SUNGARD

SECURITY IN THE CLOUD

White Paper Series

THE MOVE TO THE CLOUD

Cloud computing is being rapidly embraced across all industries. Terms like "software as a service" (SaaS), "infrastructure as a service" (IaaS), and "platform as a service" (PaaS) are already a standard part of IT vocabulary.

But this massive shift from local hardware to web-based resources is not risk- and hazard-free. Concerns about security are running high. Questions such as the following touch on the very core of business success and resiliency:

- Is my data safe?
- Will my applications be available when I need them?
- Can my system be compromised?
- How do I control and manage access?
- Will I be in compliance with federal regulations?

Migrating to the cloud must not be done until these and other key security questions have been satisfactorily answered.

THE ADVANTAGES OF CLOUD COMPUTING

Businesses are willing to address the security concerns inherent in cloud computing because of the significant benefits they reap from this new technology:

- Cost efficiencies. Cloud computing removes the need to purchase and maintain expensive hardware, permitting companies to move from a capital expenditure (CapEx) model to an operational expenditure (OpEx) model.
- Operational efficiencies. Because there is no "ramp up" time for purchasing and customizing hardware, businesses can provision and implement a cloud solution in a fraction of the time, vastly increasing their speed to market. Additionally, cloud resources offer almost limitless scalability: they can be expanded and contracted to accommodate business needs.
- Resource efficiencies. By reducing and often eliminating the need for hardware and software management, cloud solutions decrease the IT administrative burden, allowing companies to redirect staff to strategic business initiatives.

THE TYPES OF CLOUD SOLUTIONS

Various cloud solutions are available to the corporate consumer. Before examining how to minimize cloud security risks, it is important to understand the nature of each solution.

The most common approach is the **public cloud**. A public cloud is a multi-tenant model of infrastructure services. Rather than having dedicated equipment for each client (servers, networking, surge protection, storage, bandwidth, etc.), clients share a pool of resources. By sharing equipment, a public cloud offers the greatest possible cost efficiencies, as well as excellent scalability, elasticity, and automation.

However, because the public cloud is multi-tenant, security can be a concern. Access is typically through shared Internet connections, and management of the environment is in the hands of the service provider. These facts make a public cloud less than ideal for hosting mission-critical applications and data.

Additionally, in a public cloud the client is typically renting infrastructure only. The burden of setup and implementation as well as the management of the applications and data is entirely on the client. This fact, coupled with the possibility that some of the infrastructure being rented may be open source and not best-in-class, can make some businesses hesitate to enter a public cloud environment.

Businesses that are evaluating a public cloud need to consider how to reduce their risk. Look for a public cloud offering built on established infrastructure such as Vblock versus open source. Inquire with potential service providers the level of management and maintenance they provide. Ask about service level guarantees and resiliency as it relates to their public cloud offering.

For increased security, many businesses turn to a **private cloud** solution. In a private cloud, all the resources in the operating environment are dedicated to a single client, guaranteeing that the client's data never shares space with another company. With private leased line access replacing Internet connections, the client can also be granted access to security and management controls as needed.

While the opex advantages remain, some of the cost efficiencies disappear in the private cloud model. This may be considered a fair exchange for the increased security of the system, which could then be utilized for sensitive data and maintained in accordance with any applicable regulatory and compliance requirements.

In many cases, companies are starting to explore a **hybrid cloud** approach. That is, they are looking to connect public and private clouds, using a public cloud for non-sensitive data or testing, and relying on a private cloud for mission-critical data and applications. Similarly, they may maintain a **hybrid environment**, employing colocation solutions, legacy applications, and public and private clouds simultaneously.

THE MITIGATION OF RISK

As seen above, the cloud is not "one-size-fits-all." Every company must examine their own requirements, often on an application-by-application basis, to determine which cloud solution is most appropriate to their needs. Once the type of cloud solution has been selected, they must determine how they can mitigate any security risks.

It is important to recognize that risk cannot be 100% eliminated. However, it can be significantly reduced to a level that is acceptable for a given business. The most crucial step in reducing risk is vendor selection. The right vendor will work in partnership with a client company at every step in order to maximize cloud security. This is key: **security is a collaborative effort between the vendor and the client**. The vendor cannot guarantee absolute security, but can provide the means so that the vendor and client together can make security a practical reality. With this in mind, companies should take a layered approach when assessing cloud vendors.

LAYER 1: THE VENDOR

The first layer consists of a thorough examination of the vendor company itself, starting with the vendor's **longevity** and **stability**. Since cloud computing is the "latest and greatest" in the technology field, there are innumerable start-up firms offering their services. Unfortunately, these firms may disappear from the scene as quickly as they arrived. Because a cloud solution is not a stand-alone product to be purchased, but rather an ongoing service to be utilized, the disappearance of a cloud vendor can wreak havoc on their clients' business operations. Businesses should therefore keep an eye on the future and choose a firm of proven history, financial strength, and success.

It goes without saying that a vendor should have **expertise** and **experience** in the area of cloud computing. "Rookie" firms may be able to talk intelligently about cloud computing, but if they lack actual experience in the field, a company is taking a serious risk by becoming their client. Rather, businesses should look for a vendor who has worked with multiple clients; who has an intimate knowledge of the hardware, software, and systems involved; and who has practical knowledge of how businesses function on a daily basis.

Bearing in mind that all business applications probably will not migrate to the cloud immediately (if ever) and that technology requirements frequently change over time, a company should look for a vendor with a broad **portfolio of services**. A vendor with a wide array of technology services has the depth of knowledge necessary to look out for their clients' best interests, and the capabilities to keep them on the cutting edge of technology as they grow, change, and progress.

Another area of interest is a vendor's **remediation practices**. It is unreasonable to assume that there will never be any issues with a selected cloud solution. At some point, an incident will occur, whether it is a minor power loss of a few hours in duration or a catastrophic natural disaster that destroys facilities. A vendor should be able to explain how they notify their clients in the event of an incident, how they remediate or recover full services, what their business continuity and disaster recovery plan is, and what steps they take to ensure that a given incident is not repeated.

Finally, in the event that the vendor relies upon **subcontracting firms**, a company must be sure that the subcontractors provide the same levels of service, security, and availability as the actual vendor.

LAYER 2: THE FACILITIES

Because of the term "cloud computing" and the habit of referring to data and applications as being "in the cloud," it can be easy to forget that "the cloud" is housed in a physical facility. That facility is the second layer that businesses should carefully look into when assessing cloud security.

Once a potential vendor has been selected, a company should request an in-person tour of their facilities. During this tour, the company should compare what they see against a checklist that includes such items as:

- Physical structure. What is the facility like? What are the environmental controls? How are they managed?
- Security procedures. Is there a security guard at the gate and at the door to permit authorized access only? Are there security cameras? Where are they mounted? How are they monitored?
- Power supply. What is the power source? What would happen in the event of a power outage? Is there a redundant power supply?
- Equipment considerations. What type of infrastructure is in place? What is its capacity? Is it automated? Is it monitored? Is it made up of best-in-class technology, or is it cobbled together?
- Staffing concerns. Are the vendor's employees subject to background investigations? Are they onsite, or do they monitor and manage the equipment remotely? Are security personnel trained in forensic security and law enforcement?
- Processes and certifications. Does the vendor audit its processes? Can it show compliance with both general regulations as well as the standards and compliance requirements specific to your industry?

LAYER 3: THE DATA

Data is at the heart and center of the cloud. Even so, it is only after a vendor has satisfied the first two layers of security that a company should begin making inquiries into data protection. Without the foundation of a viable vendor and secure facilities, data management is meaningless.

Three questions need to be answered with regard to data:

1. How is the data guaranteed?
A company should seek three discrete guarantees from the vendor:

- Guaranteed capacity. One of the greatest benefits of cloud computing is its elasticity – that capacity can be expanded and contracted on-demand. To ensure this benefit, a service level agreement (SLA) should articulate how much added capacity is guaranteed to be available for periods of peak usage.
- Guaranteed availability. A company's business will grind to a halt if connections to the cloud are severed. Therefore, it is vital that a vendor provide an SLA guaranteeing availability, reliability, and redundancy.
- Guaranteed storage. Managed storage is a must, with integrated backup and restore capabilities.

2. How is the data encrypted?
Sound encryption protects the integrity and availability of data hosted in the cloud, ensuring that data remains confidential even if it falls into the wrong hands. Because of the immense importance of data integrity and confidentiality, a company should require that a vendor facilitate this level of security.

Encryption procedures may include SSL connections, virtual private networks (VPNs), encryption systems, and encryption key management. Encryption should extend from desktops and laptops to the handheld devices that are proliferating every day. Depending on the industry a company is part of, encryption systems may need to comply with such regulations as PCI DSS, HITECH, or HIPAA.

3. How is the data protected?
Intrusion detection and prevention is paramount in a society rife with hackers and identity theft. A company should carefully examine the vendor's firewalls, vulnerability scanning capabilities, threat management, log management, antivirus services, virtual LANs (VLANs), virtual routers, and virtual switches.

LAYER 4: THE ACCESS

The final layer of security is that of access. In many ways, this is the most challenging level of security, because it has to do with people: people who have foibles, who make errors, and who — occasionally — act with malice.

When addressing the topic of access, the first area to examine is **identity and access management**. As Gartner research notes, there is a dual concern here as both the vendor and the client will have access to the cloud through "interactive access to the customer portal, API access and access to the VMs themselves." [1] For this reason, it is essential that the company and vendor establish:

- How identity and access management is monitored.
- Who has access — both from the vendor side and the client side.
- What the policy controls are.

Application and patch management follows hard on the heels of identity and access management. Again, the company and vendor must agree on:

- Who has access to make changes in the environment.
- Who has responsibility to make changes.
- What the process is for patch and release.
- How interdependencies between applications will be managed and protected.

It is not sufficient simply to have procedures in place to guard cloud access. The vendor must **log and document** all the transactions that take place within the environment, and match those transactions against known threats. This not only offers an additional level of protection against errors or attacks in real-time, but also may be necessary for to fulfill various compliance and regulatory requirements, and to provide documentation if the company is audited.

THE OUTLOOK FOR CLOUD SECURITY

When companies take the approach outlined above and select a vendor who can meet the requirements of every layer, they have ensured themselves a favorable outlook for cloud security. Certainly not every risk can be architected for, but when vendor and client work together in a proactive partnership, risk can be kept to a minimum while the many benefits of a cloud solution are maximized.

1 "Cloud IaaS: Security Considerations," Lydia Leong and Neil MacDonald, Gartner Research, March 7, 2011.

SUNGARD www.sungardas.com

SunGard Availability Services
680 East Swedesford Road
Wayne, PA 19087
Tel: +1-610-768-4120
USA Toll Free: 1-800-468-7483