Security’s Cloud Revolution Is Upon Us
by Ed Ferrara and Andras Cser, August 2, 2013

KEY TAKEAWAYS

The Cloud Is Disrupting The Information Security Market
Cloud is not going to go away. Now is the time for security and risk pros to assess the impact of the cloud on their company’s security posture. Cloud adoption, driven by impatient business leaders, presents both risks and opportunities for security leadership and poses a major disruption to the information security market.

Information Security Will Migrate To And Be Sourced From The Cloud
There are clear and undeniable benefits for migrating workloads to the cloud. Security and risk pros have seen other business functions benefit from flexible, easy-to-use, and technically advanced cloud offerings. Security leaders will find the benefits of cloud too attractive to pass up and will take advantage of cloud-based security solutions.

The IT Balance Of Power will Shift To The Cloud
The vast majority of applications used by business today are premises-based. Over the next two to three years this is going to change, with more and more workloads moving to the cloud. This shift will force security and risk pros to create new strategies and develop new tactics to deal with a much changed IT landscape.
Security’s Cloud Revolution Is Upon Us
Understanding Information Security Amid Major Cloud Disruption
by Ed Ferrara and Andras Cser
with Christopher McClean, Heidi Shey, and Thayer Frechette

WHY READ THIS REPORT
A perceived lack of security has been one of the more prominent reasons organizations cite for not adopting cloud services. However, this attitude is changing rapidly as cloud service providers (CSPs) begin to offer comprehensive security capabilities. In 2010, Forrester predicted highly secure and trusted cloud services within five years, during which time the cloud security market would grow into a $1.5 billion market. We understated this number, to say the least. Secure cloud is here now, and these services are disrupting the way information security officers address their firms’ security needs. This report explains how CSPs are bundling security services, how security vendors are retooling their premises-based offerings to be cloud based, and how CISOs are responding to these trends. Security and risk pros must accept that cloud is here to stay and develop strategies to deal with this new reality.

Table Of Contents

2 Improvements In Cloud Security Bring New Opportunities
5 CSPs And Security Vendors Will Create Acceptance For Cloud Security
9 Security Executives Need To Get Ahead Of Their Business Partners

WHAT IT MEANS
13 Security’s Cloud Transformation Will Be Lightning Quick

Notes & Resources
Forrester interviewed 11 vendor companies: Alert Logic; AT&T; Cyber; Dimension Data; eSentire; IBM; Savvis, A CenturyLink Company; Sophos; Symantec; Splunk; and Verizon.

Related Research Documents
Predictions For 2013: Cloud Computing
February 22, 2013

The Forrester Wave™: Enterprise Cloud Identity And Access Management, Q3 2012
July 19, 2012

Control And Protect Sensitive Information In The Era Of Big Data
July 12, 2012
IMPROVEMENTS IN CLOUD SECURITY BRING NEW OPPORTUNITIES

Cloud service providers have been promising for years that they would eventually bring all of the economic and technical benefits of cloud computing to their customers, but they treated security as an afterthought.1 This is changing rapidly; because CSPs recognize that the No. 1 impediment to cloud adoption is the real or perceived lack of security. Security is moving quickly to become a well-defined feature of most cloud offerings, and this trend is accelerating.

This disruptive shift marks the beginning of a significant and sustained transformation for the IT security market that will enable companies to purchase information security services delivered from the cloud — protecting both premises-based and cloud-based workloads.2 At the same time, more workloads will shift to the cloud at the expense of premises-based data centers and colocation facilities — having a significant impact on those markets. These changes, driven by a maturing cloud market, will create new challenges and opportunities for security and risk pros.

Cloud’s Economic Model Is Too Attractive For Security And Risk Pros To Pass Up

Cloud adoption continues to accelerate as businesses strive to react quickly to changing customer needs and deliver new services to stay ahead of competitors.3 There are very few areas of IT spending that have not been affected by the cloud revolution; Forrester estimates that cloud computing will influence more than $1.5 trillion in IT spending in one form or another (see Figure 1).4 Businesses reported that in 2013 they are planning more aggressive use of the cloud, especially private cloud models.

IT bloats the balance sheets of many organizations, and many CEOs would like to see this capital used for other purposes. Cloud-based solutions help restructure the balance sheet by shifting IT investments from large capital investments (legacy and premises-based IT) to operational expenses (capex to opex). This change affects both the financial and technical architecture of firms and provides IT the opportunity to refocus on core business activities — delivering solutions that are easier and cheaper to implement, use, and support, as well as better serve the business. Notably, plans for cloud adoption between 2011 and 2012 jumped an incredible 30%, with a longer-term trend showing a meager 9% in 2009 increasing to a whopping 46% in 2012 — a five times increase (see Figure 2)! This abrupt increase in cloud adoption will lead the way for similar expansion of cloud-based security, as security and risk pros adopt cloud to take advantage of the same benefits.
Figure 1 Cloud’s Impact On The IT Market

Cloud impacted IT spend areas (US$ billions)

- Software: $364.90
- Enterprise and SMBs: $131.30
- IT consulting and system integration services: $404.30
- Communications equipment: $328.30
- Systems integration project work: $256.80
- Computer hardware support services: $68.00
- Application management: $21.10
- Hosting: $69.70
- Application outsourcing: $72.90
- Telcos: $197.00
- Infrastructure outsourcing: $72.50
- Strategy and consulting services: $147.50
- Computer equipment: $118.20
- Storage: $49.60
- Servers: $68.60
- Custom-built software: $130.20
- Application outsourcing: $72.90
- IT outsourcing and hardware maintenance: $304.20
- Computer equipment: $118.20
- Communication equipment: $328.30
- Enterprise and SMBs: $131.30
- IT consulting and system integration services: $404.30
- Communications equipment: $328.30
- Systems integration project work: $256.80
- Computer hardware support services: $68.00
- Application management: $21.10
- Hosting: $69.70
- Application outsourcing: $72.90
- Telcos: $197.00
- Infrastructure outsourcing: $72.50
- Strategy and consulting services: $147.50
- Computer equipment: $118.20
- Storage: $49.60
- Servers: $68.60
- Custom-built software: $130.20
- Application outsourcing: $72.90
- IT outsourcing and hardware maintenance: $304.20

Security Concerns Persist, But CSPs Are Responding

Information security and compliance concerns still serve as a major impediment to cloud adoption. This was true in 2010 and 2011, and it’s still true now (see Figure 3). The issues here are both real and perceived, and they have largely been self-inflicted by the CSPs themselves. Microsoft, Amazon.com Web Services (AWS), and Google, for example, were all somewhat circumspect about the security controls available for review by potential customers at the time of their launch. In 2009 for example, the Electronic Privacy Information Center (EPIC) lodged a formal complaint against Google’s security and privacy practices to the US Federal Trade Commission (FTC). Much has changed, however, and CSPs now typically provide Service Organization Control (SOC) reports attesting to the security controls these facilities have in place, and CSPs are spending significant effort to address customer security concerns and use security as a selling point. For example, in 2013, Amazon Web Services (AWS) received an Agency Authority to Operate (ATO) from the US Department of Health and Human Services (HHS) under the Federal Risk and Authorization Management Program (FedRAMP) requirements. This is a very important milestone for the cloud industry and shows that CSPs are making real progress in security.
**Figure 3** Security And Compliance Are Top Concerns With Respect To Cloud Adoption

“What are your firm’s concerns, if any, with public cloud computing IaaS?”

<table>
<thead>
<tr>
<th>Year</th>
<th>Security Concerns</th>
<th>Specific Compliance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>69%</td>
<td>39%</td>
</tr>
<tr>
<td>2011*</td>
<td>67%</td>
<td>38%</td>
</tr>
<tr>
<td>2012†</td>
<td>73%</td>
<td>40%</td>
</tr>
</tbody>
</table>

Base: North American and European enterprise IT hardware decision-makers

Source: Forrsights Hardware Survey, Q3 2010
*Source: Forrsights Hardware Survey, Q3 2011
†Source: Forrsights Hardware Survey, Q3 2012

**THE SECURITY TECHNOLOGY LANDSCAPE WILL CHANGE OUT OF NECESSITY**

2013 will turn out to be remembered as the year cloud disrupted the information security market. It’s clear that cloud architectures (IaaS, PaaS, and SaaS) have already had significant disruptive effects on security technology and services, because businesses rushed to adopt these services with or without security leadership’s approval. This means that security and risk pros need to develop hybrid security architectures to protect not only their on-premises infrastructure but cloud-based workloads as well. The idea of a strong perimeter defense is the first thing that needs to go.

**Perimeter-Based Security Is Now Even Less Relevant Because Of The Cloud**

The traditional data center and the security that surrounds it no longer fit the more dynamic and flexible modes of operation in business today. Cloud-enabled mobility, bring-your-own-device
(BYOD), IT operation (ITO), and business process outsourcing (BPO) make the way we thought about security in the era of the hardened company-owned data center obsolete. With the cloud, these fixed targets no longer exist.

A company’s perimeter is now more like the Maginot Line that "guarded" France from invasion from the Germany prior to World War II. The German army easily bypassed the Maginot Line by attacking France through Belgium (see Figure 4). US General George Patton observed that “fixed fortifications are monuments to man’s stupidity.” Similarly, cloud is replacing legacy corporate data center assets, which means the fixed fortifications designed to defend these assets need to change as well.

As the perimeter disintegrates into a set of federated cloud-based and on-premises infrastructures, effectively monitoring becomes almost impossible, unless security controls are embedded in these heterogeneous environments. This will require security professionals to reconsider and possibly redesign their security architecture and corresponding security controls and placing those controls in the cloud.

Figure 4 The German Path Of Attack Into France In World War II (1940)

Source: Forrester Research, Inc.


99302
Security Services And Technologies Merge, Grow, Evolve, And Move Into The Cloud

As the perimeter dissolves, the technology landscape will consolidate into a series of cloud and premises-based applications and infrastructure. Premises-based solutions will still exist, but the ratio between premises-based and cloud-based infrastructures will favor cloud. Security and risk pros will have the opportunity to leverage cloud-enabled security solutions that offer better economies of scale and elasticity of implementation to make their security architecture more responsive to their organizations' needs. There will be several major architectural shifts during this cloud security transformation (see Figure 5):

- **The reliance on cloud infrastructure will continue to grow, and security will follow.** As more and more organizations move into the cloud, the size and proportion of cloud infrastructure and workloads will grow dramatically. By necessity, security practitioners and vendors will have to address this trend by migrating more security infrastructure, applications, and expertise to address market needs.

- **Security solutions will grow and evolve in the cloud.** This will represent the largest shift. There will be a whole new ecosystem of cloud-optimized security solutions, available only from the cloud providers to support both on-premises and cloud (PaaS, IaaS, and SaaS) environments. AWS security and Symantec/VeriSign’s VIP authentication, as well as companies like Alert Logic, Cyber2, eSentire, Splunk, and Sophos, are harbingers of this trend.

- **Security technologies and services will merge into security-enabled vertical solutions.** Today’s discrete security technologies (IDS, IPS, firewall, IAM, SECM/SIEM, etc.) and security services provided by MSSPs in many cases are bolted on to existing application and network infrastructures. However, in the future, security services will become important features for new vertical applications. We see this happening already as telecommunication companies bring vertical solutions to market using secure clean pipe, cloud-hosted architectures.
Figure 5 On-Premises To Cloud Architecture Transition

**Today:** very loosely coupled cloud and on-premises infrastructures with on-premises dominant. Information security implemented as a series of point solutions.

**Tomorrow:** tightly coupled cloud and on-premises infrastructures with cloud dominant. Integrated cloud-based security technology.

---

CSPs And Security Vendors Will Create Acceptance For Cloud Security

As the market for cloud security heats up, three inter-related drivers will shape the nature of client demand: information security’s priority in the organization, audit pressure, and regulatory requirements. CSPs will help this transformation by implementing a series of changes:

- **CSPs will take security out of the closet.** Much of the concern about the security of cloud providers comes not merely from the technology in place, but from the customers’ inability to validate the controls these vendors claim to have in place. This goes far beyond SLAs and period audits; cloud providers need to be more transparent about their processes, certifications, locations, techniques, operational schedules, and so forth. AWS provides a good example to follow: The vendor regularly communicates and promotes its security measures through
webinars, information papers, and public events. Microsoft has established itself as a vocal proponent of application security as it pertains to cloud environments by shedding light on what it is doing with Azure (in Office, IAM, and directory infrastructures) and BPOS as well as educating other providers and helping enterprises adopt best practices.

- **CSPs will become advocates for customer needs and industry improvement.** CSPs realize it no longer works to avoid talking about security, hoping that concerns will go away — all this did was slow the pace of cloud service adoption. Successful providers will not just market security as a differentiator but will advocate for industry change on behalf of its customers. Membership by CSPs in the Cloud Security Alliance is high, and adoption of these standards has now reached critical mass.

- **CSPs will implement security standards and certifications specific to cloud environments.** CSPs now recognize they must embrace security frameworks and certifications such as the Cloud Security Alliance, Cloud Industry Forum, US government General Services Administration (GSA) FedRAMP, National Institute of Standards and Technology (NIST) guidelines, and the European Network and Information Security Agency (ENISA). Many times these requirements are passed on to CSPs' customers by their customers' customers in a cascading requirements chain. CSPs need to provide adopting organizations more detail and concrete assurances of operational practices — such as specifying both the control technologies and policies in place, access to system logs, and regular communication of results from security scans — rather than relying on general contract language. “Just trust us” only goes so far.

- **CSPs will focus on operational visibility, enabling customers to validate controls.** Operational visibility has been one of the major deficiencies across the cloud provider landscape. The efforts by many CSPs to publish security controls using SOC reports and ISO certification are moves in the right direction. This renewed focus on information security transparency will accelerate adoption and remove the barriers the observable lack of security controls posed in the past.

- **CSPs will collaborate to develop a common language for cloud security.** The NIST 800-145 standard is a good place to start for a common security language. However, more can and will be done, so that CSPs can more effectively serve their clients. While providers continue integrating security features, they offer them as a set of individual services. A common industry accepted security framework is needed to baseline a CSP’s security capabilities.

### SECURITY EXECUTIVES NEED TO GET AHEAD OF THEIR BUSINESS PARTNERS

As cloud adoption accelerates, security and risk pros need to get ahead of their business partners with a clear strategy on how to address cloud implementations. If you can't beat them, join them. The level of market demand for cloud security solutions is expanding at least as rapidly as the interest in cloud services in general. Forrester’s Forrsights® information security survey shows that
the level of interest in cloud-based security solutions is rising, with a majority of respondents willing to adopt a cloud-based technology (see Figure 6). Security and risk pros will improve their overall cloud readiness by:

- **Strengthening application security.** Application security is a critical issue and offers an attractive security control point. If an application is architected with strong security principles, the security of the underlying infrastructure is less of an issue. Therefore, it’s incumbent on the application development team to ensure that cloud applications are secure.\(^\text{14}\)

- **Implementing cloud governance.** Policy-based management of cloud applications is one of the more challenging issues of any deployment, yet it will be a critical element for organizations from a security and compliance perspective. This requirement will become even more important as the use of cloud broadens and cloud-resident applications become commonplace; without well-documented policies and procedures, it’s easy for business stakeholders to provision and manage very important applications with little regard for security concerns.\(^\text{15}\)

- **Securing data.** Similar to the need to design secure applications, data security should be a core focus, and it will likely deliver high business value. Big data, mobile users, and workloads distributed throughout a variety of infrastructures will mean that protection has to follow data wherever it goes. Data security solutions for cloud services must address cloud-specific concerns, including external attacks, malicious insiders, commingling of data, and even data access by government agencies using various legal channels.\(^\text{16}\)

- **Incorporating identity and access management, including single sign-on using cloud APIs.** Organizations recognize that cloud adoption has already fragmented the identity infrastructures they have been assiduously building and consolidating for the past 10 years. Today’s identity infrastructures need to cater to: 1) the extended enterprise of employees as well as business partners for whom the company may not even manage identities; 2) BYOD and mobility requirements, where securing non-web APIs and imbuing them with identity is the norm; and 3) supporting IAM for applications delivered by cloud service providers.\(^\text{17}\)
Security’s Cloud Revolution Is Upon Us

Figure 6 Interest In Security-As-A-Service

“What are your firm’s plans to adopt the following ‘as-a-service’ security offerings/approaches?”

<table>
<thead>
<tr>
<th>Service</th>
<th>Interested but no plans</th>
<th>Planning to implement in a year or more</th>
<th>Expanding/upgrading implementation</th>
<th>Planning to implement in the next 12 months</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application security</td>
<td>23%</td>
<td>7%</td>
<td>15%</td>
<td>6%</td>
<td>57%</td>
</tr>
<tr>
<td>Distributed denial of service</td>
<td>26%</td>
<td>16%</td>
<td>4%</td>
<td>5%</td>
<td>59%</td>
</tr>
<tr>
<td>Email filtering</td>
<td>12%</td>
<td>40%</td>
<td>10%</td>
<td>6%</td>
<td>71%</td>
</tr>
<tr>
<td>Endpoint security</td>
<td>15%</td>
<td>25%</td>
<td>11%</td>
<td>5%</td>
<td>61%</td>
</tr>
<tr>
<td>Host event log monitoring/management</td>
<td>19%</td>
<td>7%</td>
<td>19%</td>
<td>6%</td>
<td>58%</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>19%</td>
<td>7%</td>
<td>18%</td>
<td>6%</td>
<td>60%</td>
</tr>
<tr>
<td>IDS/IPS monitoring/management</td>
<td>19%</td>
<td>18%</td>
<td>7%</td>
<td>6%</td>
<td>57%</td>
</tr>
<tr>
<td>Message archiving</td>
<td>19%</td>
<td>7%</td>
<td>24%</td>
<td>4%</td>
<td>64%</td>
</tr>
<tr>
<td>Network firewall monitoring/management</td>
<td>14%</td>
<td>29%</td>
<td>12%</td>
<td>5%</td>
<td>65%</td>
</tr>
<tr>
<td>Regulatory compliance monitoring/assessment</td>
<td>22%</td>
<td>7%</td>
<td>17%</td>
<td>5%</td>
<td>59%</td>
</tr>
<tr>
<td>Security information management</td>
<td>21%</td>
<td>7%</td>
<td>15%</td>
<td>5%</td>
<td>56%</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>23%</td>
<td>7%</td>
<td>22%</td>
<td>9%</td>
<td>71%</td>
</tr>
<tr>
<td>Web content filtering</td>
<td>16%</td>
<td>29%</td>
<td>10%</td>
<td>5%</td>
<td>65%</td>
</tr>
</tbody>
</table>

Base: 2,154 IT security decision-makers

Source: Forrsights Security Survey, Q2 2012

A Full Array Of Vendors Is Available When You’ve Settled On Your Strategy

More and more vendors’ security solutions are available within cloud architectures. The number and types of security functions that can be provided “as-a-service” is substantial, and most technologies historically only available in an on-premises model are now available from cloud providers (see Figure 7). Security vendors’ shifting emphasis is well timed, as the rebounding economic climate will accelerate, not reduce, enterprise IT’s attraction to a range of as-a-service solutions.
Figure 7 Cloud Security Service Providers

<table>
<thead>
<tr>
<th>Cloud-based service</th>
<th>Representative companies (large and small)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data and database security</td>
<td>EMC, GFI, IBM, Oracle, Quantum</td>
</tr>
<tr>
<td>Distributed denial of service (DDoS)</td>
<td>AT&amp;T, CloudFlare, Zscaler</td>
</tr>
<tr>
<td>Email filtering</td>
<td>AT&amp;T, Comodo, GFI, Google, McAfee, SilverSky, Symantec, Verizon</td>
</tr>
<tr>
<td>Network-based (cloud) firewall services</td>
<td>Amazon Web Services (AWS); AT&amp;T; Dimension Data; GoGrid; Integra; Level 3 Communications; Network Box; Savvis, A CenturyLink Company; Verizon; Virtela</td>
</tr>
<tr>
<td>Governance, risk, and compliance</td>
<td>CSC, RSA-EMC, Solutionary</td>
</tr>
<tr>
<td>Cloud-based IDS/IPS</td>
<td>Amazon Web Services (AWS); AT&amp;T; Dimension Data; GoGrid; Integra; Level 3 Communications; Savvis, A CenturyLink Company; Verizon; Virtela; XO Communications; many others</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>CA Technologies, IBM, Lighthouse, Okta, OneLogin, Oracle, Ping Identity, SecureAuth, Simeio Solutions, Symplified, Verizon</td>
</tr>
<tr>
<td>Log retention and monitoring</td>
<td>Alert Logic, CloudAccess, EMC-RSA, LogEntries, Loggly, Solutionary, Splunk, SumoLogic, TripWire</td>
</tr>
<tr>
<td>Malware protection</td>
<td>AT&amp;T, Zscaler</td>
</tr>
<tr>
<td>Mobile device management</td>
<td>AirWatch, FancyFon, Fiberlink, Good Technology, Kaseya, Mobile Active Defense, MobileIron, Motorola, Notify Technology, RIM, Sybase, Tangoe, Trellia (acquired by Wyse Technology), Virtela, Wavelink, Zenprise</td>
</tr>
<tr>
<td>Patch management</td>
<td>GF Cloud, HP, IBM</td>
</tr>
<tr>
<td>Threat intelligence</td>
<td>Cyber2, eSentire</td>
</tr>
<tr>
<td>Vulnerability testing</td>
<td>eEye, IBM, iScan, McAfee, nCircle, xStorm</td>
</tr>
<tr>
<td>SECM</td>
<td>CloudAccess, SilverSky, Virtela</td>
</tr>
<tr>
<td>Web application firewall</td>
<td>Akamai, Imperva, Incapsula</td>
</tr>
</tbody>
</table>

Source: Forrester Research, Inc.
WHAT IT MEANS
SECURITY’S CLOUD TRANSFORMATION WILL BE LIGHTNING QUICK

Cloud adoption is disrupting information and cybersecurity for both security professionals and vendors. As cloud providers continue to build security into their platforms, their customers will soon see them as top security solution providers. Demand is quickly on the rise for secure cloud solutions, and the economic benefits of cloud can also be highly advantageous for security and risk pros. Several trends will accelerate these two drivers:

- **Standards for cloud security have improved, and CSPs are adopting them.** There are more than 78 industry groups working on cloud-related standards, and at least 48 of them claim to have security-related elements. For example, the Storage Network Industry Association (SNIA) has security standards related to data and storage management, NIST has published its guidelines for information security in the cloud, and FedRAMP is now mentioned in nearly every security-related conversation you might have with CSPs.20

- **More security makes good business sense for CSPs, so they’ll move quickly.** Many CSPs — including AT&T, AWS, CSC, HP, and Verizon Business — are responding directly to customer security concerns, recognizing that improved security and greater transparency will accelerate adoption of their cloud solutions. CSPs also see an opportunity to monetize the security and compliance controls that they put in place by charging customers for extra features that go above base-level protections.

- **Cloud fuels security growth, and security will fuel cloud growth.** Cloud security spending will begin to replace premises-based spending this year, and this trend will only accelerate after that. Organizations still won’t move to the cloud wholesale, but over the next three years they will expand their cloud infrastructure substantially, displacing a significant amount of their premises-based infrastructure. Security — especially managed security — will become embedded in cloud solutions but will still be offered as a standalone service as this transition unfolds. Cloud adoption will fuel absolute growth in the security market as organizations move to address risk, security, and compliance in new ways across a range of locations and a variety of providers.

- **Cloud security has shifted from inhibitor to enabler.** As cloud providers recognize and embrace the opportunities that security provides, we’ll see them exercise greater care through hardening of operating systems and hypervisors; more tightly controlled configuration and change management processes; more-rigorous analysis of network and inter-VM activity (both automated and by more-seasoned security staff); and more-diligent custodianship of data. This is a natural evolution of the market: Security will become just one component in a set of functions evaluated in the context of a broader set of services, and we’ll also see organizations adopt cloud services for the improved security protections and compliance controls that they otherwise could not provide as efficiently or effectively themselves.
ENDNOTES

1 In H1 2009, cloud-related vendor announcements were vague or centered on cloud as a delivery model for security solutions. In H2 2009, there were 21 announcements on cloud or virtualization security coming from EMC/RSA, HP, IBM, McAfee, Novell, Sun, Symantec, Trend Micro, VeriSign, and Verizon Business. There were product, managed services, and technology partnership announcements, consulting announcements, and articulations of strategy. There were also thought leadership pieces to gain visibility and build awareness. Securing cloud computing environments is now becoming a major focus of vendor efforts. See the March 3, 2010, “Market Momentum: IT Security Market, H2 2009” report.

2 The term “workload” has come into common parlance to mean applications and IT services performing specific business functions. It also implies a more flexible approach to computing resources in that workloads can be run anywhere there is suitable infrastructure to run them.

3 Since 2011 a growing number of IaaS clouds have been brought to market using the same underlying capabilities, technologies, and interfaces. Rather than build their clouds independently, providers use a cloud platform to speed time-to-market.


4 The 2013 to 2014 period will see a different pattern of tech market dynamics than what prevailed in 2012, forcing CIOs and business tech buyers to adjust their spending plans to address the current and future economic climate. Many of these areas will see strong cloud impact. See the January 3, 2013, “Global Tech Market Outlook 2013 To 2014” report.

5 Organizations will look to cloud computing to improve operational efficiency, reduce headcounts, and help with the bottom line. But security and privacy concerns present a strong barrier-to-entry. See the May 8, 2009, “How Secure Is Your Cloud?” report.

6 Service Organization Control (SOC) reports, and specifically the SOC 2 and SOC 3 reports, are now frequently used to describe the security posture of CSPs. The American Association of Certified Public Accountants (AICPA) worked to create these new standards to recognize the global nature of modern companies and the need for reports that address broader compliance issues, including information security. There are three types of reports, and each serves a different purpose: 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.

7 FedRAMP is a United States governmentwide program that provides a standardized approach for security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that hopefully will save cost, time, and staff required to conduct redundant agency security assessments. Backers feel that FedRAMP requirements will raise the security bar for the agencies, resulting in more-uniform security evaluations of a cloud provider’s security controls. Source: United States General Services Administration (GSA), About FedRAMP (http://www.gsa.gov/portal/category/102375).
8 Forrester’s surveys and client inquiries show that business units aren’t waiting for permission to deploy workloads to the cloud. Security and risk pros will need to get comfortable with the fact that development on public clouds is going to happen whether they like it or not, and it’s easier for them to engage developers and be part of the conversation about how to do it safely, securely, and with appropriate oversight. See the February 22, 2013, “Predictions For 2013: Cloud Computing” report.

9 Source: Estate of General George S. Patton Jr. (http://www.generalpatton.com/quotes/).

10 Forrester analyst John Kindervag has written extensively about the deficiencies of traditional infrastructure security design in his Zero Trust networking series of research papers. Network professionals designed the traditional hierarchical network from the outside in. New technology and new ways of doing business (especially mobile devices, social networks, and cloud computing) make the traditional approach to security antiquated. See the November 15, 2012, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture” report.

11 Forrester believes the term “security event correlation management” (SECM) more accurately reflects the state-of-the-art in terms of continuous monitoring technology. These systems have moved from reactive log scanning to proactive behavioral analysis, to more effectively protect the enterprise.

12 Source: Amazon Web Services (http://aws.amazon.com/security).


14 Cloud has become a standard part of IT department plans, and this is the year that leaders must get realistic. You’ll need to develop a plan for what you’ll move to the cloud and how you’ll do it. See the February 22, 2013, “Predictions For 2013: Cloud Computing” report.

15 Enterprise use of the cloud is now a reality and cloud use is no longer hiding in the shadows. IT and security departments can no longer deny the movement to cloud is real and business leaders that want the flexibility and economic benefits of these environments drive it. In short, cloud use in 2013 will get real. See the February 22, 2013, “Predictions For 2013: Cloud Computing” report. (http://www.forrester.com/home#/Predictions+For+2013+Cloud+Computing/quicksan-/E-RES88042)

16 S&R professionals need to be aware of the security issues surrounding big data so they can take an active role early in these initiatives. See the July 12, 2012, “Control And Protect Sensitive Information In The Era Of Big Data” report. This report will help S&R pros understand how to control and properly protect sensitive information in the era of big data.

17 From a technology perspective, identity management is one of the more developed areas of cloud security. Many of the applicable identity solutions for cloud are founded upon federated identity standards and products originally developed for extranet or SOA environments. Repositioning them for cloud requires some modification but is generally considered simpler than other techniques. The major
identity management vendors — CA, IBM, Microsoft, Novell, and Oracle/Sun — leverage standards and specifications such as SAML, OAuth, and WS-Federaion to expand their web access management and identity provisioning solutions. See the July 19, 2012, “The Forrester Wave: Enterprise Cloud Identity And Access Management, Q3 2012” report.

The National Institute of Standards and technology provides a well-accepted definition of cloud computing and cloud architecture. It is considered by most to be the gold-standard definition most often cited when defining what cloud computing is. Source: Mell, Peter; Grance, Timothy, The NIST Definition of Cloud Computing NIST 800-145, 2011. (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)

The tech services market is about to undergo a massive transformation that will call traditional provider business models into question. Four factors will combine to dramatically change the dynamics, economics, and.

FedRAMP is by far the most comprehensive framework specifically written for CSPs and unlike other frameworks, it requires an annual certification process performed by an independent third party. The burden of control implementation and ongoing compliance is entirely on the provider. Control transparency is readily available to the customer, as the entire control and assessment framework (over 300 individual control points for the CSP) is available for download. The framework is based on NIST along with additional controls specific to the FedRAMP certification requirements. AWS has been certified with ATO (Authority to Operate) in compliance with FedRAMP. See the October 29, 2010, “Q&A: Demystifying Cloud Security” report.

You can also read “AWS GovCloud (US) Achieves a FedRAMP Compliant Agency ATO,” Amazon Web Services (http://aws.amazon.com/about-aws/whats-new/2013/05/20/aws-govcloud-us-achieves-fedramp-agency-ato/).
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