FORRESTER®

For: Security & Risk Professionals

The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014

by Andras Cser and Ed Ferrara, November 17, 2014 | Updated: November 18, 2014

KEY TAKEAWAYS

These Public Cloud Platforms Provide Certifications That Significantly Enhance Workload Security

Today's economic environment is forcing S&R professionals to consider alternatives to on-premises security solutions to secure their cloud workloads. The best cloud platforms offer effective physical and logical security and a portfolio of security certifications. These capabilities will support S&R professionals' efforts to secure cloud workloads.

The Cloud Market Is Growing As S&R Pros Look For Out-Of-The-Box IaaS Security

The market of public cloud provider offered security solutions is growing. Security has been the number one impediment to adoption. S&R pros increasingly trust cloud providers to act as strategic partners and see built-in and optional cloud security services provided by the CSPs as the way to address their top cloud security challenges.

Access Control, Data Security, And Service Partners Are Key Differentiators In The Public Cloud Market

This Forrester Wave reviews the security controls available from four of the biggest public cloud platforms. Several areas differentiated the vendors: AWS, Microsoft, and CenturyLink provide strong access control. AWS and IBM have strong data security. Professional services for all vendors could be stronger.

Access The Forrester Wave Model For Deeper Insight On Infrastructure And Workload Security

Use the detailed Forrester Wave model to view every piece of data used to score participating vendors and create a custom vendor shortlist. Access the report online and download the Excel tool using the link in the right-hand column under "Tools & Templates." Alter Forrester's weightings to tailor the Forrester Wave model to your specifications.

NOVEMBER 17, 2014
UPDATED: NOVEMBER 18, 2014

The Forrester Wave™: Public Cloud Platform Service Providers' Security, Q4 2014

Public Cloud Platforms Step Up Their Security Game, But Is It Enough To Safely Deploy Critical Applications And Data To The Cloud?

by Andras Cser and Ed Ferrara
with James Staten and Jennie Duong

WHY READ THIS REPORT

Nearly every large enterprise today is building and deploying new applications on one or more of the leading public cloud platforms. But rarely is this initiative done with the security and risk (S&R) professional involved from the start. Should you be worried? Do these platforms provide the protections and security features you need to keep your company's data safe? This Forrester Wave™ evaluates four of the leading public clouds along 15 key security criteria evaluations to answer this question. The participating cloud services providers were: AWS, CenturyLink Cloud, IBM SoftLayer, and Microsoft Azure. This report details our findings about how well each vendor fulfills our criteria and where they stand in relation to each other, to help S&R professionals select the right public cloud partner with the best options for security controls and overall security capabilities.

Table Of Contents

Notes & Resources

Forrester conducted security evaluations of public cloud providers in 2014 and interviewed four vendor and user companies: AWS, CenturyLink, IBM, and Microsoft Azure.

Related Research Documents

Brief: S&R Pros Remain Unprepared To Address Virtualization And Cloud Security Risks
May 2, 2014

AWS Cloud Security
February 5, 2014

An S&R Pro's Guide To Security To, In, And From The Cloud
December 31, 2013

S&R PROS NEED TO SELECT SECURE PUBLIC CLOUD PROVIDERS

Cloud computing services are quickly becoming formal and integral members of the IT portfolio.[1] As this happens, the S&R pro's challenge shifts from understanding cloud to vetting the selected partners and working with and guiding DevOps and TM leaders to understand which cloud provider offers strong public cloud security and to make the call if these providers have the necessary tools and processes available to secure workloads running in the public cloud.[2] Organizations are rapidly adopting cloud-based platforms that provide infrastructure and application services on a pay-per-use basis.[3] And although vendors tell everyone that they can provide better security than their client organizations could on their own, as adoption rises, cloud security becomes a more critical concern. And a perceived lack of security is one of, if not the, most important reasons organizations cite for not adopting cloud services.[4] In response, cloud platforms are working hard to improve their security transparency and controls and to offer comprehensive security capabilities developed organically or through partner relationships.[5]

Given the cost pressures and imperatives from line-of-business stakeholders to improve business agility and to adopt and improve the security of "shadow IT" (TM services acquired by the line of business without IT or IT security approval or insight), S&R professionals no longer have the authority to block or significantly inhibit adoption of cloud services and technology. Instead, S&R professionals must focus on mitigating security risks with appropriate policies, procedures, and security controls without compromising functionality, ease of use, or the pace of adoption. In order to do this, security and risk pros need to understand that:

- **They need to get ahead of the cloud.** Instead of trying to retrofit legacy, on-premises security tools, and solutions to protect cloud workloads, S&R professionals need to understand the inherent and optional security controls and methods available from the leading cloud platforms and get ahead of the shift to the cloud. Then they can provide the necessary guidance and oversight to ensure that new cloud infrastructures protect company and customer information assets.[6]

- **Cloud is another form of outsourcing.** This is not the first time significant business technology infrastructures have moved outside company-owned data centers. In the 1990s and early 2000s, significant numbers of applications, servers, and the networks that support them moved to third parties, and security and risk professionals needed to put the appropriate security controls in place. Security and risk pros can learn from and build on approaches learned in securing traditional outsourcing — including contracting, service-level agreements, network, and application security.

- **Not all workloads belong in a public cloud, but many do.** S&R professionals should have a clear idea and strategy for the workload hosting in the public cloud. Because of the variability in the security controls available from cloud vendors, security and risk pros should consider carefully the information and applications deployed to these platforms.

- **There are some things you can control, and there are some things you cannot.** Public clouds operate two levels of infrastructure. The first is the infrastructure that operates the cloud environment (e.g., hardware, hypervisor, bare metal components). Security and risk pros in most cases won't have end-to-end control or visibility to the vendor's operational infrastructure. The second is the infrastructure and software environments that customers build in the vendor's cloud infrastructure. The security for this infrastructure is the S&R professional's responsibility, and control and visibility are essential — but leading cloud platforms can help their customers here as well.[7]

Security Is An Important Issue, And Only The Leading Firms Want To Talk About It

Public cloud platform security is maturing rapidly, but it still has a long way to go before we can call it mature. Forrester invited 13 public cloud platform vendors to participate in this Forrester Wave. Only four vendors finally agreed to participate; Forrester did not disqualify any vendors.[8] Forrester interprets this to be a lack of confidence on the part of the potential vendors from the following perspectives:

- **Many vendors feel that if they discuss their security, it will open them to more attacks.** This is old-school thinking — security by obscurity is unreliable, costly, and dead. Cloud vendors are already the focus of significant attacks anyway, which relates directly to the size of the firm, its number of customers, and its visibility, and not the level of transparency it provides to customers with respect to security controls.

- **Not all vendors have confidence in their security controls.** The firms that participated in the Forrester Wave all demonstrate core competencies in providing varying levels of security controls. Overall, the level of security demonstrated by all of the vendors in this Forrester Wave was impressive. We can only assume that many of the vendors who chose not to participate lacked the same confidence and competency specific to the security of their platforms.

Implementing Enterprise-Class Data Centers In The Public Cloud Is A Complex Task

Public cloud presents big opportunities to implement enterprise-class data centers in a virtualized and flexible way. However, security and risk professionals need help in the architecture and the design of these facilities. This help includes security architecture, technology selection, network design, implementation, virtual device management, and security monitoring support. We found that:

- **Many vendors need to provide more implementation support.** While all cloud platform vendors take security very seriously, implementing a secure data center in the public cloud is a daunting challenge. In these cases, vendors need to provide professional services support to create the correct security architecture and implementation plan to achieve enterprise-class security.

- **Vendors need to enhance their security technology partnerships.** It was also clear that all the participants take information security very seriously; however, only one vendor (AWS) in our Forrester Wave had the breadth of security technology partnerships to provide adequate support in their public cloud environment. Forrester expects that the market will see an increased number of: 1) platform-provided security options and 2) third-party provided security options in the platform vendors' marketplaces.

PUBLIC CLOUD SERVICE PROVIDERS' SECURITY EVALUATION OVERVIEW

To assess the state of security on the leading public cloud platforms, Forrester evaluated the strengths and weaknesses of each vendor along 15 criteria common to enterprise S&R clients.

Evaluation Criteria Focused On Functional Security Capabilities And Strategy

Enterprise customers are looking to work with vendors to run workloads more efficiently and cost-effectively to improve business performance. The vendors assessed are trying to meet the growing demand without compromising the security needs of their customers' business operations. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 15 criteria, which we grouped into three high-level buckets:

- **Current offering.** The vertical axis of the Forrester Wave graphic reflects the strength of each vendor's product offering, including its capabilities in data centers, security attestations and certifications, access control (IAM), compute functions (including hypervisor and guest operating security), storage and data security, as well as network security.

- **Strategy.** The horizontal axis measures the viability and execution of each vendor's strategy, which includes the company's security solution value proposition in the marketplace, future development and plans for security controls and technology, customer reference feedback, security service partners, vendor's own professional services for security, development and technical support staffing.

- **Market presence.** The size of each vendor's bubble on the Forrester Wave graphic represents each vendor's presence in the public cloud platform market, based on its cloud service revenue, installed customer base, and the verticals that the vendor services.

Vendors Were Selected According To Global Presence And Customer Relevance

Forrester included four vendors in this assessment: Amazon Web Services (AWS), CenturyLink Cloud, IBM SoftLayer, and Microsoft Azure. Each of these vendors has (see Figure 1):

- **Large global presence.** Each assessed vendor's public cloud platform serves customers in various countries via local vendor-owned data centers across the globe through its cloud-based infrastructure.
- **Significant subscriber base.** All vendors in this research had at least 1,000 customers in their subscription base utilizing their public cloud service solution.
- **Mindshare with Forrester's customers.** Included vendors are frequently mentioned in Forrester client inquiries and other forms of client interaction relating to cloud platform security.[9]
- **Ability to serve workloads from a public service.** Each solution has the capability to let its customers implement workloads in public cloud infrastructures. Vendors that only had private cloud platform capabilities were not included.
- **Ability to offer security capabilities for protecting client workloads.** Each evaluated cloud platform needed to offer security capabilities, either through its own professional services and security support or through third-party security solutions and partnerships.

Forrester invited 13 vendors to participate: AT&T, AWS, BT, CenturyLink, Citrix, Cisco Systems, CSC, Dimension Data, HP, IBM, Google, Microsoft, and salesforce.com. Of these, Forrester disqualified none and only AWS, CenturyLink, IBM, and Microsoft agreed to participate; the others did not.

Figure 1 Evaluated Vendors And Selection Criteria

Participating vendors
Amazon Web Services (AWS)
CenturyLink
IBM
Microsoft Azure

Vendor selection criteria
Large global presence. Each assessed vendor's public cloud platform serves customers in various countries via local vendor-owned data centers across the globe through its cloud-based infrastructure.
Significant subscriber base. All vendors in this research had at least 1,000 customers in their subscription base utilizing their public cloud service solution.
Mindshare with Forrester's customers. Included vendors are frequently mentioned in Forrester client inquiries and other forms of client interaction relating to cloud platform security.
Ability to serve workloads from a public service. Each solution has the capability to let its customers implement workloads in public cloud infrastructures. Vendors that only had private cloud platform capabilities were not included.
Ability to offer security capabilities for protecting client workloads. Each evaluated cloud platform needed to offer security capabilities, either through its own professional services and security support or through third-party security solutions and partnerships.

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

VENDORS FOCUS ON KEY CAPABILITIES FOR EFFECTIVE INFORMATION SECURITY

Forrester's Public Cloud Platforms' Security Forrester Wave uncovered a fast growing cloud platform market where vendors provide varying degrees of focus on security. Forrester's analysis focused on access control, compute (server instances and associated hypervisor), data center, network, and storage security. We were also eager to see how satisfied customers were with the vendor's security controls, as well as, the depth and breadth of the vendor's in-house and service and technology partners that could help security and risk professionals implement secure cloud workloads. Each of the vendors demonstrated differing levels of strength in each of the areas. For example:

- **Access control approaches vary across the vendors.** While most vendors offered integration with third-party identity and access management (IAM) solutions, Security Assertion Markup Language (SAML) and active directory (AD), and application programming interface (API) based IAM operations, every vendor except Microsoft lacked access governance of its users and administrators.

- **Vendors have different approaches for securing the compute environment.** AWS and IBM both offered third-party hypervisor and guest operating system security solutions, while CenturyLink and Microsoft did not. AWS, IBM, and Microsoft provide five or more security solutions, while CenturyLink provides none.

- **All vendors provide strong physical security for the data center**. These vendors provide effective physical access control. Most of the vendors have good geographic diversification providing broad global coverage. This will be useful for security and risk professionals that must address data residency and sovereignty issues. The evaluated vendors have effective business continuity and disaster recovery processes (BCDR) processes for their data centers.

- **All vendors have an effective approach to network security.** While some vendors may use the Internet for connectivity between their data centers, these same vendors also guarantee bandwidth for high-speed inter-data center communications. All vendors provided some number of third-party network security solutions, logical network segmentation, virtual firewall support, and, with the exception of Century Link, web application firewall support, and intrusion detection/prevention systems (IDS/IDP).

- **Security certifications are important to the vendors**. All vendors reviewed with the exception of IBM are ISO 27001 certified and some hold Service Organization Control (SOC) 2 attestations from reputable audit firms.[10] Both certification and attestation demonstrate the firm's effective security certification and audit processes.[11] Certifications are not the final word on a form's security controls but they do show a commitment to security as certification and audit are expensive and time consuming processes (see Figure 2).

- **Vendor professional services support varies across the vendors.** Implementing security in the cloud is a new concept for many security and risk professionals. Many companies considering the public cloud need advisory and architecture services to help them through the transition. Each of the evaluated vendors had different levels of professional services support from both in-house staff and consulting partners. Microsoft and AWS have the strongest security services partner ecosystem, IBM followed behind, and CenturyLink has no security services partners.

- **Customer satisfaction for information security is different for each vendor**. Forrester saw significant difference with respect to customer satisfaction and the availability of services partners to assist with secure workload implementation. For example, AWS's and CenturyLink's customers felt that their security controls and approach to security exceeded their expectations while IBM and Microsoft lagged in this area.

The evaluation uncovered a market in which (see Figure 3):

- **AWS leads the pack.** AWS demonstrated not only a broad set of security capabilities in data center security, certifications, and network security, but also excelled in customer satisfaction, security services partnerships, and a large installed base. AWS led with the size of its development and technical support staff as well.

- **IBM, Microsoft, and CenturyLink offer competitive options.** All of these vendors showed great data center security, a nice level of security attestations, and some level of their own professional services to implement security-related projects. No vendor is focused on single verticals; they all have a mix of financial services, healthcare, government, and media clients.

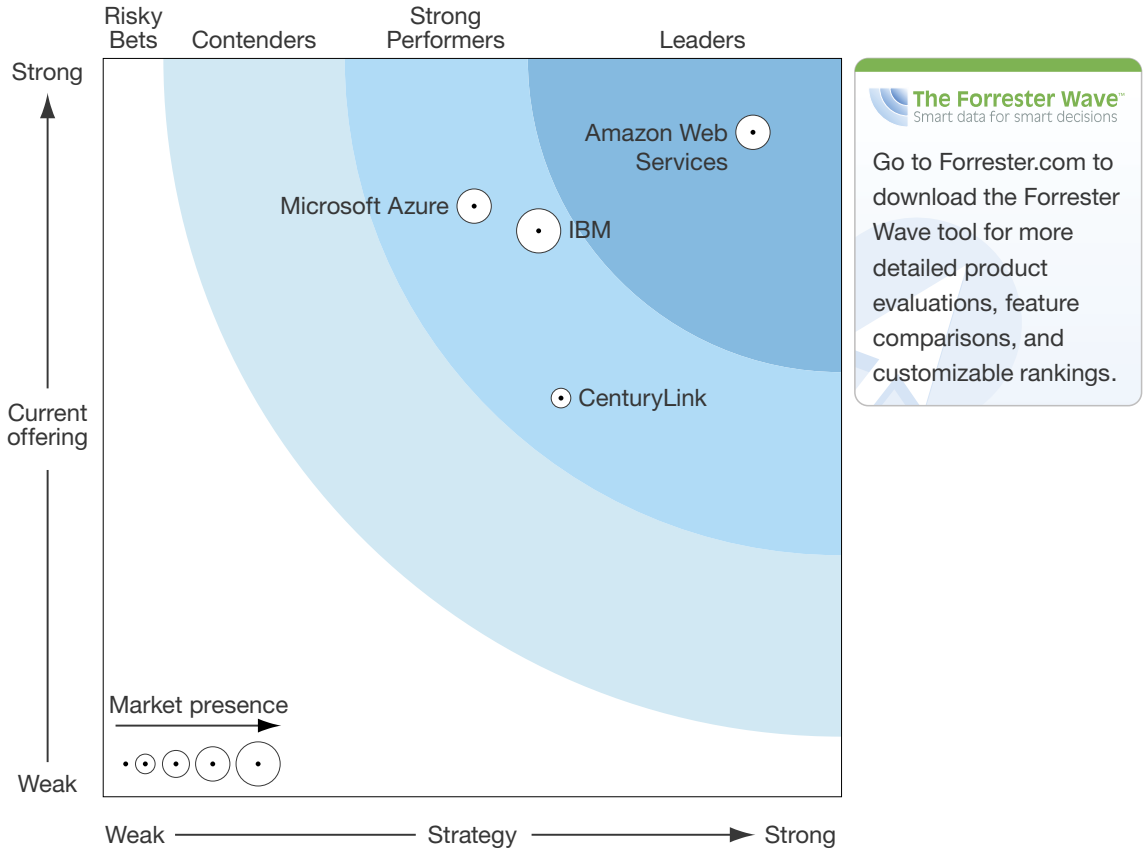
This evaluation of the public cloud platforms' security market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool.

Figure 2 Evaluated Vendors: Security Certifications And Attestations

	AWS	CenturyLink	IBM	Microsoft Azure
Security certifications and attestations	• Cloud Security Alliance — STAR Registrant • DIACAP • FedRAMP (FISMA ATO Moderate) • FIPS 140-2 • HIPAA • ISO 27001: 2005 • ITAR • PCI DSS Level 1 • SOC 1 Type 2 • SOC 2 Type 2 • SOC 3	• FedRAMP (currently in progress) • HIPAA • ISO 27001 • PCI DSS • SOC 1 Type 2 • SOC 2 Type 2	• Cloud Security Alliance — STAR Registrant • FedRAMP (currently in progress) • HIPAA • ISO 27001: 2013 • PCI DSS • SOC 1 • SOC 2	• Cloud Security Alliance — STAR Registrant • FedRAMP • HIPAA • ISO 27001: 2005 • PCI DSS • SOC 1 • SOC 2 • United Kingdom G-Cloud Accreditation

113065 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 3 Forrester Wave™: Public Cloud Service Providers' Security, Q4 '14



113065 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Figure 3 Forrester Wave™: Public Cloud Service Providers' Security, Q4 '14 (Cont.)

	Forrester's Weighting	Amazon Web Services	CenturyLink	IBM	Microsoft Azure
CURRENT OFFERING	50%	4.50	2.70	3.80	4.00
Data centers	15%	5.00	5.00	5.00	5.00
Security certifications and attestations	15%	5.00	3.00	3.00	5.00
Access control: identity and access management (IAM) for users	10%	4.00	3.00	2.00	5.00
Compute: hypervisor and guest operating security	20%	4.00	1.00	3.00	3.00
Storage and data security	20%	4.00	1.00	4.00	2.00
Network security	20%	5.00	4.00	5.00	5.00
STRATEGY	50%	4.40	3.10	3.05	2.50
Security solution value proposition in the market	10%	5.00	4.00	4.00	3.00
Future development and market plans for security controls and technology	15%	3.00	2.00	2.00	3.00
Customer satisfaction	45%	5.00	4.00	3.00	1.00
Security services partners	10%	5.00	0.00	3.00	5.00
Vendor's own professional services for security	10%	3.00	3.00	5.00	5.00
Development and technical support staffing	10%	4.00	3.00	2.00	3.00
MARKET PRESENCE	0%	3.50	1.90	4.40	3.60
Revenue	40%	2.00	1.00	5.00	3.00
Installed base	30%	5.00	2.00	5.00	5.00
Verticals	30%	4.00	3.00	3.00	3.00

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

113065 Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

VENDOR PROFILES

Leaders

- **AWS offers an overall strong solution.** AWS's public cloud platform debuted in 2008 as one of the first large-scale pay-per-use virtual infrastructures and has grown into a massive portfolio of infrastructure and application services supporting thousands of enterprise workloads. From the beginning, AWS designed each discrete capability to be a RESTful, reusable service easily consumed by developers building modern applications.[12] AWS displayed great strength in data center security, security attestations, storage, and data security in this evaluation. AWS has focused not only on building a great cloud platform offering, but also marketing its security capabilities and breadth of add-on security offerings available through the AWS marketplace. While enterprise developers love the relentless innovation AWS provides in terms of new services, capabilities, and controls, a common complaint is that it is less than forthcoming about future development and market plans and even the expansion of its own security services. (Upon customer request, AWS will provide this information to customers under NDA.) Forrester did have some concerns about Amazon's lack of profitability, draining AWS's profits on AWS's $3.1 billion estimated revenue.[13]

Strong Performers

- **IBM uses its acquisition of SoftLayer to accelerate its cloud presence and security.** IBM acquired SoftLayer to accelerate IBM's move into the market by gaining an established technology and customer base. IBM continues to expand its security footprint in the cloud with the acquisition of ISS.[14] The solution provides strong network security, storage and data security, and security certifications and attestations. Before the acquisition of Lighthouse and CrossIdeas, IBM fell behind its competition with its access control, but Forrester expects this will change positively. IBM has less differentiated future plans outside of network security (this is somewhat understandable given the newness of the acquisition of SoftLayer) and lack of development and support staff dedicated to this solution.

- **Microsoft Azure offers strong IAM but lacks end-to-end cloud security.** Microsoft demonstrated effective security controls in its Azure environment, but the solution is not as integrated and well-thought-out end-to-end as AWS. Microsoft demonstrated strong access management, security certifications, and data center security capabilities. And the Azure Marketplace provides a growing number of third-party security controls. Microsoft's customers indicated that the vendor fell short of their cloud security expectations; many customer references were not using Microsoft's security and encryption capabilities as a result.

- **CenturyLink focuses on SMB clients, lacks overall security capabilities.** CenturyLink is a smaller, SMB-focused cloud provider today, but the company is looking to expand into the enterprise and is investing to do so. CenturyLink offers a nice operations console with some

core security capabilities. But it lacks hypervisor, guest operating system, and storage and data security controls found in the competition. And it had no security services partners at the time of evaluation. In its limited security controls, CenturyLink offers decent network security capabilities and articulates its value proposition robustly. Customers said that CenturyLink offers outstanding customer service that exceeded their expectations.

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.

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 document — and then score the vendors based on a clearly defined scale. These default weightings are intended only as a starting point, and we 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

All of Forrester's research, including Forrester Waves, is conducted according to our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

ENDNOTES

[1] For more information about the cloud service provider market landscape, see the May 19, 2014, "Understand The Cloud Service Provider Market Landscape" report.

[2] For more information, see the May 24, 2012, "Rightsource Your Applications For The Cloud" report.

[3] For more information about the growing public cloud provider market, see the April 24, 2014, "The Public Cloud Market Is Now In Hypergrowth" report.

[4] Forrester publicly advocated for secure cloud platforms early on. For more information, see the August 2, 2013, "Security's Cloud Revolution Is Upon Us" report.

[5] Forrester publicly advocated for secure cloud platforms early on. For more information, see the August 2, 2013, "Security's Cloud Revolution Is Upon Us" report.

[6] Customer is an important concept for security and risk pros. Clearly understanding who the security team serves is an important first step in developing any security plan and associated architecture. For more information, see the September 17, 2014, "CISOs Need To Add Customer Obsession To Their Job Description" report.

[7] All of the CSPs have either formal or informal policies with respect to breaches to their customers' infrastructures built in their environments. Some vendors reserve the right to pursue legal action against their customer if the customer experiences a breach that causes damages and loss to the cloud vendor. S&R professionals should engage legal counsel when reviewing cloud contracts.

[8] The vendors that chose not to participate were: AT&T, BT Cloud Compute, Citrix, CISCO, CSC, Dimension Data HP, Google, and salesforce.com.

[9] Forrester utilized inquiries in 2013 and 2014 related to the public platforms and security controls of the providers.

[10] IBM supplied new information after Forrester's June 30, 2014 information submission date that IBM SoftLayer, as of October 2, 2014, received verification from their independent auditor that SoftLayer is in conformance with the requirements of ISO 27001: 2013. This auditor expects to provide full certification by mid-December, meaning SoftLayer will formally receive an ISO certificate with seal at that time.

[11] Companies use the Service Organization Control (SOC) report to document the compliance and security posture of audited organizations. There are three types of SOC reports developed by the American Institute of CPAs (AICPA) and the reports serve different purposes: 1) SOC 1 reports on financial controls; 2) SOC 2 reports on information security controls; and 3) SOC 3 reports on information security controls for public use. For more information, see the October 31, 2011, "SAS 70 Out, New Service Organization Control Reports In" report.

[12] For more information, see the October 29, 2014, "Brief: Salesforce Pivots To Modern Applications" report.

[13] Source: Adrian Campos, "Why Amazon Is Not Making Money," The Motley Fool, November 4, 2013 (http://www.fool.com/investing/general/2013/11/04/why-amazon-is-not-making-money.aspx).

[14] Source: "IBM To Acquire Internet Security Systems," IBM press release, August 23, 2006 (https://www-03.ibm.com/press/us/en/pressrelease/20164.wss).

FORRESTER®

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world's top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION

To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

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.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester's subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.

« **SEAN RHODES,** client persona representing Security & Risk Professionals