WHITE PAPER | **CLOUD SECURITY**

Cloud Security Myths and Strategies Uncovered

Forward-thinking CSOs are embracing the right security strategy and exercising appropriate caution without dampening cloud optimism. By overcoming the number one *perceived* challenge—security—CIOs can move beyond their fears to pursue their IT transformation to cloud computing.

In today's evolving information economy, cloud computing offers immense opportunity. Whether companies have started their cloud journey or not, security concerns remain the largest inhibitor to adoption. Concerns around control, data privacy, and security abound. However, the technology and expertise required to build a trusted cloud is closer than imagined. Progressive CSOs are embracing a new strategic role as a true business enabler in partnership with business leaders, to make sure that the trusted cloud becomes a reality and enterprises can capitalize on cloud technology.

Cloud computing is heralded as the latest and greatest opportunity in IT service delivery, facilitating on-demand access to shared pools of computing resources—from networks and storage to servers and applications. On top of efficiencies and cost reductions, it promises rapid delivery of services for business agility. Adoption is so pervasive that *CIO*'s 2011 Global Cloud Computing Adoption survey reveals two-thirds of responding organizations are planning or adopting cloud computing. In addition, 88 percent of respondents say they would use cloud computing more if it had the same or better security than the datacenter.

Still, security and compliance concerns continue to slow adoption—it's consistently the number one cited challenge to cloud computing. "After all, if you can't be secure in the physical world, what might the cloud introduce?" asks Arthur W. Coviello, Jr., executive chairman for RSA, the security division of EMC. While public cloud deployments offer compelling scale and cost considerations, most investments are in private cloud environments that afford more control and visibility for security-conscious buyers. However, recent trends point to adoption of a hybrid cloud model, combining the security and performance benefits of private environments with the cost and scale advantages of public cloud services.

Fortunately, security spending is getting its fair share of budget, too. According to *CSO*'s 2011 Global State of Information Security survey, 52 percent of respondents indicate that security spending will increase over the next 12 months. They cite client requirements as justification for security spending, as well as potential data exposure. Negative business impacts from security events—everything from direct revenue loss to brand damage—have increased 233 percent over the past four years. Now, after years of talking about reputational risk, enterprises understand its real impact and are addressing it.

It's these business impacts that clearly tie information security to cloud initiatives—with the cloud model extending positive impacts, and security measures protecting against negative impacts.

TOP OF MIND CONCERNS: CONTROL AND VISIBILITY

Fifty-six percent of the IT and business leaders surveyed by *CSO* say managing access to data in the cloud is a top challenge. With the amount of data being generated, the number of identities and devices accessing the cloud, and the ever-changing infrastructure, these leaders recognize that today, they may not have the needed controls and lack

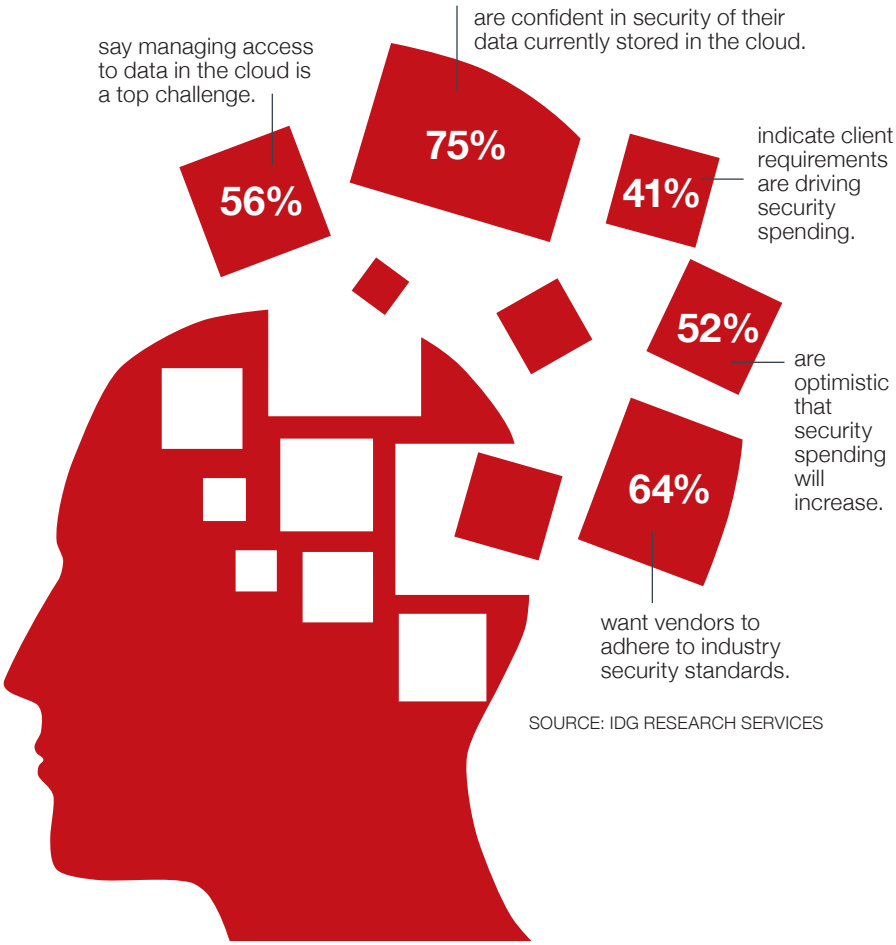
vmware®

RSA®

CSO
Custom Solutions Group

What's Top of Mind for CSOs?

RESEARCH REVEALS:



SOURCE: IDG RESEARCH SERVICES

real-time visibility. They can't manage what they can't see and they can't secure what they can't manage. Many enterprises struggle with the complexities of managing a siloed environment for which change management and compliance are cumbersome—not to mention the dynamic nature of cloud environments, where data and applications move about at a moment's notice. But starting with a foundation of virtualization actually provides greater visibility than legacy approaches.

When evaluating cloud vendors, IT and business leaders look for the ability to meet security mandates such as PCI and HIPAA, and integration capabilities. They also call for vendors to adopt industry-standard frameworks, meet organizational security standards, and allow independent audits. Many of these same requirements have been written into SLAs for years, towards which many have turned a blind eye in the race to embrace cloud computing.

It's clear that security and technology executives place a high premium on the ability to maintain control over their data and infrastructure, and the required visibility across physical and virtual components. This acknowledges the need for hands-on management of cloud infrastructure. Enterprises need to be able to affect policy, continuously monitor activity, and prove compliance, all of which requires tight integration with on-premise capabilities and full visibility across internal and external environments.

SECURITY HANGING IN THE BALANCE BETWEEN CAUTION AND OPTIMISM

But this renewed interest in security doesn't put anyone on Easy Street. Indeed, *CSO*'s research reveals diverging market conditions, and information security hanging squarely in the balance.

Uncertainty in the recent world economy means tight fiscal discipline, and key security practices are taking a backseat. And although fewer security incidents have surfaced than expected, the negative impacts on business in terms of exposure have been astonishing. In the midst of this, information security has gained greater appreciation throughout the enterprise. Client requirements are driving spend, and enterprises have better visibility into incidents and are raising the stakes. *CSO*'s research indicates the highest level of optimism about security spending in the last 15 years. This certainly bodes well for cloud initiatives.

DEBUNKING SECURITY MYTHS

With optimism in the air, cloud adoption must move forward—starting with the debunking of lingering misperceptions:

- MYTH: **The cloud simply cannot be secure.** The cloud environment absolutely *can* be secure—in fact, it can be even more secure than a datacenter. "But not all clouds are created equal," explains David Hunter, CTO of platform security at VMware. "Nor, for that matter are all datacenters." There are varying levels of vendor capabilities that make for varying levels of security. Enterprises must establish clear criteria for maintaining control and visibility. Here, an enterprise hybrid cloud model is very compelling, delivering the same common security standard across both public and private environments without compromising enterprise-class requirements or cost. And common security standards offer the flexibility to choose the right cloud deployment model. It's not about a generic security level for the cloud; it's choosing the right security for *your* cloud.

CONTROL + VISIBILITY = TRUST

CONTROL

- **AVAILABILITY:** Ensure access to resources and recovery following interruption or failure.
- **INTEGRITY:** Guarantee only authorized persons can use specific information and applications.
- **CONFIDENTIALITY/PRIVACY:** Protect how information and personal data is obtained and used.

VISIBILITY

- **COMPLIANCE:** Meet specific legal requirements and industry standards and rules.
- **GOVERNANCE:** Establish usage rights and enforce policies, procedures, and controls.
- **RISK MANAGEMENT:** Manage threats to business interruption or derived exposures.

- MYTH: **Cloud security is a new challenge.** The truth is cloud security *isn't* new; it's not even unique. "Security concerns are really independent of the cloud," claims Coviello. "They're just an extension of what's being dealt with in the physical infrastructure." Cloud computing changes the playing field, but most of the underlying security concerns, such as protecting the infrastructure and sensitive data, are old news—and within the scope of today's capabilities. Security and governance requirements are the same regardless of physical, virtual or cloud components. In the cloud, the manner in which controls are implemented changes, as does the velocity of change, making control and visibility even more important. In fact, because of virtualization technology, the cloud can be more secure than the physical environment. An investment in virtual security can provide the needed control and visibility for cloud.

- MYTH: **Compliance equals security.** Many enterprises believe that if they are certified as compliant, their systems are secure and invulnerable to attacks. In truth, compliance *doesn't* ensure security, but only attests to the state of security at a specific moment in time. Often compliance standards that are reliant on human adherence to policies and procedures instead of automation can produce errors between audits. In the long run, equating security to compliance—and vice-versa—puts the business at risk.

TRUSTED CLOUD EQUATION: CONTROL + VISIBILITY = TRUST

A cloud deployment that defies these myths is built on trust. Trust cannot be achieved without control and visibility across the cloud infrastructure, identities, and information. "Trust becomes an overarching issue—whether dealing with internal standards or regulatory concerns," adds Coviello.

The most precarious aspect of cloud computing is that information and infrastructure components are not always under the direct control of the IT organization. Control involves availability, integrity and confidentiality—ensuring access, but only to authorized users and only in a way that protects data. In terms of visibility, it's all about governance, risk management and compliance (GRC), meeting specific requirements to enforce policy and manage threats.

An "out of sight, out of mind" mentality only spells trouble. "What's out of sight should actually be top of mind. To that end," says Hunter, "enterprises need an appropriate level of control and visibility to ensure that sensitive data is being properly managed, that the right access is being granted to the right people, and that organizational and industry security standards are being upheld—just like they have in their internal environments, but with the dynamic control and change management necessary for a cloud environment."

VIRTUALIZATION: THE CORNERSTONE FOR CLOUD CONTROL AND VISIBILITY

What will it take to enable the necessary visibility and control in a cloud environment? How will enterprises be able to monitor activity and obtain transparency inside a provider's environment? The answer is virtualization.

"Security in the cloud is better as a result of virtualization," says Hunter, making the cloud "even more secure than your physical datacenter." Virtualization consolidates multiple physical components into a logical view so they can be administered from one place. This alleviates the complexity of managing and monitoring multiple moving parts across internal and external infrastructure. Virtualization is the cornerstone of greater control and better visibility.

Virtualization accommodates the fundamental attributes of a trusted cloud environment. It makes security as dynamic as the computing environment. Virtualized security can create zones of trust around information, applications and endpoints—not just infrastructure components—and can be adapted to follow workloads through the cloud. Automated policies can assess risk and immediately initiate remediation.

Checklist for Your Trusted Cloud

WHEN IT COMES TO BUILDING A TRUSTED CLOUD:

- ✔ Use virtualization as your foundation.
- ✔ Build control and visibility into your security framework.
- ✔ Extend your security perimeter to include applications and endpoints.
- ✔ Adopt the three-layer controls framework: controls enforcement, controls management, and security management.
- ✔ Select a cloud vendor with offerings that can meet enterprise-class cloud security requirements across private and public clouds.
- ✔ Ensure services are secured to a common standard, in a transparent and auditable fashion.
- ✔ Tap prescriptive guidance from industry coalitions such as the Cloud Security Alliance (www.cloudsecurityalliance.org).

A FRAMEWORK FOR SUCCESS

A cloud implementation must ultimately create trust zones in a lightweight, streamlined process with automated policy enforcement. The framework for a trusted cloud is comprised of three critical layers of control:

1. **Control enforcement layer:** Security enforcement occurs at this layer. Controls are embedded directly into the virtualization infrastructure for complete coverage and consistency, while simplifying management. This provides protection for the perimeter, information, applications, and even endpoints. It leverages the appropriate security technologies, such as firewalls and accelerated antivirus protection.

2. **Control management layer:** At this layer, enterprises provision and monitor security controls by consolidating administration. Role-based access control enables management and integration of third-party security services. Enterprises must enforce policy for sensitive data, and manage authentication requests and encryption keys.

3. **Security management layer:** Policies for compliance, best practices, and risk management are defined here. This layer manages events and alerts, and remediates them as necessary. Integrated GRC tools map regulations and standards to policies, identify risk, analyze and prioritize event data, and continuously assess, remediate, and verify compliance.

The technology required to build a trusted cloud is already available and can be implemented within the network. "It's really just a matter of adapting the fundamental security controls you have in a physical environment into your cloud, while taking advantage of virtualization technology," says Coviello. Security needs to be applied and managed a bit differently, but by tightly integrating technologies across the framework outlined above, enterprises gain a holistic view of security and compliance with unparalleled control and visibility.

THE NEW CSO: A BUSINESS ENABLER

So what does all of this mean to the CSO? With IT innovations like cloud computing driving business strategy, information security is infinitely more important—from the datacenter all the way up to the boardroom—putting senior management in the hot seat.

As a result, security leaders are no longer back-office tacticians, but front-office strategists. Progressive CSOs are high-level risk managers, and must deliver strong business value in partnership with the CIO and other C-level peers. According to *CSO*'s security study, CSOs are increasingly reporting to the CEO, CFO, COO, or even the board of directors.

That's a real indicator of the CSO's budding influence as an innovator and evangelist for the trusted cloud. "More than ever before, the CSO is critical in standing up the new cloud environment," notes Hunter.

THE BOTTOM-LINE REALITY

Cloud computing promises untold business opportunity, so waiting for all the stars to align is not an option, especially when it comes to security. Security is merely a perceived risk that can be overcome with today's technology. An enterprise hybrid cloud offers the perfect balance between the control and visibility of a private cloud and the agility and cost advantage that comes with a public cloud.

Remember, the real risk here is not an IT risk, it's a business risk—the risk of missed opportunity in not adopting cloud technology. Don't miss that opportunity because of misperception. ■