WAVE REPORT

The Forrester Wave™: Enterprise Email Security, Q2 2023

The 15 Providers That Matter Most And How They Stack Up

June 12, 2023

By Jess Burn with Joseph Blankenship, Angela Lozada, Michael Belden

Summary

In our 26-criterion evaluation of enterprise email security providers, we identified the most significant ones and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Additional resources are available in the online version of this report.

We're Entering The Golden Age Of Email Security

A golden age is a time of great achievement in a society or industry — a time of innovation and the furthering of new ideas via new mediums or technological advancements. Email security is now entering a golden age after stagnating for the better part of a decade. Mass customer migration to cloud email, rapid adoption of machine learning, and the widespread use of APIs to connect systems and share data have brought forth improved offerings and capabilities and innovative roadmaps from legacy providers and newer players. As a result, customers have more choice than ever when it comes to protecting how employees, customers, and partners communicate and collaborate. Often, those customers are choosing more than one email security partner in a layered or multilayer approach to protection. In fact, of the 37 customer references interviewed for this research, only two were working with a single enterprise email security vendor. This approach, as confirmed by customer references, provides greater efficacy — and peace of mind — as attackers continue their own innovations to compromise users and gain access to the data and dollars needed to fuel their malicious enterprises.

As a result of these trends, enterprise email security customers should look for providers that:

- **Offer flexibility in deployments and integrations.** The majority of customer references employing two or more email security vendors report mixing capabilities from each vendor based on strengths or ease of integration with other tools or systems. For example, a customer might leverage the advanced phishing and business email compromise (BEC) detection machine learning models of one vendor and the data loss prevent (DLP) and encryption capabilities of another. Others noted a preference to feed the telemetry from one or more email security solutions into security analytics tools to initiate investigation and response actions. And still others prefer to hang onto their gateway deployments for spam and graymail filtering, adding a cloud-native API-enabled email security (CAPES) deployment to "catch what makes it through." The email security vendors you work with should demonstrate an ability to connect and share data with each other and with key tools in your security tech stack.
- **Make it easy for security teams to respond.** The speed and ease with which a security analyst can investigate and respond to an alert or incident is highly dependent on the speed and ease with which the analyst can: 1) be trained on the solution and 2) complete tasks. Legacy enterprise email security players and larger

platform players offering email security alike have developed or acquired capabilities over time, leading to differences in access, user interface, and levels of context between often loosely linked offerings. Customer references noted that many solutions still require users to jump to different consoles to perform tasks, slowing down investigation and remediation activities. Many vendors, however, recognize the importance of analyst experience (AX) and are making strides to deliver more seamless workflows. Ask current or prospective vendors about their plans and timelines to improve AX in their own products and with their major technology partners.

- **Look beyond email to deliver holistic human protection.** The email inbox is often, and justifiably, seen as the critical battle line that must be held. As a result, vendors are investing in detection capabilities for sophisticated social engineering, cleverly embedded malware, and highly realistic landing pages for attacker campaigns. These capabilities are all necessary, but there are other fronts. The use of messaging, collaboration, file sharing, and enterprise software-as-a-service (SaaS) applications across multiple devices all contribute to employee productivity and employee experience. Protections developed for the email inbox must extend to these environments, yet few vendors in this evaluation currently offer this support, though many plan to add capabilities in the next 24 months. Additionally, awareness and training efforts must move beyond standard phishing testing and compliance checkbox courses to adaptive human protection, like real-time "nudges" to encourage vigilance and secure handling of sensitive information. Look at vendors delivering or prioritizing a more comprehensive approach to protecting all the ways in which people work.

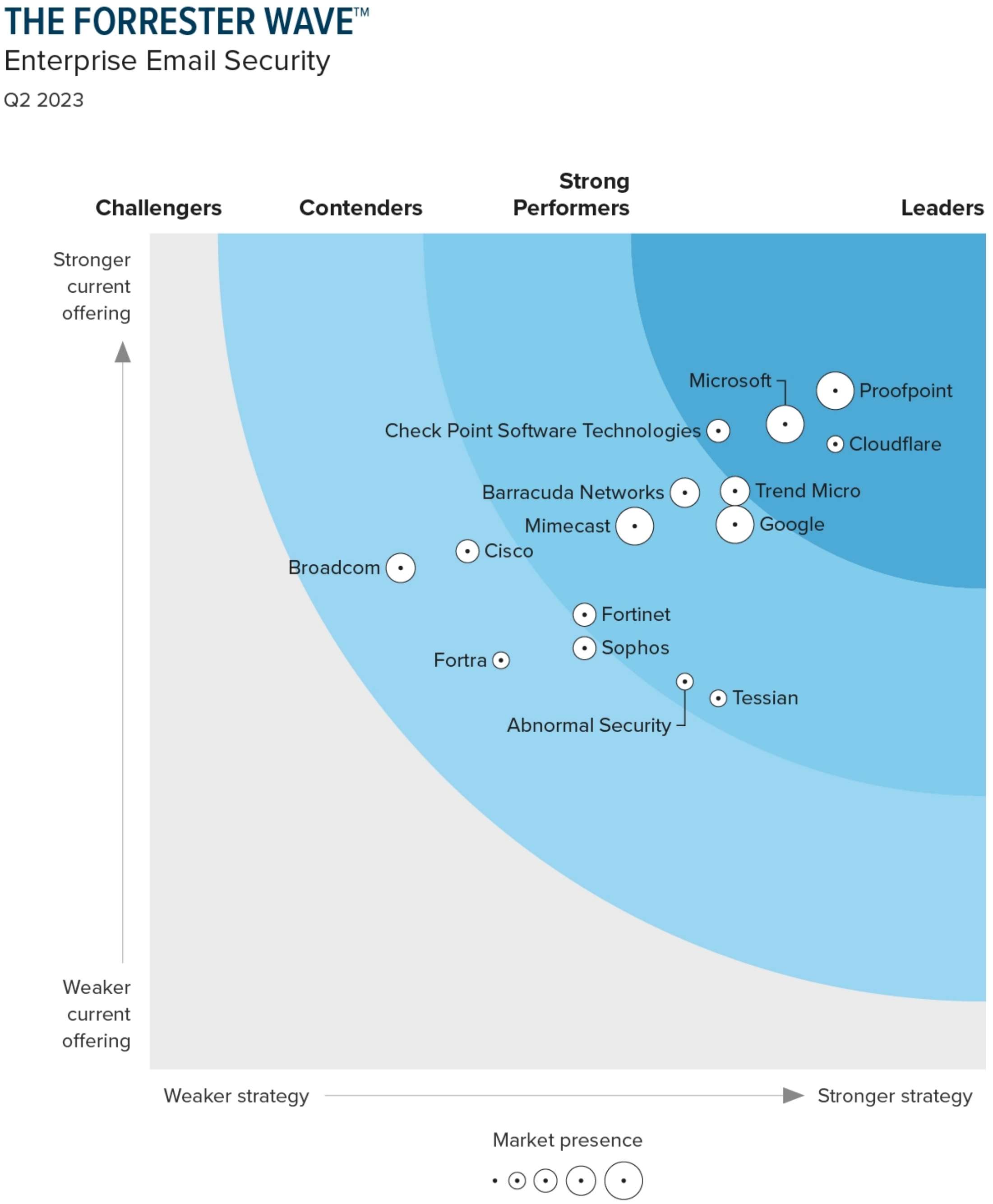
Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market; it doesn't represent the entire vendor landscape. You'll find more information about this market in our report on The Enterprise Email Security Landscape, Q1 2023.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figures 1 and 2). Click the link at the beginning of this report on Forrester.com to download the tool.

Figure 1

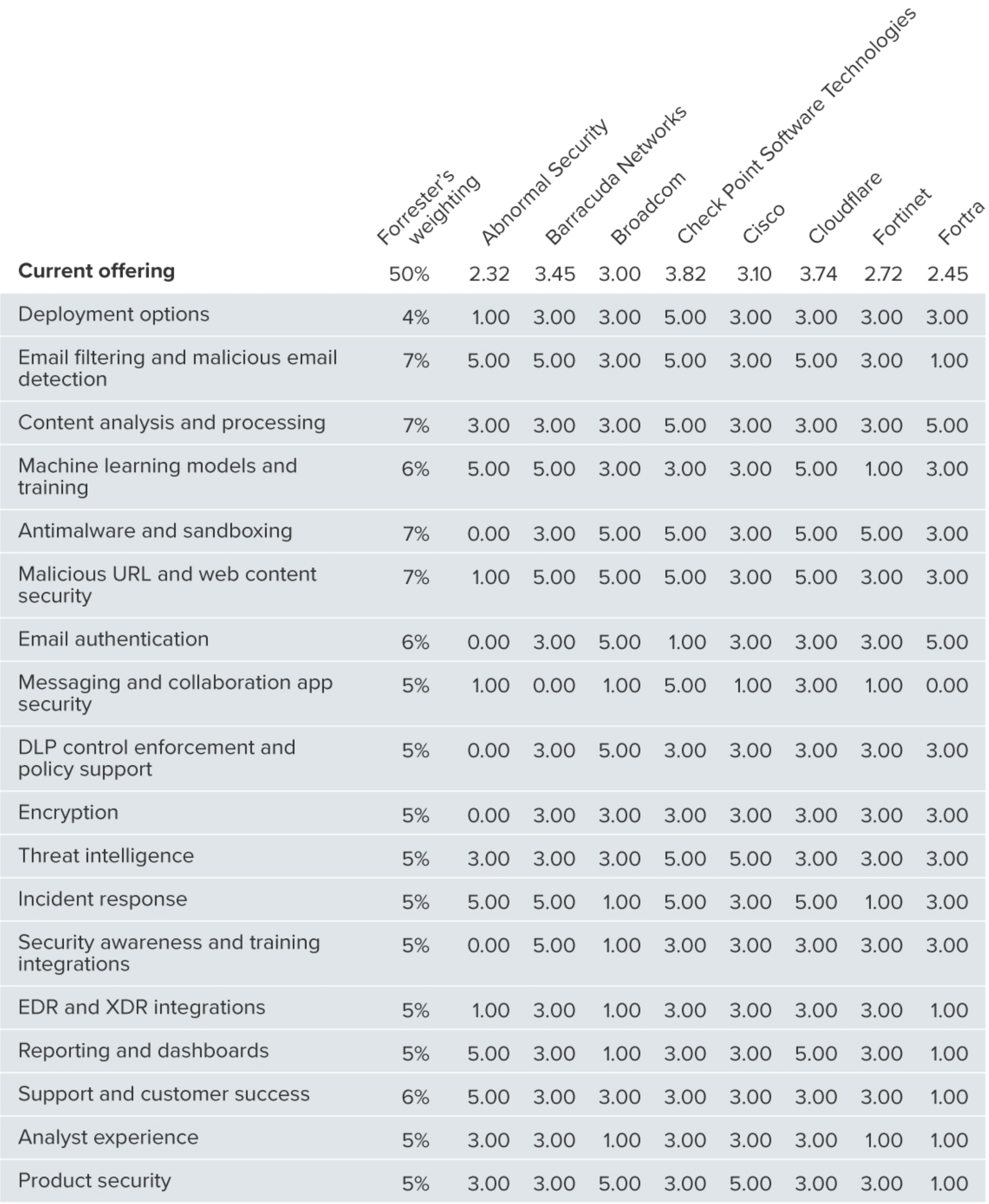
Forrester Wave™: Enterprise Email Security, Q2 2023



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2

Forrester Wave™: Enterprise Email Security Scorecard, Q2 2023



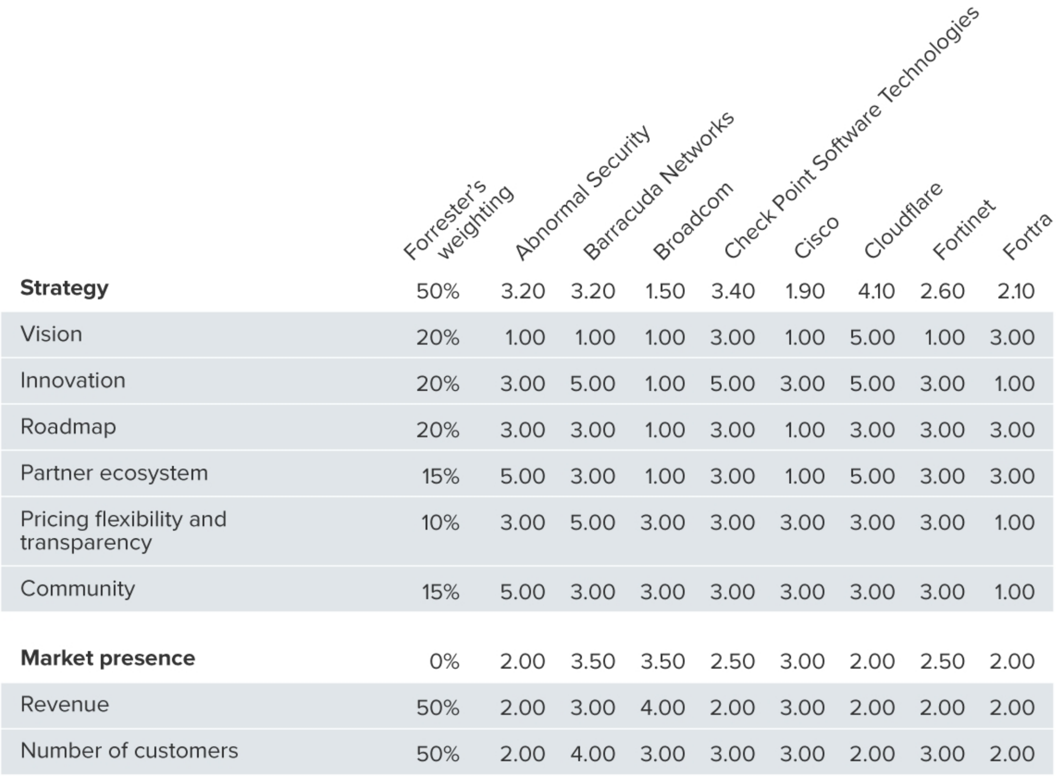
	Forrester's weighting	Abnormal Security	Barracuda Networks	Broadcom	Check Point Software Technologies	Cisco	Cloudflare	Fortinet	Fortra
Current offering	50%	2.32	3.45	3.00	3.82	3.10	3.74	2.72	2.45
Deployment options	4%	1.00	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Email filtering and malicious email detection	7%	5.00	5.00	3.00	5.00	3.00	5.00	3.00	1.00
Content analysis and processing	7%	3.00	3.00	3.00	5.00	3.00	3.00	3.00	5.00
Machine learning models and training	6%	5.00	5.00	3.00	3.00	3.00	5.00	1.00	3.00
Antimalware and sandboxing	7%	0.00	3.00	5.00	5.00	3.00	5.00	5.00	3.00
Malicious URL and web content security	7%	1.00	5.00	5.00	5.00	3.00	5.00	3.00	3.00
Email authentication	6%	0.00	3.00	5.00	1.00	3.00	3.00	3.00	5.00
Messaging and collaboration app security	5%	1.00	0.00	1.00	5.00	1.00	3.00	1.00	0.00
DLP control enforcement and policy support	5%	0.00	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Encryption	5%	0.00	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Threat intelligence	5%	3.00	3.00	3.00	5.00	5.00	3.00	3.00	3.00
Incident response	5%	5.00	5.00	1.00	5.00	3.00	5.00	1.00	3.00
Security awareness and training integrations	5%	0.00	5.00	1.00	3.00	3.00	3.00	3.00	3.00
EDR and XDR integrations	5%	1.00	3.00	1.00	3.00	3.00	3.00	3.00	1.00
Reporting and dashboards	5%	5.00	3.00	1.00	3.00	3.00	5.00	3.00	1.00
Support and customer success	6%	5.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Analyst experience	5%	3.00	3.00	1.00	3.00	3.00	3.00	1.00	1.00
Product security	5%	3.00	3.00	5.00	3.00	5.00	3.00	3.00	1.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Not Licensed For Distribution.

For more information, see the Citation Policy, contact citations@forrester.com, or call +1 866-367-7378.



	Forrester's weighting	Abnormal Security	Barracuda Networks	Broadcom	Check Point Software Technologies	Cisco	Cloudflare	Fortinet	Fortra
Strategy	50%	3.20	3.20	1.50	3.40	1.90	4.10	2.60	2.10
Vision	20%	1.00	1.00	1.00	3.00	1.00	5.00	1.00	3.00
Innovation	20%	3.00	5.00	1.00	5.00	3.00	5.00	3.00	1.00
Roadmap	20%	3.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00
Partner ecosystem	15%	5.00	3.00	1.00	3.00	1.00	5.00	3.00	3.00
Pricing flexibility and transparency	10%	3.00	5.00	3.00	3.00	3.00	3.00	3.00	1.00
Community	15%	5.00	3.00	3.00	3.00	3.00	3.00	3.00	1.00
Market presence	0%	2.00	3.50	3.50	2.50	3.00	2.00	2.50	2.00
Revenue	50%	2.00	3.00	4.00	2.00	3.00	2.00	2.00	2.00
Number of customers	50%	2.00	4.00	3.00	3.00	3.00	2.00	3.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

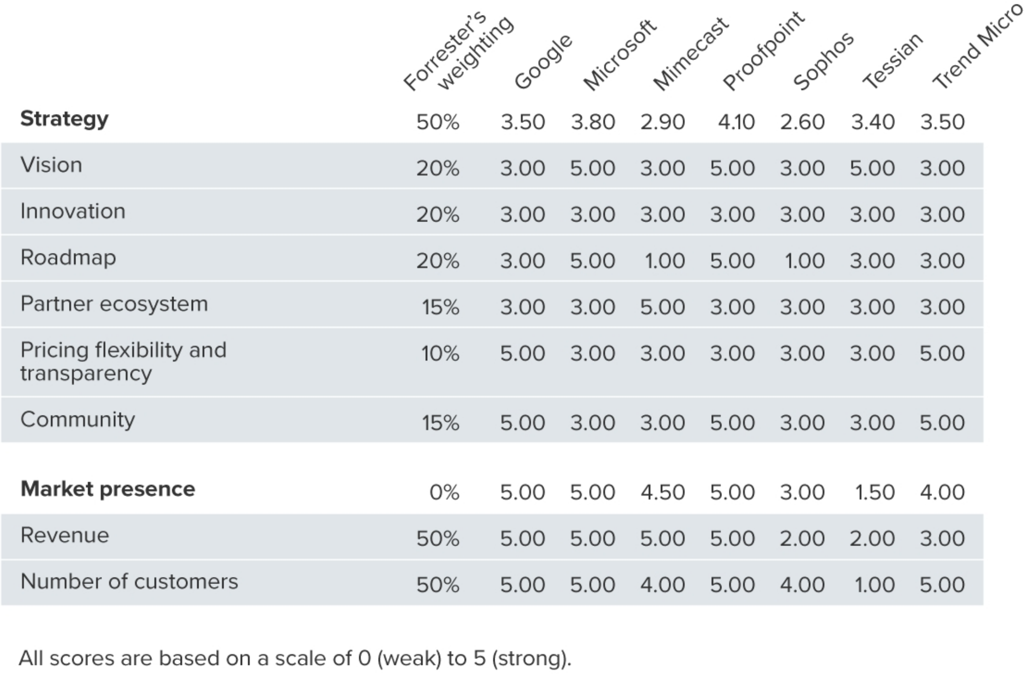
Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Not Licensed For Distribution.

	Forrester's weighting	Google	Microsoft	Mimecast	Proofpoint	Sophos	Tessian	Trend Micro
Current offering	50%	3.26	3.86	3.25	4.06	2.52	2.22	3.46
Deployment options	4%	1.00	1.00	3.00	3.00	3.00	3.00	3.00
Email filtering and malicious email detection	7%	3.00	3.00	3.00	5.00	3.00	3.00	3.00
Content analysis and processing	7%	3.00	3.00	3.00	5.00	3.00	1.00	5.00
Machine learning models and training	6%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Antimalware and sandboxing	7%	3.00	3.00	5.00	3.00	3.00	1.00	3.00
Malicious URL and web content security	7%	5.00	5.00	5.00	5.00	1.00	1.00	3.00
Email authentication	6%	3.00	3.00	5.00	5.00	1.00	0.00	3.00
Messaging and collaboration app security	5%	3.00	5.00	0.00	3.00	1.00	0.00	3.00
DLP control enforcement and policy support	5%	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Encryption	5%	5.00	5.00	3.00	5.00	3.00	0.00	3.00
Threat intelligence	5%	5.00	5.00	3.00	5.00	3.00	3.00	5.00
Incident response	5%	3.00	5.00	3.00	3.00	3.00	3.00	3.00
Security awareness and training integrations	5%	3.00	3.00	3.00	5.00	3.00	3.00	3.00
EDR and XDR integrations	5%	3.00	5.00	3.00	5.00	3.00	3.00	3.00
Reporting and dashboards	5%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Support and customer success	6%	3.00	3.00	3.00	5.00	1.00	5.00	5.00
Analyst experience	5%	3.00	5.00	3.00	1.00	3.00	3.00	3.00
Product security	5%	3.00	5.00	3.00	3.00	3.00	3.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.



	Forrester's weighting	Google	Microsoft	Mimecast	Proofpoint	Sophos	Tessian	Trend Micro
Strategy	50%	3.50	3.80	2.90	4.10	2.60	3.40	3.50
Vision	20%	3.00	5.00	3.00	5.00	3.00	5.00	3.00
Innovation	20%	3.00	3.00	3.00	3.00	3.00	3.00	3.00
Roadmap	20%	3.00	5.00	1.00	5.00	1.00	3.00	3.00
Partner ecosystem	15%	3.00	3.00	5.00	3.00	3.00	3.00	3.00
Pricing flexibility and transparency	10%	5.00	3.00	3.00	3.00	3.00	3.00	5.00
Community	15%	5.00	3.00	3.00	5.00	3.00	3.00	5.00
Market presence	0%	5.00	5.00	4.50	5.00	3.00	1.50	4.00
Revenue	50%	5.00	5.00	5.00	5.00	2.00	2.00	3.00
Number of customers	50%	5.00	5.00	4.00	5.00	4.00	1.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **Proofpoint makes good on its mission to protect people and defend data.** Enterprise email security stalwart Proofpoint, after going private, made moves over the past 18 months to ensure its platform remained relevant with customers' changing email infrastructure as they migrated to cloud email infrastructure environments. It released its CAPES deployment option in 2022, which includes key features like its Very Attacked Person threat reporting and browser isolation, as well as BEC detection and automated remediation capabilities. It also acquired identity threat detection and response vendor Illusive, adding additional protection against ransomware by discovering and remediating identity and privileged identity risks. Proofpoint's roadmap focuses on the threats posed to organizations by their suppliers with preemptive protection against compromised suppliers and BEC attempts via supplier impersonation or account takeover.

  Proofpoint offers expansive inbound and outbound email protection, including DLP and encryption. Reference customers highlighted its threat feeds and its hosted email fraud protection services to monitor incoming and outgoing email for legitimacy. Proofpoint provides out-of-the-box integrations with major identity, detection and response, and security analytics solutions, including Microsoft Defender. It also offers a strong security awareness and training platform. One roadmapped area for improvement evident in the vendor's product demonstration (and noted by reference customers) is the need for Proofpoint to better integrate with itself for a more seamless user reporting and investigation experience. Security and risk pros looking for a fully loaded, infrastructure-and-platform-agnostic email security solution now committed to evolving with its customers should consider Proofpoint.

- **Cloudflare makes a strong entry into email security with its Area 1 acquisition.** Cloudflare's acquisition of Area 1 Security in 2022 brought the content delivery network and cloud security provider both in-line and API-enabled email security capabilities to thwart multichannel phishing attacks. The acquisition furthers Cloudflare's vision of applying Zero Trust principles across all internal and external network, web, and email traffic. Cloudflare holds innovation weeks several times a year to improve capabilities, forge new partnerships, and strengthen platform integrations. Its roadmap includes active simulation (where real attacks against organizations are neutralized and turned into an attack simulation), tighter integration between its email security and cloud access security broker (CASB) offerings, and new capabilities to detect compromised third parties.

  Cloudflare uses its preemptive crawling approach to discover phishing campaign infrastructure as it's being built. Its Small Pattern Analytics Engine (SPARSE) combines multiple machine learning models, including natural language modeling, sentiment and structural analysis, and trust graphs. This is combined with content disarm and reconstruction capabilities to protect users before, during, and after email delivery. Reference customers note the ease and speed of its search capabilities during investigations. Cloudflare's managed email IR and threat hunting service, PhishGuard, includes a unique dashboard element for customers that estimates the time and money saved by thwarting specific monetary fraud attempts. Though it offers proprietary DLP, Cloudflare relies on email infrastructure providers and partnerships for encryption. Cloudflare's Zero Trust approach to email security is a fit for organizations that need easily communicated data and insights in addition to in-depth content analysis and processing.

- **Microsoft delivers communication protection with streamlined analyst experience.** Now a security tech powerhouse, Microsoft's continued investment in security is paying off as it protects end users from attacks that target communication and collaboration environments in addition to email. Email and collaboration security are key elements of Microsoft's extended detection and response (XDR) strategy, adding prevention capabilities to its unified approach to detection, investigation, response, and remediation. Highlights on its roadmap include integrated security training tips and end-user "nudges," enhancing capabilities to disrupt attacks in progress, and further optimizing security operations center (SOC) work and investigation flows.

Backed by trillions of native signals and a massive threat research organization, Defender for Office 365 delivers protection across all native communication and collaboration channels like Teams and SharePoint. It can expand to third-party applications like Slack and Box, but with a less integrated user experience. It also offers comprehensive DLP and easy-to-use email encryption. Though Microsoft supports email authentication protocols, it lacks the hosted and managed authentication management and reporting services offered by several competitors. Reference customers praised the streamlined analyst experience, manual and automated IR capabilities, and simple integrations with third-party tools. However, they dinged Microsoft on inconsistencies in reporting across dashboards and on the number of malicious emails that continue to reach inboxes despite the arsenal of well-regarded detection and response capabilities the vendor brings to bear. Organizations that are all in on Microsoft's security offerings should evaluate Defender for Office 365's tightly integrated, continually improving capabilities.

- **Check Point Software Technologies' novel deployment delivers communication and collaboration protection.** Check Point acquired CAPES vendor Avanan in 2021 and has since focused on integrating email security into its platform, leveraging its native ThreatCloud threat intelligence capabilities to deliver Phishing360 protection across endpoints, browsers, and SaaS applications. Check Point is focused on email security as a key area of growth through 2025 with the goal of, and aligned incentives for, significantly increasing market share. Its roadmap addresses many of the gaps it needs to fill to become a fuller-service email security solution, like Domain-based Message Authentication, Reporting & Conformance (DMARC) monitoring, proprietary security awareness and training, and data residency in more geographies to support regional regulatory requirements.

  Check Point is currently the only enterprise email security vendor to offer an in-line CAPES deployment option that works with both Microsoft 365 and Google Workspace. This configuration provides gateway-like capabilities like spam and graymail filtering, antimalware, and DLP with the power of API-enabled deployments like BEC and internal email protection. It is also one of the only vendors to provide full protection for communication and collaboration applications like Teams, SharePoint, Slack, and Dropbox. Check Point doesn't currently offer its own email authentication capabilities. It does offer email incident response services for user-reported malicious emails, and customers noted the ease of investigations within one screen in the tool. Reference customers tout Check Point's superior efficacy but noted that alerts could use more context. Security and risk pros interested in a move to an API-based solution without some standard secure email gateway (SEG) features should evaluate Check Point Harmony Email & Collaboration.

Strong Performers

- **Trend Micro email security strongly complements its cybersecurity platform.** Trend Micro's Vision One cybersecurity platform brings together its XDR offering with attack surface risk management and includes both SEG and CAPES email security capabilities in its complete but not yet fully integrated solution. Trend Micro plans to extend security orchestration, automation, and response (SOAR) capabilities with its recent announcement to acquire SOC technology provider Anlyz and is currently working to bring its solutions together to enhance analyst experience with minimal jumping between toolsets. On its roadmap, Trend Micro plans to build a proprietary, human risk-focused security awareness and training solution to complement its Phish Insight phishing simulation offering.

  Trend Micro's threat intelligence is bolstered by customers' ability to bring in their own feeds and, through its Zero Day Initiative, a vendor-agnostic bug bounty program that published over 1,600 advisories in 2022. The vendor provides customers with a wide range of AI and heuristic content analysis and processing capabilities as well as malicious URL protection and active content sanitization to strip files of risky elements and offers protection for chat and collaboration in both Microsoft 365 and Google Workspace environments as well as other file-sharing apps. Slack is on its roadmap. Its email security offerings integrate only with its own endpoint detection and response (EDR) and XDR platform, but it does offer API integrations for major security information and event management (SIEM) and SOAR solutions. Reference customers appreciate Trend Micro's global customer support and strong two-way communication. Organizations interested in ensuring email telemetry is fully integrated into their detection and response strategies should consider Trend Micro's suite of offerings.

- **Google's security-by-design approach is regulation aware.** Productivity and collaboration infrastructure giant Google sees email security as one piece of a larger, baked-in cloud and privacy-focused security strategy, built on its BeyondCorp Zero Trust framework. Google is a major supporter of email security protocols and open standards that benefit the greater security community, like the BIMI standard for verified brand logos. It also offers a simple licensing model with options to fit organizations of any size. Google's email and collaboration security roadmap includes further enhancements to its phishing simulation capabilities and tighter integrations with its security operations suite, Chronicle.

  Google recently released an end-to-end, client-side email encryption capability that gives customers, especially those with strict regulatory requirements, full control of their data. Encryption keys are maintained by customers, and data is encrypted prior to moving through Google servers. No add-ons are required to send and receive fully encrypted messages. Google offers contextually rich dynamic content warning banners to assist users in engaging with messages. DLP capabilities cover all Workspace applications, as does protection against malicious links and attachments. Outside messaging and collaboration apps are covered through its Context-Aware Access offering. Integrations with outside EDR and XDR solutions are offered. Reference customers noted dissatisfaction with Google's logging and reporting capabilities, preferring to use third-party security analytics tools for analysis, investigation, and reporting. Google's approach to encryption and its by-design approach to security are a fit for security and risk (S&R) pros in need of privacy-and-compliance-focused email protection for Workspace.

- **Barracuda Networks delivers strong email incident response but a blurry vision.** Seeing the market shifting back in 2016, Barracuda Networks was one of the first legacy SEG vendors to release a CAPES deployment option. However, this option does not yet cover Google Workspace. The vendor also lacks a cohesive vision beyond further improvements and integrations. It is, however, bringing Zero Trust access to its Microsoft 365 CAPES product to better protect organizations from account takeovers and MFA exhaustion campaigns with passwordless authentication via granular device policies. Roadmap highlights include machine learning improvements such as the ability for administrators to tune models themselves; modernizing and unifying the user experience; and extending protection to Google Workspace and collaboration applications like Teams and Slack.

  Barracuda's combined SEG and CAPES offerings deliver phishing and BEC protection, including multiple machine learning models, malware detection and sandboxing, malicious URL protection, and one-click URL blocking of URLs with its incident response capability. The offering does not include browser isolation or protection for messaging and collaboration apps. Barracuda offers proprietary multilanguage security awareness and training capabilities that are well regarded by customers across geographies. Reference customers rave about Barracuda's efficacy — especially against impersonation attempts — and built-in incident response capabilities, including SOAR for fast, intuitive investigation and remediation activities. The vendor offers limited out-of-the-box EDR and XDR integrations beyond its own platform. S&R pros looking to manage both email threat prevention and response in a single solution should consider Barracuda Networks.

- **Mimecast delivers on malicious URL protection but offers a murky roadmap.** Mimecast, a longtime cloud-based SEG vendor, rolled out its CAPES deployment option in mid-2022. Both deployment options are powered by Mimecast's X1 platform encompassing its detection tech, data analytics, threat intelligence, and policy engines. It offers a strong Technology Alliance partner program delivering shared threat intelligence, signals, and telemetry with over 200 applications. Mimecast's vaguely timed roadmap features improvements to awareness training, archiving, DLP, and its DMARC Analyzer to bring its CAPES solution up to parity with its SEG. It also includes the expansion of its CAPES deployment to Google Workspace.

  Mimecast delivers malicious URL protection and web security in a single console and offers a proprietary browser isolation solution, but messaging and collaboration app protections are roadmap items. It delivers a full library of security awareness and training content in addition to its SAFE Phish simulation solution that turns blocked malicious messages into defanged, simulated phishing assessments. Its hosted DMARC reporting tool and services offerings help organizations deploy and maintain optimal configuration. Mimecast offers real-time awareness and training with contextual warning banners via its CyberGraph social graph model that detects anomalies in communication behaviors. Reference customers found Mimecast's reporting capabilities useful and the data easy to export but weren't as bullish on CyberGraph, citing usability and configuration issues that broke workflows. S&R pros looking for help with email authentication who can wait on roadmap item execution should look at Mimecast's email security offerings.

- **Tessian focuses on protecting the human layer but is still building out a full solution.** Tessian got its start protecting end users from themselves with a focus on preventing data loss — both accidental and malicious — in outbound email communication. It has since evolved to offer inbound and outbound protection. Tessian has refined its superior vision to not only focus on protecting the human layer but also to frame email security as a means to elevate security culture within organizations. Roadmap items include expanding DLP capabilities to file-sharing applications; API-integrated remediation orchestration with major SIEM, SOAR, EDR, and XDR players; and expansion of protection to messaging and collaboration applications.

  Tessian's core capabilities center around its Behavioral Intelligence Model (BIM), a social graph that ingests 12 months of historical data for each user to understand typical behavior and spot anomalies. It offers a soft email quarantine with detected anomalies and delivers real-time security coaching to end users in the form of dynamic, contextual warning banners. Though Tessian provides more capabilities than other CAPES vendors, it lacks malware sandboxing, browser isolation, web security, encryption, and email authentication support. Reference customers are happy with Tessian's support and willingness to customize features as well as its easy-to-use interface, but they knock elements of its ML-driven solution, namely its user risk scoring for being overly generic, and hard and soft quarantine inconsistencies. S&R pros interested in linking email security with security coaching and culture should consider Tessian as an additional (human) layer of protection.

- **Abnormal Security is the added protection you need if you don't need anything else.** Abnormal Security was born out of the need for protection against the BEC, advanced phishing campaigns, and internal communication threats traditional SEGs were not catching. This extra layer of protection brought the CAPES vendor to market prominence, but its vision remains firmly grounded in its current capabilities with only limited plans to add capabilities covered by email infrastructure providers. Abnormal takes a collaborative approach to channel partnerships and forms strong technical partnerships, like the recently announced bidirectional integration with CrowdStrike for greater account takeover protection and the strategic partnership with Microsoft that includes co-selling and joint marketing initiatives. Abnormal plans to add to its core capabilities with a roadmap that includes protection of communication, collaboration, and SaaS applications, as well as its own form of DLP and security awareness and training (SA&T).

Abnormal's single deployment option absorbs six months of email behavior from end users, learns what normal looks like, and organizes the collected signals into four knowledge bases — application, vendor, tenant, and people. Its behavioral AI engine is continuously trained by the malicious emails it blocks and by Detection 360°, its direct feedback loop for false positive and negative reporting. Customers praise Abnormal for its superior ability to block malicious email from inboxes and its ability to combat account takeovers and compromised third-party vendors, but this is currently its narrow focus. S&R pros heavily invested in the native capabilities of their email security infrastructure providers — or those planning to keep an SEG for other critical forms of malicious email, file, and attachment detections — should evaluate Abnormal Security.

- **Fortinet delivers email security in its platform but doesn't make it easy.** Fortinet's vision of email security going beyond email remains unchanged since 2021 and is now limiting. Its definition of "beyond email" includes security tooling like EDR, XDR, CASB, and SIEM/SOAR but not the applications users employ to communicate and collaborate. The vendor's focus is on furthering integration of FortiMail into its Security Fabric, made up of the aforementioned tooling plus threat intelligence and managed security services. Notably, Fortinet was the only vendor in this evaluation to place emphasis on its hardware email security appliances. On its lengthy roadmap, Fortinet plans to expand its CAPES deployment option to Google Workspace, offer hosted DMARC monitoring, enhance content analysis with a new image engine and QR code scanning, and further integrate with its own platform.

  Fortinet offers standard capabilities for email filtering and malicious email detection but is not transparent in its communication of how its ML models are trained. It offers integrations with sandbox and BIT, but EDR and XDR integrations beyond its own platform are limited. Content disarm and reconstruction and URL protection are offered in the middle and top pricing tiers, and a proprietary phishing simulation tool is available as an add-on. Usability remains an issue with cluttered dashboards and outdated user interfaces. Additionally, reference customers noted difficulty in configuring incident response capabilities and unintuitive interfaces requiring multiple drill-downs to complete tasks. Fortinet is a fit for S&R pros invested in the Fortinet platform who need managed email security services, those at smaller enterprises, or organizations still in need of on-premises or hybrid deployments that include physical or virtual appliances.

Contenders

- **Sophos continues to build out its email security capabilities but still needs some basics.** Cybersecurity platform provider Sophos' vision is to enhance the SOC analyst experience across its product portfolio. The vendor plans to ensure email security and telemetry, in combination with its MDR and XDR offerings, as part of that strategy. Yet its roadmap features a list of standard items like future integration with Google Workspace, on-demand email claw-back, DMARC reporting, and AI-enabled behavioral profiling through a social graph model.

  Sophos offers standard filtering and malicious email detection capabilities for inbound protection. Its outbound protection includes proprietary DLP and encryption capabilities. Insight into Sophos' machine learning models is limited, as is support for web security. Sophos Phish Threat provides phishing simulations and security awareness training in the console. Analysts can deliver targeted training to risky users via integrations with Azure AD. Its email security offering integrates only with Sophos platform technologies, not third-party solutions. Dashboards provide good detail, and reference customers noted the ease of setup and policy creation in the tool. References also remarked on middling customer support and a need for encryption improvement. S&R pros leveraging their email infrastructure provider's basic protections — and those who are short-staffed — should consider Sophos email security as part of a larger managed security services relationship.

- **Cisco brings its offerings into the modern age but relies heavily on third parties.** Longtime SEG player Cisco released its Email Threat Defense (ETD) solution in 2020, which adds a CAPES deployment option for Microsoft 365, and integration with its SecureX XDR platform in 2023. The vendor aims to keep legacy SEG customers as they migrate to new cloud email security infrastructure environments. Email security and the associated telemetry are a key element of Cisco's XDR story. Its staid vision for email security, however, focuses on becoming best-in-class by improving detections and on aggressive pricing to encourage retention. Cisco plans to internally develop capabilities formerly or currently supported by OEM relationships and strategic partnerships. Its roadmap includes further modernization like automated abuse mailbox monitoring, supply chain compromise monitoring, and rolling out a new detection every quarter.

  Cisco ETD is backed by its Talos threat intelligence feeds and message content analysis. Transparency about model training is lacking despite the thorough and easily navigable Cisco Trust Center for product security information. Reference customers note SecureX's usability, with orchestrated remediation actions that can easily be taken within the ETD interface. ETD does not integrate with third-party EDR or XDR solutions yet uses third parties for several key capabilities, like hosted DMARC through a partnership with dmarcian and SA&T and DLP through OEM relationships. Messaging and collaboration protection is limited to Cisco's CASB offering under Cisco Umbrella. S&R pros in predominantly Cisco shops looking to upgrade legacy SEG appliances should evaluate Email Threat Defense integrated with SecureX XDR.

- **Fortra is combining acquisitions into a comprehensive solution but isn't there yet.** Fortra, the tech provider formerly known as HelpSystems, made a series of email security acquisitions over the past two years. Its vision is to stitch together a comprehensive email security solution from Clearswift (SEG), Agari (CAPES and email authentication), Terranova Security (SA&T), and PhishLabs (threat intelligence). Fortra's plan is to move these acquisitions from separate solutions, to single sign-on, to a unified user interface within the next 12 months. This vision is also the focus of Fortra's innovation efforts and roadmap.

  Fortra's standout capability, in its collection of converging solutions, is its email authentication technology and services under Agari DMARC Protection. This helps customers get to optimal configuration and investigate causes of improper configuration in customer and third-party environments. Agari DMARC Protection offers threat feeds for domain impersonation that can be sent to PhishLabs for takedown, and Agari Phishing Defense delivers machine learning-based trust scoring and attack classifications for messaging with search-and-destroy capabilities. Additionally, Clearswift offers largely standard content analysis and processing, with the exception of its anti-steganography capabilities which keep data from being exfiltrated by being embedded in pictures or other types of files. The portfolio of loosely coupled solutions lacks a cohesive analyst experience and a central dashboard for reporting and offers limited EDR and XDR integrations. Forrester was unable to reach reference customers Fortra provided for this evaluation. S&R pros at organizations in need of help with email authentication should investigate Fortra's converging email security offering.

- **Broadcom has solid outbound protection but is on a long road to a modern offering.** Symantec was once an email security titan. Its acquisition by Broadcom, however, stymied the product suite's growth and innovation, leaving it to languish as competitors, some of which were also acquired, moved forward with the development of new capabilities and deployment options. The vendor's weak vision is to start offering the capabilities, such as CAPES deployments and advanced phishing and BEC protection, that customers are looking for in 2023. Broadcom's roadmap includes several incremental improvements, including improved URL risk scoring, better policy controls, and more granular rules to enforce domain age policies.

Broadcom offers standard content analysis and processing, antimalware and sandboxing, and malicious URL protection, including web security and browser isolation. It also offers comprehensive enterprise and email DLP and delivers easy-to-use email encryption through its partnership with Echoworx. Additional partnerships fill key functionality gaps, including email fraud protection powered by a partnership with email authentication vendor Valimail. The Symantec Security View dashboard, which brings together telemetry from its email security, CASB, and DLP products, is viewed through security analytics vendor Splunk. Reference customers cite poor efficacy and outdated consoles but expressed appreciation for the periodic health check reports to ensure tooling is properly configured and that customers are getting the most out of their investment in the product. S&R pros reliant on Broadcom's comprehensive DLP product should assess the vendor's Symantec Email Security offering.

Evaluation Overview

We grouped our evaluation criteria into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include content analysis and processing, machine learning models and training, malicious URL detection and web content security, antimalware and sandboxing, and email authentication.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product vision, innovation, roadmap, and community.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's revenue and number of customers.

Vendor Inclusion Criteria

Each of the vendors we included in this assessment has:

- **Global product revenue over $30 million USD.** The vendor has at least $30 million in email security revenue from two or more geographies.

- **A productized commercial offering.** The offering can be delivered as a secure email gateway (SEG) or a cloud-native, API-enabled email security solution (CAPES), but it cannot be a custom managed or professional service. The majority of vendor revenue must come from enterprise sales, not OEMs or MSPs. The vendor must offer a product version of the solution that was generally available prior to February 23, 2023. Forrester only evaluated capabilities released and generally available to the public by this cutoff date.
- **Significant interest from Forrester customers.** Forrester considers the level of interest and feedback from our clients based on our various interactions, including inquiries, advisory, and consulting engagements.

Supplemental Material

Online Resource

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by March 16, 2023 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with our vendor review policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with our vendor participation policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the integrity policy posted on our website.

FORRESTER

We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

Learn more.

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

Learn more.

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

Learn more.

FOLLOW FORRESTER

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com