TechTarget

Protecting This House: IT's Role in Cloud Security

The increasing complexity of cloud computing and the resulting security challenges are a force IT teams must reckon with. To succeed, admins need to solidify company-wide governance plans and policies.

Shifting Security Needs to Maintain Effective Cloud Requirement

Cloud computing's rise in popularity has been mirrored by its increasing complexity and heterogeneity. Organizational security needs are changing because of this transition, and IT is charged with managing the ever-growing need to protect these resources. Thus, the challenge is to provide employees with a way to effectively use the cloud while adhering to company-specific cloud-use policies.

Identity access management helps to achieve this goal, especially when coupled with the right organizational approach. Governance plans should fit into this overall strategy, so IT needs to be able to balance these needs without limiting the effectiveness of its cloud infrastructure.

In this handbook, security expert David Linthicum walks us through both the planning processes and potential costs for an effective cloud implementation. He addresses the challenges that arise during planning, industry best practices and the main players. Linthicum also looks at the "real" cost of cloud security—the people—and how this can be limited without sacrificing quality. ■

Patrick Hammond
Associate Features Editor ,
Data Center and Virtualization Group,
TechTarget

How to Pound Out an Enterprise Cloud Security and Governance Action Plan

Securing applications and data is essential for any organization, but the responsibility isn't evenly distributed. IT needs to come up with specific compliance policies or principles that the rest of the organization can follow.

Public cloud removes some of the infrastructure and administrative overhead of the traditional data center, but the onus to meet cloud governance requirements still falls squarely on IT's shoulders. In the ever-shifting cloud landscape, it's important to create a governance model that resembles an ongoing process, not a product. Therefore, necessary adjustments can be made to help facilitate progress and limit any holdups.

Matching cloud providers to your data location, your privacy and governance needs, as well as best practices for creating an organization-wide cloud governance strategy, are important considerations for any IT shop.

CLOUD SECURITY CHALLENGES

Most businesses don't have a good grasp of what's reality and what's fiction when it comes to cloud security. According to Alert Logic's Fall 2012 State of Cloud Security Report, the variations in threat activity are not as important as where the infrastructure is located. Anything that can be accessed from outside—enterprise or cloud—has a relatively equal chance of being attacked, because attacks are opportunistic in nature, but this isn't always the case.

Web application-based attacks hit both service provider environments and on-premises environments, comprising more than 40% of the total attacks on each environment. Though these events were the most prevalent type of attack, they hit on-premises environments with much more frequency. On-premises environment users also suffered significantly more brute-force attacks compared to their

counterparts in service-provider environments.

The 2012 report still rings true—the recent data breaches at Sony, Home Depot and Target were unrelated to the cloud. Indeed, most attacks occur on traditional systems because those security systems are aging, and vulnerabilities have been exposed.

Indeed, most recent attacks occur on traditional systems because those security systems are aging, and numerous vulnerabilities have been exposed.

The importance of having effective security strategies and technologies has increased significantly. This is because cloud computing continues to grow in popularity and because the implementations become more complex and heterogeneous.

Identity and access management (IAM), also known as identity management, is not new, but the emergence of cloud computing has put it at center stage. Many cloud providers, such as Amazon Web Services (AWS), provide IAM as a service right out of the cloud. Others require customers to select and deploy third-party IAM systems.

The concept is simple: Provide a security approach and technology that allows the right individuals to access the right resources at the right times and for the right reasons. The concept follows the precept that everything and everyone gets an identity, including humans, servers, devices, APIs, applications and data. Once that verification occurs, it's just a matter of defining which identities can access other identities and creating policies that define the limits of that relationship.

One example would be to define and store the identity of a set of cloud-based APIs that are leveraged only by a single set of smartphones that are running an application. The APIs each have an identity, as do the smartphones, the applications and the humans who are using the phones. An IAM service would authenticate the identity of each entity each time an entity interacts with another resource.

A prime example of IAM is the AWS version, which is a full-blown identity management and security system that allows users to control access to AWS cloud services. This IAM allows

you to create and manage AWS users and user groups by way of permissions, which allow and disallow access to data. The benefit of Amazon's IAM is the ability to manage who can access what, and in what context.

OTHER PLAYERS IN THE GAME

Of course, not everyone runs AWS. Fortunately, many new IAM players are focusing on cloud and usually promise to provide both identity management and single sign-on services. These players include Bitium, Centrify, Okta, OneLogin, Ping Identity and Symplified.

Each of the providers approaches cloud security and IAM differently, so you'll need to review each product with regard to your specific requirements. When selecting the right cloud security approaches, be certain to consider the following:

- The integration of cloud-based identity management solutions, or other security solutions, with enterprise security systems. Security should be systemic to both cloud and non-cloud systems, and you should consider ones that meet both sets of requirements.
- The design and architecture of your identity-based security solution. Sometimes security services can come from your cloud provider. In many other cases, you have to select and deploy third-party security tools.
- Importance of testing, including "white hat" security tests. They are telling, in terms of the actual effectiveness of your security systems.
- The effect on performance. In some instances, security can slow your system to the point that it affects productivity.
- Industry and all required regulations for compliance.

CHALLENGES IN GOVERNING THE CLOUD?

Cloud governance comes in many different flavors, including service-level, data-level and platform-level. What's more, cloud governance

and security typically work together, thus you can't select the right security approaches and technology without first understanding your governance strategy.

Service-level, or API governance, installs policies around access to services exposed by public or private clouds—those who want to access cloud services have to go through a centralized mechanism that checks to see that those who request access are appropriately authorized. This mechanism also forces compliance with pre-defined policies that can dictate when and how the services can be accessed. Companies that provide API/service management and governance products include Mashery and Apigee.

Data-level governance, much like service-level governance, focuses on the management of both storage and data. Once again, policies are placed around data and data storage systems to define and control access.

Data governance is becoming more important for businesses that implement cloud computing. The Cloud Security Alliance (CSA) has a Cloud Data Governance Working Group that is defining approaches and standard technology. Perspecsys and Acaveo are among the vendors in the cloud data governance market.

Platform-level governance, sometimes called a cloud management platform, is related to the management of the platforms themselves. This means placing automation services around the governance and management of a cloud platform, including provisioning and deprovisioning of cloud resources as needed by applications or data.

The objective of platform-level governance is to provide a single point of control for complex, distributed, and heterogeneous public and private cloud-based resources. This allows

Data-level governance, like service-level governance, focuses on the management of both storage and data. Again, policies are placed around data and data storage systems to define and control access.

policies to define when and where resources are put to work and makes sure users leverage only what is necessary. The end result is that we do not overpay for subscription-based services, and the system works around issues such as outages. RightScale and ServiceMesh (now owned by CSC) are among the vendors offering platform-level governance products.

CREATING YOUR OWN APPROACH

Your customized approach to cloud security and cloud governance requires a great deal of work to define your requirements, both business and technical. Once that's accomplished, it's easy to create a comprehensive strategy and then proceed to implement the right technology.

Most organizations continue to be concerned about the risks introduced by cloud computing. Those risks, however, are substantially less than many of the traditional systems in use today.

The cloud has too many benefits to ignore, and the risks around security and governance are now solvable problems. —*David Linthicum*

Cloud Data Security Comes at a Cost

Breaches are a recurring event in the IT world, with the U.S. Postal Service's computer network among the latest victims. Authorities suspect the attack compromised sensitive data—names, date of birth, Social Security information, addresses and employment records—of more than 800,000 employees. This attack follows significant credit card data breaches at Target and Home Depot. But these attacks were not cloud-related. Hackers exploited poorly protected traditional systems. As cloud adoption rises and hackers continue their attacks, cloud data security, which isn't cheap, becomes paramount.

So the question not only becomes how to protect your cloud-based systems, but can you afford it?

BREAKDOWN OF CLOUD SECURITY COSTS

The technology needed for cloud security can be expensive, so admins tasked with securing the cloud should prepare their CIOs for a big bill. The cost of the talent needed to create proper security architectures and approaches and then to run them effectively, will set companies back.

Clouds are complex distributed systems, so what's the best way to protect them? The best cloud security model and practice is identity access management (IAM). Many cloud providers, such as Amazon Web Services (AWS), provide IAM as a service. Others require third-party IAM systems.

To ensure cloud data security, use the method and technology that enable the right individuals to access these resources at the right times and for the right reasons. This means that everything and everyone gets an identity—including humans, servers, APIs, applications, data and more. After verifying identities, define which can access other

identities and create policies to define the limits of those relationships.

EXPLORE DIFFERENT CLOUD SECURITY AVENUES

There are a few approaches to cloud security, including using IAM for your cloud provider, IAM software and a third-party cloud. Cloud-based IAM system expenditures, such as those provided by AWS, are nominal. Most businesses, however, choose security options that are not tied to a single cloud provider.

The cost to run an IAM system, whether on-premises or as a service, varies. The average yearly cost is $5,000 per application, so it can get expensive if you manage 1,000 applications in private or public clouds and traditional systems. Everything needs to be locked up the same way; if cloud-based systems are secure, but traditional systems aren't, then the system isn't completely secure. Just ask Target and the U.S. Postal Service.

However, technology isn't the real expense—it's the security engineers needed to build and operate effective cloud security systems that cost the most. Indeed.com reports that the average annual salary for a U.S. worker with the words "cloud security" in his or her title is $134,000. And these talented engineers are extremely hard to find, so you'll pay even more for the best talent. Capable consultants can cost $2,000 to $2,500 per day.

Moving to the cloud has tremendous benefits, but security done right is costly.

—David Linthicum

DAVID LINTHICUM *is with Cloud Technology Partners and an internationally recognized cloud industry expert and thought leader. He is the author and co-author of 13 books on computing, including the best-selling* Enterprise Application Integration. *Linthicum keynotes at many leading technology conferences on cloud computing, SOA, enterprise application integration and enterprise architecture.*

TechTarget

Protecting this House: IT's Role in Cloud Security is a SearchCloudComputing.com publication.

Margie Semilof | *Editorial Director*

Phil Sweeney | *Managing Editor*

Patrick Hammond | *Associate Features Editor*

Linda Koury | *Director of Online Design*

Neva Maniscalco | *Graphic Designer*

Rebecca Kitchens | *Publisher*
rkitchens@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

COVER ART: THINKSTOCK