NEWSIGNATURE

Cloud services and security:

what you need to know

Cloud-based services deliver a host of benefits, from lower capital expenditure to scalability and ease of access. However, security practices need to change along with an organization's IT systems. What are the key security considerations for cloud-based solutions?

WHY THE CLOUD IS INCREASINGLY POPULAR

According to Forbes, cloud computing is projected to be a $162bn industry by 2020, with a compound annual growth rate of 19%. In 2017 alone the market is projected to grow by 17%.[1]

The cloud enables enterprises of any size to choose a more flexible, adaptable technology solution than the traditional option of hosting hardware on-site. Cloud computing provides convenient, on-demand resources such as networks, servers, storage, applications and services that can be provisioned and released rapidly with minimal management.

These solutions are accessed via the internet, which means businesses no longer need to store, maintain and configure their own in-house hardware and software.

Cloud solutions are popular in organizations of any size. Off-the-shelf products such as Office 365 and Microsoft Azure provide an easy entry route into using the cloud, with dramatically reduced lead-in times for developing, testing and deploying applications.

DIFFERENT MODELS OF CLOUD USAGE

There are many different ways of accessing cloud services. Firstly, users can choose between a public, private or hybrid cloud. A public cloud is provided by a third party and shared by many users, while a private cloud is privately owned and restricted to the owner's usage. Hybrid models provide a mix of third party and self-owned resources.

Cloud services also vary from providing access to finished applications, to providing the underlying infrastructure for users to create their own systems and applications.

[1] https://www.forbes.com/sites/louiscolumbus/2017/04/29/roundup-of-cloud-computing-forecasts-2017/#772a0f6231e8

Software as a Service (SaaS) offers services such as email, office automation and customer relationship management through a cloud-based application using a cloud provider's infrastructure. Platform as a Service (Paas) offers a computing platform for developers to use facilities such as databases, operating systems and programming execution environments. Infrastructure as a Service (Iaas) is the foundational cloud platform layer, giving IT administrators the ability to access processing, storage and other fundamental computer resources.

HOW DOES USING THE CLOUD IMPACT YOUR SECURITY?

Transitioning to cloud services requires a different way of thinking about your data security. It's no longer about defending the information stored on your premises, but managing the cloud systems that control your data.

There tends to be a confusion point around the difference between data residency and data sovereignty. Residency is about whether your data is stored, and sovereignty relates to which country's laws apply to it. Just because your cloud provider is based in another country, that does not mean that the laws of those countries will apply.

It is important to understand the laws and regulations that apply to your data, especially if you are handling customer data using cloud systems. Some regions such as the EU apply stringent fines against any company found to be in breach of its rules, so be sure your compliance processes are up to date and that employees understand their responsibilities.

Understanding how security responsibilities are shared

Cloud security is a shared responsibility. You can't fully entrust your service provider with protecting your data, although they certainly have a role to play. Some security problems do vanish as you adopt a cloud service, for example physical data center security, server hardware and virtualization.

Although these security problems are effectively outsourced, it remains important for you to choose a cloud provider carefully to ensure you have the right level of protection. Most cloud providers offer protection against network-based Distributed Denial of Service (DDoS) attacks, but it's important to check that the service provided is truly of a quality that matches the provider's claims. Some security issues remain the user's responsibility. These include threat and risk assessments, end-user training, data classification and identity management. Other issues can be outsourced to a third-party managed services provider; for example, monitoring, patch management and compliance audits can all be handled in this way.

SaaS and Identity and Access Management

The biggest issue with using SaaS applications is identity and access management (IAM). The user will need to manage multiple accounts and control privileges so that, for example, a junior employee can access and control much less than a senior executive.

It can be challenging to keep track of IAM in a SaaS environment. An important security challenge for many organizations is keeping track of employees as they leave and removing their accounts and privileges promptly. Without this control, critical data and systems can be left open to outside influence.

Microsoft Azure offers an innovative way to manage IAM. A single location (Active Directory or AD) provides a management hub for controlling access to over 2800 applications supported by the platform. Users authenticate with Azure AD to access SaaS applications and privileges are easy to remove and adjust.

SaaS encryption and tokenization

Certain data sets will be too unsuitable to entrust to the cloud, whether because of their sensitive nature or because of regulatory constraints. This type of data can still be accessed using cloud services through encryption and tokenization.

Encryption scrambles data, which can then only be decrypted using a decryption key kept in an on-premises key server. Tokenized SaaS applications display digital tokens rather than data, which issue an instruction to the agent on the user's computer to access data from another location - usually a data center owned by the user.

SaaS and backup or audit services

Some organizations feel a little uncertain about trusting a cloud provider to be the sole custodian of their data. A third party backup service can be helpful in this situation. The backup provider makes a remote copy of your SaaS data, which can be retrieved if there are any issues with your cloud provider's service.

Those who are nervous about cloud services might also consider using an audit service along with their SaaS facilities. This involves paying extra to store logs of how applications have been used. The storage time for these logs varies widely between applications, making it challenging to uncover actions for compliance purposes. Audit services provide you with a trail for extra peace of mind in addressing problems.

PaaS and application-layer security

PaaS provides developers with the opportunity to spin up container-based operating systems for a few seconds at a time to support a particular tasks. These short-term environments remove many security headaches associated with traditional host protections, such as intrusion detection and prevention.

Whereas attacks through the operating system and network layers used to be a concern, in the modern world the application layer is more likely to contain attack vectors. This means users should consider application-layer firewalls which govern what is sent to and from an application.

PaaS systems provide a wide range of tools and hooks which can be used to manage other security issues, capturing crucial information about events to help build a clear security analytics picture.

IaaS and virtual machines

Tools for IaaS allow users to create and destroy virtual machines to serve virtual tasks. The location of a virtual machine is critical, as a misconfigured machine could be accessible via the internet through a remote access port.

Effective policy management should prevent this, but controls about where virtual machines land are crucial to protecting data when using IaaS/

How IaaS interacts with other systems

Users of IaaS need to make important decisions about how data from IaaS will be stored, including encryption and the management of encryption keys. IaaS also needs to be carefully combined with in-house security measures such as firewalls or intrusion prevention systems. If these are transferred to the cloud, reconfiguration is likely to be necessary.

IEM is also a key consideration for IaaS systems. Who can access your IaaS layer, and what privileges do they have? Users need to have robust systems for protecting and verifying credentials to provide good identity management.

ARE YOU READY TO EMBRACE CLOUD TECHNOLOGY?

Cloud services have so much to offer enterprises in terms of flexibility, scalability and cost reduction that it’s hard to think of an organization that would not benefit from them in some way. However, as with all computing systems the security implications need to be thought through carefully. The best way to do this is in careful planning before introducing cloud solutions, but it’s never too late to improve your systems.

About New Signature

New Signature helps organizations transform their business with full-service Microsoft solutions. We deliver managed services and professional services to customers across all company sizes, geographies and industries. We are passionate about driving transformational results in every interaction.

New Signature was named the top Microsoft partner in the United States in 2014 and 2015—becoming the first partner ever to win the prestigious US Partner of the Year award two years in a row. With the backing of Columbia Capital, New Signature acquired 5 outstanding Microsoft partners in the United States, Canada and the United Kingdom.

For more information, please visit www.newsignature.com.