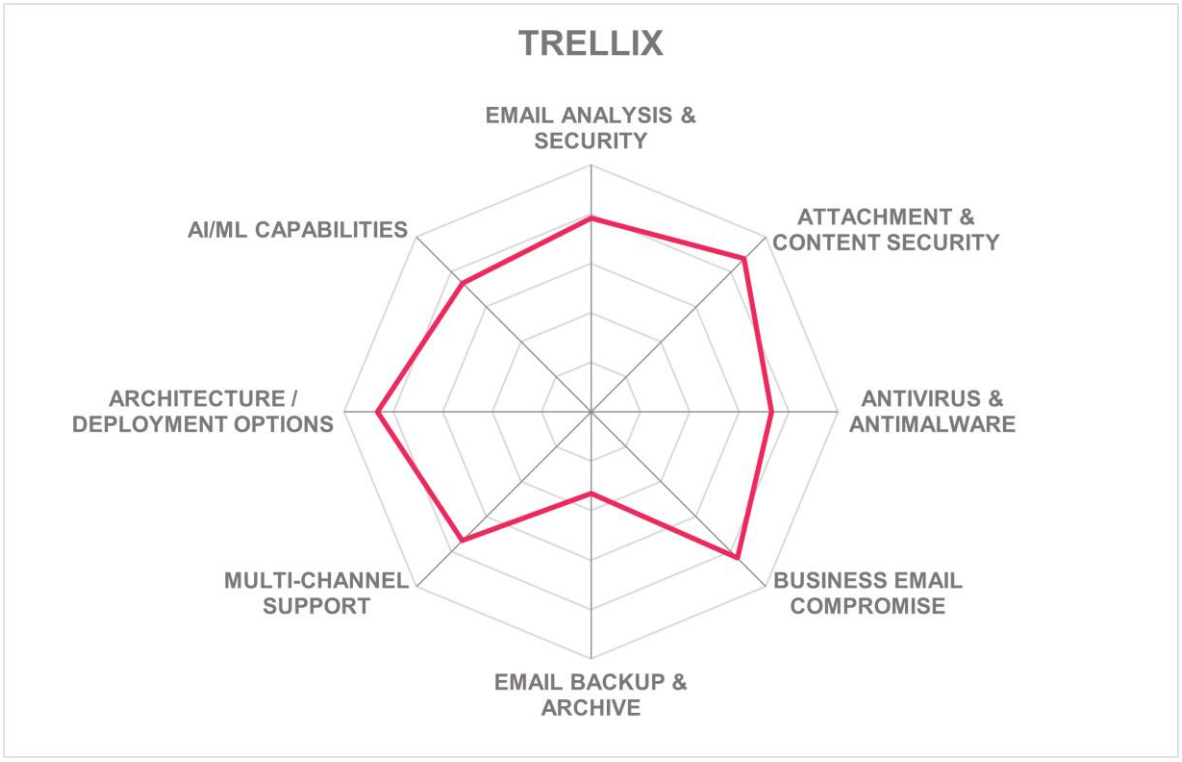
Strengths

- Comprehensive integration with Sophos MDR.
- Effective phishing and BEC defense.
- Advanced AI-powered threat detection.
- Can act as an Microsoft 365 “overlay”, seamlessly expanding Microsoft’s own capabilities.
- Fine-grained DLP options.
- Strong support for email authentication standards
- Flexible authentication support to the platform including passkey support.
- Excellent multi-language analysis and support.

Challenges

- No integrated email backup capabilities, as of the publication of this report.
- Lacks e-discovery and litigation hold functionality.
- Limited third-party training solution integrations.
- Email archiving dependent on external solutions.

Trellix – Security Platform



Leader in

Trellix, headquartered in the United States, was established in 2022, evolving from FireEye's legacy in email security. The company offers a robust email security solution designed to address contemporary cyber threats, underscoring its commitment to addressing email and collaboration security as the cornerstone of broader workspace security. The solution is part of the Trellix Security Platform, integrating with SOC, MDR, and IR operations to cater to enterprise-scale threat models. Trellix's email offering supports multiple deployment models, including cloud services and on-premises setups, delivering flexibility to meet varied customer needs across global regions, including North America, EMEA, APAC, and Latin America.

The key capabilities of Trellix Email Security focus on robust AI and ML enhancements, delivering advanced threat detection and minimizing false positives to empower security teams. It offers risky user handling, advanced antivirus/antimalware detection with a multi-layer approach, including sandboxing and heuristic analysis, alongside proactive BEC prevention. Users benefit from sophisticated email content analysis that detects and

mitigates phishing and impersonation threats. Trellix supports critical industry standards and certifications such as SPF, DKIM, and DMARC for email authentication. Additionally, its certification suite covers major compliance frameworks, reinforcing its reliability in safeguarding sensitive information.

Trellix distinguishes itself through its pioneering use of AI-driven innovations and a strong emphasis on integrating threat intelligence, which harnesses insights from its tens of thousands of customers. Its Unique Selling Proposition (USP) lies in its ability to catch threats that other market leaders like Microsoft may overlook, offering a purported 99.999% detection accuracy rate. The recent introduction of a phishing simulator, Gen-AI assisted investigations, and native DLP capabilities mark significant steps forward.

Trellix Email Security supports various deployment models, including cloud, on-premises, and hybrid configurations. The platform functions as a SEG and interoperates via APIs with major platforms like Microsoft 365, Google Workspace, and legacy email systems. Trellix delivers strong interoperability, enabling integration with cybersecurity ecosystems like SIEM, SOAR, and XDR solutions.

Trellix serves a wide range of sectors, including finance, defense, and governmental organizations, providing significant value to large-scale enterprises and those in highly regulated industries. Its email security solutions are particularly well-suited for customers seeking thorough protection that extends to enterprise applications and collaboration platforms. Organizations with complex and extensive IT infrastructures will find Trellix's integrated and flexible deployment options advantageous, enabling seamless adaptation to existing environments, whether on-premises or in the cloud.

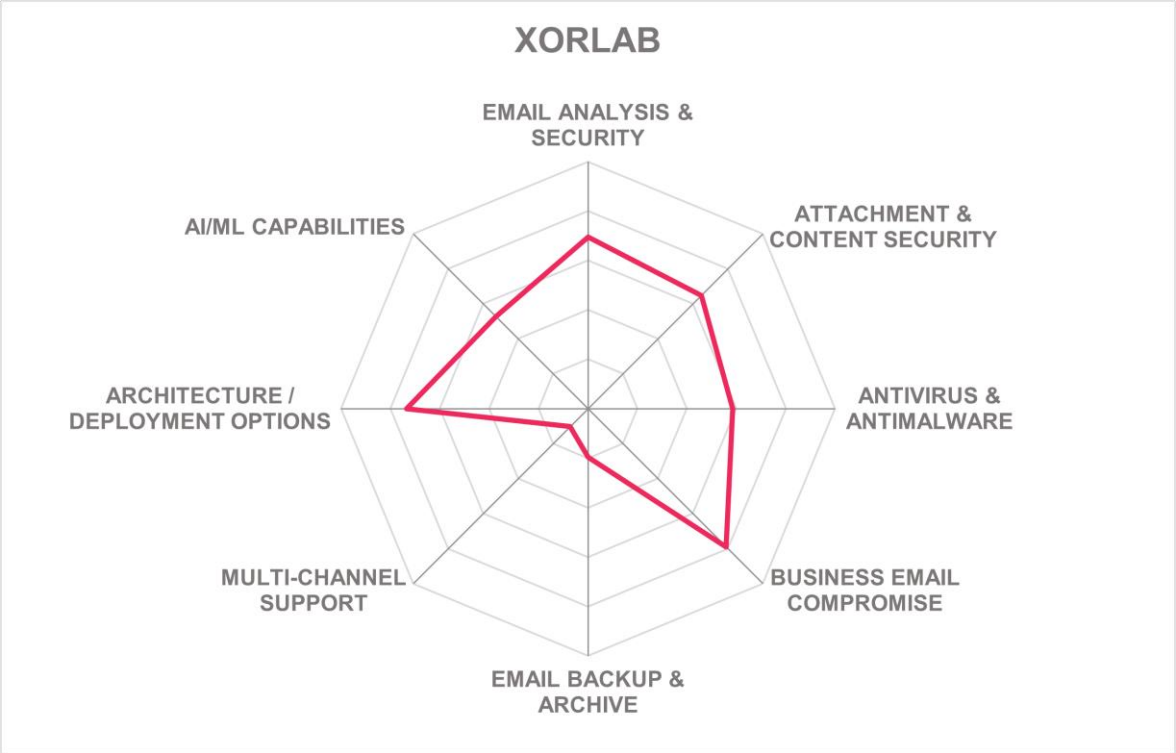
Strengths

- Advanced threat detection capabilities
- Extensive use of AI and ML
- Sophisticated multi-layer security approach
- Deep integration with enterprise applications
- Broad deployment model support
- Strong global threat intelligence network
- Proven high detection accuracy
- Comprehensive coverage of email and collaboration platforms as well as user risk protection for enterprise applications such as ServiceNow and Workday.

Challenges

- Integration improvements desired for administrative functions
- High complexity in setup for smaller organizations
- Third-party SIEM integration options based on syslog only, no deeper out-of-the-box integrations
- Initial learning curve due to feature richness

xorlab – Email Security



Established in 2015 and headquartered in Zurich, Switzerland, xorlab AG is a dynamic player in the email security domain. The company offers the xorlab Email Security solution, an integrated platform focused on preventing sophisticated, communication-based cyber-attacks. The solution is available as an on-premises appliance, cloud service, or managed service. xorlab is a wholly European alternative in the cybersecurity landscape. The company leverages significant innovation to address the increasing complexity of email-borne threats.

xorlab deploys robust features for handling email security challenges, such as risky user management, email authentication, and antimalware detection. The solution employs ML throughout its detection processes to evaluate atypical behaviors and cyber threats via static and dynamic analysis, along with sandboxing capabilities. Furthermore, xorlab supports key standards, including SPF, DKIM, and DMARC, to authenticate emails. Security integration

with Microsoft Active Directory and Microsoft Entra ID, alongside support for SAML federated authentication, enable the product's interoperability with existing enterprise environments.

xorlab distinguishes itself with its use of relationship and behavior analysis to detect new and targeted email threats proactively. By continually evolving its detection rules and policies using machine learning, xorlab addresses zero hour phishing and BEC effectively. Recent innovations include the introduction of contextual email banners, multi-tenancy capabilities, and improved dashboards that highlight key metrics. However, areas for improvement include enhanced support for encrypted emails and further integration with security ecosystems like SOAR systems. The platform's promise of optimized policymaking and automated incident response offers a forward-looking approach in dealing with modern threats.

xorlab's Email Security can be implemented as an on-premises appliance or via cloud deployment. It is also available as a managed service. It supports integrations with cybersecurity solutions such as SIEM systems for reporting and logging activities and Azure Active Directory for authentication. The system comes with good built-in security, including SAML authentication and RBAC. The platform's integration capabilities extend to Microsoft Exchange and LDAP.

With a primary customer base concentrated within the DACH region, xorlab serves sectors such as finance, healthcare, IT, and construction, among others, supporting enterprises of varied sizes, from small businesses to large organizations. The company is particularly suited for industries requiring enhanced visibility into email traffic and threat identification capabilities. Enterprises seeking to bolster email security with a European-centric solution, particularly those leveraging Microsoft environments, will find xorlab an attractive option. The solution's AI-driven, data-centric framework enables rapid adaptation to emerging threats, making it a compelling choice for security-conscious enterprises.

Strengths

- Innovative use of AI and behavior analysis.
- Robust risk management features.
- Comprehensive email authentication support.
- Proactive threat detection capabilities.
- Multi-faceted malware detection approaches.
- Flexible deployment options.
- Support for a variety of email systems, including legacy systems.
- Data residency for EU customers.

Challenges

- Limited encryption and digital signature support.
- Restricted interoperability for certain external integrations.
- Developing market presence outside core region.
- Enhancements needed in integration capabilities with broader security infrastructure.
- Lack of multi-channel support.

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless may offer a significant contribution to the market space.

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.

Arkose Labs

Arkose Labs offers risk-based authentication and bot mitigation solutions, primarily known for their challenges and anomaly scoring to protect digital channels from credential stuffing, fake account creation, and other forms of abuse. While their core focus is not Email Security, their technology can support broader anti-fraud strategies across user interaction points.

Why worth watching: While not a dedicated Email Security vendor, Arkose Labs may be interesting in scenarios where bot mitigation intersects with credential phishing defense. Arkose Labs' platform includes Email Intelligence, which can prevent New Account Fraud from invalid email addresses and domains, and it can detect invalid users at popular email providers such as Gmail, Microsoft Outlook and Hotmail. Email Intelligence interdicts both volumetric and low-and-slow registration attacks.

Barracuda Networks

Barracuda Email Protection provides both gateway and API-based deployment models, with coverage for traditional SEG use cases and integrated inbox defense for Microsoft 365. Capabilities include anti-phishing, malware protection, data protection, incident response, and integration with broader Barracuda security tools including XDR and backup.

Why worth watching: Hybrid deployment options, layered protection, and extended capabilities beyond email security.

Darktrace

Darktrace offers a cloud-native Email Security solution that integrates natively with Microsoft 365, Exchange, and Google Workspace. Using advanced ML-based threat detection and

user behavior analytics, Darktrace Email Security addresses a range of attack vectors including phishing and social engineering.

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

Echoworx

Echoworx is a specialized provider focusing on email encryption. They do not provide full email security capabilities as asked for in this Leadership Compass but can be complementary 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.

eleven cyber security

eleven cyber security is a German provider focused on email filtering, encryption, and continuity, typically delivered as managed services through partners. The solution supports standard SEG functions with anti-malware and anti-spam filtering and integrates with compliance-focused components such as archiving.

Why worth watching: Regional vendor offering managed email security services with a focus on compliance and data privacy.

ESET

ESET provides both a Secure Email Gateway and API-based Email Security, embedded into a broader cybersecurity portfolio including XDR. Their on-prem SEG supports Exchange and Domino, while the cloud solution supports Microsoft 365 and Google Workspace with post-delivery protection.

Why worth watching: European vendor with integrated email security capabilities across on-prem and cloud environments.

Forcepoint

Forcepoint sits on the outgoing channel of email security, offering 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 (includes Perception Point)

Fortinet's acquisition of Perception Point adds sophisticated email security features to their broader cybersecurity portfolio. The solution includes API-based protection, dynamic sandboxing using a hardware-assisted platform, deep file analysis, and extended support for collaboration tools beyond email.

Why worth watching: Advanced sandboxing and inspection capabilities now integrated into a wider enterprise security portfolio.

Fortra (includes Agari & Titus)

Fortra delivers email security through Agari's Cloud Email Protection and DMARC solutions, along with Titus' classification and DLP capabilities. The integrated offering provides inbound protection, data classification, and sender authentication controls.

Why worth watching: Comprehensive email security coverage through integrated classification, DLP, and threat protection tools.

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. They also provide secure data rooms and secure data transfers.

Why worth watching: Add-on to email security for encryption and secure information sharing.

Google

Google's Email Security is natively integrated into Gmail, enhanced by AI-driven spam filtering, phishing and malware detection, as well as tools like Google Safe Browsing. It is primarily available to Google Workspace customers and tightly embedded into the wider Google security stack.

Why worth watching: Built-in protection with strong AI capabilities and tight integration into the Google Workspace ecosystem.

GoSecure

GoSecure provides email security as part of its MDR-centric platform, with SEG capabilities, threat analysis, and forensic investigation support. GoSecure emphasizes its human-led response service for complex threats.

Why worth watching: Combines traditional SEG capabilities with MDR-style threat response and analysis.

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.

Group-IB

Group-IB, founded in 2003 and headquartered in Singapore, offers an extensive range of solutions, prominently featuring their Managed Extended Detection and Response (MXDR) capabilities. The company's Unified Risk Platform includes the Business Email Protection (BEP) module, which focuses specifically on combating BEC and offers advanced functionalities to scrutinize and disable potential email-based threats.

Why worth watching: Delivering managed Email Security successfully to high-profile customers.

Heimdal Security

Heimdal Security is a provider of an integrated set of cybersecurity solutions and services, including email security. They provide a SEG that helps customers to protect 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.

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.

Mailprotector

Mailprotector provides cloud-based email security and encryption for Microsoft 365 and other services, sold via MSPs. Features include spam and malware filtering, encryption, archiving, and policy enforcement.

Why worth watching: MSP-friendly solution with modular services for encrypted and protected email.

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 delivery of only safe content to users.

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

Pointsharp

Pointsharp offers email security within its secure access and identity-focused portfolio. Their product emphasizes secure mobile email, encryption, and user authentication, targeting regulated sectors.

Why worth watching: Suitable for organizations looking to combine secure identity and access with encrypted email delivery.

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.

Retarus

Retarus provides a European-hosted email security platform with ICES, encryption, continuity, and transactional email capabilities. The solution is API-based and includes OEM-integrated malware and phishing detection tools, plus patented post-delivery protection.

Why worth watching: Enterprise-grade platform hosted in Europe, supporting compliance-driven customers.

Securepoint

German vendor providing email security as part of an integrated UTM and endpoint portfolio. The solution supports anti-spam, phishing protection, and basic archiving.

Why worth watching: Entry-level integrated solution attractive for SMBs in the DACH region.

SonicWall

SonicWall provides a SEG product integrated with their firewall and threat detection ecosystem. Capabilities include anti-malware, encryption, and DLP, with an emphasis on protecting legacy and cloud-based email environments.

Why worth watching: Longstanding player with integrated SEG functionality for on-prem and cloud transitions.

SSH Communications

Primarily known for secure access solutions and encrypted communication tools, SSH Communications offers secure file and email transmission products, though without a comprehensive email security platform.

Why worth watching: Niche provider of encryption technologies that may be useful in sensitive email workflows.

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.

TitanHQ (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).

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.

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.

Xcitium

Xcitium (formerly Comodo Security) includes Email Security in its endpoint and containment-focused security portfolio. Their SEG and filtering options aim to isolate and remove threats before endpoint contact.

Why worth watching: Integration of email security with zero-trust endpoint isolation tools.

ZeroBounce

ZeroBounce focuses on email validation and hygiene, aiming to improve email deliverability and remove risky addresses. Their solution is not an email security tool per se but can support secure outbound mail and reduce bounce-related vulnerabilities.

Why worth watching: Complements email security with email hygiene and validation services.

Zivver

Solution focused on secure email delivery, including sending encrypted email, supporting email recalls, proof of delivery, and a range of other features. Complementary 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.

Related Research

Leadership Compass Email Security (2023)

Buyer’s Compass SaaS Security Posture Management

Buyer's Compass Security Services Edge

Leadership Compass Security Orchestration, Automation and Response

Leadership Compass Managed Detection and Response (MDR)

Analyst’s View Managed Detection and Response (MDR)

Buyer’s Compass eXtended Detection and Response (XDR)

Leadership Compass eXtended Detection and Response (XDR)

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole 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 technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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