The Forrester Wave™: Cloud Security Gateways, Q4 2016

The Eight Providers That Matter Most And How They Stack Up

by Andras Cser

November 15, 2016

Why Read This Report

In our 23-criteria evaluation of cloud security gateway (CSG) providers, we identified the eight most significant ones — Bitglass, Blue Coat/ Symantec, CipherCloud, CloudLock/Cisco, Imperva, Microsoft, Netskope, and Skyhigh Networks — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways

Blue Coat/Symantec And Skyhigh Networks Lead The Pack

Forrester's research uncovered a market in which Blue Coat/Symantec and Skyhigh Networks lead the pack. CloudLock/Cisco and CipherCloud offer competitive options. Imperva, Bitglass, Netskope, and Microsoft lag behind.

S&R Pros Want Activity Monitoring And Data Protection

The CSG market is growing because more S&R professionals see CSG as an effective and simple way to address their top cloud security challenges, and they increasingly trust CSG providers to act as strategic partners, advising them on top cloud security decisions.

Encryption And Partner Ecosystems Are Key Differentiators

As on-premises network security tools become outdated and less effective, improved behavioral and cloud malware detection and data loss prevention will dictate which providers will lead the pack. Vendors that can provide data encryption, a large implementation, and a partner ecosystem position themselves to successfully deliver cloud security to their customers.

The Forrester Wave™: Cloud Security Gateways, Q4 2016

The Eight Providers That Matter Most And How They Stack Up

by Andras Cser
with Stephanie Balaouras, Salvatore Schiano, and Peggy Dostie

November 15, 2016

Table Of Contents

Notes & Resources

Forrester conducted lab-based evaluations in August 2016 and interviewed 32 vendor and user companies, including: Bitglass, Blue Coat/ Symantec, CipherCloud, CloudLock/Cisco, Imperva, Microsoft, Netskope, and Skyhigh Networks.

Related Research Documents

Global Cloud Security Market Sizing And Forecast, 2015 To 2020

Market Overview: Cloud Data Protection Solutions

An S&R Pro's Guide To Security To, In, And From The Cloud

Vendor Landscape: Cloud Access Security Intelligence (CASI) Solutions

FORRESTER®

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

CSGs Provide Integrated Data Protection And Activity Monitoring

As companies move their workloads and data to the cloud, the question is no longer "Should we move our data to the cloud?" but rather "What security precautions should we take to move our data to the cloud?"[1] Forrester's clients tell us that, at a minimum, they need to:

- **Detect and intercept unusual or fraudulent activities associated with data in the cloud.** A normal pattern of behavior for sales reps at your firm might include accessing 10 to 15 customer records in Salesforce per day. If a sales representative accessed or downloaded several thousand records in a day, this is a sign of suspicious and likely fraudulent activity. It's critical that S&R pros receive alerts on this type of behavioral anomaly. After detecting such anomalous activity, S&R pros may decide to intercept the user session and lock out the user to prevent a breach or exfiltration of sensitive data. CSG solutions offer detection of anomalous activity.
- **Detect, neutralize, and eliminate malware in cloud platforms.** Box, Dropbox, and OneDrive are great cloud storage and productivity platforms. However, users can easily upload, store, and download files containing malware to cloud storage platforms. If left undetected, this malware can quickly spread throughout the enterprise. Traditional endpoint protection software can't detect malware sitting in or moving between cloud platforms. This malware will often allow hackers to compromise the credentials of privileged admins who have unfettered access to Google Apps, OneDrive, etc., thus providing an easy way to siphon off sensitive corporate data. CSG solutions often provide the ability to detect, quarantine, and neutralize malware and malicious cloud applications.
- **Detect and monitor unsanctioned cloud applications and platforms usage.** In large corporations, although the company provides a sanctioned storage platform (for example, Google Drive), employees often use unsanctioned cloud applications (typically cloud storage and productivity platforms such as Box, Dropbox, and OneDrive) to store and even share corporate data. Unsanctioned use of cloud applications may lead to data loss, higher costs (as users may ask to be reimbursed for unsanctioned application subscription costs), and a weakened governance of cloud data. CSG solutions can detect traffic and file uploads to these unsanctioned platforms, giving S&R leaders and the CIO visibility into unsanctioned cloud apps.
- **Protect against leaks of confidential information.** Forrester's interviewees tells us that employees unwittingly leak valuable company data, such as spreadsheets with employee personally identifiable information (PII) or design diagrams containing intellectual property (IP), to cloud email and storage platforms. This increases the chances of a data breach and jeopardizes future company plans and compliance with such regulations as PCI, SOX, and HIPAA. Traditional data leak prevention (DLP) solutions deployed on-premises can't extend coverage to data moving between cloud applications and platforms. CSG solutions with DLP specialize in this kind of coverage.

- **Encrypt structured and unstructured data in cloud platforms.** Cybercriminals can't monetize encrypted data by selling it on black markets, so there is little incentive to steal it. Centralized, selective, and configurable encryption of structured data fields in a cloud CRM solution or of unstructured data in cloud platforms, both via the web and in native mobile applications, protects data. Many S&R pros tell Forrester that while their cloud platform provides built-in data encryption, they prefer to use a third-party CSG vendor for storage and management of encryption keys and search, filter, and sort indices of the data.
- **Aid investigation of suspicious users and incidents.** When a CSG solution detects unusual or suspicious user activity or a data leak or malware incident, S&R professionals need an integrated response and investigation platform that allows for not just investigation (who did exactly what, when, and where) but also for visually reporting and trending of incidents in business-user-friendly dashboards. These tools can highlight massive unsanctioned use of cloud applications, help with trends analysis, and improve the company's security posture as it moves its data to the cloud.

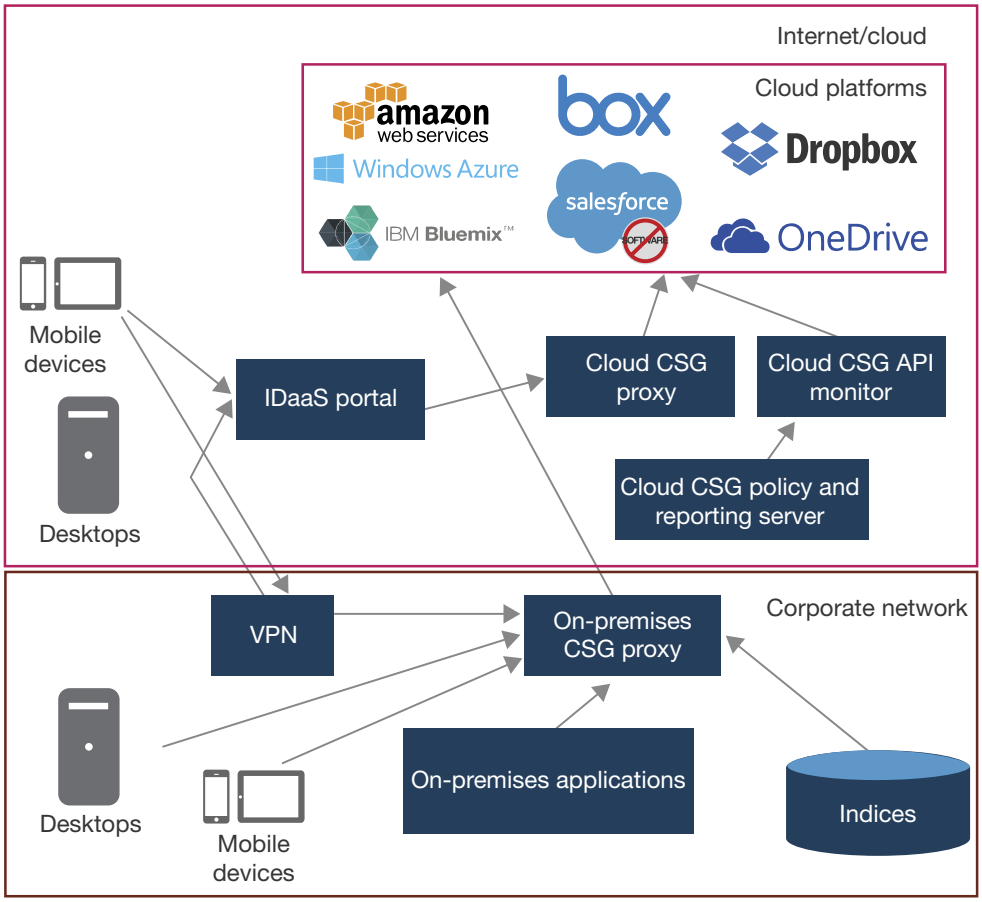
CSGs Intercept Traffic And Monitor Cloud Platform APIs

CSG solutions: 1) intercept and monitor network traffic as it moves between the corporate network and cloud platforms and 2) monitor the APIs of cloud platforms (IaaS, PaaS, SaaS) to show how data enters and leaves these platforms (see Figure 1). Specifically, CSGs:

- **Intercept user traffic from a mobile or desktop browser or native app to the cloud.** CSG vendors' solutions intercept this traffic by modifying the web proxy automatic configuration file on the user's device, installing a desktop plug-in, or working with a mobile device management solution. This ensures that traffic from the mobile device or desktop can only reach the cloud platform through the CSG proxy and that it is not possible for the user to bypass the CSG proxy when they access the cloud platform. Many CSG vendors also offer integration with secure web gateways or on-premises firewalls.[2] CSG vendors partner with IDaaS solutions such as Microsoft, Okta, and OneLogin to use IDaaS solutions to steer traffic to the CSG gateway.[3]
- **Look for unusual activity, malware, and DLP violations, and encrypt data.** As the user's traffic from their mobile device or desktop moves through the CSG proxy to the cloud platform, the CSG proxy examines the traffic and looks for: 1) unusual activity or actions; 2) malware patterns; 3) data patterns that violate DLP rules; and 4) use of unsanctioned or nonsanctioned cloud platforms. The CSG proxy talks to the CSG policy server, which in turn trends the data, reports the activity, and offers investigation functionality to S&R pros. Optionally, the CSG proxy can also encrypt data in transit and encrypt it in storage but ensure that it remains searchable in the cloud platform. On retrieval of data, the CSG proxy decrypts the data in transit.
- **Monitor APIs and assess activities directly connected to the cloud platform.** During initial setup, an admin uses the firm's administrative credentials in the cloud platform to establish a behind-the-scenes connection from the CSG API monitor to the cloud platform. From this point

forward, using the cloud platform's API, the CSG API monitor directly sees all data and user activities. It intercepts not only data and user activities between the user's desktop or mobile device and the cloud platform, but also activities between cloud platforms.

FIGURE 1 High-Level Architecture Of CSG Solutions



CSG Evaluation Overview

To assess the state of the CSG market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top CSG vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 23 criteria, which we grouped into three high-level buckets:

- **Current offering.** In this bucket, we evaluated: 1) sanctioned and unsanctioned application monitoring; 2) support for IaaS platforms, desktop agents; 3) automatic user activity monitoring and profiling; 4) cloud malware detection; 5) data leak prevention; 6) data protection and encryption for both structured and unstructured data; 7) integration, reporting, and scalability; 8) overall solution complexity; and 9) overall intuitiveness and consistency of user interfaces.
- **Strategy.** In this bucket, we assessed the vendor's: 1) future development and marketing plans; 2) differentiation of data protection strategy; 3) relative customer satisfaction compared with other vendors in this Forrester Wave; 4) North American, Central and South American, EMEA, and Asia Pacific implementation and reseller partner ecosystems; and 5) proportionate solution development and sales strengths.[4]
- **Market presence.** In this bucket, we graded the vendor's: 1) SaaS CSG revenues; 2) on-premises CSG revenues; and 3) total direct and indirect customer install base sizes.

Evaluated Vendors And Inclusion Criteria

Forrester included eight vendors in the assessment: Bitglass, Blue Coat/Symantec, CipherCloud, CloudLock/Cisco, Imperva, Microsoft, Netskope, and Skyhigh Networks. Each of these vendors has (see Figure 2):[5]

- **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.
- **Total CSG revenues of at least $8 million with at least 15% growth.** We included vendors that have at least $8 million in revenues, including CSG solutions with at least 15% year-over-year growth.
- **At least 80 paying CSG customer organizations in production.** We included vendors that have an install base of at least 80 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.

FIGURE 2 Evaluated Vendors: Product And Vendor Information And Selection Criteria

Vendor	Product evaluated
Bitglass	Bitglass
Blue Coat/Symantec	Blue Coat Elastica CloudSOC 2.71 Blue Coat Cloud Data Protection 4.9.1
CipherCloud	CipherCloud Trust Platform: Cloud Discovery v4.0 Cloud Security Broker Cloud Security Gateway v4.5
CloudLock/Cisco	CloudLock Security Fabric
Imperva	Imperva Skyfence Cloud Gateway
Microsoft	Microsoft Cloud App Security
Netskope	Netskope Active Platform: Active Cloud DLP Active Introspection Active Encryption Active Threat Protection Netskope Discovery v42
Skyhigh Networks	Skyhigh Cloud Access Security Broker v3.0

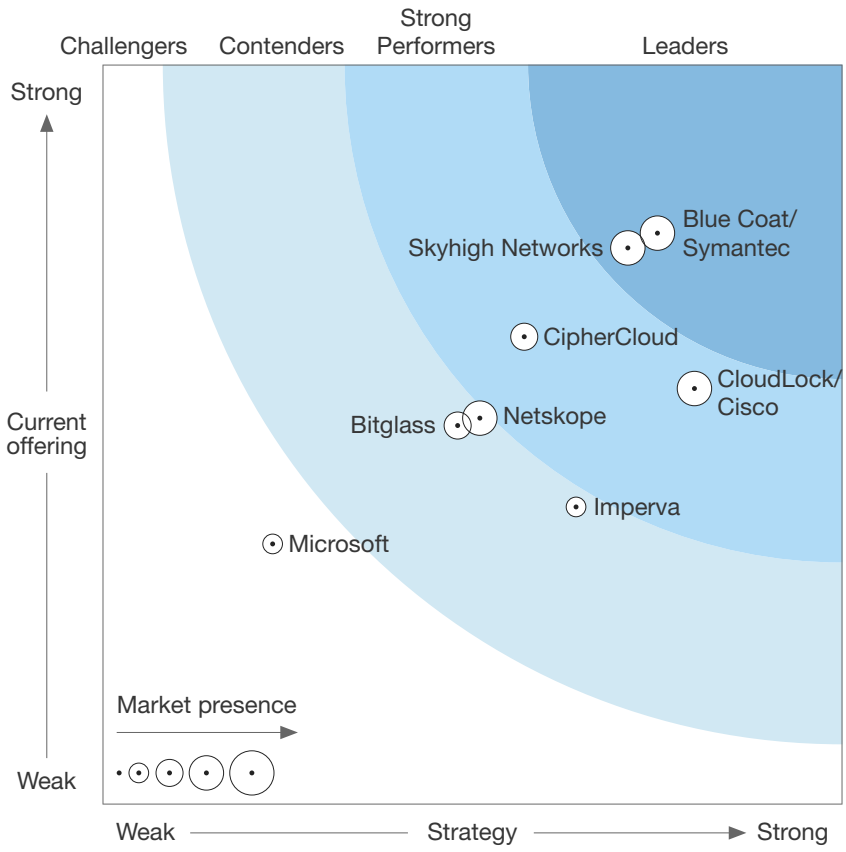
Evaluated vendors and inclusion criteria

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.
Total CSG revenues of at least $8 million with at least 15% growth. We included vendors that have at least $8 million in revenues, including CSG solutions with at least 15% year-over-year growth.
At least 80 paying CSG customer organizations in production. We included vendors that have an install base of at least 80 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.

Vendor Profiles

This evaluation of the CSG market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 3).

FIGURE 3 Forrester Wave™: Cloud Security Gateways, Q4 '16



FORRESTER® **RESEARCH**
The Forrester Wave™

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.

FIGURE 3 Forrester Wave™: Cloud Security Gateways, Q4 '16 (Cont.)

	Forrester's weighting	Bitglass	Blue Coat/Symantec	CipherCloud	CloudLock/Cisco	Imperva	Microsoft	Netskope	Skyhigh Networks
Current offering	50%	2.55	3.85	3.15	2.80	2.00	1.75	2.60	3.75
Sanctioned and unsanctioned application (shadow IT) detection	5%	5.00	5.00	3.00	3.00	4.00	4.00	4.00	5.00
IaaS platform, desktop agent, on-premises application support, and activity list	5%	4.00	4.00	3.00	2.00	4.00	3.00	4.00	3.00
User activity monitoring, profiling, and threat protection	10%	2.00	5.00	1.00	1.00	4.00	3.00	4.00	4.00
Cloud malware detection	10%	1.00	4.00	3.00	3.00	1.00	2.00	5.00	3.00
Data leak prevention	10%	2.00	2.00	4.00	3.00	3.00	1.00	3.00	3.00
Data protection: Salesforce, Office 365, encryption, sorting, filtering encrypted data	20%	2.00	4.00	4.00	1.00	0.00	0.00	0.00	5.00
Data protection: mobile device support, cryptography selection, tokenization, and hardware security modules	15%	3.00	4.00	4.00	3.00	0.00	0.00	2.00	2.00
Integration, reporting, and scalability	10%	2.00	4.00	4.00	5.00	4.00	3.00	3.00	5.00
Overall solution complexity	5%	5.00	2.00	1.00	4.00	2.00	4.00	4.00	1.00
Overall interface intuitiveness and consistency; organization of screens	10%	3.00	4.00	2.00	5.00	3.00	3.00	2.00	5.00

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

FIGURE 3 Forrester Wave™: Cloud Security Gateways, Q4 '16 (Cont.)

	Forrester's weighting	Bitglass	Blue Coat/Symantec	CipherCloud	CloudLock/Cisco	Imperva	Microsoft	Netskope	Skyhigh Networks
Strategy	50%	2.40	3.75	2.85	4.00	3.20	1.15	2.55	3.55
Future development and market plans for CSG and technology	15%	5.00	5.00	3.00	3.00	3.00	4.00	3.00	3.00
Differentiation of the vendor's data protection vision	15%	2.00	5.00	4.00	3.00	1.00	1.00	1.00	5.00
Customer satisfaction	15%	2.00	3.00	1.00	5.00	4.00	1.00	3.00	4.00
North American implementation and strength of reseller partner ecosystem	10%	0.00	3.00	3.00	5.00	5.00	0.00	4.00	2.00
Central and South American implementation and strength of reseller partner ecosystem	5%	0.00	3.00	0.00	5.00	4.00	0.00	0.00	0.00
EMEA implementation and strength of reseller partner ecosystem	10%	0.00	3.00	5.00	5.00	4.00	0.00	3.00	3.00
APAC implementation and strength of reseller partner ecosystem	5%	0.00	5.00	3.00	3.00	5.00	0.00	0.00	4.00
Proportionate solution development strength	15%	5.00	2.00	4.00	3.00	1.00	1.00	4.00	5.00
Proportionate solution sales strength	10%	3.00	5.00	1.00	5.00	5.00	1.00	2.00	3.00
Market presence	0%	2.50	3.25	2.25	3.50	1.50	1.75	3.50	4.00
SaaS CSG revenue	25%	2.00	4.00	0.00	4.00	1.00	3.00	5.00	5.00
On-premises software CSG subscription and perpetual license and maintenance revenue	25%	2.00	4.00	5.00	0.00	1.00	0.00	3.00	3.00
Direct customer install base	25%	4.00	0.00	3.00	5.00	1.00	3.00	2.00	5.00
Indirect customer install base	25%	2.00	5.00	1.00	5.00	3.00	1.00	4.00	3.00

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

Leaders

- **Blue Coat/Symantec integrates CSG with its on-premises secure web gateway.** The solution supports both proxy-based and API monitoring of cloud platforms (both AWS and Azure) and cloud applications. It has strong capabilities for Salesforce and other structured data protection, including search, sort, and filtering operations, and offers a wide selection of encryption and decryption policy options. The solution's built-in cloud application catalog, support for Office 365, and mobile-device-based encryption lag. Forrester expects that the vendor plans to: 1) expand the unsanctioned IT discovery solution to process more log types; 2) integrate the CSG platform with Symantec's on-premises DLP; and 3) integrate the CSG platform with the Blue Coat Cloud Web Security Services offering.
- **Skyhigh Networks offers unsanctioned IT detection and extensive application support.** The solution supports extensive log file integration, nice representation of Active Directory users, and investigation of suspicious user activity and has support for data encryption and management in Salesforce, Office 365, and other cloud platforms. The solution lacks wizards for DLP setup and policies as extensive as some of the other vendors (where users can specify which encryption algorithms the solution can use), and it does not support tokenization. The vendor plans to: 1) enable DevOps to extend CSG to on-premises apps; 2) add more SaaS long-tail applications to its application catalog; and 3) become a cloud configuration management database (CMDB).

Strong Performers

- **CloudLock/Cisco offers an intuitive solution with great reporting features.** Cisco Systems acquired CloudLock on August 1, 2016, essentially enabling the Cisco worldwide sales force to sell the CSG solution globally across all of Cisco's channels. CloudLock's CSG solution is API-based only, while Cisco plans to integrate it with its on-premises firewall solutions. Reporting and policy management are fairly extensive and easy to set up in the solution. The solution lacks Office 365 email encryption, and searching, sorting, and filtering capabilities for encrypted data and today lacks productized integration with an on-premises DLP solution. The vendor plans to: 1) integrate CSG with OpenDNS; 2) enhance threat protection with Cisco Talos threat feeds; and 3) extend CSG controls to IaaS platforms.
- **CipherCloud offers robust structured data protection and on-device encryption.** The vendor has one of the largest CSG revenues in this Forrester Wave — most of which comes from an on-premises deployment model. It offers capabilities to protect data on mobile devices using an on-device mobile application and has an extensive array of encryption options for encrypting, sorting, searching, and filtering data in Salesforce and other cloud apps. The solution lacks exposing the tuning of machine learning algorithms to the end user, and it cannot suppress alerts on a user or stop or intercept suspicious behaviors. The vendor plans to: 1) extend visibility, policy controls, and encryption for additional cloud apps and platforms; 2) perform ongoing research into risk analysis of unsanctioned cloud apps; and 3) implement encryption and tokenization as a service to protect data in custom or private cloud apps.

Contenders

- **Imperva provides extensive IaaS support and works with a large SI partner ecosystem.** The solution offers both API- and proxy-based monitoring of cloud applications and platforms and has extensive log file importing capabilities. It has explicit support for AWS and Azure and offers a desktop agent on Windows to monitor traffic. It can also intercept suspicious user activities in cloud applications. The solution lacks its own engine for malware detection for data in cloud applications and a view for discovered, dynamic user clusters, and it does not provide data encryption or tokenization in cloud applications. The vendor plans to: 1) use unified behavioral analytics for on-premises and cloud apps; 2) implement actionable user risk scoring and incident response; and 3) improve threat and business intelligence.
- **Netskope's DLP and pattern matching algorithms are some of the most extensive.** The solution's DLP and machine learning capabilities are very robust and extensive. It offers natural language processing and wizard-based DLP policies. Reporting and trending are also strong in the solution. However, the solution lacks productized, on-premises DLP integration and does not offer field-level encryption and setup in cloud applications. The vendor plans to: 1) expand scope and depth of monitoring activity in cloud apps and platforms; 2) unify internal and external inputs and outputs and integrate them with user behavioral analytics and security analytics solutions; and 3) make its API decoding 100 times faster.
- **Bitglass pleases users with an easy-to-use, simple, consistently designed solution.** The solution's focus is on API-based detection of traffic, although it also offers proxy-based detection. The solution offers its on-premises log discovery agent as well as deep integration with AWS and Azure cloud platforms and a broad cloud application catalog. The solution cannot suppress suspicious user activity alerts in an investigation, and it does not offer limited malware detection or automatic malware encryption. Forrester expects that the vendor plans to: 1) integrate antimalware engines with API scans; 2) extend IaaS support beyond AWS and Azure; and 3) implement field-level encryption for ServiceNow and Marketo.

Challengers

- **Microsoft offers API-only monitoring today, with a proxy in beta preview.** At the cutoff date, Microsoft only offered API monitoring of cloud platforms. The solution has support for AWS and Azure APIs, documents activity types of users, and exposes tuning of its statistical models to administrators. The solution (by design) has no Windows desktop agent, no documented support for on-premises applications, and it offers no data encryption in structured or unstructured data storage cloud apps. The vendor plans to: 1) invest in information protection and encryption; 2) provide session and access control, extending the capabilities of Azure AD; and 3) provide detection and assessment of device risk and enforce access policies based on device posture.

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 iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave

Forrester used a combination of five data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by June 30, 2016.

- **Hands-on lab evaluations.** Vendors spent one day with a team of analysts who performed a hands-on evaluation of the product using a scenario-based testing methodology. We evaluated each product using the same scenario(s), creating a level playing field by evaluating every product on the same criteria.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls with three of each vendor's current customers.
- **Unsupervised demonstration environment usage.** We asked vendors to provide us with uninterrupted and unsupervised access to the demonstration environments in which we could test the products' features and recreate the product demos at will.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria to be evaluated in this market. From that initial pool of vendors, we then narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

[1] To protect your sensitive data in the cloud from security breaches, privacy abuses, and other incidents, you need an overarching strategy and a detailed road map that includes cloud discovery and workload management, data protection, activity and threat monitoring, data loss prevention, and identity and access management. To learn more, see the following Forrester report: "Create Your Cloud Security Technology Strategy And Road Map."

[2] In Forrester's 26-criteria evaluation of web content security delivered as a software-as-a-service (SaaS) solution, we identified the eight most significant providers in the category — Barracuda Networks, Blue Coat Systems, Cisco, iboss, Intel Security (McAfee), Symantec, Websense, and Zscaler — and researched, analyzed, and scored them. To learn more, see the following Forrester report: "The Forrester Wave™: SaaS Web Content Security, Q2 2015."

[3] In Forrester's 17-criteria evaluation of B2E cloud identity and access management (IAM) vendors, we identified the nine most significant SaaS providers in the category — Bitium, Centrify, IBM, Microsoft, Okta, OneLogin, Ping Identity, SailPoint, and Salesforce — and researched, analyzed, and scored them. For more information, see the following Forrester report: "The Forrester Wave™: B2E Cloud IAM, Q2 2015."

[4] Relative strength of development staff aims to express the degree to which the company as a whole is vested in developing and selling CSG solutions.

[5] On August 1, 2016, Cisco Systems announced it completed its acquisition of CloudLock, and Symantec announced it completed its acquisition of Blue Coat. The product names listed here reflect the offerings before our evaluation cutoff date of June 30, 2016. Blue Coat's CSG products are now called Symantec Elastica CloudSOC 2.71 and Symantec Cloud Data Protection 4.9.1.

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.

133801