The Forrester Wave™: Enterprise Email Security, Q2 2021

The 15 Providers That Matter Most And How They Stack Up

by Joseph Blankenship and Claire O'Malley

May 6, 2021

Why Read This Report

In our 25-criterion evaluation of enterprise email security providers, we identified the 15 most significant ones — Agari, Area 1 Security, Barracuda Networks, Broadcom Symantec, Cisco, Forcepoint, Fortinet, Google, Microsoft, Mimecast, Proofpoint, SonicWall, Sophos, Trend Micro, and Zix — 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.

The Forrester Wave™: Enterprise Email Security, Q2 2021

The 15 Providers That Matter Most And How They Stack Up

by Joseph Blankenship and Claire O'Malley
with Stephanie Balaouras, Allie Mellen, Shannon Fish, and Peggy Dostie
May 6, 2021

Email Gateways Are Pivoting To Support The Infrastructure Behemoths

Forrester's 2021 Wave evaluation of the email security market revealed that secure email gateways (SEGs) are slowly becoming dinosaurs as customers turn to the native security capabilities of cloud email infrastructure providers like Google and Microsoft. Security pros supplement these native capabilities with third-party solutions like cloud-native API-enabled email security (CAPES) solutions. Email security vendors (including SEG providers) respond by expanding API integrations to integrate with email infrastructure vendors to deliver complementary capabilities and an additional layer of protection. Some geographies, like Germany, are increasingly skeptical of relying on US-based cloud providers for communications and security, however. As a result, vendors are delivering services in customers' geography of choice, allowing customers to choose where their data resides. This negates most use cases for on-premises deployments, as hardware appliances are no longer recommended for anything but edge cases. Further, the recent attacks targeting on-premises Microsoft Exchange Server vulnerabilities are likely to drive more organizations to the cloud.

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

- **Supplement their infrastructure provider's capabilities with API integrations.** Infrastructure behemoths Google and Microsoft have been working hard to both expand their overall security suite and strengthen native email security capabilities like content analysis, malicious email detection, and antimalware. However, for more protection, many customers are purchasing solutions to supplement their email infrastructure provider's capabilities so that their customers can fully protect their inboxes. CAPES vendors and SEG providers deliver capabilities like antiphishing, business email compromise (BEC) prevention, and data protection via API integrations with infrastructure providers. This approach enables a best-of-both-worlds strategy for email security.
- **Integrate with other security solutions in customer environments.** The best email security solutions integrate across customer environments with solutions like EDR, web content security (including browser isolation), and security awareness and training (SA&T). Some vendors include email security as part of their extended detection and response (XDR) strategy, which tightly integrates endpoint detections with telemetry from other security tools, including email. Email

FORRESTER®

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

security has been a surprisingly powerful integration in the XDR ecosystem, as it links malware seen on the endpoint with the phishing attacks from which they originate. Leading email security solutions also work with SOAR tools or include automated workflows to support incident response actions to save time in the SOC and accelerate remediation.

- **Extend protection to also defend messaging applications.** Messaging applications like Google Chat, Microsoft Teams, Skype for Business, and Slack have become as essential to organizations as email. As a consequence of the pandemic, many users are working remotely, and messaging applications offer them instant communication and a sense of community. The most differentiated email content security solutions today expand their protection to go beyond the inbox and also protect the communications within these messaging applications.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our reports on enterprise email security providers.

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 Figure 1 and see Figure 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 2021

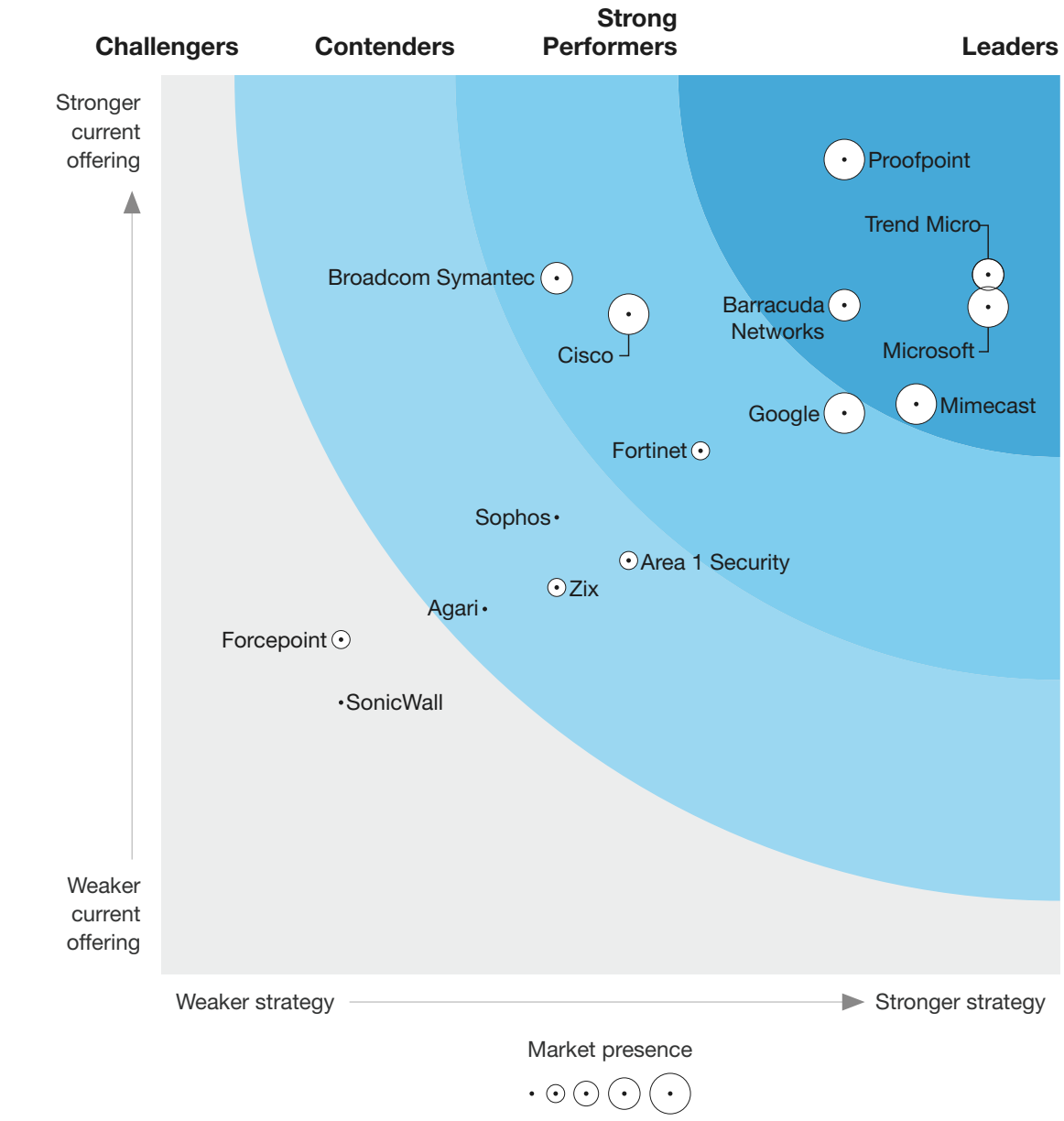

FIGURE 2 Forrester Wave™: Enterprise Email Security Scorecard, Q2 2021

	Forrester's weighting	Agari	Area 1 Security	Barracuda Networks	Broadcom Symantec	Cisco	Forcepoint	Fortinet	Google	Microsoft	Mimecast
Current offering	50%	2.03	2.30	3.72	3.87	3.67	1.86	2.91	3.12	3.71	3.17
Deployment options	5%	3.00	3.00	5.00	5.00	5.00	5.00	5.00	1.00	1.00	1.00
Email filtering	30%	1.65	3.40	3.30	4.80	3.70	1.20	2.80	4.20	3.00	4.10
Threat intelligence	5%	3.00	1.00	3.00	3.00	5.00	3.00	3.00	3.00	5.00	1.00
Data leak prevention	10%	0.00	0.50	3.00	5.00	3.00	3.00	2.00	1.00	3.00	3.00
Integrations	10%	1.50	2.25	2.50	3.50	2.80	2.00	2.70	2.80	3.10	3.40
Reporting	5%	3.00	1.00	3.00	3.00	3.00	1.00	3.00	3.00	3.00	3.00
Incident response	10%	3.00	3.00	5.00	5.00	5.00	1.00	3.00	3.00	5.00	3.00
Performance and operations	10%	1.80	3.00	3.80	3.80	3.80	3.00	3.00	3.80	5.00	3.00
Support and customer success	15%	3.00	1.00	5.00	1.00	3.00	1.00	3.00	3.00	5.00	3.00
Strategy	50%	1.80	2.60	3.80	2.20	2.60	1.00	3.00	3.80	4.60	4.20
Product strategy	80%	2.00	2.00	4.00	2.00	2.00	1.00	3.00	4.00	5.00	4.00
Pricing	20%	1.00	5.00	3.00	3.00	5.00	1.00	3.00	3.00	3.00	5.00
Market presence	0%	1.00	2.00	3.50	4.00	5.00	1.50	2.00	5.00	5.00	4.50
Installed base	50%	1.00	3.00	5.00	5.00	5.00	1.00	3.00	5.00	5.00	5.00
Revenue	50%	1.00	1.00	2.00	3.00	5.00	2.00	1.00	5.00	5.00	4.00

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

FIGURE 2 Forrester Wave™: Enterprise Email Security Scorecard, Q2 2021 (Cont.)

	Forrester's weighting	Proofpoint	SonicWall	Sophos	Trend Micro	Zix
Current offering	50%	4.53	1.51	2.54	3.89	2.15
Deployment options	5%	5.00	3.00	1.00	5.00	1.00
Email filtering	30%	4.60	1.70	3.30	4.00	2.10
Threat intelligence	5%	5.00	3.00	1.00	3.00	1.00
Data leak prevention	10%	4.00	2.00	1.00	3.00	4.00
Integrations	10%	4.70	1.00	2.50	3.10	0.75
Reporting	5%	3.00	1.00	1.00	1.00	3.00
Incident response	10%	5.00	1.00	3.00	5.00	3.00
Performance and operations	10%	3.80	1.00	3.00	3.80	0.40
Support and customer success	15%	5.00	1.00	3.00	5.00	3.00
Strategy	50%	3.80	1.00	2.20	4.60	2.20
Product strategy	80%	4.00	1.00	2.00	5.00	2.00
Pricing	20%	3.00	1.00	3.00	3.00	3.00
Market presence	0%	5.00	1.00	1.00	4.00	2.00
Installed base	50%	5.00	1.00	1.00	5.00	3.00
Revenue	50%	5.00	1.00	1.00	3.00	1.00

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

Vendor Offerings

Forrester included 15 vendors in this assessment: Agari, Area 1 Security, Barracuda Networks, Broadcom Symantec, Cisco, Forcepoint, Fortinet, Google, Microsoft, Mimecast, Proofpoint, SonicWall, Sophos, Trend Micro, and Zix (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Agari	Agari Bundle 1
Area 1 Security	Area 1 Horizon
Barracuda Networks	Barracuda Total Email Protection
Broadcom Symantec	Symantec Email Security Solution
Cisco	Cisco Secure Email 13.7
Forcepoint	Forcepoint Email Security 8.5.4
Fortinet	FortiMail 6.4.3
Google	Google Workspace
Microsoft	Microsoft Defender for Office 365
Mimecast	Mimecast Email Security with Targeted Threat Protection
Proofpoint	Proofpoint Email Security
SonicWall	SonicWall Email Security 10.0.0.9 & SonicWall Cloud App Security 2.6.25
Sophos	Sophos Email Security
Trend Micro	Trend Micro Email Security
Zix	Zix Email Security & Compliance Suite

Vendor Profiles

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

Leaders

- **Trend Micro delivers advanced, integrated email security.** Trend Micro offers a broad portfolio of security solutions, including network, cloud, and endpoint security. Its Apex Central provides centralized monitoring for the vendor's endpoint, email, and other solutions. Email security is part of Trend Micro's aggressive Vision One XDR strategy, which combines endpoint, network, and email for threat detection and response. Trend Micro delivers email security through the cloud, virtual appliances, and hybrid deployments.

Reference customers noted Trend Micro's easy integration with Microsoft 365, security suite tools, and variety of malicious traffic detections and strong points. They mentioned reporting and frequent, confusing branding changes as weaknesses. Enterprises seeking an email security solution with strong endpoint integration (especially for Trend Micro-protected endpoints) and IR capabilities should evaluate Trend Micro.

- **Proofpoint differentiates with its "Very Attacked People" capabilities.** Proofpoint has a reputation as an email security vendor, although it has aggressively expanded via acquisition to become a broader security portfolio vendor. The vendor provides inbound email filtering, phishing and BEC defense, Domain-based Message Authentication, Reporting and Conformance (DMARC) authentication, extensive DLP and encryption capabilities, and SA&T. These capabilities are bundled by tiers, with more-advanced capabilities available in higher-priced tiers. Proofpoint also integrates with messaging applications like Google Chat, Microsoft Teams, and Slack. Proofpoint's unique Very Attacked People concept illuminates who the most targeted people are in a client organization, to provide additional protections or target them for extra training. This focuses protection where it's most needed. The vendor supports cloud, on-premises appliances (physical or virtual), and hybrid deployments.

  Proofpoint reference customers mentioned customer service and support, along with a fast implementation, as strengths. In addition, they cited the solution's advanced threat capabilities and stability as strong suits. Client references stated that decreased or slowed innovation, "price creep," and expensive add-ons were weaknesses. One reference pointed out that "difficult integration between their latest acquisitions and core products" is an issue, which may explain the slowed pace of innovation. Enterprises seeking a full-featured email security solution that can deploy on-premises or in the cloud should consider Proofpoint.

- **Microsoft continues to strengthen its email security capabilities.** Tech titan and email infrastructure provider Microsoft continues to bolster its expanding portfolio of security solutions. Enterprises have been migrating from their on-premises email solutions (mostly Exchange) to Microsoft 365 with increasing speed in the past couple of years, making it attractive for them to adopt Microsoft's native security controls. Microsoft Defender for Office 365 (MDO) delivers a wide array of security capabilities, which include inbound filtering, phishing defense, antimalware, DLP, encryption, and SA&T. These features are bundled in Microsoft's pricing packages — EOP, MDO (P1 and P2), and E5 — with the more-advanced features offered in the higher-cost tiers. MDO integrates with other Microsoft solutions like Microsoft Defender (EDR) and Azure Sentinel (SIEM). It's also part of the vendor's XDR strategy. As a cloud-based email infrastructure service, the solution is only available via the cloud and only supports Microsoft 365 customers.

  Client references noted the integration with other Microsoft solutions as a key strength. They also cited the vendor's overall strategy, product evolution, and incident response capabilities as strengths. Reference customers called out reporting, rules customization, and the nonintuitive UI

as weaknesses. In addition, they remarked that the lack of integration with third-party solutions is a weak spot. Customers of all sizes, especially those heavily invested in Microsoft solutions, seeking embedded security controls as part of their email infrastructure, should evaluate Microsoft.

- **Barracuda Networks offers a unified approach to email security.** Barracuda Networks offers a product portfolio that includes integrated solutions for email security, cloud backup, email archiving, DMARC authentication, SA&T, and web security. Barracuda Networks Sentinel uses data science techniques to detect phishing and BEC attacks. The vendor's SA&T solution, PhishLine, analyzes customers' historical email data to learn user behaviors and drive targeted training content. Barracuda Networks delivers email security via multiple form factors, including SaaS and as an on-premises appliance (physical and virtual). The vendor integrates with Microsoft 365 via API for detection and remediation but doesn't currently support Google.

  Barracuda Networks customer references indicated Barracuda Networks' customer service and reporting as strengths. One reference commented that Barracuda Networks' incident response feature "is a superior product for the continuous remediation option provided as well as the straightforward process for starting remediations." Reference customers called out Barracuda Networks' slow development lifecycle and pricing as weaknesses. Small and midsize enterprises seeking an email security provider with an extensive security portfolio should look at Barracuda Networks.

- **Mimecast expands its email security capabilities to the enterprise.** Mimecast offers an extensive email security portfolio that includes security awareness and training, DMARC authentication, DLP, and encryption. The vendor bundles these capabilities into packaged solutions. Extensions like web security and browser isolation are available as add-ons. Mimecast currently doesn't integrate with or offer any protections for customers messaging applications. The acquisition of MessageControl in 2020 provides API integration into Microsoft 365 for additional message inspection. Its security awareness and training materials go beyond the traditional phishing education and cover the entire swath of security threats that are presented in an engaging manner. Mimecast delivers exclusively through the cloud and doesn't support on-premises deployments.

  Mimecast has long been known for delivering email security for the midmarket. Client references indicated Mimecast's efficacy, ease of use, and pricing as strengths. They noted Mimecast's reporting and slow response as weaknesses. Enterprises of all sizes looking for a provider that can natively address multiple email controls, especially security awareness and training, should consider Mimecast.

Strong Performers

- **Google embeds security and focuses on ease of use.** Google is an email infrastructure provider that provides email security for users of its cloud-based Google Workspace service. Security capabilities like malicious email filtering are built into the service by default, and enterprise features like sandboxing and DLP are available through Google Workspace offerings. Simplicity is the

name of the game as the vendor seeks to make the solution as easy to operate as possible while delivering effective email defense. Protection for messaging apps is limited to Google Chat, and integrations are largely limited to other Google solutions. As a cloud-delivered service, the security features are only available through the cloud.

Google reference customers called out Google's usability and built-in security features as strengths. They noted Google's over focus on simplicity and difficulty navigating the large organization as weaknesses. One reference remarked that the "lack of visibility behind the Google curtain" is an issue. The emphasis on ease of use makes the solution ideal for small, less-mature security teams but "leaves power users behind." Reference customers also indicated the DLP capabilities were not sophisticated enough for their needs. Small and midsize enterprises and educational institutions seeking an email infrastructure provider that's easy to use and features built-in security controls should consider Google.

- **Cisco offers email security as part of its broad security portfolio.** Networking and security behemoth Cisco has long delivered SEG as part of its security portfolio. Cisco Secure Email provides a mix of native and OEM capabilities for phishing defense, authentication, DLP, encryption, and SA&T. The vendor integrates across its portfolio, including its EDR solution, with its SecureX orchestration capability. SecureX also integrates with third-party SOAR tools to automate aspects of investigation and response. Cisco Secure Email is available in multiple formats including cloud, virtual, on-premises hardware, and as a hybrid deployment.

  Client references appreciate Cisco's ability to easily integrate with the rest of their security suite and security technology investments. One reference stated, "The combination of solutions from Cisco Systems has provided us a very effective and easy-to-use security solution." They also note the effectiveness of Cisco's Talos threat intelligence. However, client references noted Cisco's difficult deployment and nonstandard logging (which the vendor has recently addressed) as areas of weakness. The vendor lacks coverage for messaging apps and depends on partnerships for many capabilities. Large enterprises, especially those invested in other parts of the Cisco Systems portfolio, should consider Cisco for email security.

- **Broadcom Software: Symantec delivers email defense for enterprises.** Email security is part of the vendor's Broadcom Software Group, which delivers a suite of Symantec security capabilities. The email security solution integrates with other Symantec capabilities like web security gateway, browser isolation, EDR, and DLP. Symantec builds on its AV vendor heritage, offering multiple native AV engines with proprietary AV signatures to dissect and identify malicious emails. The vendor delivers email security in multiple form factors, including cloud, on-premises appliances, software, and hybrid deployments.

  Broadcom's acquisition of Symantec initially caused significant disruption for many legacy Symantec customers, but the dust has finally settled, at least for the vendor's enterprise customers. Client references appreciate Symantec's wide portfolio but note education programs as a weakness. Reference customers also call out customer service and slow response to issues

due to the Broadcom acquisition and transition as pain points. Reference customers noted a lack of visibility into the business and product roadmap as concerns. Large enterprises, especially those invested in other Broadcom solutions, should investigate Broadcom Symantec.

- **Fortinet has an email security vision that goes beyond email.** Fortinet is best known for its firewalls and network security solutions, but the vendor's vast portfolio also includes email, endpoint, and cloud security as well as security analytics. Its email security solution, FortiMail, connects to other Fortinet capabilities, like FortiEDR and FortiSandbox, via the Fortinet Security Fabric. FortiMail works with the vendor's web security solutions, including its FortiIsolator browser isolation product. Fortinet delivers email security as on-premises appliances, virtual machines, cloud SaaS, and direct API integration into Microsoft 365, which allows for post-delivery message scan and claw back of messages.

  Fortinet client references lauded Fortinet's product ecosystem and ease of installation as strengths. They also praised the vendor about its support, value received, and feature quality for the price. Reference customers noted Fortinet's dated, visually unappealing portal, and difficulties with administration as weak spots. Enterprises looking for an email security vendor with a big-picture threat landscape focus and those invested in other Fortinet security solutions should consider Fortinet.

Contenders

- **Area 1 Security supports multiple deployment options to stop phishing.** Area 1 Security can deploy as a SEG or act as a CAPES vendor, sitting alongside the native protections of the email infrastructure provider. The solution can be deployed as a gateway, behind the gateway, via API, as a journaling service, and hybrid (a combination of these). The vendor focuses on inbound protection and doesn't deliver outbound capabilities like DLP. The vendor detects and filters out phishing attacks using a small pattern analytics engine, SPARSE, which uses a combination of factors to detect malicious email. It also uses data science models to scan message content for context. For emails that make it through to the inbox, Area 1 Security offers URL rewriting for time-of-click analysis and has a recursive DNS service to stop users from visiting malicious sites. Area 1 Security deploys as a cloud-native solution and doesn't support on-premises deployments.

  Client references called out Area 1 Security's phishing protection as a strength. However, they also noted the console and reporting as areas of weakness. The vendor doesn't have a native SA&T solution or any partnerships that connect its customers to those resources. Email customers seeking extra phishing capabilities with extensive content analysis should engage with Area 1 Security.

- **Sophos builds on its endpoint security foundation.** Sophos delivers email security as part of its portfolio that includes next-gen firewalls, web filtering, and endpoint security — each of which integrate with Sophos Email Security. Sophos Central is a SaaS-based console for managing all these solutions. The vendor's content processing capabilities are native and use natural language processing to examine the tone of emails, including the body and subject line, to determine

maliciousness. Phish Threat, the vendor's SA&T solution, is customizable and expands beyond the traditional phishing education and tests. Sophos delivers email security as a SaaS and doesn't support on-premises deployment.

Client references mentioned Sophos' endpoint protection and sandboxing as strengths. They called out Sophos' technical support responsiveness, reporting, and UI as desired areas for improvement. Sophos doesn't integrate with broad DLP or encryption solutions and lacks API integrations for email infrastructure providers like Google and Microsoft, although those are on the roadmap. SMB organizations, small enterprises, and those invested in Sophos elsewhere in their security stack should look at Sophos.

- **Zix sustains email security with easy-to-use encryption.** Zix has a legacy of delivering email encryption as an OEM partner for other vendors and as a standalone solution. With acquisition of AppRiver in 2019, the vendor now delivers a suite of productivity and security solutions for small and midsized enterprises. The vendor's email solutions include email archiving, email threat protection, and encryption. Zix delivers email security as a SaaS or can deploy its encryption capabilities on-premises as a virtual appliance.

  Client references mentioned excellent support and easy integrations as Zix strengths. They noted a tedious setup and a confusing administration portal as weaknesses. Zix doesn't have native or integrated security awareness and training capabilities or integrations, web content security integrations, or any EDR capabilities or integrations. SMBs seeking an easy-to-use email security solution and enterprises looking for a strong email encryption solution should seek out Zix.

- **Agari defends against phishing and authenticates with DMARC.** Unlike many of the other vendors we evaluated, Agari isn't a SEG and doesn't deliver all of its traditional capabilities. Instead of acting as a gateway, Agari supplements email infrastructure providers' security capabilities as a CAPES vendor by adding an extra protection layer to prevent phishing and business email compromise (BEC) attacks. The extra layer comes from the vendor's DMARC capabilities, which includes record hosting and support for multiple outbound signing methods (DMARC, SPF, DKIM, and BIMI) as well as proprietary phishing detection capabilities. Agari Phishing Defense combines data science and authentication to identify valid and malicious emails. Once detected, the solution can remove malicious emails from the inbox. Agari delivers as a cloud service via API integration with email infrastructure providers or deployed on-premises as a virtual appliance.

  Client references noted Agari's strong customer community, understanding of the threat environment, and DMARC knowledge as strengths. They indicated that Agari's reporting has room for improvement, especially for reports to senior leadership. Organizations seeking a vendor with strong email authentication expertise and advanced phishing protection capabilities should consider Agari.

Challengers

- **Forcepoint pursues an integrated portfolio approach.** Forcepoint delivers a suite of security capabilities that include email, web, DLP, CASB, and UBA. Forcepoint Email Security is available as a standalone package or can be bundled with the vendor's other solutions for web filtering, data, and user protection. The vendor delivers robust, integrated web filtering capabilities along with browser isolation as add-ons to protect users from malicious websites. Forcepoint offers a full range of deployment options and can fully integrate with Google email or Microsoft email infrastructure.

  Forcepoint was spun out of parent company Raytheon and divested to Francisco Partners, an investment firm in late 2020, and it's too early to tell what impact the change in ownership will have on the email security solution. Forrester was unable to obtain feedback from Forcepoint reference customers for this Forrester Wave. While the solution integrates well with other Forcepoint solutions, it doesn't provide protection for messaging solutions or integrate with third-party EDR and SOAR tools and lacks APIs. Forcepoint does, however, have API integrations into email infrastructure providers like Google and Microsoft. Enterprises seeking an integrated suite for DLP, web filtering, and email security should evaluate Forcepoint.

- **SonicWall delivers email security with an easy-to-use UI.** SonicWall, best known for its firewalls, provides inbound and outbound email security with an easy-to-use UI that is especially appealing for SMBs and smaller security teams. The vendor prides itself on being easy to set up and administer. SonicWall includes UBA to detect suspicious user behavior as a feature. The solution provides time of click protection for malicious URLs but doesn't integrate with web content security providers or BIT. The vendor delivers email security via cloud, software, and on-premises appliances. SonicWall also offers API integration with infrastructure providers for email scanning, search, and remediation.

  Client references cite knowledgeable staff, flexible configuration, and the licensing model as SonicWall strengths. However, reference customers mentioned a limited international presence, complexity, and a lack of full enterprise support as areas that need improvement. Small and midsize enterprises and local governments seeking easy-to-use email security with Google and Microsoft integrations should investigate SonicWall.

Evaluation Overview

We evaluated vendors against 25 criteria, which we grouped 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 email filtering, threat intelligence, data leak prevention, integrations, reporting, incident response, performance and operations, and support and customer success.

- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated product strategy and pricing.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's installed base and revenue.

Vendor Inclusion Criteria

Forrester included 15 vendors in the assessment: Agari, Area 1 Security, Barracuda Networks, Broadcom Symantec, Cisco, Forcepoint, Fortinet, Google, Microsoft, Mimecast, Proofpoint, SonicWall, Sophos, Trend Micro, and Zix. Each of these vendors has:

- **Enterprise client base.** The vendor serves enterprise clients.
- **Product revenues over $30 million.** The vendor has at least $30 million in email security revenue.
- **Global revenue.** The vendor has revenue from two or more geographies.
- **A productized commercial offering.** The offering can be on-premises or cloud delivered, but it cannot be a custom managed or professional service. The majority of vendor revenues must come from enterprise sales, not OEM. The vendor must offer a product version of the solution that was generally available prior to December 1, 2020. Forrester only evaluated suite capabilities that were released and generally available to the public by this cutoff date.
- **Significant interest from Forrester customers.** Forrester considered the level of interest and feedback from our clients based on our various interactions, including inquiries, advisories, 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 Guide 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 January 22, 2021 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 The Forrester Wave™ and New Wave™ 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 The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor 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.

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

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.