netmagic
An NTT Communications Company

WHITEPAPER

Dispelling the vapor around Cloud Security

The final barrier to adopting cloud computing is security of their data and applications in the cloud.

This White Paper examines the perceived risks, assesses whether they are justified, and examines the technology and measures that can make the Cloud's 'virtual' security a reality.

The last barrier to cloud adoption

Cloud computing holds powerful attractions for an organization. It offers instant access to an infinitely flexible computing resource and the ability to make major cost savings through outsourcing. Yet for many organizations, the final barrier to adopting cloud computing is security of their data and applications in the cloud.

This White Paper examines the perceived risks, assesses whether they are justified, and examines the technology and measures that can make the Cloud's 'virtual' security a reality.

What makes the 'Cloud' so attractive?

Cloud computing supplements or replaces an organization's physical computing environment with flexible, scalable Internet and virtualization technology. With Cloud computing, the organization doesn't have to keep adding capital-intensive IT assets to meet growing storage and processing requirements. It can access computing resources as required (including sudden peaks in demand) and simply pay for what it uses.

As data is stored remotely, employees can access it wherever they are; this allows flexible working and stimulates productivity. Meanwhile, IT employees previously involved in maintaining in-house data center resources can now take on other, business facing roles.

In a recent Forrester survey of 2,803 IT decision-makers, 49% of North American companies and 45% of European companies reported that pursuing a strategy of embracing cloud infrastructure services will bes a high or critical priority during the next 12 months.

The survey also found that while public cloud deployments offer compelling scale and cost considerations, most investments are in private cloud environments that afford more control and visibility for security-conscious buyers. However, recent trends point to adoption of a hybrid cloud model, combining the security and performance benefits of private environments with the cost and scale advantages of public cloud services.

CIO's 2011 Global Cloud Computing Adoption survey reveals that 56% of the IT and business leaders say managing access to data in the cloud is a top challenge. With the amount of data being generated, the number of identities and devices accessing the cloud, and the everchanging infrastructure, these leaders recognize that today, they may not have the needed controls and lack real-time visibility.

The main issues with Cloud security

For many CIO's today, the perceived barriers to Cloud computing remain security, regulation and compliance.

Organizations seek reassurance on several points: accessing the Cloud will not compromise their security; their sensitive data and intellectual property will be protected; they can retrieve their data if they want to change Cloud provider, or their provider winds up operations; and they can maintain their customer service standards and competitive performance.

CIO's 2011 Global Cloud Computing Adoption survey reveals that 56% of the IT and business leaders say managing access to data in the cloud is a top challenge. With the amount of data being generated, the number of identities and devices accessing the cloud, and the ever-changing infrastructure, these leaders recognize that today, they may not have the needed controls and lack real-time visibility. They can't manage what they can't see and they can't secure what they can't manage. Many organizations have siloed environments that are complex and difficult to manage. In such organizations, the dynamic nature of cloud environments, where data and applications move about at a moment's notice only add to the complexities. However,for organizations with siloed environments, starting with a foundation of virtualization before moving on to the cloud will provide greater visibility than legacy approaches.

A look at the three deployment models and security

The three deployment models of cloud computing - software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) havetheir own level of controls for the cloud provider and the organization purchasing the cloud service.

Software as a service (SaaS)

This model puts most of the responsibility for security management with the cloud provider and is commonly used for services such as customer relationship management and accounting. SaaS is considered low-risk because it primarily deals only with software and not hardware or storage. With SaaS, companies are able to control who has access to these cloud services and how the applications are configured. The cloud provider is responsible for software installation, maintenance, upgrades and patches in this case.

Platform as a service (PaaS)

This is similar to SaaS but often includes further application-specific software to help businesses create customized services. For example, a company using PaaS could develop its own custom cloud software to perform some specialized task. Most PaaS offerings are multi-tenant which implies that some of the services may be shared with other organizations. This means it is critical for companies who use PaaS to have a well-defined trust relationship with the provider on security issues such as access, source code distribution, navigation history and application usage.

Infrastructure as a service (IaaS)

In this companies get a unified, scalable cloud package that offers tighter control over many aspects of a traditional IT infrastructure than they do with SaaS or PaaS. Companies using IaaS pay on a per-use basis to access services and applications, and can also tap the operating system that supports virtual images, networking and storage environments for additional control. Often, IaaS is offered as a private cloud, giving companies complete internal control over access and security.

Large-scale data breaches have become all the more prevalent. According to an article in Forbes in 2008, the number of personal records that hackers exposed, such as Social Security numbers, medical records and credit card information had skyrocketed to 220 million. This represents the largest collection of lost data on record.

The threat landscape continues to evolve and become more complex

According to the Global Internet Security Threat Report (ISTR), cyber-criminals have become increasingly professional and commercial in the development, distribution, and use of malicious code and services. While cyber-crime continues to be driven by the motive of financial gain, cyber-criminals are now using more professional attack methods, tools, and strategies to conduct malicious activity. Based on the data collected in the report, the current security threat landscape is predominantly characterized by the following:

- Malicious activity has become Web-based
- Attackers are targeting end users instead of computers.
- The underground economy is becoming consolidated and mature
- Attackers and attack activity are adapting rapidly

In addition to malware, Distributed Denial of Service (DDoS) attacks are bringing mission-critical systems and business operations to a standstill. These attacks lead to loss of revenue opportunities, decrease in productivity and damage business reputations for organizations. It has been observed that over the past few years, DDoS attacks have grown in frequency and are carried out for a specific purpose such as extortion, market manipulation and cyber terrorism.

Large-scale data breaches have become all the more prevalent. According to an article in Forbes in 2008, the number of personal records that hackers exposed, such as Social Security numbers, medical records and credit card information had skyrocketed to 220 million. This represents the largest collection of lost data on record.

Organizations falling victim to such attacks find it difficult to bring applications and operations back on track and require extensive cleanup of the entire IT infrastructure, applications and processes. While large organizations have the scale and scope to have expert security services being operated in-house, most companies, especially small to mid-sized organizations, face several challenges like:

Set up/ Running Costs: SMBs generally cannot afford an in-house IT security set up. In addition to the massive expenditure on purchase of infrastructure which includes software, hardware and personnel, there is also the cost and administrative liabilities of running an in-house security service.

Efficient Threat Management: Prevention, detection and elimination of threats is what IT security is ultimately about. New threats are being generated round the clock across the globe and take less than a day to have a worldwide impact. This leaves organizations with barely any time to detect such threats and take preventive measures. Also, a robust set up is required to comprehensively cover all aspects of IT across the organization. It takes an expert MSSP to provide such levels of IT security.

Data Security: Personnel handling IT security have access to all of the data of the organization, including the most confidential. Not being bound by non-disclosure contracts or standards of governance, the risk of data leaks and thefts can be high.

Organizations also have to face the repercussions of brand damage. In addition to the financial losses incurred in fines and legal costs to fight lawsuits and pay out huge settlements, companies have to deal with the loss of customers and plunging market shares.

Demystifying Cloud security myths

Myth 1 – The Cloud is inherently insecure

The cloud environment can be absolutely secure - it can be even more secure than a datacenter. Infact, a cloud can be more secure than your internal IT infrastructure. A key advantage to third-party cloud solutions is that a cloud vendor's core competency is to keep its network up and deliver the highest level of security. In fact, most cloud service providers have clear SLAs around this.

In order to run a cloud solution securely, cloud vendors can apply for becoming PCI DSS compliant, SAS 70 certified and more. Undergoing these rigorous compliance and security routes can provide organizations with the assurance that cloud security is top of mind for their vendor and appropriately addressed. The economies of scale involved in cloud computing also extend to vendor expertise in areas like application security, IT governance and system administration.

This makes the case for an enterprise hybrid cloud model very compelling, where the same common security standard can be delivered across both public and private environments without compromising enterprise-class requirements or cost.

Myth 2 – The Cloud is a new concept altogether, therefore Cloud security is a new challenge

There's a misconception that cloud is a new technology and, therefore, cloud security is a brand new challenge that has not been addressed. True that the cloud represents a brand new target for attack that hackers love to go after, but the vulnerabilities and security holes are the same ones that exist in traditional infrastructure.

Infact, today's cloud security issues are much the same as any other outsourcing model that organizations have been using for years. What companies need to remember is that when you talk about the cloud, you're still talking about data, applications and operating systems in a datacenter, running the cloud solution. In fact, virtualization of IT infrastructure can make the cloud more secure than the physical environment and an investment in virtual security can provide the needed control and visibility for cloud.

Myth 3 - Compliance means Security

Many enterprises believe that being compliant ensures that their systems are secure and invulnerable to attacks. In actual fact, compliance does not ensure security, but only attests to the state of security at a specific moment in time. Compliance standards are reliant on human adherence to policies and procedures and not on automation. This can lead to errors and misjudgment. In the long run, equating security to compliance— and vice-versa—can put the business at risk.

Myth 4 – All Clouds are created equal

While the cloud can absolutely be as secure as or even more secure than an on-premise solution, all clouds are NOT created equal. There are huge variances in security practices and capability, and you must establish clear criteria to make sure any solution addresses your requirements and compliance mandates.

The Security Checklist

Integration: Look for integration points with security and identity management technologies you already have, such as Active Directory, and controls for role-based access and entity-level applications. Privacy. Make sure a cloud service includes data encryption, effective data anonymization, and mobile location privacy.

Identity and access: When you place your resources in a shared cloud infrastructure, the provider must have a means of preventing inadvertent access. How can identities federate across different services and from your internal environment to the cloud? How are the databases protected for access?

Compliance: What certifications does your provider possess? How do you handle dispute resolution and liability issues? What industry or government standards do you comply with? Are there clearly defined metrics for the cloud service to be monitored? How are e-discovery and criminal compliance requests handled? What are the processes to move into the cloud and back? Service integrity. How is the software protected from corruption (malicious or accidental)? How does your provider ensure the security of the written code? How do they do threat modeling? What is the hiring process for the personnel doing administrative operations? What levels of access do they have?

Jurisdiction: The location of a cloud provider's operations can affect the privacy laws that apply to the data it hosts. Does your data need to reside within your legal jurisdiction? Federal records management and disposal laws may limit the ability of agencies to store official records in the cloud. Information protection. Who owns your data? Can it be encrypted? Who has access to encryption keys? Where is the backup located, and do you have an on-premise backup? How is the backup purged? What requirements do you have with regard to the physical location of your data?

The ideal cloud equation

Control + Visibility = Trust

A cloud deployment that overcomes these myths is built on trust. Trust cannot be achieved without control and visibility across the cloud infrastructure, identities, and information.

Control

- Availability: Ensure access to resources and recovery following interruption or failure.
- Integrity: Guarantee only authorized persons can use specific information and applications.
- Confidentiality/privacy: Protect how information and personal data is obtained and used.

Visibility

- Compliance: Meet specific legal requirements and industry standards and rules.
- Governance: Establish usage rights and enforce policies, procedures, and controls.
- Risk management: Manage threats to business interruption or derived exposures.

Changing realities

While security emerges as a major concern among the adversaries of cloud computing, the key to understanding security in cloud computing is to realize that the technology is not new, or untested. It represents the logical progression to outsourcing of commodity services to many of the same trusted IT providers we have already been using for years.

Having said that, cloud security is part of the inevitable progression of IT. It must be embraced by organizations to stay competitive. Companies who approach cloud computing in a mature manner need not be afraid about entering the cloud because of security concerns. Dealing with security in the cloud is no more difficult than addressing it internally. And there are steps you can take that can make cloud security just as effective-oreven more so-as your internal IT.

1800 103 3130
marketing@netmagicsolutions.com