Enterprise Security in the Cloud: Shadow IT Reality Check

As cloud computing offers on-demand access and less IT involvement, risks prevail and security is an absolute necessity.

Symantec

CSO Custom Solutions Group

THE IT ORGANIZATION IS LOSING CONTROL. It is no longer the purveyor of all systems and applications in use within the enterprise. Users are turning elsewhere to meet their technology needs. Increasingly, they are turning to the cloud.

But users don't understand what constitutes the cloud, the risks of using cloud computing services or the ramifications of bypassing IT. Their main concern is that applications on the Web allow them to get their jobs done more easily and faster. Worse still, IT is often ignorant of this growing, organic cloud use. And IT can't manage or secure what it doesn't know is there. The result is a glaring disparity between the use of cloud computing services and the implementation of security controls. The purpose of this paper is to educate CIOs on the reality of cloud computing use in the enterprise and how to mitigate associated risks.

The State of Cloud Computing Adoption in the Enterprise

Definitions of cloud computing are many and varied, causing confusion even among IT professionals. For our purposes, let's establish a common understanding of the cloud. According to the National Institute of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Boil that down, and the cloud is convenient, on-demand and requires minimal management effort. Compare that to the traditional IT organization, whose processes to get a new server provisioned or application procured can be seen as an obstacle to innovation. The cloud makes it easy to order, provision and consume technology services without the hassle of going through IT. It is so easy, in fact, that users embrace the cloud even when their IT organizations do not. And so we have shadow IT—use of cloud computing services without the IT organization's involvement.

More often than not, company data is put at risk by users skipping internal processes and moving corporate IT tasks to the cloud. In the Security in the Cloud Quick Poll conducted by *CSO* magazine on behalf of Symantec, 37 percent of respondents indicated they believe individual users or business units at their organization are frequently or occasionally deploying applications or putting data in the cloud without consulting IT. CSOs have no idea who these users are, but they know that the services are being used.

Determining who is using cloud computing services and what those services may be is not easy. Quite simply, many end users don't understand what constitutes cloud computing. According to the results of the NPD Group's Digital Software and the Cloud Report, 22 percent of U.S. consumers are familiar with the term "cloud computing." And yet 76 percent of U.S. respondents reported using an Internet-based cloud service in the past 12 months. But these results shouldn't be surprising. Employees have been using Web-based email services from the likes of Yahoo! and Google for

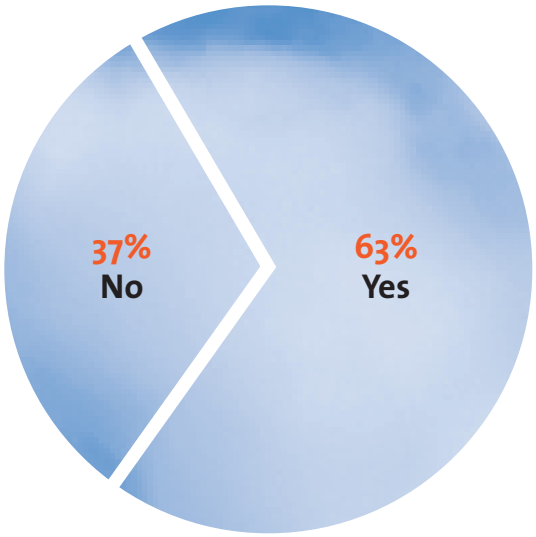
The purpose of this paper is to educate CIOs on the reality of cloud computing use in the enterprise and how to mitigate associated risks.

years. What's important to the user is that these applications help them get their job done. And they get the job done sooner than they would if they had to submit a request to IT.

Consider, for example, cloud-based file sharing. These services allow users to back up, store or share their data in the cloud where the user can access it from other devices, such as a smartphone or tablet PC. This is a hot market and users can benefit from very competitive pricing, including free services for up to 50 GB. If Bob Smith is late completing a report but he's expected at home for his son's birthday dinner, he can quickly upload the data he needs to the cloud so he can later access it from his home PC and finish his report after hours. Google Docs allows users to upload and share documents, and track changes, similar to a file share system. Instead of emailing interview notes and other background research to a freelance writer covering a breaking story, a newspaper editor puts the material on Google Docs. The writer later saves his story to Google Docs where his editor can edit and read it, and request revisions. The two continue to work this way for the duration of the project, and because of the improved efficiency, do so for future assignments as well.

Shadow IT Policies

More than three out of five (63%) organizations are putting policies or processes in place to minimize the instances in which individual users or business units are deploying apps in the cloud without consulting IT.



Base: 109 qualified completes

Other examples of cloud services employees often use outside of IT include Infrastructure as a Service where a server can be rented by the hour, cloud email, and the rampant use of social media in the enterprise. These are just a few examples of how cloud computing use can spring up within the corporate rank and file. But there are hundreds of cloud-based apps at your users' fingertips. And in reality, cloud use is often higher than either users or IT realize. While 37 percent of the CSO survey respondents recognize that shadow IT is a problem, this is likely understated since many end users don't consider using cloud-based services such as Gmail or WebEx as the cloud.

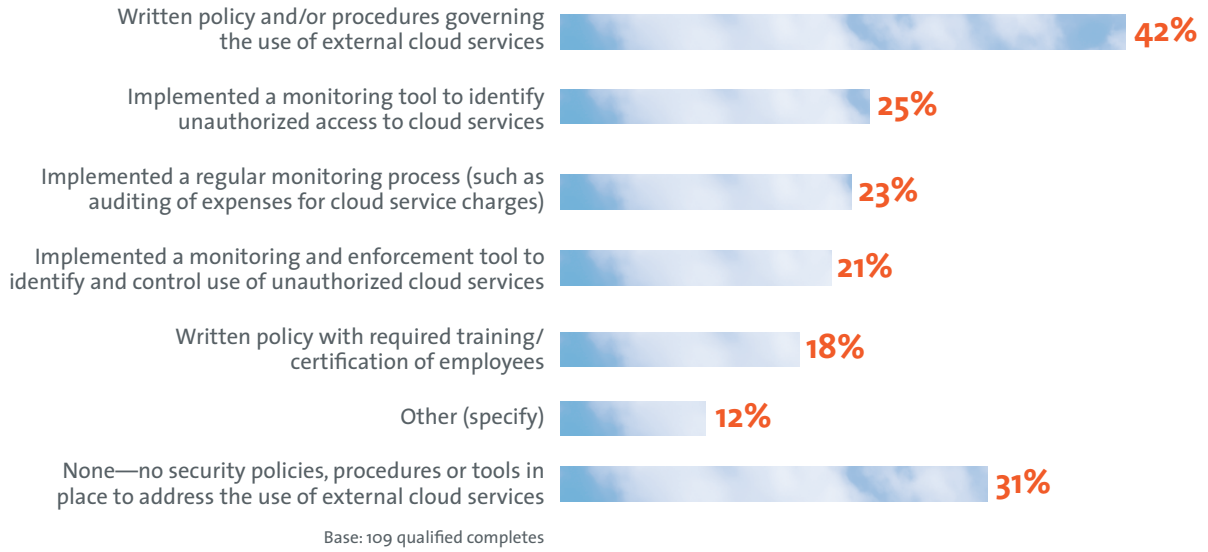
Employees and lines of business adopt applications pragmatically. They have a job that needs to get done. These applications—that happen to be on the Web—are inexpensive and can immediately meet their needs. Users are likely unaware that they are even doing anything wrong. If they can do their job and do it better, then what's the harm? But regardless of how end users think about the cloud, shadow IT is a growing risk factor. IT has the same challenges of securing critical information and protecting the enterprise regardless of whether users recognize a Web-based application as a cloud computing service.

Security Risks of Shadow IT

Cloud computing services—whether or not they are IT-approved—introduce a host of security concerns. For respondents to CSO's Quick Poll, a lack of transparency with regard to cloud providers' security controls tops the list of security concerns pertaining to the cloud. Other top security concerns include ensuring regulatory compliance at 31 percent, and setting and maintaining security policies at 29 percent. Because cloud service providers lack structured ways to report on their internal operations, including security controls, availability, uptime, and governance, IT is challenged to ensure that the service meets its security and regulatory requirements. It all comes down to controls and visibility. Cloud service providers do not have a model to provide IT organizations that visibility and control. As a result, the cloud might look like a black box to IT.

These risks are difficult enough to manage when cloud use is approved by IT, but are compounded by shadow IT. You cannot begin to mitigate risk if you don't know the risk is there in the first place. A black box, as risky as it may be, is far less dangerous if its presence is known than if its presence is not known.

Written policies are the most common way organizations govern the use of external cloud services.



Base: 109 qualified completes

How to Create a Secure Cloud Computing Strategy

From the beginning of cloud usage, IT experts and analysts questioned the security risks of putting sensitive data in the cloud. Even as the cloud matures, security remains a primary concern among IT organizations and serves as the deciding factor as to whether or not to adopt a cloud service. So it comes as a surprise that IT organizations lack a solid approach to shadow IT. But this is indeed the case as shown by the results of the CSO Quick Poll. At 42 percent, a written policy is most commonly used by organizations to govern the use of external cloud services. However, only 25 percent of organizations use a monitoring tool to identify unauthorized access to cloud services. A whopping 31 percent have no security policies, no procedures and no tools in place to address the use of external cloud services. Given the level of awareness and concerns around cloud computing's risks, one can only reason that these organizations don't know how to address shadow IT.

Reducing the risk of shadow IT can be done. At Symantec, we advise customers to take a "pick one" approach. Identify what it is that users need. If users need file sharing, collaboration or social media, choose a cloud solution that addresses that need. Effectively bless it, certify it, implement controls on it, and let your employees use it. Once you've given users what they need, lock down all competing cloud services. If you've decided to allow employees to use Dropbox, for example, block all the other Web-based storage providers: Box.net, Windows Live SkyDrive, Amazon Cloud Drive, etc. The key to making this strategy work is to use a combination of policies, process, training and tools. Simply telling employees that they can use Dropbox will not keep them from using other solutions. You must have the tools in place to monitor and prevent unauthorized cloud usage.

Symantec offers a variety of solutions to help IT organizations enable the secure use of cloud computing services.

DEVELOPING AND ENFORCING IT POLICIES:

- **Symantec™ Control Compliance Suite** addresses IT risk and compliance challenges by delivering greater visibility and control across the IT infrastructure, data and people. Through a holistic, fully automated policy management solution, IT organizations can effectively manage security risks while reducing the cost and complexity of compliance.
- **Symantec™ Data Loss Prevention** detects data transmission to public clouds while also managing risk of breach and enforcing

Once you've given users what they need, lock down all competing cloud services.

compliance. It also detects data-spill events within public clouds.

- **Symantec™ Network Access Control** controls access to corporate networks, enforces endpoint security policy and easily integrates with existing network infrastructure. Regardless of how endpoints connect to the network, Symantec Network Access Control discovers and evaluates endpoint compliance status, provisions the appropriate network access and provides automated remediation capabilities.

SECURING AND KEEPING INFORMATION AVAILABLE:

- **PGP Encryption** enforces control against breach of data through encryption of key intellectual property assets that may be stored within public clouds. It helps enterprises protect against data breaches and meet regulatory compliance requirements.
- **Symantec NetBackup™ and Backup Exec™** provides visibility into virtual file systems and applications as well as transparent backup and recovery across physical and virtual silos.
- **Symantec Enterprise Vault™** is an archiving platform that bridges the gap between legal and IT by adding intelligence to the way information is stored, managed and discovered. Enterprise Vault dedupes information, reduces backup and storage costs, and enables a repeatable and defensible discovery process.
- **Veritas™ Volume Replicator from Symantec** provides a foundation for continuous data replication, enabling rapid and reliable recovery of critical applications at remote recovery sites.

AUTHENTICATING IDENTITIES:

- **VeriSign™ User Authentication** provides strong authentication of end users of public cloud systems, allowing enterprises to control the risk of breach from unauthorized third-party access.

MANAGING SERVICES AND SYSTEMS:

- **Altiris™ IT Management Suite from Symantec** offers a modular approach to managing diverse and distributed IT infrastructures. It improves visibility while reducing operational costs.

PROTECTING THE INFRASTRUCTURE:

- **Symantec™ Web Gateway** features a comprehensive itemization of the top providers of cloud computing capability to help you hunt for shadow IT and control associated risks.
- **Symantec™ Messaging Gateway** provides inbound and outbound messaging security, with real-time antispam and antivirus protection, advanced content filtering, data loss prevention and email encryption.
- **Symantec™ Security Information Manager** enables a documented, repeatable process for security threat response and IT policy compliance via integrated log management and incident response.

Conclusion

No doubt about it, the cloud is here to stay. Whether or not IT organizations plan for cloud usage, it will happen—most likely, it is already happening. Looking the other way does not eliminate the risk of data loss or regulatory fines resulting from users bypassing IT. Security is a necessity, and Symantec can help. With 15 years of Software as a Service experience and applications that are deployed in more than 200 clouds, Symantec has an in-depth understanding of the threat landscape and is a trusted advisor on the risks that really matter. ■

For more information, visit www.symantec.com/cloud.