The Forrester Wave™: Cloud Security Gateways, Q1 2019

The 10 Providers That Matter Most And How They Stack Up

by Andras Cser

February 20, 2019

Why Read This Report

In our 34-criterion evaluation of cloud security gateway providers, we identified the 10 most significant ones — Bitglass, CensorNet, CipherCloud, Cisco, Forcepoint, McAfee, Microsoft, Netskope, Saviynt, and Symantec — 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, McAfee, And Netskope Lead The Pack

Forrester's research uncovered a market in which Symantec, McAfee, And Netskope are Leaders; Bitglass, Forcepoint, and CipherCloud are Strong Performers; Microsoft, Saviynt, and Cisco are Contenders; and CensorNet is a Challenger.

Cloud Malware, Monitoring, And Data Protection Are Key Differentiators

As on-premises technology continues to be less effective at protecting data stored in the cloud against a new class of threats, improved cloud malware detection, monitoring, data loss prevention, and encryption will dictate which providers will lead. Vendors that have integrated, easy-to-navigate environments; customizable trending dashboards; and a large, global partner ecosystem position themselves to successfully deliver critical capabilities to their customers.

The Forrester Wave™: Cloud Security Gateways, Q1 2019

The 10 Providers That Matter Most And How They Stack Up

by Andras Cser
with Stephanie Balaouras, Robert Perdoni, and Peggy Dostie
February 20, 2019

Table Of Contents

2 Cloud Malware, Monitoring, And Data Protection Differentiate

2 Evaluation Summary

6 Vendor Offerings

7 Vendor Profiles

Leaders

Strong Performers

Contenders

Challengers

10 Evaluation Overview

Vendor Inclusion Criteria

11 Supplemental Material

Related Research Documents

Best Practices: Selecting And Deploying Cloud Security Gateways

Forrester Data: Cloud Security Solutions Forecast, 2016 To 2021 (Global)

The Forrester Wave™: Cloud Security Gateways, Q4 2016

FORRESTER®

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

Cloud Malware, Monitoring, And Data Protection Differentiate

Protecting cloud applications from data loss or theft, privacy abuses, advanced threats, and other risks is very challenging. In the evolving market for cloud security gateways (CSGs), enterprises increasingly want to monitor and secure all their cloud workloads using as few solutions as possible. CSGs detect and intercept anomalous cloud application activity using integration with next-gen firewall logs, endpoint agents, in-line proxies, and cloud platform APIs. Security and risk professionals considering CSG solutions should look for providers that:

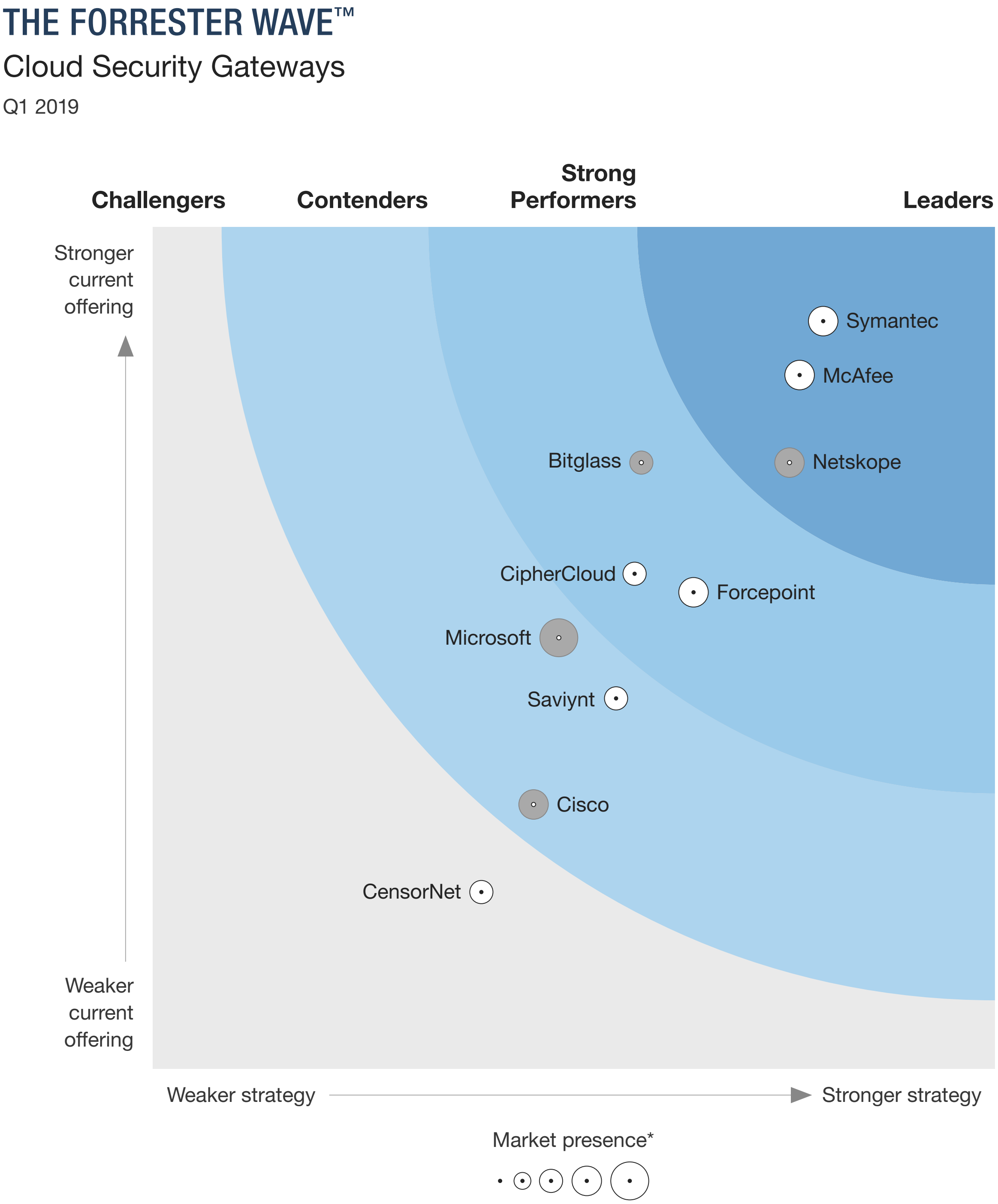
- **Offer cloud malware detection and integration with existing endpoint security tools.** Cloud applications represent a new frontier in cloud data protection. Given that you can't install agents in Box, DropBox, OneDrive, etc., you have to use a CSG solution that connects to the APIs of cloud apps and storage platforms to quickly find and neutralize (remove or quarantine) files containing malware. The ability to integrate the CSG solution with an agent framework of an existing endpoint detection and response (EDR) solution greatly helps here.[1]
- **Monitor and defend infrastructure-as-a-service (IaaS) platforms.** While the CSG market started out with most solutions focusing on the discovery of sanctioned and unsanctioned (shadow IT) software-as-a-service (SaaS) apps, security pros quickly started demanding API connectivity to IaaS cloud platforms (e.g., AWS, Azure, Google Cloud Platform). This allows security teams to uniformly monitor IaaS platform configurations, prevent potential misconfigurations, and prevent or discover the storage of unprotected sensitive data in cloud storage (e.g., AWS S3 buckets) or in SaaS apps (e.g., Salesforce).
- **Protect and encrypt data in cloud applications.** For sensitive data such as personally identifiable information (PII), intellectual property, and data subject to regulatory compliance (e.g., HIPAA, PCI-DSS), CSG solutions can monitor data in transit. This includes between on-premises and cloud apps and between cloud apps. We also now see structured and unstructured data encryption and tokenization as an important part of the CSG solution capability set.

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™: Cloud Security Gateways, Q1 2019



*A gray marker indicates incomplete vendor participation.

FIGURE 2 Forrester Wave™: Cloud Security Gateways Scorecard, Q1 2019

	Forrester's weighting	Bitglass*	CensorNet	CipherCloud	Cisco*	Forcepoint	McAfee	Microsoft*	Netskope*	Saviynt	Symantec
Current offering	50%	3.60	1.05	2.94	1.57	2.83	4.12	2.56	3.60	2.20	4.44
Sanctioned and unsanctioned application (shadow IT) detection	12%	3.00	1.00	3.00	3.00	3.00	5.00	3.00	3.00	0.00	5.00
User activity monitoring	11%	3.00	0.00	1.00	1.00	3.00	5.00	3.00	5.00	3.00	5.00
Infrastructure-as-a-service monitoring	11%	5.00	1.00	3.00	1.00	5.00	5.00	1.00	5.00	5.00	1.00
Cloud malware detection	11%	5.00	0.00	3.00	0.00	3.00	5.00	3.00	5.00	0.00	5.00
CSG data leak prevention	11%	5.00	1.00	5.00	1.00	3.00	3.00	3.00	5.00	3.00	5.00
Data encryption and protection	11%	3.00	0.00	5.00	1.00	0.00	3.00	1.00	1.00	0.00	5.00
Reporting	11%	3.00	3.00	1.00	3.00	1.00	3.00	3.00	3.00	5.00	5.00
Scalability	11%	1.00	1.00	3.00	3.00	5.00	5.00	3.00	1.00	3.00	5.00
Navigation, integrated environment	8%	5.00	3.00	3.00	1.00	3.00	3.00	3.00	5.00	1.00	5.00
Static and contextual documentation	3%	3.00	1.00	1.00	1.00	1.00	3.00	3.00	3.00	1.00	1.00

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

*Indicates a nonparticipating vendor.

FIGURE 2 Forrester Wave™: Cloud Security Gateways Scorecard, Q1 2019 (Cont.)

	Forrester's weighting	Bitglass*	CensorNet	CipherCloud	Cisco*	Forcepoint	McAfee	Microsoft*	Netskope*	Saviynt	Symantec
Strategy	50%	2.90	1.95	2.86	2.26	3.21	3.84	2.41	3.78	2.75	3.98
Unsanctioned cloud app plans	7%	3.00	3.00	3.00	1.00	3.00	5.00	3.00	5.00	0.00	3.00
User activity monitoring plans	7%	5.00	1.00	3.00	1.00	3.00	5.00	3.00	5.00	5.00	5.00
Cloud malware detection plans	7%	3.00	1.00	1.00	1.00	5.00	5.00	3.00	3.00	0.00	5.00
Cloud DLP plans	7%	5.00	1.00	3.00	3.00	3.00	3.00	3.00	5.00	3.00	3.00
Cloud data governance plans	7%	1.00	1.00	3.00	3.00	1.00	5.00	1.00	1.00	5.00	5.00
Cloud encryption plans	7%	3.00	0.00	5.00	1.00	3.00	5.00	0.00	3.00	0.00	5.00
IaaS platform monitoring plans	7%	3.00	3.00	3.00	1.00	3.00	5.00	3.00	3.00	3.00	3.00
Customer satisfaction	7%	3.00	5.00	3.00	3.00	1.00	3.00	1.00	5.00	5.00	3.00
Vendor's RFP response	7%	3.00	1.00	1.00	1.00	5.00	1.00	3.00	3.00	3.00	3.00
Vendor's PoC and demonstration	7%	3.00	3.00	3.00	1.00	5.00	1.00	3.00	5.00	5.00	3.00
Services and partners	7%	3.00	5.00	5.00	5.00	0.00	3.00	1.00	3.00	1.00	5.00
Development staffing	7%	3.00	1.00	5.00	3.00	3.00	5.00	1.00	5.00	1.00	5.00
Sales staffing	7%	1.00	1.00	1.00	5.00	5.00	5.00	3.00	3.00	3.00	5.00
Support staffing	7%	1.00	1.00	1.00	3.00	5.00	3.00	5.00	5.00	5.00	3.00
Pricing terms and flexibility	2%	5.00	3.00	3.00	1.00	3.00	3.00	5.00	0.00	1.00	3.00

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

FIGURE 2 Forrester Wave™: Cloud Security Gateways Scorecard, Q1 2019 (Cont.)

	Forrester's weighting	Bitglass*	CensorNet	CipherCloud	Cisco*	Forcepoint	McAfee	Microsoft*	Netskope*	Saviynt	Symantec
Market presence	0%	2.86	2.50	2.61	3.26	3.27	3.41	4.15	3.33	2.25	3.37
Total vendor revenue	2%	1.00	1.00	2.00	5.00	3.00	4.00	5.00	3.00	2.00	4.00
CSG SaaS revenue	15%	3.00	1.00	1.00	4.00	2.00	5.00	5.00	4.00	2.00	5.00
CSG SaaS revenue growth	12%	3.00	4.00	5.00	1.00	5.00	4.00	1.00	3.00	2.00	3.00
CSG direct installed base	15%	1.00	1.00	4.00	5.00	2.00	2.00	4.00	5.00	3.00	1.00
CSG indirect installed base	12%	1.00	5.00	1.00	4.00	3.00	4.00	5.00	2.00	1.00	5.00
North American presence	11%	2.00	1.00	4.00	3.00	1.00	5.00	5.00	3.00	5.00	5.00
Latin American presence	11%	5.00	1.00	2.00	5.00	4.00	3.00	5.00	3.00	1.00	3.00
EMEA presence	11%	4.00	5.00	3.00	2.00	5.00	2.00	4.00	3.00	1.00	1.00
Asia Pacific presence	11%	5.00	3.00	1.00	1.00	5.00	2.00	4.00	3.00	3.00	4.00

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

Vendor Offerings

Forrester included 10 vendors in this assessment: Bitglass, CensorNet, CipherCloud, Cisco, Forcepoint, McAfee, Microsoft, Netskope, Saviynt, and Symantec (see Figure 3).

FIGURE 3 Evaluated Vendors And Product Information

Vendor	Product evaluated	Version
Bitglass	Next-Gen CSG	
CensorNet	CensorNet Cloud Application Security (CAS)	
CipherCloud	CipherCloud CASB+	
Cisco Systems	Cloudlock	
Forcepoint	Forcepoint CASB	2018 R3
McAfee	McAfee MVISION Cloud	
Microsoft	Cloud Application Security	
Netskope	Netskope Security Cloud	
Saviynt	Saviynt Security Manager, Saviynt Security Analyzer	5.2
Symantec	Symantec CloudSOC	2.102

Vendor Profiles

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

Leaders

- **Symantec.** The solution sports an easy-to-use admin interface, which is very intuitive. The solution offers a marketplace for Securlets (API connectivity) as well as Gatelets (proxy-based policy enforcement). Risk definitions of cloud applications are very security-centric and contain many attributes for regulatory certification.[2] However, policy management is separate for Securlets and Gatelets, which can cause challenges. In Forrester's assessment, IaaS admin action tracking is behind competitors, especially Azure.[3] In contrast with other vendors, the solution's cloud DLP component does not offer proximity settings in DLP policies. The vendor plans to: 1) further integrate CloudSOC with Symantec's Web Security Service; 2) expand CloudSOC console to improve support for DLP, encryption, and identity; and 3) add additional IaaS controls to Google Cloud Platform.
- **McAfee.** The solution offers comprehensive policy management, which is uniform for forward and reverse proxy, and APIs. The solution also covers sanctioned and unsanctioned application monitoring, DLP, and reporting/dashboarding very well. However, its user interface is unintuitive and lags other vendors' more modern interfaces. Integration with on-prem DLP makes the product hard

to navigate, and its response policies can have a more limited set of outcomes than competitors, requiring admins to define a large number of them. The vendor plans to offer: 1) end-to-end data protection using McAfee endpoint, network, and data discovery solutions; 2) a unified solution for public cloud security; and 3) productized support for more long-tail SaaS and custom applications.

- **Netskope.** The solution provides leading machine learning algorithms in threat detection as well as in DLP. IaaS monitoring, DLP, and cloud malware detection are above the competition. The solution also offers innovative ways (IPsec and GRE) to steer traffic to the Netskope proxy. However, the solution is behind in data encryption capabilities, scalability, and cloud data governance plans. Forrester also heard customer complaints about scalability and policy management ease-of-use for larger organizations. Forrester expects that the vendor plans to: 1) expand the Netskope solution to protect IaaS platforms; 2) implement structured data and searchable encryption; 3) increase the number of points of presence to improve performance; and 4) improve incident response capabilities. Netskope declined to participate in our research.

Strong Performers

- **Bitglass.** The vendor offers a comprehensive and easy-to-navigate environment. It offers comprehensive Office 365 protection, cloud malware detection, DLP, and IaaS monitoring services. The vendor also implemented searchable encryption in data and offers vertical-specific offerings for healthcare, manufacturing, financial services, and education. The vendor's IDaaS integration and identity-centric view of cloud app and data protection is robust. However, the vendor's revenues and development staff are long-term viability concerns for enterprise buyers. The vendor plans to: 1) expand cloud encryption capabilities; 2) improve IaaS monitoring; and 3) increase the size of the supported SaaS app catalog. Bitglass declined to participate in our research.

- **Forcepoint.** The vendor acquired CSG specialist Skyfence from Imperva in 2017. Forcepoint has strong network security presence (next-generation firewall, web and email security), and offers its own reporting portal with an intuitive user interface. Incident response explanations on policy violations are detailed, and admins can create new baselines for user behavior and get detailed information on cloud app risk. However, the solution has no productized integration with an IP reputation service, has no canned list of drug names for HIPAA compliance, offers no encryption and tokenization support, and the supported managed cloud application list is significantly smaller than the leaders. The vendor plans to: 1) build a unified policy management and reporting with the Forcepoint product ecosystem, 2) create risk-adaptive protection with dynamic policy/mitigation levels based on user risk and UBA inputs; and 3) add support for additional cloud service providers.

- **CipherCloud.** Given the DNA of the vendor, the solution is very strong in cloud app DLP, cloud encryption, and tokenization. It offers outstanding field-level, sortable, and searchable data encryption in SaaS apps as well as digital rights management (DRM) in mobile applications. However, the solution is less functional than the competition in user activity threat monitoring, reporting, and canned cloud app risk assessments. Machine learning algorithms are black box, and roles in role-based access control are static.[4] The vendor plans to: 1) increase the breadth of supported SaaS applications; 2) open up its SDK for joint development with third parties; and 3) improve the intuitiveness of its UI for user activity monitoring.

Contenders

- **Microsoft.** Microsoft has integrated CSG functionality into its cloud application security portfolio. Architectural options include API, reverse proxy, and log-based deployment. The solution has a large install base (Forrester expects that its users are predominantly Microsoft O365 and Azure customers). The solution is behind in IaaS monitoring, data encryption and tokenization, and cloud data governance. Forrester expects that the vendor plans to: 1) integrate further with threat protection solutions; 2) obtain additional certifications; and 3) scan IaaS content for malware. Microsoft declined to participate in our research.

- **Saviynt.** Based on the vendor's identity management and governance pedigree, the solution offers strong detection, data analytics, and user governance capabilities to certify users and their activities in cloud applications. It offers strong IaaS monitoring capabilities and extensive reporting. However, it lacks sanctioned and unsanctioned IT discovery, cloud malware detection, and DLP, and it is behind in providing contextual help to users. The solution tested by Forrester was rather fragmented (analytics, dashboards, etc.); all live in different apps, and not all links worked in the demo environment.[5] The vendor plans to: 1) expand its partnership and integration with Microsoft and VMware; 2) invest in its privileged access management capabilities; and 3) enhance its machine learning capabilities into data scanning to be able to ingest large volumes of data.

- **Cisco.** Cisco acquired Cloudlock and integrated it into its Cisco Umbrella Secure Internet Gateway platform. The solution has high scalability and an extensive cloud malware reputation service as well as predefined data protection and privacy policies. Cisco integrated Webex Teams with the Cloudlock CSG offering. However, it is behind other vendors in proxy-based application control, cloud app risk definitions, user activity monitoring, and IaaS monitoring. The original Cloudlock interface has a number of useful wizards for policy management, but it's harder to get full CSG functionality (including proxy) across Cisco's entire Umbrella line, including the Web Security Appliances, to integrate with Cloudlock. Forrester expects that the vendor plans to: 1) revamp and further integrate OpenDNS and Cloudlock user interfaces under Umbrella; 2) add coverage for more cloud apps; and 3) implement malware scanning functionality. Cisco declined to participate in our research.

Challengers

- **CensorNet.** The solution offers on-par reporting, has flexible dashboarding, and is easy to navigate. It also has support for images in its DLP and change tracking in the AWS console. However, it lacks user activity monitoring, data encryption, and cloud malware detection, and it is behind in shadow IT discovery and DLP. Cloud application risks are much less detailed than with other vendors. The vendor plans to: 1) implement context and state data continuously in real time and 2) expand its cloud app catalog.

Evaluation Overview

We evaluated vendors against 34 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 sanctioned and unsanctioned application (shadow IT) monitoring; user activity monitoring; infrastructure-as-a-service monitoring; cloud malware detection; CSG data leak prevention; data encryption and protection; reporting; scalability; navigation, integrated environment; and static and contextual documentation.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated unsanctioned cloud app plans, user activity monitoring plans, cloud malware detection plans, cloud DLP plans, cloud data governance plans, cloud encryption plans, IaaS platform monitoring plans, customer satisfaction, vendor's RFP response, vendor's PoC and demonstration, services and partners, development staffing, sales staffing, support staffing, and pricing terms and flexibility.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's total vendor revenue, CSG SaaS revenue, CSG SaaS revenue growth, CSG direct installed base, CSG indirect installed base, North American presence, Latin American presence, EMEA presence, and Asia Pacific presence.

Vendor Inclusion Criteria

Forrester included 10 vendors in the assessment: Bitglass, CensorNet, CipherCloud, Cisco, Forcepoint, McAfee, Microsoft, Netskope, Saviynt, and Symantec. Each of these vendors has:

- **A thought-leading CSG portfolio of products and services.** We included vendors that demonstrated CSG thought leadership and CSG solution strategy execution by regularly updating and improving their productized CSG product portfolio. They must have the ability to provide CSG functions: 1) sanctioned and unsanctioned application IT detection; 2) user activity monitoring and profiling; 3) cloud malware detection; 4) cloud data loss prevention (DLP); 5) cloud data governance; and 6) human intelligence and incident response in a productized offering.
- **Total CSG revenues of at least $8 million with at least 20% growth.** We included vendors with at least $8 million annual CSG revenues which grew at least 20% in the 12 months ending on the cutoff date.
- **At least 75 paying CSG customer organizations in production.** We included vendors that have an install base of at least 75 paying CSG customer organizations in production.
- **An unaided mindshare with Forrester's customers.** The vendors we evaluated are frequently mentioned in Forrester client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.

- **An unaided mindshare with vendors.** The vendors we evaluated are frequently mentioned by other vendors during Forrester briefings as viable and formidable competitors.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

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 with a GA date of September 20, 2018. 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] See the Forrester report "The Forrester Wave™: Endpoint Detection And Response, Q3 2018."

[2] The efficacy of the malware detection is industry leading.

[3] The vendor plans to improve this.

[4] The vendor believes that to support a large scale of users and cloud apps, machine learning algorithm should not be exposed and algorithms should consume context. The vendor believes that tuning of algorithms should be done by the vendor's professional services team.

[5] However, the solution is a singular application that provides all the use cases — the vendor enables features based on license in the same core code-base.

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.