ADEPT4

IT AS A SERVICE

Now We're Talking:
Ten steps to securing the Cloud

www.adept4.co.uk

Introduction

The cloud sounds great, but is it secure?'

It's a phrase on the lips of many a business leader, particularly within small and medium sized enterprises. And it's an understandable position. However flexible, scalable and adaptable the cloud might be, it also demands a radical shift in how we think about corporate IT security. No longer is there a clear rack of servers that can be physically locked away – instead, vital business data and applications are hosted mysteriously in the ether.

As such, any migration to cloud computing, whether a shift of the entire organisational infrastructure or a partial migration of specific applications or datasets, must include a clear framework of expectations and agreements with the cloud provider or providers being used. There are different security risks and benefits associated with different aspects of cloud computing, and these must be clear and agreed between all stakeholders. Additionally, regulatory frameworks and legal requirements for cloud security services vary between different sizes of organisation and those operating in different sectors.

This Insight Guide, then, aims to take small and medium enterprises through ten key steps they need to consider when securing the cloud – so that they can take advantage of all its benefits, with complete peace of mind.

1. Ensure that data stored in cloud has not been tampered with

The first step to securing the cloud is ensuring the security of whatever you are migrating to it.

In particular, this means ensuring that any data you move to a cloud environment has not been tampered with or infected at any point prior to the migration. All content to be hosted in the cloud, then, should be comprehensively scanned, filtered and authorised before migration takes place.

2. Identify relevant regulatory and compliance frameworks

As mentioned above, different organisation's cloud processes are subject to different legal, regulatory and compliance processes according to factors like the size and sector of the business in question, and the markets in which it operates.

Clarity around the procedures that must be adhered to as a matter of course is essential before beginning any cloud project. Remember that a great deal of regulatory compliance depends not just on achieving certain levels of stringent security, but also being able to prove and demonstrate the steps taken at any time. Typically, this requires automatic audit trail generation to be built into cloud processes.

'...regulatory compliance depends not just on stringent security, but demonstrating the steps taken'

3. The human link in the chain

It's an oft-cited statement that people are the weakest link in any security chain. From basic human error – which can, of course, never be avoided entirely – through to the rarer, yet sometimes devastating malicious actions of disgruntled staff – a significant proportion of enterprise IT incidents are due to people, rather than technology.

Robust cloud security, then, needs to take this into account from a number of perspectives. First, there is the matter of identifying and authorising all users, providing each with a level of cloud access appropriate to their role while ensuring that no individual has overly generous access levels which could prove a security vulnerability. The cloud provider chosen must have a clear system for provisioning unique identities for all users and services – and indeed, all endpoints connected to the cloud infrastructure. There's also the question of ongoing training to ensure that every user is as aware of possible of the latest security threats and their role in mitigating them, and of clear processes for managing user access when individuals leave the organisation.

4. The provider and the partner ecosystem

Few, if any, cloud projects are delivered entirely internally. Third parties are almost always involved - including, of course, specialist providers of cloud hosting and security services.

It is vital for any organisation undertaking a cloud migration to understand that, in doing so, they are expanding the web of security responsibility in their organisation outwards to include these organisations.

As such, third party providers and partners should be chosen extremely carefully. They should be able to demonstrate, through testimonials and certifications wherever relevant, their ability to deliver robust levels of security and compliance, and have clear audit mechanisms built into their processes.

5. Identity and authorisation

Once a cloud is up and running, a great deal of security hinges on clear identification and authorisation of both users and devices.

This is particularly important in Internet of Things (IoT) environments, whereby a large number of additional endpoints is added to a corporate infrastructure. Security keys such as encryption keys and SSL keys are a critical part of this; your organisation needs a clear mechanism for provisioning, authorising and managing them.

6. Ensure robust protection of data and apps in storage

Data and applications hosted in the cloud must, of course, be protected adequately in their new homes.

Such protection covers everything from the physical security a cloud provider has in place around the buildings hosting their hardware, to the tools such as firewalls used to protect data from malicious online access and infection. In particular, it is vital for all data held in the cloud to be fully encrypted in storage, and for sensitive data sets to be appropriately segmented to prevent lateral exploration of the cloud infrastructure. Personal information such as signatures or contact details may require additional masking, while particularly sensitive data, or those subject to additional regulatory frameworks, such as financial or medical information, may require extra levels of protection again.

7. Ensure robust protection of data and apps in transit

It is not enough to merely protect information at rest – it also needs to be properly protected in transit.

This means ensuring that data encryption applies at all times, not just while data is in storage. It also means examining the communication links both within and outside the cloud environment, and ensuring that these are thoroughly protected.

8. Management, monitoring, maintenance

As with all aspects of enterprise IT, an operational cloud environment requires an ongoing strategy of monitoring and maintenance, so as to identify and mitigate any potential faults or malicious incidents as early as possible.

Some cloud providers deliver this as a managed service, while other organisations choose to take it on themselves in their IT department. It is important to remember that many regulatory frameworks require audit trails and demonstration of adherence at regular intervals, and this often comes under the remit of ongoing security management.

9. Backups and recovery

Should the worst happen and a malicious incident – or, more likely, a technological failure or natural disaster – cause a cloud outage, it is vital for all data and systems to be restorable from a backup system, as rapidly as possible.

An inability to do this leaves organisations particularly vulnerable to one of the latest and most insidious forms of cyberattack – ransomware – while also risking business continuity in the event of incidents like power failures, fire and flood, or hardware failure. Disaster recovery can be managed in-house or, increasingly commonly, offered as-a-service from the cloud itself.

10. Exit strategies

Finally, it is important to consider the implications for security if your organisation decides to move away from particular cloud processes in the future.

Whether that involves migrating from one cloud provider to another, transitioning between different public, private and hybrid cloud models or even removing certain material from the cloud altogether, cloud exit procedures are as integral to overall security as everything that came before.

About Adept4

Adept4 is a managed services provider.
It enables organisations to become operationally and culturally agile through smart, adaptive cloud based technology strategies that respond effectively to everyday challenges.

Adept4 is a northern based power house delivering hybrid IT, Microsoft cloud and managed services that enable organisations to securely transition, flex and integrate between on premise and cloud-based services.

Adept4 is a market–leader in developing solutions that enable mid-market sized organisations to make faster decisions, improve operational efficiency and gain competitive advantage.

If you're ready to start your journey to the Cloud then book in for a free free Cloud Readiness Assessment with one of our consultants.

Book Assessment

ADEPT4

IT AS A SERVICE

Head Office

Adept4 Managed IT Ltd
7750 Daresbury Business Park
Daresbury Office Village
Warrington, Cheshire
WA4 4BS

t. 0808 252 4444
e. info@adept4.co.uk

Aberdeen

3 Merkland Road East
Aberdeen
AB24 5PS

t. 0808 252 4444
e. info@adept4.co.uk

Leeds

Adept4 Managed IT Ltd
Victoria Spring Business Park
Liversedge
West Yorkshire
WF15 6BE

t. 0808 252 4444
e. info@adept4.co.uk

www.adept4.co.uk