

Cloud Security: CIOs Have More Pressing Things to Worry About

■ **According to a recent online poll of IT and business leaders conducted by IDG Research Services, virtually all enterprises are using or plan to use at least one application and/or a portion of their computing infrastructure via a hybrid cloud model.**

While lured in by game-changing promises—everything from greater flexibility and innovation to resource efficiency and CapEx savings—CIOs still harbor concerns. “Hybrid cloud implementations effectively straddle internal and public infrastructures and can introduce complexities,” says Martin Capurro, Director of Applications and Infrastructure Solutions for Qwest, a network services provider based in Denver, CO. With two separate infrastructures, CIOs must break down barriers and even share data with their cloud provider.

The Security Debate

Obviously, security concerns wiggle their way into cloud adoption plans. After all, we’re talking about loosening control of data protection in a dual environment that can compound security risks. “A threat in one environment could permeate into the other,” explains Troy Herrera, Enterprise Marketing Director for Juniper Networks, a network infrastructure provider based in Sunnyvale, Calif. An innovative mal-intent who infiltrates a cloud application could make his way into the enterprise network, and vice versa.

But will security ultimately unravel big plans for cloud adoption? Not likely. In fact, cloud security does not appear to be as scary as other threats. Dealing with lost or stolen devices, for example, is seen as a significant security risk for 75 percent of respondents, while 65 percent point to IT consumerization and 56 percent to mobility. On the flip side, only 49 percent consider cloud security worrisome.

Perhaps that’s because respondents, in part, hope hybrid cloud implementations can actually enhance security through improved service performance, extended support, and functional expertise. Coupled with the security technologies available to mitigate the risks, cloud computing appears more contained than the booming trends that have CIOs reeling.

“The key is to implement the proper security measures with the goal of achieving end-to-end security,” says Herrera, conceivably resulting in greater overall protection.

A Mixed Bag

When it comes to locking down cloud applications, CIOs have plenty of options. They can own the function outright with on-premise implementations that ensure a single security authority, more control over data protection, full visibility into one’s risk and compliance posture and less complexity. Or they can relinquish some of their control by outsourcing security. This approach offers financial and management relief and the specialized security resources of a third-party.

Interestingly, 45 percent of the IDG survey respondents indicate that a hybrid or mixed approach to cloud security is the best option. That way, CIOs enjoy all the benefits of managed security services while keeping a tight rein on data protection. “A service provider can complement what you’re doing,” Herrera notes, “and even enhance protection.” And the approach can prove a more affordable way to add security capabilities when budgets are tight.

Of course, there may be challenges in terms of visibility and the ability to enforce security, but by working together holistically, the internal-external partnership can be exceptionally productive.

Inside-Out

One respondent advises that CIOs should “start by extending existing capabilities into the cloud.” Security is a long-standing tradition within today’s IT organizations and existing investments should be leveraged whenever possible. Some 82 percent of respondents concur, saying interoperability with existing security solutions is very important.

Security Integration for the Cloud

(Among all respondents)	Currently Implemented	Plan to Implement	No Plans
Anti-virus	85%	15%	-
Spyware	85%	10%	5%
SPAM Filters	83%	14%	3%
VPN Encryption	78%	20%	2%
Web Filtering	70%	19%	11%
Intrusion Detection and Prevention (IDP/IPS)	67%	30%	3%
Network Access Control	63%	33%	4%
Firewall upgrades to support increased WAN traffic demands	54%	34%	12%
Identity and Access management (I&AM)	45%	47%	8%
Security Incident and Event Manager (SIEM)	39%	50%	11%
Wan Acceleration/Optimization	39%	35%	26%
Data Loss Prevention (DLP)	36%	50%	14%

Source: IDG Research, October 2010

Of course, many security solutions can work together effectively—whether on-premise or in the cloud. For example, an in-house network access control solution can identify users by working with an outsourced VPN. CIOs just need to coordinate with their vendors to ensure interoperability.

Part of the process, Capurro suggests, involves integrating core infrastructure elements with the cloud environment. In fact, one respondent urges technology leaders to “make sure that the hosting provider has a clear strategy on how to extend the network into the cloud.” Today, that’s all Internet-based, but eventually the cloud will be delivered on different fabrics, such as Ethernet.

Getting Technical

For specific technology integration projects, CIOs have zeroed in on the most pressing security concerns. Most respondents have already implemented anti-virus, spyware, spam filters, and VPN technology, while many have deployed Web filtering, intrusion detection, network access control and firewalls. “These core technologies have been part of IT for a while,” Herrera says. “Now, CIOs need to focus on upgrades to accommodate the changing environment and performance shift that comes with cloud infrastructure.”

New technology investments will be critical as infrastructure becomes more complex. The top priority for roughly half of respondents in the near future will be security incident and event management, data loss prevention and identity and access management (IAM). Capurro believes IT professionals should also focus on service-level agreements for performance assurance. Application performance management solutions can supplement those agreements with needed visibility into platform performance.

No or Go?

So should CIOs embrace the cloud—even when their most critical information lies in the balance? Herrera says “absolutely, you just have to be smart in management.”

Start with savvy shopping. “The cloud is as dangerous as posting your data to Facebook if you have not done a security review of the cloud vendor,” warns one respondent. Another

advises CIOs to “use only trusted solutions.” Evaluate an offering’s scalability and performance and establish a “trust zone” for data protection. Technology solutions should be geared toward longevity and operational simplicity.

Bottom line:

When done right, there’s no reason not to reach for the clouds.

For more information

For further results and insight into this IDG Research Services survey, visit www.cio.com/whitepapers/juniper_qwest and download the whitepaper “Reaching for the Cloud.”

