ONLINE REPORT
SPONSORED BY:

QTS

SPECIAL REPORT: CYBERSECURITY

BREAKING THROUGH THE SECURITY CLOUD

INSIDE

P2 SECURITY IS STILL A BARRIER TO CLOUD ADOPTION

P3 HYBRID CLOUD EMERGES AS THE FRONT RUNNER

P4 IAM IS ESSENTIAL FOR HYBRID CLOUDS

P5 ENCRYPTION IS TAGGED FOR DATA SECURITY

P6 COMPLIANCE IS A HEADACHE FOR CLOUD ADOPTION

SECURITY IS STILL A BARRIER TO CLOUD ADOPTION

Cloud computing has just about passed through its hype-and-adoption cycle, with the first rush of enthusiasm replaced by confusion over how to implement cloud and cloud services, to the point now where many public and private organizations are either in the process of adopting or planning to adopt them.

Security, however, remains a major barrier.

That's been a concern from the beginning, focused for the most part on the exposure an organization's data would have when sharing space in a cloud vendor's infrastructure with that of other organizations. This co-tenancy feature of the public cloud has been consistently high on the list of cloud users' fears.

Other threats have since joined this on the list, to where security is now seen as a broad-based concern for the cloud that spans a wide range of issues. The Cloud Security Alliance (CSA), a global forum that collects best practice expertise from both government and private organizations, last year published what it called its "Notorious Nine" cloud computing threats:

- Data Breaches
- Data Loss
- Account or Service Traffic Hijacking
- Insecure APIs
- Denial of Service
- Malicious Insiders
- Abuse of Cloud Services
- Insufficient Due Diligence
- Shared (multi-tenant) Technology

On top of these, so-called Shadow IT—apps and services that are being used without an IT department's knowledge or permission—has become a pervasive concern. Earlier in 2015, the alliance said that some 72 percent of the 200 executives and IT managers it canvassed for a survey admitted that they didn't know the number of Shadow IT apps in their organizations.

Other revelations over the past year have only served to highlight the current state of flux of cloud security. MeriTalk, for example, found that just one-third of the agencies it talked to had met a June 5, 2014 deadline to ensure that their particular cloud solutions met FedRAMP (Federal Risk and Authorization Management Program) security criteria. Nearly 90 percent of agency IT executives said they were apprehensive about migrating applications to the cloud.

The Office of Management and Budget's 2014 Federal Information Security Management Act (FISMA) report to Congress, released in February 2015, commented on security weaknesses with contractor systems, some of which resided in the cloud, found at the 17 agencies it examined. A third of them had systems that were "not compliant with FISMA requirements, OMB policy, and applicable NIST guidelines," the OMB said.

Other concerns were that agencies didn't reliably know if security controls of contractor systems and services were implemented properly, and that agencies did not have a complete inventory of systems contractors that were operating on their behalf.

Despite all of this, however, moving to the cloud has for most organizations become a matter of when and how, rather than if. Costs and other concerns mean IT organizations no longer have the resources to themselves implement and manage every system and application that's needed by agencies. The flexibility of the cloud for manipulating such things as network loads and shared services is also driving cloud demand.

Still, with security fears so rampant, organizations are being cautious. Most studies now suggest two-thirds or more of those either planning or actually moving to the cloud are choosing hybrid cloud as their platform, such as keeping sensitive and mission critical apps and data in private clouds behind the agency firewall, and moving less sensitive things such as Web, email and collaboration apps to the public cloud. •

HYBRID CLOUD EMERGES AS THE FRONT RUNNER

The simplest way for an organization to have a cloud in which the data is maximally secured is a private cloud, where the servers and data that reside on them are totally contained within the organization's own enterprise infrastructure, and behind the organization's firewalls and other security systems. In that way, it has total control over systems and data.

That, however, largely does away with the cost savings and flexibility that can be had with a managed public cloud. So, the hybrid cloud is quickly being adopted as the best-of-both-worlds solution, to provide cost reductions where possible while ensuring the best security for the most sensitive services and data.

A hybrid solution also allows agencies to craft an IT strategy with an evolutionary path to a fully managed cloud as decision makers and users become more comfortable with the idea of the cloud, said John Lind, sales vice president for government markets at Quality Technology Services (QTS).

"This allows agencies to keep some technology they have today in place, while migrating new and improved services into their IT architecture," he said. "Some users will be reluctant to move from the systems they know, so a hybrid cloud helps keeps those end users comfortable while the agency overall gradually moves to the cloud."

There are lots of different ways to construct a hybrid cloud. In its Special Publication 800-145, the National Institute of Standards and Technology (NIST) defines a hybrid cloud infrastructure as "a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability."

That hides a multitude of possible combinations, however. A hybrid cloud infrastructure could, for example, include both onsite private and community clouds as well as their outsourced cousins, where the function is similar to the onsite cloud but managed by a cloud vendor. Then there could be the wholly managed public cloud that needs to co-exist with these. Over time, these elements could change as various kinds of clouds join and leave the hybrid cloud.

Added to the mix are the environments the hybrid cloud serves, such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), or Platform-as-a-Service (PaaS), each of which carries its own security, reliability and compliance concerns. IaaS lets users more closely control the configuration of servers and other elements of the cloud, for example, while PaaS provides a more standardized implementation.

For these reasons, there is no such thing as a standard hybrid cloud design. Each cloud is uniquely suited to the requirements of the user, so such things as where the connection between the user datacenter and the public portion of the hybrid cloud is made are important. Who secures the link after the data leaves that private-user cloud is critical, as is where the data is stored in the public cloud, who has ultimate control of it and how users can retrieve it.

Organizations that are still fearful about moving sensitive data to public clouds can opt to keep that data on their own servers and simply use the public portion of the hybrid cloud for additional computational capacity as and when that's required. However, cost and other resource pressures are likely to force IT organizations to move and store more of their data in the cloud.

Many cloud providers, as a reaction to user concerns, have begun to offer their own managed services to meet the range of security and compliance requirements organizations are demanding in hybrid clouds. Those increasingly involve also managing users' on-premise security, including such things as vulnerability assessment, network intrusion detection, and continuous monitoring services.

That kind of end-to-end security is likely to become more of a necessity as hybrid cloud becomes the predominant model. Gartner, for example, predicts 2016 will be the point at which users move from private cloud to hybrid, with nearly half of all large enterprises deploying hybrid clouds by the end of 2017. •

IAM IS ESSENTIAL FOR HYBRID CLOUDS

As the traditional hard edge of the network with its known points of entry and exit devolves into a much softer focus, as mobile devices and similar means of access proliferate, user identity has grown in importance, to the point where identity is now considered the new network perimeter. It will be even more important with hybrid cloud.

It already speaks to user fears about cloud security. A recent survey of the 250,000-plus members of LinkedIn's Information Security Community revealed unauthorized access through misuse of employee credentials and improper access controls as the major cloud security concern of nearly two-thirds of them. The ability to set and enforce consistent security policies across clouds was the number one method seen by 50 percent of those surveyed for "closing the security gap" in the cloud.

But it's easier said than done. Managing identities, group security policies and access with, for example, Microsoft's Lightweight Directory Access Protocol (LDAP) and Active Directory (AD), has been a well-known technique in traditional enterprises, with applications hosted in on-premise systems. In the cloud, however, it's much more difficult for IT departments to know which users are accessing which applications and services.

Nevertheless, says the Cloud Security Alliance (CSA), "extending an organization's identity services into the cloud is a necessary pre-requisite for strategic use of on-demand computing resources." It identifies four identity and access management (IAM) functions—identity provisioning/deprovisioning, authentication and federation, authorization and user profile management, and support for compliance—as the essentials for successfully managing identities in the cloud.

Federated identity management is seen as the best way to go for hybrid cloud, using hierarchical, identity-based cryptography. Single sign-on solutions can use the AD and LDAP systems an organization has already been using for its internal access management, which should mean minimal disruption in extending that to the cloud. No one will be able to access cloud apps and services without having an account in AD, and use of those apps and services can be tracked just as they can be for traditional access.

However, integrating traditional, on-premise IAM solutions with those needed for the cloud is not simple, plus the Windows-centric AD and LDAP don't easily translate to the kind of Web-based apps more often found in the cloud. That's prompted the recent rise of possible solutions such as Identity-as-a-Service (IDaaS).

IDaaS is a generic term that covers one or many of the services that comprise an identity ecosystem, according to the CSA, such as policy enforcement points, policy decision points, policy access points, services that provide entities with identity and that provide reputation.

They also "need to include people, processes and systems that are used to manage enterprise resources by assuring the identity of an entity is verified, then granting the correct level of access based on this assured identity."

Major cloud vendors have already jumped into this market, with Microsoft itself offering Azure Active Directory as a way of providing a cloud-based directory that synchronizes with on-premises AD, but also to non-Microsoft cloud apps. Market researcher Gartner has predicted a major adoption for IDaaS over the next five years, but so far its take-up has been slow, with many organizations cautious about moving IAM functions to the cloud. •

ENCRYPTION IS TAGGED FOR DATA SECURITY

While the security of the cloud overall is a concern for users, the hybrid cloud poses particular problems because data will be used in both a private cloud, where tight security and oversight can be applied, and with the public cloud component where security is less certain. Securing data in both kinds of cloud, and when moving data between them, is a major priority.

A recent survey of the 250,000-plus members of LinkedIn's Information Security Community found a range of preferences for technologies to protect data in the cloud, including access control, intrusion detection and prevention, firewalls and log management and analysis. But, encryption—for both data at rest and in motion—was clear winners.

That said, it's not a case of simply encrypting all data since encryption, which also means decryption at some point, adds complexity and overhead management costs. Sensitive data obviously needs to be encrypted, and that may even be required for compliance reasons, but other data that's considered not so sensitive could be left unencrypted.

The Cloud Security Alliance says a range of factors has to be understood when considering encryption:

Encryption should be implemented for data at rest, in motion, and in use. Use data-centric encryption for unstructured files that must be protected or stored in the cloud, or use encryption embedded into the file format whenever practical to apply protection directly to the files.

Don't forget to protect files that are often overlooked but that also can hold sensitive information, such as log files and metadata.

Use "sufficiently durable encryption strengths" that comply with the same standards used for encrypting files that are internally maintained within the enterprise. The National Institute of Technology and Standards (NIST) recommends encryption that's FIPS 140-2 compliant should be used.

Understand how all encryption/decryption keys will be managed for the entire lifecycle of the data, and whenever possible the data owner should control the encryption keys and not the cloud provider. That ensures the owner has access to critical information both now and in the future.

Agencies should not assume that simply choosing cloud providers that are certified through the Federal Risk and Authorization Management Program (FedRAMP) process will fully protect them when it comes to encryption and key management. FedRAMP refers only to a baseline of necessary security controls, so organizations should expect to have to specify key management through the service level agreements they negotiate with cloud providers.

Where data is encrypted and decrypted is also important. The user encrypting data before it's sent to the cloud provides the highest level of security since it ensures protection even if something happens to the data on the way there, or when it arrives. It also means that data, when it's stored in the cloud, can only be decrypted by the user if the keys are always controlled by the user.

However, encryption at this level is a complicated issue. Large IT departments may be capable of doing it, but smaller ones won't have the resources, which is where managed security services will prove valuable.

There are alternatives to encryption such as data anonymization, where, for example, personally identifiable or sensitive information can be stripped out of the data before it's processed. Data stored in a private cloud can also be altered before it's sent to the public cloud and include only a reference to private cloud data. For most purposes, however, encryption now seems to be the preferred method for hybrid cloud data protection. •

COMPLIANCE IS A HEADACHE FOR CLOUD ADOPTION

While the hybrid cloud is becoming the preferred choice for organizations who want to move IT to the cloud, actually getting there could prove a headache. Outside of the technical requirements, moving to the cloud and staying compliant with government mandates and guidelines is apparently no easy thing.

In September 2014, the Council of the Inspectors General published its findings of an examination of 77 commercial cloud contracts that federal agencies issued as they transitioned to the cloud. All of them, the council said, lacked the detailed specification recommended in Federal cloud computing guidelines and best practices documentation.

"Additionally," the report said, "59 cloud systems reviewed did not meet the requirements to become compliant with FedRAMP by June 5, 2014, even though the requirement was announced on Dec. 8, 2011."

The report concluded, damningly, that none of the 19 participating agencies the council's review examined had adequate controls in place to manage its cloud service providers and the data that reside within its cloud systems.

Earlier studies had come up with similar findings. In 2013, for example, The Ponemon Institute conducted a survey of more than 4,000 organizations in seven countries and found that just over half of the respondents said they didn't know exactly what their cloud provider does to protect their data, and only 30 percent said they did. At the same time, respondents still expressed a "marked increase in confidence" about the ability of cloud providers to protect sensitive and confidential data.

FedRAMP (Federal Risk and Authorization Management Program) and FISMA (Federal Information Security Management Act) are the two directives most closely related to cloud adoption by government agencies. OMB set the 2014 deadline for vendor compliance with FedRAMP, which describes a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FISMA compliance, which requires agencies to develop, document and implement information security measures for such things as cloud services, is tested every year.

In the final version of its US Government Cloud Computing Technology Program, issued in September 2014, the National Institute of Standards and Technology (NIST) detailed 10 requirements that needed to be part of any agency cloud initiative, including one that said agencies should ensure that cloud services and products meet unique policy and compliance requirements.

Cloud service consumers "need to be able to precisely specify and receive services," NIST said.

There are some systemic barriers that stand in the way of cloud initiatives coming into compliance. Even though the OMB has mandated that all cloud systems used by government agencies comply with FedRAMP, for example, the FedRAMP program management office has no authority to enforce compliance at the agency level.

In order to spur better compliance, the Council of Inspectors General has recommended that the OMB:

Establish standardized contract clauses that agencies must use when adopting cloud computing technologies;

Determine how best to enforce FedRAMP compliance; and

Establish a process and reporting mechanism to ensure Federal agencies require cloud providers to meet the FedRAMP authorization requirements in a timely manner.

This is where managed cloud services can provide the greatest value for agency users, said David Weisbrot, federal cloud business manager at QTS, some of whom may not have the technical resources or expertise to meet the very specific compliance requirements. They can be used to continually watch an intrusion detection system, for example, or collect and archive security logs, all things required to meet FISMA Moderate needs. •