Introduction

Public and private clouds are extending their reach across business functions and networks, remaking the way companies store, manage, and share data. Nearly all large organizations use some form of cloud computing, according to a 2012 study conducted by the Open Data Center Alliance, and many are finding the technology to improve efficiency, productivity, and agility in ways that would have been unimaginable only a few years ago.

Yet over this environment of promise and change hangs the need for robust security and strong controls. Openness and interoperability are balanced against the need to shield sensitive information and protect against negative impacts on business. That means enterprise-class computing must include protections that are built into the foundation of cloud platforms and extend to all endpoints.

Meanwhile, the task of securing the cloud is becoming more complex. The same initiatives that ratchet up business rewards also amplify dangers; strategic use of social media, bring your own device (BYOD) policies, and the rise of networks that intertwine with business partners, third-party sites, and customers all pose data-management challenges. This fast-changing risk portfolio requires companies to think about cloud security in a fundamentally different way from conventional IT security, and adopt an information-centric approach that extends beyond traditional “defense in depth,” which relies solely on multiple layers of security controls and protections. “The security landscape of 2013 is very different to that of 2001,” says Richard Evans, a principal at IT consulting firm Ovum. “There were no enterprise social networks, tablet computers, or cloud collaboration services.”

Our global survey of 200 business and IT executives shows that the biggest challenge to using the cloud is ensuring consistent security, a view held in every region of the globe. In fact, concern over this issue dwarfs any of the other challenges of cloud computing, such as regulatory compliance, the fragmentation of information, and data migration problems.

What is a cloud platform?

At its most basic, a cloud platform—also known as Platform-as-a-Service (PaaS)—is a system that delivers over the Internet (and as a utility) the easy-to-deploy infrastructure and services needed to develop, prepare, and run applications, as well as other services, including application integration and portals. The pre-built infrastructure rapidly unlocks the key benefit of these platforms by removing the considerable developer time and bandwidth traditionally required to make applications ready for use (e.g., server administration, software maintenance, OS patches, and application upgrades) with on-premise alternatives. Instead, cloud platforms enable developers to focus solely on coding innovative applications. Cloud software typically works in “stacks,” with Infrastructure-as-a-Service (IaaS) sitting at the bottom, Platform-as-a-Service (PaaS) in the middle, and Software-as-a-Service (SaaS) positioned on top.
Users are adopting a variety of approaches to address security for cloud platforms. Survey respondents identified as “leaders” in adopting and exploiting cloud technologies—based on their planned investment in clouds, adoption of cloud platforms by a majority of business functions, and approach to managing cloud risk—stand out from their peers on security as well. They are more likely to emphasize concerns about operational risk, and less likely to focus on data security and IP risk. Leaders also stress the establishment of strong BYOD policies and manage risk by focusing on specific business functions and associated workflows.

Security also rates as the leading challenge associated with the use of business networks in the cloud—environments that go beyond traditional marketplace functions to allow complex business-to-business collaboration. The high level of integration and coordination across networks and multiple service providers also raises the threat level; approximately two-thirds of respondents identify security as their primary concern about business networks, a finding that is remarkably consistent across regions (65%), industries (65%), and company sizes (63%). But the fact that a vendor might host or manage software, infrastructure, or platforms means that a high level of integration and coordination must exist across networks and multiple service providers.
Protecting the Cloud

Fig. 2: Business networks need protection

% of executives who view security as a major challenge to their business networks

Human factors must also be addressed. Cloud security requires strong governance models, along with clearly articulated policies, employee education, and ongoing training, as some breaches occur due to worker error or unanticipated breakdowns in processes and workflows.

Securing the cloud means addressing this broad array of issues. To do this, information must be classified and tracked more effectively, computing environments must become more scalable and extensible, and cooperation across enterprises must improve. “The increasing use of mobile technology and clouds is creating a data dispersion that leads to significant security and business integrity concerns,” says Lincoln Wallen, Chief Technology Officer at DreamWorks Animation. Keeping up with data as it moves far beyond traditional confines is the challenge of cloud security.

“The increasing use of mobile technology and clouds is creating a data dispersion that leads to significant security and business integrity concerns.”

Lincoln Wallen, Chief Technology Officer at DreamWorks Animation
Who took the survey?

This report, the third in a series of papers that analyze the strategic adoption of cloud computing, is based upon a global survey of 200 senior business and IT executives, conducted in December 2012 and January 2013. The largest group of respondents (16%) came from the US, followed by Brazil, India, Mexico, and the UK (13% each); Germany (10%); Canada (9%); China (6%); Japan (4%); Australia (3%); and Saudi Arabia (3%). Respondents came from five industries: retail (29%), consumer products (28%), banking (25%), telecommunications (13%), and capital markets (7%). More than one-quarter of respondent companies had sales between $1 billion and $4.9 billion. Larger companies made a significant showing, with 10% of respondents reporting sales between $5 billion and $9.9 billion, and 12% over $10 billion. Small and mid-size firms also were well represented: Nearly one in five respondents had sales of $25 million to $99 million, while 18% had sales between $100 million and $499 million, and 14% weighed in between $500 million and $999 million. Chief Executive Officers made up the largest group of respondents (25%), followed by IT infrastructure managers (19%), business-unit heads (15%), and Chief Intelligence Officers (13%). Other titles included Chief Operating Officers (8%) and Chief Innovation Officers (7%), along with Developers, Chief Architects, and EVP/SVP of Technology, Operations, and Marketing.

In addition to the quantitative survey, we conducted interviews with executives at Bonobos, DreamWorks Animation SKG, Mövenpick Hotels & Resorts Management, NYSE Euronext, and Verizon Terremark. We thank everyone who participated in the research.

Fig. 3: Respondents by title
Building security into the cloud

Many of the fears associated with cloud computing and cloud platforms are rooted in the fact that data often resides outside the walls of the enterprise. The idea that an outside vendor or service provider stores and manages an organization’s data—including valuable intellectual property and highly sensitive documents—is nothing less than unnerving for CIOs, CSOs, and other executives. These concerns are understandable, particularly in an environment where technology undergoes constant change, and vendors frequently come and go.

What’s more, the business environment is becoming riskier. Symantec, in its *Internet Security Threat Report 2013*, for example, notes that threats are increasingly targeted, sophisticated, and destructive. These attacks and intrusions take place with greater frequency, and with a growing focus on cyber-espionage and phishing techniques.

The dangers are even more prevalent given the way cloud platforms are deployed. In many situations, cloud services fall within specific departments or groups with varying requirements and knowledge of security practices. “While there is a tremendous opportunity for CIOs and other top executives to be champions and brokers of cloud computing, there are also tremendous compliance and security risks that line-of-business executives don’t want to handle—and many aren’t equipped to deal with,” says John Considine, Chief Technology Officer at Verizon Terremark.

One thing that makes cloud seem so risky is the difficulty in knowing exactly where data is stored at any given moment—including intellectual property and customer information and records. Virtualization technology creates multiple instances of data, and in many cases the data can reside on partner and third-party servers—sometimes without the knowledge of cloud users. Difficult situations can arise easily—when a company goes out of business, for example, or is sold—and a service-level agreement (SLA) is only as good as the ability to enforce it. Unsurprisingly, then, data integrity and IP protection are major concerns when operating business networks in the cloud.

---

“While there is a tremendous opportunity for CIOs and other top executives to be champions and brokers of cloud computing, there are also tremendous compliance and security risks that line-of-business executives don’t want to handle—and many aren’t equipped to deal with.”

John Considine, Chief Technology Officer at Verizon Terremark

---

**Fig. 4: Security trumps data integrity and IP protection**

Major challenges associated with cloud-based business networks

<table>
<thead>
<tr>
<th>Security</th>
<th>60%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data consistency (e.g., master data across applications and job roles)</td>
<td>50%</td>
</tr>
<tr>
<td>IP protection issues</td>
<td>50%</td>
</tr>
<tr>
<td>Proprietary integration interfaces</td>
<td>45%</td>
</tr>
<tr>
<td>Lack of end-to-end monitoring</td>
<td>40%</td>
</tr>
<tr>
<td>Lack of qualified, interested partners</td>
<td>30%</td>
</tr>
<tr>
<td>Lack of expertise or direction in-house</td>
<td>20%</td>
</tr>
<tr>
<td>Internal resistance to change</td>
<td>10%</td>
</tr>
</tbody>
</table>

% of respondents
But for New York-based clothing retailer Bonobos, a third-party provider is part of the solution as well. Bonobos, a fast-growing, web-centric business, uses a vendor to store and manage cloud-hosted customer data, including credit card information, says John Rote, the company’s vice president of product and experience. “The service provider is able to deliver a much higher level of PCI compliance [a payment-card industry data-security standard] and overall protection than we are capable of achieving on our own,” he says. This approach also “alleviates the day-to-day complexity and stress of managing security details.”

At NYSE Technologies, the commercial technology division of the NYSE Euronext stock exchange company, an industry-specific Secure Financial Transaction Infrastructure (SFTI) wide-area network provides for a high level of protection. It establishes strict controls for the approximately 2,000 firms that connect to the firm’s infrastructure. “Unlike a generic cloud-based environment, where every node or VM in the cloud needs to be able to talk to any computer, anywhere in the world over the Internet, this cloud requires a much higher level of security and therefore cannot be accessed directly over the Internet,” says Feargal O’Sullivan, SVP and Head of Sales for the Americas.

Overall, 80% of survey respondents identify data security and IP risk among their top three concerns of operating in the cloud. Among cloud leaders, this figure drops significantly, to 65%. But leaders’ views converge with others when it comes to regulatory and compliance risk, as 79% of all executives rank this among their top three concerns, along with 75% of cloud leaders. A similar, stronger pattern is evident in their concern over brand and reputational risk: 78% of both groups rank this among their top three concerns (see Fig. 5). Clearly, the ability to operate in strict legal compliance while protecting brand value is of fundamental importance; violations in the former case can result in significant fines and penalties, while injuries to reputations can lead to diminished trust among the press and public. A spate of high-profile data breaches over the last few years, including Citibank, Equifax, Visa, MasterCard, Barnes & Noble, LinkedIn, LivingSocial, Jawbone, and the CIA website have done little to diminish these fears.

**Fig. 5: Where leaders diverge—and where they join the crowd**

Perceived risks in the cloud (% moderately to highly concerned about these risks)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Leaders</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data/IP security risk</td>
<td>64%</td>
<td>64%</td>
</tr>
<tr>
<td>Financial risk</td>
<td>69%</td>
<td>69%</td>
</tr>
<tr>
<td>Reputational risk</td>
<td>65%</td>
<td>65%</td>
</tr>
<tr>
<td>Regulatory and compliance risk</td>
<td>71%</td>
<td>71%</td>
</tr>
<tr>
<td>Business continuity risk</td>
<td>54%</td>
<td>54%</td>
</tr>
<tr>
<td>Operational risk</td>
<td>56%</td>
<td>56%</td>
</tr>
</tbody>
</table>
Avoiding such problems requires a focus on security from the start, and an understanding of how different systems affect risk. Mr. Wallen at DreamWorks Animation puts it this way: “The practical deployment of clouds, along with the integration and coordination they require, actually increases data fragmentation and complexity in enterprise. It’s crucial to address this question of where the data fits and how to orchestrate it appropriately in order to satisfy corporate security policies, access policies, and other requirements.”

Security issues are also increasingly shifting to mobile environments. In fact, the use of mobile devices generates a variety of concerns, particularly as organizations adopt BYOD, and users merge personal and company data on the same devices. There are liability questions (who is accountable for private and corporate data?), and the possibility that privately installed software (apps) could violate corporate security policies. A lost or stolen smartphone or tablet can result in significant damage to corporate data security—and damage can spread rapidly through cloud environments and virtualization tools that replicate data and create virtual machines. Although the gains related to employees using personal devices for work are substantial, these smartphones and tablets must be managed to minimize the occurrence of rogue apps and ensure that data is not misused.

Many organizations are turning to mobile device management (MDM) solutions to manage devices and data; these solutions also provide security features such as “remote wipe,” in case a device is compromised. Yet while MDM and other security tools such as virtual desktop infrastructure (VDI), encryption, and endpoint systems can aid in protecting data, executives must adapt policies, codes, and rules that provide a framework for digital business. What’s more, it is vital to formulate appropriate policies and rules for different constituencies and groups within an organization.

For this reason, some companies are opting to supplement traditional security tools such as authentication, encryption, malware protection, and data loss prevention (DLP) with more nuanced strategies centering on data. For example, some organizations now restrict their most valuable data to internal servers while relying on cloud applications, services, infrastructure, and platforms to support core functionality and business operations. In other words, the application or development platform may run in the cloud, but the data remains in house.

Security-savvy organizations also recognize that external threats are only part of the overall picture. Employees, independent contractors, and customers also represent risks, since nothing is as dangerous as an employee with bad intentions.
In all, 65% of respondents report that physical and network security is a challenge in cloud environments. One-third say that end-to-end monitoring is a challenge. Ultimately, cloud security—like all enterprise security—involves more than technology and technical acumen. It requires a thorough understanding of business processes as well as systems, connection points, and processes—so that security executives can map out data flow and put the right combination of tools and strategies in place to provide maximum protection. Only then is it possible to build an enterprise-wide cloud platform security strategy.

Our survey finds that executives have security concerns in a number of areas, including cybercrime, virus attacks, identity theft, and security of APIs and interfaces. These worries are fairly consistent across the four industries surveyed, with consumer products standing out somewhat for its greater fear of identity theft and unauthorized access to data. But all industry groups still need to take these risks more seriously.

**Fig. 6: Industries agree on security issues**

Top security worries in the cloud

- Security of corporate data
- Security of IP
- Security of customer data
- Security of API and interfaces
- Identify theft
- Unauthorized people accessing sensitive data
- Virus attacks
- Cybercrime

% of respondents
Taking a more secure approach

Organizations that adopt a comprehensive and holistic approach to security are better equipped to deal with the challenges that inevitably occur in cloud environments. This requires a focus on information and how it flows into and through the enterprise. Although specific and targeted security tools remain important—the traditional multilayered approach is not going away anytime soon—they are not strong enough to adequately protect an organization in the era of the cloud.

An organization concerned with security should map out its business processes and workflows to understand potential vulnerabilities. It is also essential to classify data and know how they are being shared and stored throughout their lifecycle. In many instances, sensitive archival data might reside in the cloud—unbeknownst to business and IT leaders. What’s more, as business networks reach across groups of organizations, data increasingly flows through third-party servers and outside organizations. “It’s critical to understand where data is localized and how it moves around in a cloud service provider’s environment,” notes Mr. Wallen of DreamWorks Animation.

But an effective strategy requires more than simply identifying and classifying data into tiers. It is critical to understand the value of specific data sets and the potential cost of a data breach, and at the same time to identify gaps in existing compliance and security policies. Understanding the types of damage that can occur if these gaps are exploited is also important. These vulnerabilities can affect everything from brand image to sales, share price, and employee morale.

Armed with a complete picture of a threat environment, it is possible to assemble security systems and tools in a far more targeted way. Companies can configure and layer firewalls, VPNs, data encryption, DLP tools, web filtering, MDM software, and anti-malware tools for the specific requirements of the enterprise—as well as the context of a particular situation. These systems must also provide scalability and flexibility, and the capabilities must extend to servers, bandwidth, software applications, and other areas. Vendors should be required to provide total transparency and access to all log files so that an organization can track data and estimate security risks. Finally, there is data privacy to consider: The breach of sensitive customer information can result in bad press, damage to a brand, diminished sales, potential fines or lawsuits, and government action.

Fortunately, respondents are taking steps to address security risks in the cloud. These include installing identity and access-management tools (61%), performing regular security audits (55%), tracking users (53%), and embedding traditional/onsite protections in cloud applications (50%). Other measures include collaborating with cloud partners on security strategy and implementation (37%) and engaging third-party security partners (16%). Only 2% of respondents say they have taken no steps to deal with cloud security risks. Large companies ($5 billion to $9.9 billion in revenue) tend to be more active in these areas; mid-size firms ($500 million to $999 million) often lag their smaller and larger peers. Again, leaders stand out: They focus on overall IT security rather than individual business units and departments, and show a high degree of collaboration and cooperation with third-party service providers. Governance ranks at the top of their security strategy.
Organizations must also increase the use of education and training; these too must continue to evolve in order to keep up with the threats. Today’s rapidly morphing security risks include ever more ingenious attacks. In some cases, attackers are willing to invest months or years to extract small pieces of data that, once assembled as a whole, represent enormous value. They also are using phishing techniques, SQL injection, and an assortment of other methods that specifically target individual workers—and that often appear to be part of legitimate business operations. Today, basic knowledge of security issues, risks, and requirements must extend across the entire organization and out to the ecosystem in which a corporation does business.

Finally, it is critical for enterprises to avoid a locked-in approach to security. Most organizations should take an open-standards approach and ensure that vendors do not box them in with a set of proprietary tools and technologies. In fact, some executives are turning to a Security-as-a-Service approach in order to plug in protections in a more agile and flexible manner and avoid ongoing patches, upgrades, and changes.

Today, basic knowledge of security issues, risks, and requirements must extend across the entire organization and out to the ecosystem in which a corporation does business.
Views from the executive suite

Where you stand on cloud security depends on where you sit. Views differ, sometimes sharply, according to the title of the respondent. For example, 52% of business-unit heads say that the biggest challenges they face from cloud computing is ensuring consistent security. CEOs see things the same way, but IT executives (39%) and executives in operations (30%) are less likely to list security as their top challenge.

Why the disconnect? IT and operations have a more granular focus on all aspects of cloud computing, which gives them a variety of things to worry about, from regulatory compliance (a major concern for operations) to avoiding silos in information and business process flows (more of an issue for IT than any other group). CEOs and business-unit heads, meanwhile, are most attuned to the high-level business risks of security problems.

This pattern continues as one looks deeper into the survey data. For example, CEOs are more focused on the financial risks of cloud adoption (70% concerned or highly concerned) than are IT executives (58%); CEOs also worry more about brand and reputation risk (62% vs. 54%), while IT is somewhat more concerned with the nuts-and-bolts of regulatory compliance than chief executives.

The lesson from these numbers is unsurprising, but bears repeating: Security in the cloud is a multi-faceted problem that presents issues across the enterprise.
Securing gains

Cloud leaders place a premium on centralized identity and access management, have embedded traditional security tools in the cloud, are more likely to perform security audits on a regular basis, and collaborate with cloud partners on security strategy and implementation. Overall, these organizations address cloud security in a comprehensive and holistic manner. They build these defenses into the fabric of their cloud platforms from the beginning and constantly reevaluate their needs as technologies and business requirements change. Executives at these cloud-savvy firms typically focus on several key issues:

■ **Tearing down silos.** In many instances, gaps and breakdowns occur when different departments or divisions procure cloud services—sometimes in a haphazard or ad hoc way. An organization must integrate services and platforms to ensure that tools, systems, and strategies function comprehensively.

■ **Adopting strong integration tools and practices.** Well over half (58%) of respondents have purchased integration tools. Almost as many (55%) have a dedicated team focused on cloud integration, while 52% use integration-service providers. All three of these approaches are crucial.

■ **Developing solid communications with cloud providers.** It is important to understand roles and responsibilities, and to know what is included in service-level agreements (SLAs) and what third-party certifications a vendor has achieved. Companies should be well informed regarding what security protections are offered, particularly when tiered service options exist, and how and when maintenance, patches, and upgrades will take place.

■ **Implementing data-centric controls.** Once an organization has identified and classified its data, it is essential to have a strategy to ensure that the data is managed and stored in a secure way. This may include the use of encryption, firewalls, and numerous other tools. Virtualization and cloud make this task more difficult—but even more essential. Visibility into systems—including hosted services—is key.

■ **Applying role-based authentication.** A cookie-cutter approach to authentication is an invitation for problems. Secure access—knowing that only those with the right credentials can access data—serves as the foundation of an effective cloud strategy.

■ **Using VM (virtual machine)-specific tools.** When it comes to clouds and cloud platforms, data boundaries and separation are everything. The use of physical and virtual firewalls—as well as other security tools that ensure that data isn’t inadvertently shared—is a vital component.

■ **Insisting on complete oversight.** A secure enterprise requires full knowledge of operations at any given moment. This translates into a need for robust audit capabilities, user tracking, ongoing risk assessment, regular compliance inspection, and consistent reporting. In some cases, compliance must function across multiple organizations.

■ **Maintaining physical security.** A vendor or hosting service must have strong physical protections in place, including access controls and 24x7 video surveillance and monitoring systems that can detect unauthorized access to server rooms and other sensitive areas.
Conclusion

As cloud platforms enter the enterprise, organizations must review, update, and sometimes reinvent security practices for a new and different era. There is a growing realization that vendors offer an equivalent—if not superior—level of protection than exists within an enterprise. Although many of the fundamentals of cloud security are the same as those in the traditional client-server world, it is critical to apply broader and more information-centric thinking to the challenge.

Currently, about 62% of organizations put the IT department in charge of managing cloud risk. About 21% rely on a risk/legal department, 10% rely on finance, and about 6% depend on operations. Although there is no one-size-fits-all approach, organizations must make cloud data security an enterprise issue and involve executives from all corners of the organization in order to ensure that a holistic and comprehensive model is being used.

As Roger MacFarlaine, Vice President, Technology and Systems at Mövenpick Hotels & Resorts Management, an operator of 71 hotels in 25 countries, puts it: “The question isn’t whether to be in the cloud—this is inevitable. It’s how to build the best security possible into a cloud environment. It’s important to start with the mentality that you will find a way to build in protections.”

In the end, a robust and effective cloud security strategy revolves around a comprehensive and well-defined plan, incorporated into existing on-premise landscapes. A thorough understanding of vulnerabilities and gaps, a trusted relationship with cloud vendors and service providers, and a clear understanding of long-term goals are the essentials.

More than anything else, clouds and cloud platforms require a more nuanced and layered approach to security. Organizations that assemble a strategy and put the right components in place are in a position to reap the benefits of clouds and achieve a strategic advantage. They are able to outsource software, services, infrastructure, and various other IT tasks—while achieving the controls and protections necessary for the digital age.