UNISYS
imagine it. done.

How to Secure the Enterprise Class Cloud

White paper

We are constantly bombarded with articles and presentations about the security risks in cloud computing and why organisations need to be concerned about them as they consider a move. The truth is that organisations do need to be concerned about security, but they needn't be paralysed by fear.

In fact, the heightened concern we're seeing has actually become a spur to action and has begun to drive cloud security to a whole new level. Large enterprises have by and large not yet taken the leap into the cloud – concerned about the ability to secure and protect the confidential and valuable data as it passes through “the cloud”.

Paul Allen, practice director, data centre transformation, Unisys Asia-Pacific, confirms that security in the cloud is a legitimate concern and outlines the steps enterprises need to follow to secure the enterprise class cloud.

Security is a permissible concern in a cloud environment since sensitive customer and enterprise data is frequently shared and accessed through the cloud. It is the foremost consideration in a Government cloud, where mission critical defence and intelligence data is exchanged. And it's true that there are some cloud security challenges. So why should you worry about them?

Let's first remember that cloud computing, by definition, means that you are sharing a computing resource with other users. We should also remember that most conventional business applications contain sensitive data, such as customer, patient, employee, financial, or other proprietary information that must be guarded and protected. Unlike conventional computing, where we can control the entire infrastructure within our own firewalls, and where we can lock down data in controlled means, a shared cloud resource must also be secured to be able to meet most security compliance requirements.

Small business has led the way in adopting the cloud based approach for the delivery of IT infrastructure, applications and services. However, while many enterprises are interested, data security concerns hold them back from handing over responsibility for their data and networks to a third-party.

In a recent poll[1] conducted by Unisys, more than half (51%) of respondents identified security and data privacy concerns as the major barriers to the adoption of cloud computing services.

This is a reasonable – and valid – reaction. Enterprises want to be reassured that their data will be secured from other enterprises that are also using the public cloud or sharing facilities in multi-tenant environments as well as protecting data from being hacked while it transits the internet.

Organisations keep highly sensitive customer data and business rules in enterprise resource planning (ERP) systems and other key applications. They have spent years building walls to protect this vital information, so it's understandable if they don't yet trust the internet as a delivery mechanism under a cloud model.

While they are starting to move non-critical applications with in-built security, such as email, to the cloud, they baulk at the opportunity to unleash applications from behind their corporate firewall onto the web. That's why an enterprise that is looking to reap the cost saving and flexibility benefits of the cloud delivery model must seek a service provider that takes security as seriously as they do. An SMB solution won't meet the grade. A cloud solution for the enterprise must be designed for the enterprise user – in order to protect and support mission critical applications.

Therefore, the qualities to look for in a cloud solution designed for the needs of the enterprise are:

- Security and isolation of information within the boundaries of the third-party's data centre
- Transformation services that can handle dramatic changes in workloads
- Proven and verifiable processes and procedures
- Disaster recovery plans and procedures
- Global reach for service and support as well as local compliance

There have been high-profile breaches which have sustained fears about cloud security. In 2009, users of Google Docs saw their documents exposed to unauthorised users. In the same year Salesforce.com suffered a major outage that rendered thousands of its users around the world helpless, while their critical business applications remained inaccessible for the better part of an hour. Also in 2009, contacts, calendar entries, photographs and other personal information of Sidekick users was lost following a service disruption at Sidekick provider Danger, a Microsoft subsidiary
The key advantage of cloud technology is that users share resources in a multi-tenant environment where multiple customers share resources to lower capital and operating costs. Sharing is a key factor in the cost model but it also raises a warning flag to IT professionals within enterprise-class organisations.

Although these security concerns are well founded, cloud services can be secure if the right technologies and processes are in place. If they're not, businesses are at risk.

[1] Unisys Poll Shows Security Concerns as Leading Cause of User Hesitancy in Adopting Cloud Computing – 15 September 2009 - poll of 312 respondents: http://www.unisys.com/unisys/news/detail.jsp?id=10021300024

Technology

Perhaps the weakest link in the cloud computing chain is the level of security when data is transmitted across the internet from the service provider to the customer – this is called data-in-motion. Organisations that are contemplating moving back-office applications to the cloud should consider new encryption technologies to secure data during data transmission.

Unisys Stealth takes encryption of data-in-motion to the next level because it not only provides a higher level of encryption than the standard approach; it also breaks the information apart into multiple streams (bit-splitting) where data packets are split into multiple units as they are transported through the network, essentially cloaked during transmission, before being reassembled and delivered to end users.

A similar approach can be applied to data-at-rest, such as data stored on a disk, where data is split into bits and each bit is encrypted.

Unisys Stealth was initially designed for the US government and it is currently being trialled by the US Joint Forces Command (JFCOM) to enable the country's Department of Defence networks operating at different security levels to use a single network while ensuring data can only be accessed by authorised groups[2].

People

At the crux of an IT manager's security concerns is the age-old dilemma between sharing information and the need to safeguard it from others. The traditional approach has been to silo information within systems – effectively building "walls" by using physically distinct and non-interconnected networks to manage access to that information.

Unisys Stealth Solution allows multiple communities of interest to share the same network without fear of another group accessing their data or even their workstations and servers. The result is a much simpler network infrastructure, increased agility to react to new opportunities, and enhanced security of network data.

Process

The other area of security is not software, but a repeatable set of proven processes which minimises the risk of human error. Look for cloud data centres that have attained ISO 27001 and ISO20000 certification for best practice in Information Security Management, SAS 70 – type II certification for information processing and ITIL v3 certification for service management.

A service provider should allow its clients to conduct regular audits of its data centres to ensure their data is protected, private and compliant with various rules around data sovereignty. In New Zealand, for instance, the Reserve Bank's Outsourcing Policy[3] stipulates that "any outsourcing arrangements for bank functions must not create risk to the bank's ability to continue to provide and circulate liquidity in the economy, under normal business conditions or circumstances of stress or of failure of the bank or of a service provider to the bank".

[2] 'Encryption Evolution', Military Information Technology Magazine, December 2009

[3] Reserve Bank of New Zealand Outsourcing Policy, P4: http://www.rbnz.govt.nz/finstab/banking/regulation/bs11.pdf

5 steps to secure the enterprise-class cloud

1. **Look for a cloud provider experienced in multi-tenant environments**

   Ensure that your cloud service provider has experience running multi-tenant data centres where multiple organisations share the same hardware and network equipment. Operating this type of environment can be difficult, because each customer's data, applications, invoices, trouble tickets and reports have to be kept separate. The provider should also offer security and isolation of information within the boundaries of the data centre.

2. **Secure data-in-motion via high level encryption**

   Seek a cloud provider that takes the security of your company data as seriously as you do. Take encryption to the next level by combining with bit-splitting to break apart information into multiple streams.

3. **Look at communities of interest**

   Manage data access levels via multiple communities of interest rather than the traditional walls between IT systems.

4. **Examine application security**

   Applications, be they commodity, customised or complex, will require a detailed security assessment to gauge the required security posture in a multi-tenancy cloud environment. Application workloads which depend on sensitive data normally restricted to the enterprise due to security requirements will require particular attention. Choose a cloud provider with both experience and assessment capability in application management and migration, not just infrastructure management.

5. **Look for a service provider with best practice certifications**

   The provider should have proven and verifiable processes and procedures and allow third party audits. They should also have certifications as follows:

   ISO/IEC 27001: The information security standard that requires providers to rigorously examine their security risks and implement processes and controls that address those risks.

   ISO/IEC 20000: The international standard for IT service management that promotes an integrated approach to delivering managed services to meet customer requirements.

   SAS 70 – type II: Short for 'Statement on Auditing Standard', SAS 70 is a type of audit which validates that a service provider has professional standards and satisfactory internal controls and safeguards when hosting or processing information on behalf of customers.

   ITIL v3: Best practice IT service management framework which describes how IT resources should be organised to deliver business value, documenting the processes, functions & roles of IT service management.

Unisys' global network of data centres is frequently audited and certified to these standards. The centres also employ a layered approach to security with intrusion detection and prevention services, firewall management, 24x7 security monitoring, advanced correlation and analysis and auditable logs.

Conclusion

Clouds are here to stay, no matter what the voices of dissent may say. Given the changing economic environment and the ongoing emphasis on cost savings, cloud adoption is the way of the future. As enterprises rethink their cost models and look for ways to access data anytime and anywhere, the one decisive factor that can make or break the cloud is the security and privacy it offers.

If the right security policies are not in place, organisations are at risk of their data being exposed and open to attack. If they are, cloud infrastructure can be just as secure as systems kept behind the corporate firewall.

For more information, please visit our website at www.unisys.com.au