OMDIA UNIVERSE

Publication date:
13 Dec 2023

Author(s):
Fernando Montenegro, Senior Principal Analyst, Cybersecurity
Rik Turner, Senior Principal Analyst

Omdia Universe: Email Security, 2024

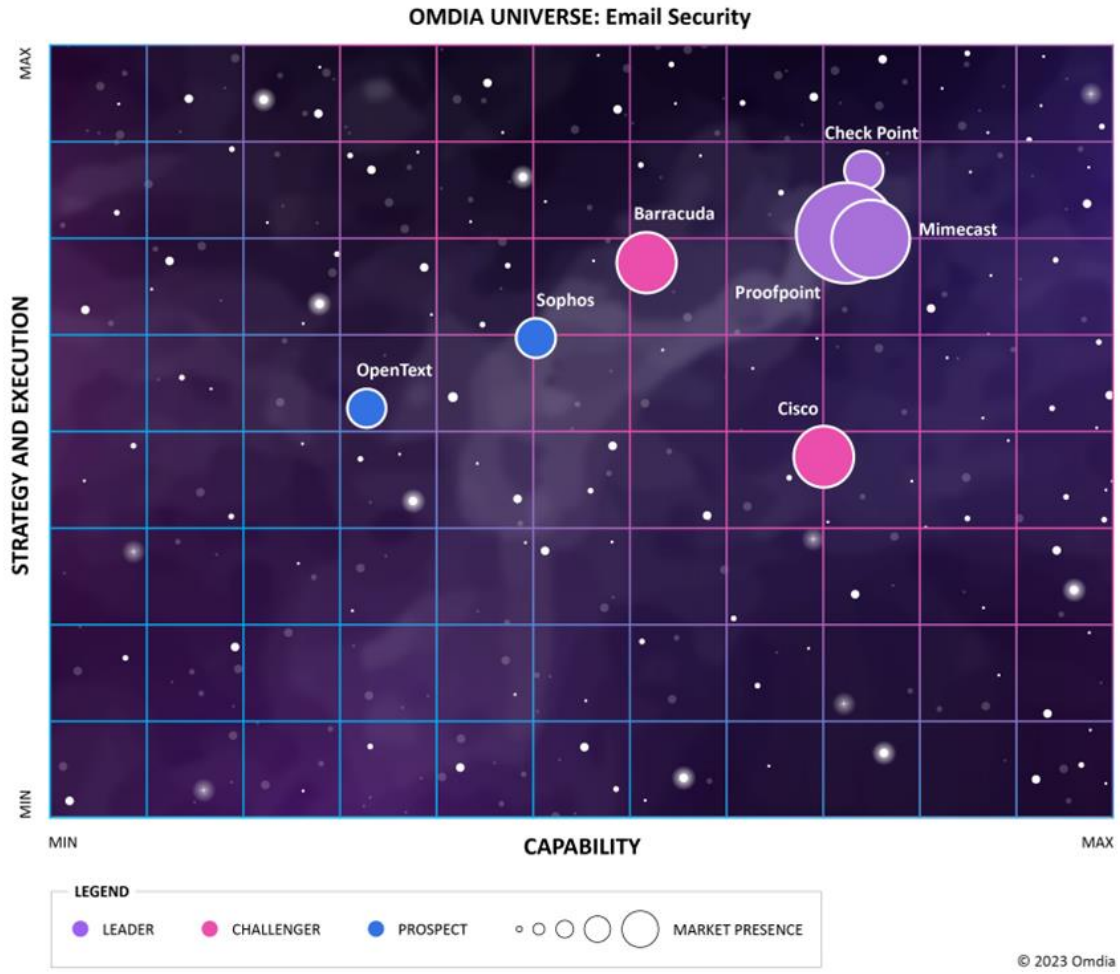
OMDIA
Brought to you by Informa Tech

Summary

Catalyst

Email security is a tremendously interesting sector: while it has been around since the early days of networking, it now sits at the border between security and "the business": criminals and other attackers have found ways to profit from exploiting flaws in email security without those flaws being necessarily "technical" in nature.

Figure 1: The Omdia Universe for Email Security



Source: Omdia

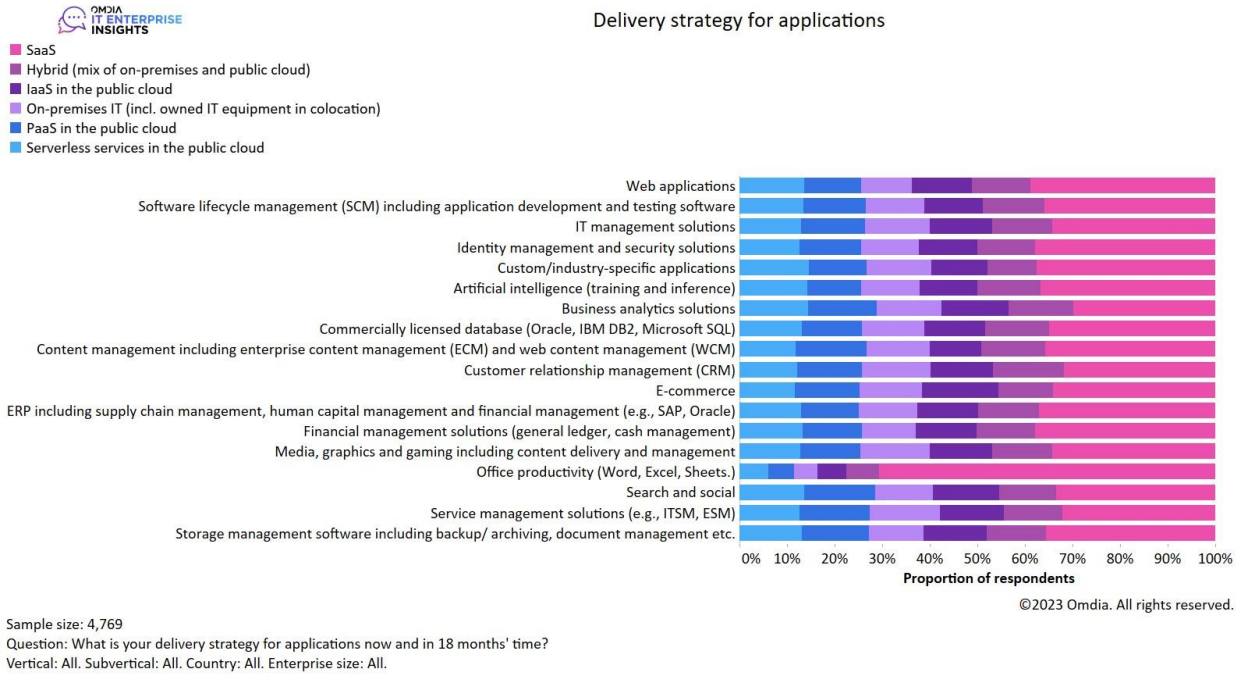
As email service providers—notably Microsoft, but also Google and others—add email security capabilities, what else is needed? Is there a role for third-party email security vendors? This report looks at several of them to understand what capabilities they offer. **Figure 1** illustrates how some of these vendors compare, with the rest of this report providing more information about the relative position of each vendor.

Omdia view

Several factors are in play in email security.

While email has been around for a long time, how it gets consumed has shifted significantly. In essence, we have mostly moved from on-premises to SaaS. This is perfectly illustrated in **Figure 2** on delivery strategy for applications, as captured by Omdia's IT Enterprise Insights survey: while all other application options in the survey have an approximately equal distribution between environments, office productivity—which is widely understood to include email services—has a massive preference for SaaS-based delivery.

Figure 2: What is your delivery strategy for applications now and in 18 months time?



Sample size: 4,769
Question: What is your delivery strategy for applications now and in 18 months' time?
Vertical: All. Subvertical: All. Country: All. Enterprise size: All.

Source: Omdia

While some others remain in the market, it is safe to have the base expectation that an organization will use email services from one of their main productivity providers—Microsoft or Google. Importantly, both providers have been adding significant amounts of email security functionality: Microsoft offers Exchange Online Protection and Defender for Office 365, while Google offers advanced phishing and malware protection features.

The shift in email consumption also severely impacts email security architecture.

Traditionally, the way to deliver email security was to use a gateway approach (secure email gateway (SEG)). In this approach, customers choose to configure email routing (via DNS MX records) so that emails first flow into the email security component—be it software running on a general-purpose server, dedicated email security appliances, or, more recently, a cloud service—and only then forwarded to the final destination. While it is conceptually simple to deploy, using this route through an external gateway potentially loses out on whatever security features the email providers themselves are adding. Organizations may be asking themselves—if my provider already does a lot of email security, do I need more?

For a vendor, this poses a significant challenge—how can they position themselves to cooperate with the email service provider who themselves are increasingly offering more email security features? Even as email

providers offer new ways of interfacing with the systems via application programming interfaces (APIs), opportunities for differentiation are getting harder to come by.

At this point, it's also critical to consider what the modern threat landscape looks like. More than the annoyance of unsolicited messages (“spam” and other variations such as “graymail”), organizations are keenly aware that email is often one of the key vectors for serious multi-stage attacks that can have material consequences for the organization. It's important to clarify some of these:

- **Phishing** attacks consist of tricking users into disclosing credentials that can then be used by attackers to log into the organization. Email is a key vector for delivering these attacks by convincing users to click on links to malicious sites that capture those credentials.
- **Malware** attacks will usually get the victims to execute attack code on their endpoints, thereby giving attackers a foothold in the organization. Malware is often embedded in emails.
- **Business email compromise** (BEC) attacks and variations consist of abusing existing business processes, such as accounts payable and others, to steal money from an organization via fraudulent transfers. These attacks arrive as email messages.

While not specifically attacks themselves, it's important to clarify two major terms:

- **Data exfiltration:** The practice of attackers stealing copies of sensitive organizational information.
- **Ransomware**: A broad attack campaign that starts with infiltration of an organization and, following lateral movement and privilege escalation across many systems, results in extortion attempts where the company is expected to pay to recover files that were encrypted or for the attacker not to release files that were exfiltrated.

This is relevant as organizations should be thinking broader—beyond just email security as a technical challenge. Sure, it is still a technical domain that requires expertise, but the end goals of email attacks are multifaceted and transcend what we normally describe as cybersecurity into a broader domain of anti-fraud.

This is the way we see forward-looking organizations thinking about email security: email is the current conduit for the attacks described above, so it must be dealt with, but the bigger issue is protecting against those broader attacks. Particularly as organizations incorporate other forms of communication in their workflows—collaboration applications such as Microsoft Teams, Slack, Google Meet, and others, or chat-like capabilities in a variety of applications such as software development and version control (GitHub, GitLab, and many others), and more—the optimum way forward is not only to address core email security needs of the present but also to think of expanding, both into other collaboration technologies and deeper, into a broader understanding of the organization's own business processes.

Analyzing the Email Security Universe

Market definition

Email technology has been around since even before we had full TCP/IP connectivity—emails were exchanged in the early 70s in ARPANET. The need to secure this medium against unwanted messages arose in the early 90s and has only grown since then, including the use of machine learning (ML) techniques (back then referred to as statistical techniques) such as Bayesian filtering in the early 2000s.

The market has developed significantly since then, following a broad evolution of how enterprises are opting to implement email functionality: there is a wholesale migration of email functionality from locally managed email servers to consuming it as a service. Here, Microsoft has captured a significant share of the market with its Microsoft 365 offering (formerly known as Office 365) and variations such as Exchange Online.

While Microsoft has included a growing set of security features within its email service offerings, many organizations choose to deploy separate capabilities for email security. Many of these vendors were providing email security capabilities well before the surge in "email as a service," and since that time, vendors used primarily a "gateway" approach: email would flow through the vendor's email security software (and later a cloud-based service) prior to delivery.

Nowadays, most email security vendors offer architecture options that, besides the use of gateway architectures, rely on one of the many application programming interfaces (APIs) offered by Microsoft and other email service providers for directly integrating with the core email platform, effectively going into the recipient's inbox to handle their emails, removing anything deemed suspicious.

Regardless of how the email security vendors inject themselves into the flow of email—as a gateway before email reaches the organization or deeply embedded with the email platform via APIs—we recognize that there are specific capabilities that should be supported.

Core email security functionality

Core email security functionality refers to a set of capabilities that cover the fundamental use cases associated with email security. These consist of:

- **Malicious file protection:** Preventing weaponized content from reaching victims.
- **Unwanted message protection:** Preventing spam and other types of unwanted content.
- **Specific attack protection:** Techniques for detecting and blocking phishing attempts, business email compromise attacks, and more.
- **Internal email protection:** To account for possible scenarios of internal email compromise.

To implement these capabilities, vendors will often use a variety of techniques, including integration with anti-virus and anti-malware analysis services, use of reputation analysis, identification of anomalous message traffic patterns, and, increasingly, extensive use of ML techniques for numerous tasks.

Additional capabilities

Additional capabilities refer to other important aspects of email security that typically fall outside the core functionality. For this analysis, Omdia looked at:

- **User interaction:** What end users and administrators experience when using the proposed solution, including options for security awareness training, visual cues in applications, administrator experience when searching, and experience handling different types of messages.
- **Outbound protection:** How the proposed solution can assist with preventing malicious emails from leaving the organization.
- **Management:** Integration of the proposed solution with a variety of enterprise technologies, such as directories and endpoint management tools, as well as how administrators manage the proposed solution.
- **Supporting technologies:** Integration with specific technologies such as extended detection and response (XDR), security automation platforms, content disarm technology, remote browser isolation, and varied use of threat intelligence.

Other areas

In addition to the key functionality covered in the two sections above, this report also analyses vendors from other angles:

- **Solution Breadth:** How the proposed vendor offering supports different technology architecture patterns and email technology/service vendors such as Microsoft, Google, and others.
- **Strategy & Innovation:** The vendor's go-to-market approach, alignment to key industry trends, and an evaluation of the proposed vendor roadmap vis-à-vis technology trends and competitive markets.
- **Market Momentum:** How the vendor offer is growing within the market. This is a composite metric that looks at total revenue, revenue growth, and growth in the number of customers.
- **Vendor Execution:** A composite of different categories, primarily centered around customer experience score, implementation capabilities by the vendor, and partner ecosystem.

Market dynamics

Email security is dynamic in its innovation—it is often at the forefront of applications of AI/ML—but also as a market. Over the past couple of years, there have been numerous interesting strategic transactions.

First and foremost, the year 2021 saw a few significant transactions affecting key email security vendors at the time: Thoma Bravo acquired Proofpoint for a massive $12bn, and shortly thereafter, Mimecast was taken private by Permira for about $5.8bn (the deal closed in mid-2022). At about the same time as the Mimecast transaction was announced in December 2021, OpenText announced it had closed the acquisition of Zix, a provider with a strong pedigree in email encryption, that it had announced earlier that year. That year also saw Check Point’s successful acquisition of Avanan.

Additional deals in 2022 included Cloudflare's acquisition of Area1 Security in February 2022 and Hornetsecurity's acquisition of IT-Seal for security awareness in May 2022.

This year saw two significant acquisitions. First, Cisco announced it was acquiring ArmorBlox in May 2023, with a heavy emphasis on the target's capabilities in AI/ML. Second, Proofpoint announced in late October that it intends to acquire email competitor Tessian.

These transactions help solidify a picture of a market with very distinct players, each navigating their own path:

- Microsoft casts a large shadow in the market as the dominant provider of email services for corporate environments and of email security capabilities in its own right. Google remains in a distant second place. As Microsoft becomes an even larger security vendor, will it swallow email security whole?
- The large specialist vendors in the space—Proofpoint and Mimecast—are now both privately owned, reflecting the more mature nature of the market, yet one still needing significant investment to keep up with threats. Both companies have made advancements in moving beyond their historical gateway-based offerings, thereby undercutting some of the argument that "SEGs are dead."
- Numerous vendors have a strong platform message—Cisco, Sophos, OpenText, Barracuda, and Check Point, among others. These vendors are positioning themselves with email security as a component of their broader vision, with benefits to organizations if they buy into a broader security architecture. These benefits are both financial (discounts for buying more of their products) and operational since the email component becomes another source of telemetry for their back-end XDR platform and thereby helps strengthen the overall security posture of the organization.
- There is then a long tail of other vendors, some as standalone email security vendors and others with email embedded as part of their platform offer, be it targeting end-user organizations or managed services providers.

Figure 3: Vendor rankings in the Email Security Universe

Vendor	Products evaluated
Leaders	
Check Point Technologies	Harmony Email Client
Mimecast	Mimecast Email Security Cloud Integrated
	Mimecast Email Security Cloud Gateway
Proofpoint	Aegis Threat Protection Platform
Challengers	
Barracuda Networks	Barracuda Email Protection
Cisco Systems	Cisco Secure Email Gateway
	Cisco Secure Email Threat Defense
Prospects	
OpenText	Webroot Advanced Email Threat Protection
	Webroot Advanced Email Encryption powered by Zix
Sophos	Sophos Central Email Advanced

Source: Omdia

Market leaders

The market leaders in this study have demonstrated three core qualities:

- They have addressed the numerous technical requirements of the different capability areas of the email security evaluation.
- They have an expansive view of the role of email security within the modern threat landscape.
- They have executed well in the market as measured by their growth, which in some cases was substantial.

Comparatively, their average rankings in relation to other vendors were the highest across all six comparison categories.

Market challengers

Market challengers also performed well in three areas:

- Being able to handle the variety of use cases related to email security, including phishing, BEC, and malware.
- Offering a vision of where email security fits into a broader architecture.

- Market presence.

The delineation between challengers and leaders comes down to challengers typically exhibiting more inconsistency in performance than the leaders. Their average rankings across the six categories were in the middle of the pack.

Market prospects

Market prospects are those that, compared to the broader vendor groups, came behind in direct comparisons. This is not to say these are not capable offerings that may be well-suited for specific types of customers—indeed, study participants were all capable vendors selected based on specific criteria (refer to methodology in Appendix)—but these vendors' combination of offering features, strategy, Market Momentum, and Vendor Execution fell behind the others. Their average rankings across the categories were the lowest.

Opportunities

At Omdia, we refer to the modern state of affairs, where technology permeates everything, as "digital dominance." There's no organization of any meaningful size—including down to the smallest mom-and-pop shop—that can exist today without some tethering to technology.

Email is often part and parcel of that tethering: it is the medium through which significant communication between parties takes place and is used both in an ad hoc manner between collaborators as well as part of automated business processes. With that, email security is essential, be it to protect it from nuisance in the form of spam or as protection against more nefarious adversaries.

The opportunities for the market in email security arise from the status of essential technology that can grow in different directions.

One direction is a deeper understanding and integration with business processes: if an organization's email security system can help thwart attacks because it understands the logic of how business operates, it is likely to be highly valued. This is one area where more sophisticated analytical methods—yes, using AI/ML—can shine in bringing more context to how email is handled.

Another interesting opportunity is, as mentioned before, growth into other collaboration environments. Here, as organizational boundaries become more porous, there is tremendous potential to deploy similar capabilities that were originally just used for email security into chats, social apps, and more.

The third interesting area to explore is the potential for email security to flourish as a key capability of integrated security suites, providing context to additional modules. This has been the path that the industry has started on with using email telemetry as part of extended detection and response (XDR) systems, but this can be taken even further as vendors bring to market offerings closer to true "security as a service."

Vendors in email security may look at these opportunities both in the context of strategic directions as well as potential partnerships.

Threats

As mentioned above, in this age of "digital dominance," we expect email security to remain essential as a topic. Still, there are clouds—pun intended—on the horizon, as a combination of factors threaten to challenge vendors that offer specific email security offerings.

The first factor is that email service providers—notably Microsoft, given its success with Microsoft365/Exchange Online—become even more competitive in the marketplace through a combination

of technical prowess and business strategy. Email service providers already implement numerous email security features such as anti-spam, anti-malware, and anti-phishing protection, and they can leverage the existing business relationship to simplify deployment and procurement. While independent email security vendors often point to their results detecting attacks above and beyond the capabilities of the email provider, at which point does the value of those extra detections potentially no longer justify the additional investments?

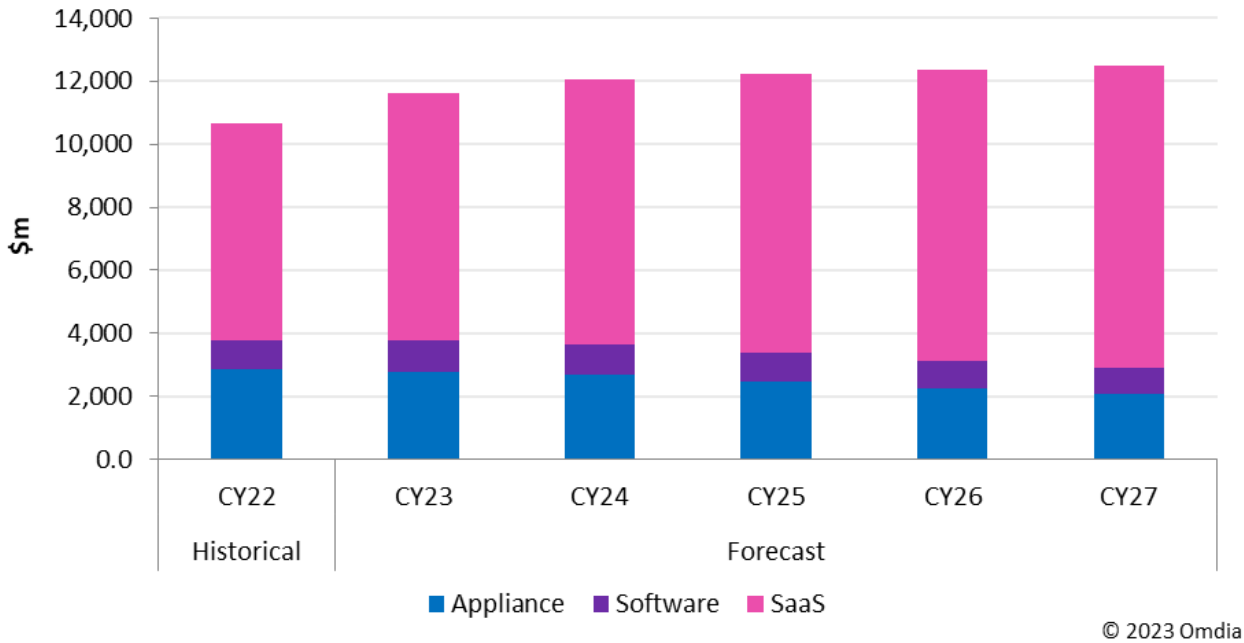
Another potential threat to email security vendors is the rise of security platforms that have embedded their deeper capabilities with their own email security. This is not unlike the first factor above in the sense that in the first factor, the decision about email security is absorbed into the decision about email service, whereas here, the decision is absorbed into a broader security platform decision. If an organization makes a strategic decision to align with a vendor that offers network security, endpoint security, cloud security, analytics, etc., and email security as well, the challenge for independent vendors is demonstrating how they offer enough value as an independent to justify the exception.

Market outlook

We continue to see the market evolving both in size and technology.

According to Omdia's *Content Security Gateway Appliances, Software, and SaaS 2Q23* report, which includes messaging as a key component, the market for messaging security is worth approximately $3bn in 2023 and is growing at a CAGR of 5.6% to approximately $3.5bn in 2027. As can be seen from the chart below, most of that market is for SaaS-based delivery of messaging security.

Figure 4: Category breakdown, CY22–CY27 ($m)



Source: Omdia

We expect that the market will continue to evolve in terms of technology as email security vendors continue to deploy newer analytical methods—using the ever-present AI/ML techniques and their evolutions—as well as increasing their coverage across other collaboration applications.

We also expect to see an uptick in the number of vendors delivering email security features as part of integrated security suites aimed at smaller organizations, which are typically resource-constrained. These organizations are also more likely to consider the use of core email security functionality from their existing email service providers.

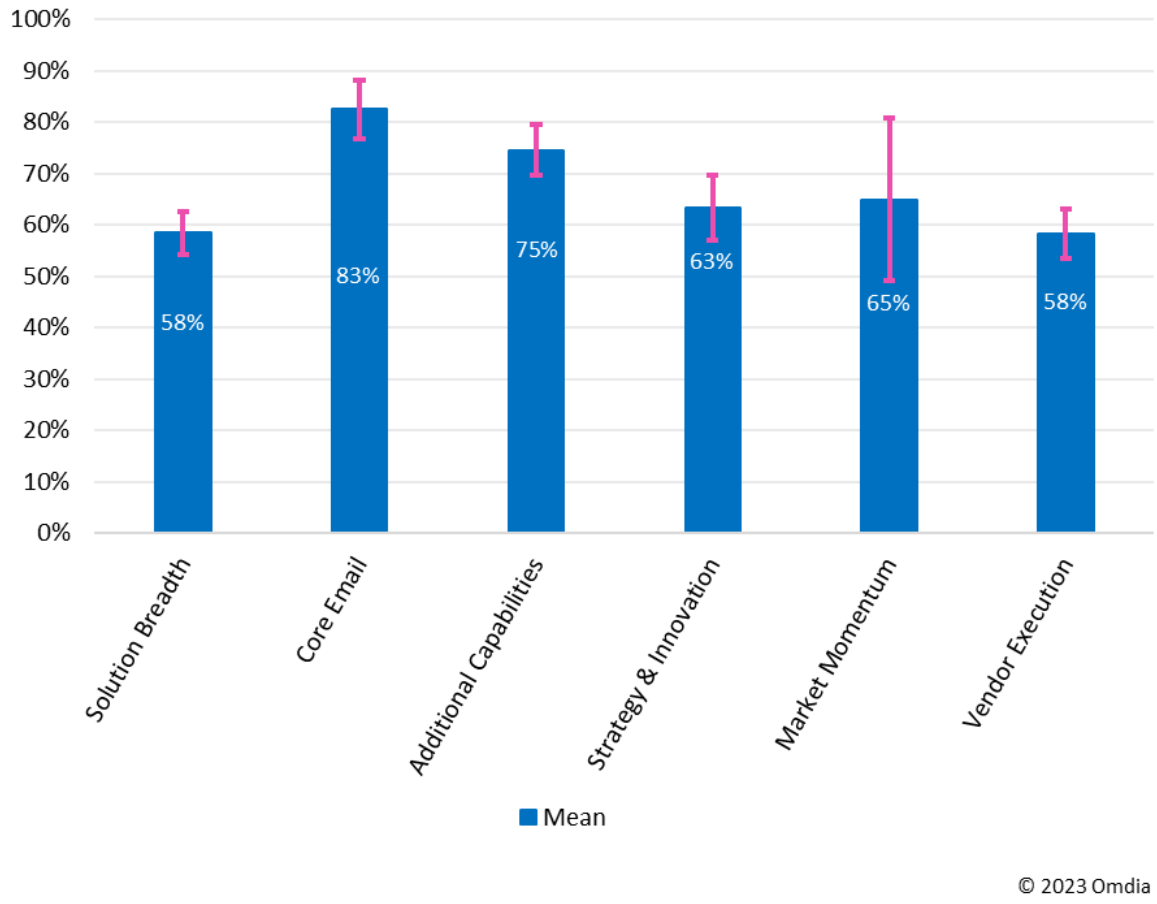
Vendor analysis

Score analysis

The results for each vendor can be found in their respective sections, but a few aggregate results are notable:

- The **Core Email Security** area had the highest average score (83%) with a small deviation (6%), reflecting the dynamic that many vendors in this study covered the key areas well and that email security is a mature market segment.
- **Additional Capabilities** was the second highest average score (75%), again with a small deviation (5%) which again speaks to how the vendors in this study have approached the central topic of email security.
- **Market Momentum** was the area with the highest deviation (16%), which captures the dynamic of how different vendors are seeing traction in the market.

Figure 5: Average score and deviation for each area (%)



Source: Omdia

Mimecast (Omdia recommendation: Leader)

Mimecast should appear on your shortlist if you are looking for a broad and comprehensive offering for email security that builds on a set of solid email security functionality. The Gateway offer is particularly applicable to larger and/or complex environments, while the Integrated version is well suited to more straightforward deployments.

Overview

Mimecast is one of the most recognizable names in email security, having been founded in 2003. It currently has some 2,200 employees across the world and is headquartered in London, England. It had a stint as a public company but has been privately owned since 2022, when Permira bought it for approximately $5.8bn. The company has structured its offerings around a message of protecting communications, people, and data.

Mimecast has two main offerings for email security: a gateway-less offering named Mimecast Email Security Cloud Integrated ("Integrated") and a traditional gateway approach named Mimecast Email Security Cloud Gateway ("Gateway"). Both offerings share significant back-end infrastructure, such as Mimecast's X1 platform that houses data analytics, service fabric, and detection engines. As with other email security vendors, there is widespread use of AI/ML capabilities in multiple areas of the overall architecture.

The Integrated offering targets simpler environments, ingesting emails via routing rules for inspection after Microsoft 365 processing but before delivery to end users, and provides a streamlined interface, while the Gateway is more suited to larger and/or more complex deployments and offers more customization and integration options as well as connecting via traditional MX insertion.

Mimecast is classified as a Leader in the Omdia Universe based on a combination of solid scores across Solution Breadth, Strategy & Innovation, and Vendor Execution. The company offers a robust platform that can tackle numerous email security use cases.

Figure 9: Omdia Universe ratings—Mimecast

Source: Omdia

Strengths

Mimecast scored well across multiple areas, particularly around Solution Breadth, Strategy & Innovation, and Vendor Execution. One of the benefits of the company's longstanding in the industry is that it has a wide network of partners across both go-to-market and technology. The company boasts of having over 75 pre-built integrations, including leading identity management, endpoint, network, and web security vendors.

The breadth of the overall portfolio for Mimecast is positive as it covers email security, secure portal, awareness training, collaboration security (Teams is supported, and other options are on the roadmap), incident response, brand protection, and archiving, among others. While the Integrated offer is limited to Microsoft environments, the Gateway version can also connect to Google Workspace or other email environments.

The Strategy & Innovation scores were helped by the company's broad go-to-market efforts, its use of a comprehensive back-end platform that offers multiple services, integration hooks (Mimecast refers to it as its "mesh"—Mimecast Extensible Security Hooks—technology), and capabilities, and its aggressive plans to expand beyond email security into broader collaboration applications.

Lastly, the Vendor Execution scores showed positive results in terms of customer experience, particularly with a focus on providing implementation and managed security services, vendor certifications (the company has multiple external certifications), and more. The company also has a robust network of distributors, resellers, implementation partners, and managed services providers across most large markets.

Limitations

In terms of limitations, Mimecast didn't fare as well, primarily in Market Momentum, and it had a middle-of-the-pack performance in some of the core email security functions. The Market Momentum score is understandable as the company is working to grow what is already a sizeable pool of customers (Mimecast mentions it has over 42,000 customer organizations, for which it processes well over a billion emails a day). For core email functions, the company scored well in specific attack protection but middle-of-the-road in other areas.

One of the caveats to be aware of is that Mimecast is navigating the current disparity between its gateway-centric offering and its gateway-less offering. The company indicates that while both offerings provide the same level of email security protection, the gateway product offers more integration options, while the gateway-less product is limited to select Mimecast offerings. Customers should be aware of the differences between the offerings.

Appendix

Methodology

Omdia Universe

Omdia's rigorous methodology for the Universe product involves the following steps:

- Omdia analysts perform an in-depth review of the market using Omdia's market forecasting data and enterprise insights survey data.
- Omdia creates a matrix of capabilities, attributes, and features that it considers to be important now and in the next 12–18 months for the market.
- Vendors are interviewed and provide in-depth briefings on the current solutions and future plans.
- Analysts supplement these briefings with other information obtained from industry events and user conferences.
- The Universe is peer-reviewed by other Omdia analysts before being proofread by a team of dedicated editors.

Inclusion criteria

Vendors were included in the research based on a multi-stage process:

- Pre-selection based on analyst insights on the market, including ongoing participation in events, direct discussions with analysts, mentions in research, and more.
- From a broader list of vendors, the following additional criteria were applied:
  - Based on independent analyst research, a vendor solution is expected to include support for at least 75% of the solution categories in the Omdia vendor questionnaire for this project.
  - The vendor must have a global presence with customers in the following three regions: Asia & Oceania, EMEA, and North America.
  - The vendor is expected to have at least 500 customers, who must be a mix of midsize (1,000–4,999 employees) and large enterprises (5,000+ employees).

Selected vendors were invited to participate in the research. Participation was not contingent on any commercial relationship with Omdia.

Further reading

Fundamentals of Inbound Email Security (August 2021)

Omdia Market Radar: Outbound Email Security (November 2020)

Fundamentals of Outbound Email Security (September 2020)

Content Security Gateway Appliances, Software, and SaaS 2Q23 (September 2023)

"Proofpoint bolsters its AI expertise in email security with Tessian" (November 2023)

"Open Text puts outbound email security in the spotlight with its Zix buy" (December 2021)

"The value of outbound email security goes beyond highly regulated industries" (December 2020)

Author

Fernando Montenegro, Senior Principal Analyst, Cybersecurity

Rik Turner, Senior Principal Analyst, Cybersecurity (peer reviewer)

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com