The Forrester Wave™: Enterprise Email Security, Q2 2019

The 12 Providers That Matter Most And How They Stack Up

by Joseph Blankenship
May 16, 2019

Why Read This Report

In our 32-criterion evaluation of enterprise email content security providers, we identified the 12 most significant ones — Barracuda, Cisco, Clearswift, Forcepoint, Microsoft, Mimecast, Proofpoint, Retarus, Sophos, Symantec, 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.

Key Takeaways

Symantec, Trend Micro, Barracuda, Proofpoint, And Cisco Lead The Pack

Forrester's research uncovered a market in which Symantec, Trend Micro, Barracuda, Proofpoint, and Cisco are Leaders; Microsoft, Forcepoint, Mimecast, and Sophos are Strong Performers; and Zix, Retarus, and Clearswift are Contenders.

Threat Intelligence, Cloud Integration, And Deployment Options Are Key Differentiators

Vendors that offer needed threat intelligence, integrate well with cloud email solutions like Microsoft Office 365 and Google Gmail, and deliver in any deployment scenario (on-premises, cloud, or hybrid), position themselves to provide strong email protection to their customers.

The Forrester Wave™: Enterprise Email Security, Q2 2019

The 12 Providers That Matter Most And How They Stack Up

by Joseph Blankenship
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie
May 16, 2019

Table Of Contents

Related Research Documents

The Forrester Wave™: Email Content Security, Q4 2012

New Tech: Secure Communications, Q4 2018

Now Tech: Data Loss Prevention, Q1 2019

FORRESTER®

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

Email Content Security Is Still Critical For Protecting Your Enterprise

Email is a critical business function deeply embedded in the DNA of business processes. Its openness and ubiquity also make email a platform for credential phishing attempts, malware, spam, and business email compromise (BEC). Protecting enterprises from malicious email is a critical capability for security teams. Security pros must also protect the enterprise from leaking sensitive data via email, so robust data lost prevention (DLP) and encryption capabilities are key. To ensure you're getting the most from your email content security solution (ECS), look for providers that have strong:

- **Antiphishing and BEC defense to stop credential theft and malware.** Many data breaches start with a simple phishing email that convinces users to give up their credentials, open a malware-laden attachment, or visit a malicious website. Forrester Analytics survey respondent data from global enterprise security decision makers shows that 27% of external attacks where an enterprise was breached were carried out using stolen credentials.[1] According to the FBI, BEC attacks were responsible for $12.5 billion in losses globally from 2013 to 2018.[2] Unfortunately, these attacks are notoriously difficult to detect because they closely resemble legitimate emails. Defending against these attacks requires multiple techniques and integrated web security defense.
- **Malicious URL detection to stop users from visiting malicious sites.** Attackers embed malicious URLs in emails and attachments in order to lure users to websites that ask for their credentials or download malware to their device. Attackers know that malicious sites and domains are discovered and blocked quickly, so they obfuscate malicious URLs or compromise legitimate domains.[3] ECS solutions need malicious-URL detection that will analyze links and the sites they link to in real time so that users don't have the opportunity to become a victim.
- **DLP to ensure regulatory compliance and protections of IP.** Email is a common source of sensitive data loss (accidental and intentional) as users send emails outside the organization. Native or integrated DLP capabilities detect sensitive data in email and take action to protect it. These actions may include blocking the data, rerouting, quarantining, or encrypting it, according to the organization's data handling policies and compliance requirements. Enterprises handling sensitive data need an ECS solution with DLP that supports their needs.[4]

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.

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 2019

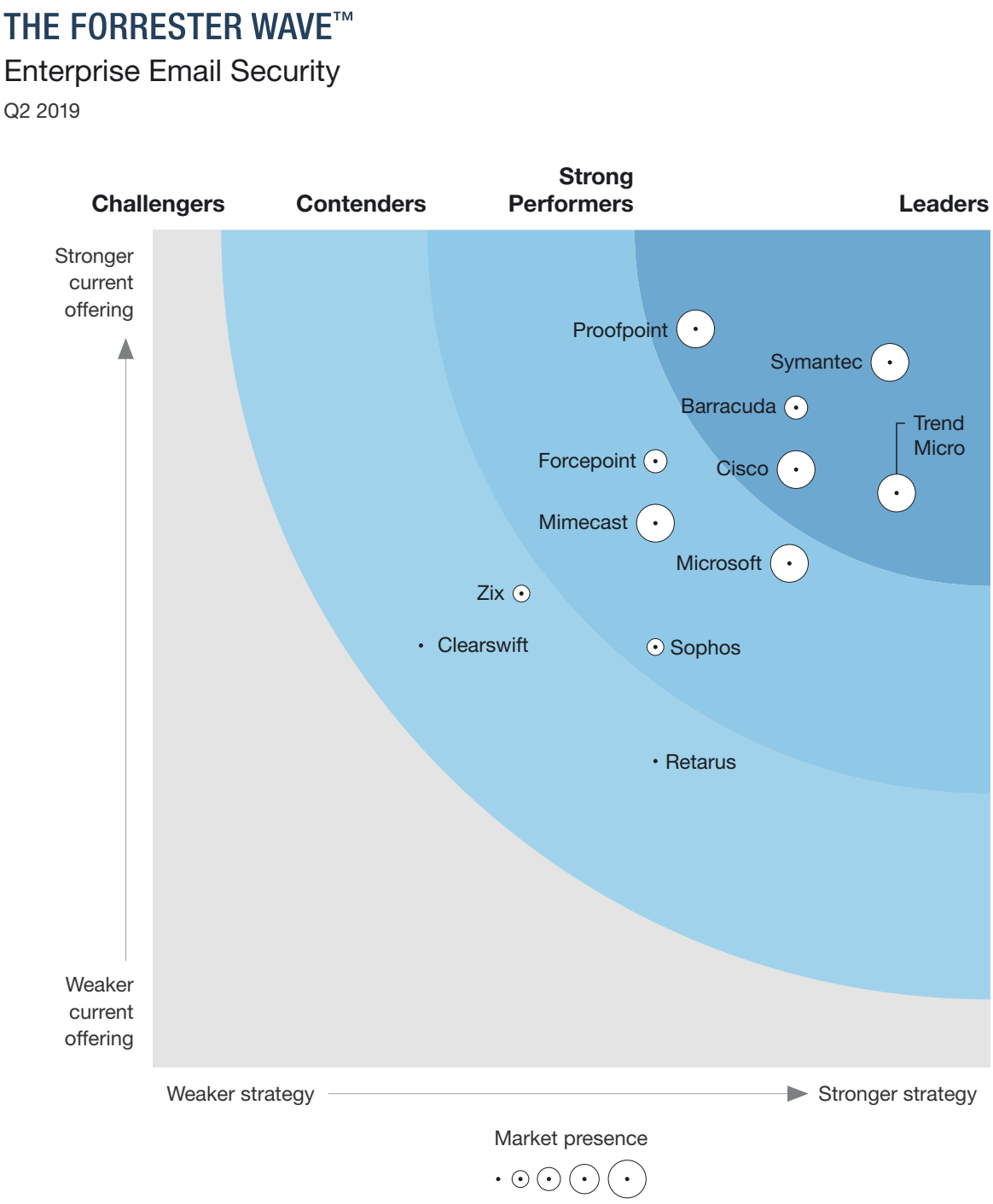

FIGURE 2 Forrester Wave™: Enterprise Email Security Scorecard, Q2 2019

	Forrester's weighting	Barracuda	Cisco	Clearswift	Forcepoint	Microsoft	Mimecast	Proofpoint	Retarus	Sophos	Symantec	Trend Micro	Zix
Current offering	50%	3.94	3.57	2.52	3.62	3.01	3.25	4.41	1.83	2.51	4.21	3.43	2.83
Deployment options	10%	5.00	5.00	5.00	5.00	1.00	1.00	5.00	1.00	5.00	5.00	5.00	3.00
Email filtering	15%	3.54	3.30	2.22	3.46	3.38	3.36	4.42	2.06	2.82	4.12	3.58	2.82
Threat intelligence	10%	3.00	4.20	1.00	3.00	4.20	3.00	5.00	1.00	3.00	5.00	3.80	1.00
Data leak prevention	10%	2.56	3.00	2.38	4.46	2.56	3.00	5.00	1.72	2.56	3.44	1.38	3.54
Cloud integration	5%	5.00	3.00	1.00	3.00	5.00	3.00	3.00	3.00	1.00	3.00	5.00	1.00
Reporting and management	10%	3.00	3.00	3.00	5.00	2.00	3.00	3.00	2.00	1.00	3.00	3.00	2.00
Incident response	10%	5.00	3.00	1.00	3.00	3.00	3.00	5.00	3.00	1.00	3.00	3.00	1.00
Performance and operations	10%	3.00	5.00	3.00	3.00	3.80	3.00	3.00	3.00	1.80	5.00	4.20	3.00
Support and customer success	20%	5.00	3.00	3.00	3.00	3.00	5.00	5.00	1.00	3.00	5.00	3.00	5.00
Strategy	50%	3.84	3.84	1.60	3.00	3.80	3.00	3.24	3.00	3.00	4.40	4.44	2.20
Product strategy	70%	4.20	4.20	1.00	3.00	5.00	3.00	4.20	3.00	3.00	5.00	4.20	1.00
Pricing	30%	3.00	3.00	3.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00	5.00	5.00
Market presence	0%	3.00	5.00	1.00	3.00	5.00	5.00	5.00	1.00	2.00	5.00	5.00	2.00
Installed base	50%	3.00	5.00	1.00	3.00	5.00	5.00	5.00	1.00	1.00	5.00	5.00	3.00
Revenue	50%	3.00	5.00	1.00	3.00	5.00	5.00	5.00	1.00	3.00	5.00	5.00	1.00

Vendor Offerings

Forrester included 12 vendors in this assessment: Barracuda, Cisco, Clearswift, Forcepoint, Microsoft, Mimecast, Proofpoint, Retarus, Sophos, Symantec, Trend Micro, and Zix (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated
Barracuda	Barracuda Total Email Protection
Cisco	Cisco Email Security
Clearswift	SECURE Email Gateway
Forcepoint	Forcepoint Email Security
Microsoft	Office 365
Mimecast	Mimecast Security Email Gateway with Targeted Threat Protection
Proofpoint	P2 with EFD
Retarus	Retarus E-Mail Security
Sophos	Sophos Email (cloud-based) Sophos Email Appliance
Symantec	Symantec Email Security.cloud
Trend Micro	Trend Micro Email Security
Zix	ZixProtect Premium

Vendor Profiles

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

Leaders

› **Symantec email security is a strong part of its security portfolio.** Symantec has a large installed base and product portfolio, making it one of the leading security portfolio vendors. The vendor delivers ECS as an on-premises appliance (physical and virtual), as SaaS, and as a hybrid offering. Customers note Symantec's ease of use and customer support as strengths. The ECS offering integrates with other parts of the Symantec portfolio such as the web security offering, browser isolation technology, and DLP solution.

Customers noted that the solution needs more policy options and flexibility with spam rules and quarantine rules. References also remarked that UI customization was a shortcoming. Enterprises of all sizes that have inbound email filtering and outbound data protection needs, especially those that use other Symantec solutions, should consider Symantec.

- **Trend Micro builds on 20-plus years of email security investment.** Trend Micro Email Security is delivered as an appliance (physical and virtual), on-premises software, SaaS service, and hybrid solution. As one of the pioneers of email security, Trend Micro has a long history of protecting inboxes and delivering innovations like Writing Style DNA, for preventing email impersonation, and Computer Vision, for detecting fake login sites. The vendor offers strong protection from malicious emails, antimalware, and malicious-URL detection. The ECS offering integrates with other parts of the Trend Micro portfolio such as its web gateway security and endpoint solutions. Clients cite effectiveness, ease of deployment, and configurability as strengths.

  While Trend Micro does well protecting against malicious inbound and internal emails, its DLP features are a weakness. Customers remarked that they would like to see a higher quantity and quality of data available to SIMs and improved DLP customization. Enterprises seeking a solution for defending against malicious and malware-laden emails should consider Trend Micro.

- **Barracuda has evolved since the early days of its ubiquitous airport ads.** Barracuda has expanded from its early days as an email appliance vendor, now offering a portfolio that includes integrated solutions for email archiving, phishing simulation and training, and web security. The vendor also offers next-generation firewalls, web application firewalls (WAFs), and data protection. The ECS solution is offered as SaaS and in an appliance (physical and virtual). Barracuda also provides an innovative AI-based solution, Sentinel, to protect against phishing and BEC attacks. Customers praise Barracuda's innovation, its Office 365 integration, and its customer support.

  Barracuda catered to the SMB and midmarket space for years before moving upstream to serve enterprise customers that demand more-flexible, customizable offerings. Customers noted that customization, reporting, and documentation were issues. Small and midsize enterprises, especially those that have moved to Office 365, should consider Barracuda.

- **Proofpoint offers well-rounded inbound and outbound email protection.** Proofpoint offers a variety of deployment options that include appliances (physical and virtual), SaaS, and hybrid solutions. Customers praised Proofpoint for its technology leadership, overall performance, and DLP capabilities. The vendor takes a unique approach for securing the very attacked people (VAP) in your organization to defend against spearphishing and BEC attacks. In addition to its ECS offering, Proofpoint offers email archiving, security and awareness training, and security automation and orchestration (SAO).

Proofpoint is more expensive than competing solutions. References listed the vendor's pricing as a shortcoming. Customers also noted implementation complexity, especially for advanced configurations, as a shortcoming. Proofpoint offers deployment services to assist customers with deployment and configuration. Enterprise customers seeking a full-featured ECS platform and those looking for hybrid deployment should consider Proofpoint.

› **Cisco delivers flexible email security for enterprises.** One of the world's largest networking and cybersecurity vendors, Cisco integrates its email security solutions across its ecosystem. Cisco provides ECS as appliances (physical and virtual), SaaS, and hybrid solutions and is working with several OEMs to expand features like authentication and DLP. Cisco customers appreciate the solution's flexibility and the reliability that working with a large vendor affords.

Cisco Email Security is one of the most mature offerings in the ECS space, and the vendor recently gave the solution a much-needed update to its UI and reporting capability. While all features are accessible via the UI, it may be more efficient to access some advanced features via the command-line interface on the appliance version. Customers remarked that reporting and dashboards are weaknesses, although these could be holdovers from older product versions. Large enterprises, especially those with large Cisco footprints, with the need for a flexible ECS solution should consider Cisco.

Strong Performers

› **Microsoft provides native Office 365 integration for email security.** Microsoft is uniquely positioned to provide native services for protecting customers that use its Office 365 platform. Microsoft is becoming more and more of a player in the security market. Reference customers appreciate Microsoft's ease of use, scalability, and integration with Office 365.

Enterprises have sought third-party solutions to make up for gaps in the Microsoft feature set. Microsoft's efficacy for detecting malicious emails is improving, but there are still feature gaps compared to competitive offerings. Customers would like to see more-granular policy creation, better reporting, and improved information delivered to the SOC. Enterprises of all sizes that are moving to Office 365 should consider using Microsoft's native email security.

› **Forcepoint provides competitive protection and control of inbound/outbound emails.** Forcepoint's strategy and messaging revolve around the individual user, with email as an important part of protecting users and the data they interact with. Forcepoint email delivers as a cloud SaaS offering, an on-premises appliance (physical and virtual), and via hybrid deployment. The solution integrates with the vendor's web security offering and even shares the same management interface. Similarly, the solution integrates with Forcepoint's DLP offering for robust sensitive-data protection. Customers cite the ability to create custom policies and the vendor's DLP capabilities as strengths.

Forcepoint is integrating numerous acquisitions to offer a portfolio of security products. Email makes up a portion of the portfolio but may not be the highest priority as evidenced by a dated UI and lackluster ECS road map that focuses on integrations. Customer references mention

the user interface, consistency of technical support, and the high cost of premium support as weaknesses. The vendor has launched a retooling of its customer support process in the past year to address the support issues. Enterprises needing robust DLP as part of their ECS solution should consider Forcepoint.

- **Mimecast is a strong choice for those seeking a pure SaaS solution.** Mimecast provides an ecosystem of SaaS email and security solutions that include ECS, archiving, eDiscovery, awareness training, and web security. The vendor employs a multipronged approach for antiphishing attacks that includes integrated awareness training and an Outlook plug-in for users to report suspected phishing. Customers appreciate the solution's UI, ease of use, and integrations with adjacent technologies.

  Mimecast has focused historically on the SMB space but is evolving to serve more midsize and large enterprises, which will require it to deliver deeper and more-flexible features. Customers commented that Mimecast may not be as mature as competitive offerings and that the solution was not as flexible as they'd like. Small and midsized enterprises seeking a SaaS-only solution should consider Mimecast.

- **Sophos expands on its endpoint heritage.** Sophos Email Security delivers as a SaaS offering (Sophos Email), a physical and virtual appliance (Sophos Email Appliance), and a hybrid offering. The solution integrates with other parts of the Sophos portfolio such as its web security offering, next-generation firewall, and endpoint solution which can detect compromised mailboxes sending malicious email from the organization's domain. Sophos offers a companion offering, Sophos Phish Threat, which incorporates phishing training and user education. A single management interface, Sophos Central, manages all portfolio components. Customers note ease of use and customer service as strengths.

  Sophos is focused on delivering simple, easy to use email security that fits in the customer's security ecosystem. Customer-reported weaknesses include the ability to customize the UI, reporting, and integration with the web security solution. Future plans call for integrations with cloud providers and further integrations within the vendor's product portfolio to deliver a more complete experience. Small and midsize enterprises looking for an easy-to-use ECS solution should consider Sophos.

Contenders

- **Zix makes email security easy for small to midsize companies.** Zix has a long history of delivering email encryption as an OEM partner for other solutions and as a standalone solution. Its ECS offering, ZixProtect, is delivered as SaaS and appliances (physical and virtual) for on-premises DLP and encryption. Zix acquired vendor AppRiver in January 2019 to increase its focus on SMB customers.[5] This focus is evidenced by the attention Zix places on ease of use, which customers appreciate. Customers also cite Zix's UI in addition to its encryption capabilities as positives. As might be expected from its history, Zix delivers differentiated encryption capabilities.

Enterprise customers may not find Zix capable of meeting their need for flexible policy creation and granularity in reporting. Customers noted customization, reporting, and searchability of emails as weaknesses. The vendor's road map is focused on delivering SaaS capabilities for SMB clients and integrating its acquisitions. Small and midsize enterprises, especially those with strong encryption requirements, should consider Zix.

- **Retarus specializes to the needs of European enterprises.** Headquartered in Germany, Retarus delivers a variety of enterprise messaging and enterprise security solutions. Its ECS solution, Retarus Email Security, delivers as a pure-SaaS solution. Retarus also offers adjacent solutions for email archiving, application email security, and secure SMS messaging. The vendor delivers innovative Patient Zero Detection that detects previously unknown phishing URLs and malware. Customers appreciate Retarus for resiliency, flexibility, and the overall user experience.

  Unlike many of its competitors, Retarus doesn't deliver threat intelligence advisories to customers or have a large, dedicated threat intelligence capability. Instead, it largely relies on its OEM partnerships for threat intelligence that feeds its malicious email detection. Customers say that challenges during the implementation process are a weakness. Small and midsize enterprises with large presence in EMEA and those with messaging security needs beyond email should consider Retarus.

- **Clearswift is a great partner for critical infrastructure and defense contractors.** Clearswift has been delivering ECS and web security for over 20 years. The solution, Clearswift SECURE Email Gateway, delivers as cloud-hosted, on-premises appliance (physical and virtual), and a cloud-hosted or -managed cloud offering. The vendor's strong relationships with defense and critical national infrastructure (CNI) organizations helped train Clearswift's Deep Content Inspection tool to be tuned to threats specific to those verticals. Customers remark that the Deep Content Inspection tool, customizability, and the ability to support multiple customized policies are strengths.

  Clearswift delivers specific protection for the customers it serves, but some features like malware detection, malicious-URL detection, and reporting are behind competitive solutions. The road map is mostly focused on closing those gaps. Customers note false positives, search capabilities, and complicated policies as weaknesses. Enterprises in the defense and CNI verticals should consider Clearswift.

Evaluation Overview

We evaluated vendors against 32 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 deployment options, email filtering, threat intelligence, data leak prevention, cloud integration, reporting and management, 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 planned enhancements, technology leadership, and pricing.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's install base and revenue.

Vendor Inclusion Criteria

Forrester included 12 vendors in the assessment: Barracuda, Cisco, Clearswift, Forcepoint, Microsoft, Mimecast, Proofpoint, Retarus, Sophos, Symantec, Trend Micro, and Zix. Each of these vendors has:

- **Product revenues greater than $10 million.** Forrester evaluated vendors that generate more than $10 million annually from content security products. We excluded consulting revenue related to custom and specialized solutions.
- **Enterprise client base.** Forrester evaluated vendors having more than 50 clients with over 5,000 users.
- **DLP and encryption.** Forrester only considered solutions with DLP and encryption capabilities.
- **Threat research.** Forrester only included vendors that maintain their own threat research team that monitors and incorporates threat information into the product to improve antispam, antimalware, and antiphishing capabilities.
- **A productized commercial offering.** The offering can be on-premises or cloud delivered, but it cannot be a custom managed or professional service. The vendor must offer a product version of the solution that was generally available prior to December 17, 2018. We 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 February 8, 2019 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™ 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.

Endnotes

[1] Base: 143 global enterprise security decision makers who experienced an external attack when their company was breached. Source: Forrester Analytics Global Business Technographics® Security Survey, 2018.

[2] Source: Mathew J. Schwartz, "FBI: Global Business Email Compromise Losses Hit $12.5 Billion," Bank Info Security, July 16, 2018 (http://www.bankinfosecurity.com/fbi-alert-reported-ceo-fraud-losses-hit-125-billion-a-11206).

[3] Source: Danny Palmer, "Hundreds of compromised Wordpress and Joomla websites are serving up malware to visitors," ZDNet, March 29, 2019 (https://www.zdnet.com/article/hundreds-of-compromised-wordpress-and-joomla-websites-are-serving-up-malware-to-visitors/).

[4] See the Forrester report "Now Tech: Data Loss Prevention, Q1 2019."

[5] Source: "Zix Closes Acquisition of AppRiver, Creating Leading Cloud-based Cybersecurity Solutions Provider," Zix press release, February 20, 2019 (http://investor.zixcorp.com/news-releases/news-release-details/zix-closes-acquisition-appriver-creating-leading-cloud-based?field_nir_news_date_value[min]=2018).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

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.