How to create a secure cloud architecture

Numerous trends are pushing organizations to consider the cloud model of information technology, in which computing and storage capacity are delivered as a service. Yet, many organizations hesitate to adopt cloud computing due to security concerns.

This white paper describes how adoption of cloud technology can potentially change an organization's security requirements and how organizations can adapt their IT and security infrastructure to address these challenges. By developing a roadmap for their IT and security infrastructure, organizations are more likely to feel confident adopting and reaping the benefits of the latest cloud technologies.

Companies are able to leverage strategic solutions in the cloud to address crucial business issues.

Why organizations are considering the cloud

A number of trends are pushing organizations to look beyond traditional approaches to IT and consider adopting cloud technology:

- Data and intellectual property have become a critical part of most organizations' brands. This means data and IP must be created and accessed in a decentralized manner throughout the global organization.
- Organizations have become increasingly dependent on applications and services from all over the world.
- As mobile devices proliferate, employees are further leveraging these devices for work-related purposes to input and access data into corporate IT systems.
- Organizations are looking to expand the capacities of their data center, but may not be able to build out data centers to handle peak loads due to restrictions on time and/or capital dollars.
- Organizations are looking to reduce data center costs by consolidating technologies and facilities.

These trends mean that organizations of all sizes can no longer keep their IT architectures strictly within the four walls of their data center. Many organizations are looking to meet today's demands by considering cloud computing. Because the cloud is available over a WAN or the Internet, it can be used to make applications and data available to a global audience. Users can access cloud-based systems through any device that can access the Internet, which means mobile users can access corporate applications via the cloud from their smart devices.

SUNGARD®
AVAILABILITY
SERVICES™

WHITE PAPER

Thought Leadership

Compound annual growth rate[1]

19.5%

SOFTWARE AS A SERVICE (SaaS)

27.7%

PLATFORM AS A SERVICE (PaaS)

41.3%

INFRASTRUCTURE AS A SERVICE (IaaS)

22%

SECURITY SERVICES

The cloud can be used to deliver additional capacity beyond that available in-house, without the cost of building out their infrastructure. And cloud computing takes advantage of virtualized IT architectures, which allows organizations to consolidate their data center infrastructure and reduce expense.

However, the Adoption of cloud-based data services through 2016 will grow by a compound annual growth rate of SaaS at 19.5%, platform as a service (PaaS) at 27.7%, infrastructure as a service (IaaS) at 41.3% and security services will grow at 22%.[1] However, security and privacy are still the biggest challenges to cloud adoption. Organizations are also showing increasing concern over the impact of data privacy.

Evolving requirements for network security

Over the last 20 years, security services have adapted to meet changing IT requirements and address new threats.

In green-screen, thin-client mainframe environments, security was physical, consisting only of a door lock and a password at the workstation, and was used primarily to prevent espionage and theft. With the advent of PCs and LANs, intelligence moved to the user workstation, and IT needed to keep workstations from accessing one another. Security remained physical and was used to prevent theft and human error. Network security was unnecessary because corporate networks remained within the corporation's four walls.

Only after organizations became connected globally through the World Wide Web did corporate information begin to become exposed to the broader community and crime appeared on the radar. Initially, cybercrime was innocuous; it primarily came from computer science prodigies looking for recognition. Nonetheless, vendors began introducing network security devices and applications. Security evolved from a basic perimeter-based architecture of firewalls and anti-virus protection to a multi-layered design that combines anti-virus software, intrusion detection systems (IDS) and intrusion prevention systems (IPS) and more, along with firewalls to protect multiple OSI layers in the corporate network.

As the Internet has matured, newer technologies, such as virtualization led to the development of the cloud. Cloud computing enables intelligent applications to utilize centralized processing power and capacity on a shared server infrastructure to provide business functions to end users on-demand. No network configuration or server provisioning is necessary because the cloud is self-provisioned and fully automated.

As cloud technology has developed, so has the number of, and sophistication of threats, including a proliferation of client-side, web-based and mobile attacks. With these new threats, not only does security need to protect the network and devices, organizations must also ensure that users are educated and follow corporate and network usage policies to guard against such attacks as Phishing. Such attacks use email with attachments or hyperlinks to malicious sites; when the user clicks on the links or attempts to open the attachment, malware is installed on the user's machine, which then creates a tunnel or open access into a corporate network.

[1] Gartner: "Forecast Overview: Public Cloud Services, Worldwide, 2011-2016, 4Q12 Update"

How to create a secure cloud architecture

Today, organizations are reluctant to adopt cloud technology primarily due to security. They need confidence that their cloud delivers on the requisite security and compliance requirements for their business. In addition, many organizations have existing legacy infrastructure they need to maintain.

The key is for organizations to evolve their IT and security infrastructure to incorporate the latest developments. In fact, security technologies are available today that enable organizations to fully protect their cloud-based infrastructures and data.

Organizations can take a practical approach to implementing a secure cloud infrastructure, while still transitioning existing infrastructure. The following steps provide guidance .

Create a cloud architecture capable of being secure

The first stage in the process of an evolving IT architecture to the cloud is for organizations to separate data from the physical architecture to create a fully virtualized environment.

This task can be accomplished by completing three phases: virtualization, automation, and self-provisioning.

Virtualization

In a traditional data center environment, applications and data are provisioned for a discreet appliance that is built and sold for a specific purpose. Virtualization separates software from the actual hardware, which allows multiple virtual machines (VMs), each running its own application, to coexist on a shared server. Virtualization enables organizations to reduce costs through increased server utilization.

For many organizations, virtualization is a difficult transition. Organizations must take the time to become comfortable constructing an environment where applications are virtualized and shared on a stack of servers.

Automation

In the initial stages of virtualization, data centers still require a map of the real-time relationships between workloads and physical computers. Automation capabilities enable multiple unmodified operating systems and their apps to run independently in virtual machines while sharing physical resources. Automation capabilities help the virtualized environment deliver the right capacity at the right time through the ability to measure, monitor, and report on the physical and virtual layers and advanced modeling capabilities. These automation capabilities enable IT organizations to understand current capacity needs, accurately optimize resources and predict future capacity requirements.

Self-provisioning

Self-provisioning allows users to spin up an application or service themselves without the direct intervention of an IT organization or a service provider. User self-provisioning can be used in public, private and hybrid cloud scenarios.

Simultaneously develop the security framework

Comprehensive security solutions are available today that enable organizations to implement security for cloud environments in-house. Alternatively, organizations can partner with a service provider for advice on a cloud strategy or to outsource security and/or their cloud infrastructure to support corporate initiatives. The security solution selected should deliver a full complement of security product and service offerings that detect attacks, protect data, and provide reports.

Security offerings address three levels:

- **Person** — they must enable individual users to access what they need, when they need it, while protecting private information. Endpoint protection applications have evolved to support any mobile device in the marketplace today. They incorporate features such as encryption and data loss prevention tools to ensure the physical device is protected and mirrors the types of protections in place in the cloud.
- **Place** — they must fully protect the physical infrastructure that supports the cloud, securing all of the different layers within the cloud infrastructure. Let's face it, the cloud requires a complex, physical infrastructure. And even some of the more mature security applications such as firewalls and intrusion prevention remain critical components of a strong security framework.
- **Process** — they must protect transactional data as it travels between and within destinations. In the cloud, data moves through many different virtual applications, which may be managed on a single shared server or on multiple servers. As it travels, the data must be protected from vulnerabilities that might reside on the shared infrastructure.

Evolve security with the virtualization architecture

As organizations create a virtualized environment using the step-by-step process described in the previous section, they must simultaneously implement and evolve their security infrastructure.

At the virtualization stage, many organizations develop so called "trust zones." Each VM represents a unique business application, and different business applications have different levels of criticality. A print server VM, for example, is not considered a critical application, whereas an ERP application is essential to the business. Each of these applications requires different levels of security. Many organizations form trust zones within their virtualized environments to ensure that critical and non-critical applications coexist without conflict and risk.

The automation step allows organizations to place different trust levels on the same physical servers. This step allows organizations to evenly distribute their business applications across the server-based infrastructure to provide the best performance with the least risk (by implementing the right level of security).

As organizations add self-provisioning, they need to ensure that the system enforces security policies down to the user level.

Strategically utilize the public cloud

Many organizations wish to use the public cloud as a way to reduce infrastructure costs for non-critical applications, such as CRM or email by subscribing to the infrastructure rather than building it in-house. Another reason to consider the public cloud is to add capacity to handle peak traffic without needing to build out costly infrastructure that will not be in constant use. For example, a retailer might handle day to day operations on a private cloud while turning to the public cloud to handle peak processing on "Cyber Monday."

> **Per Gartner, "Cloud computing security, and its impact on regulatory compliance, continues to be one of the most commonly cited reasons for not using public clouds."**
>
> Source: Gartner. Hype Cycle for Cloud Security, 2013. July 2013.

Securing the public cloud

Most public cloud service providers do not take ownership for securing the use, applications, or data for customers moving to their infrastructure. Instead, service providers typically require organizations to purchase security applications and services on top of the shared infrastructure. Organizations must therefore establish a security framework to assess whether or not a particular public cloud is right for their business.

Some public cloud service providers have begun to share ownership for furnishing security and will even provide a security service level agreement. These services greatly improve security and reduce complexity for organizations moving to the public cloud.

Organizations considering a public cloud service provider should make sure the vendor offers:

- A security SLA
- A full complement of security product and service offerings that protect people, place and process by detecting attacks, protecting data, and providing reports
- Expertise in helping customers meet their specialized security requirements

By delivering a full complement of security solutions and expertise, public cloud service providers give organizations the confidence of knowing that when they move to the cloud, their applications will be fully and expertly secured without significant effort and complexity on the part of the customer.

How to create a secure cloud architecture

Conclusion

By evolving from a traditional data center environment to a virtualized, self-provisioned, and automated environment with appropriate security, organizations can benefit from the cloud while fully protecting their data and applications. These organizations can thereby access their data in a decentralized manner and take advantage of applications and services all over the world using both computers and mobile devices — with the confidence that their data and applications are secure. They can then take the next step to strategically utilize the public cloud.

Partnering with a cloud service provider that shares ownership for securing the organizations' data and applications can significantly reduce the burden of moving to the public cloud. This means organizations can more quickly and easily take advantage of public cloud benefits of reduced data center costs and the ability to cost effectively handle peak loads.

For more information please visit our website at:
www.sungardas.com/cloud

Additional reading

Security in the Cloud

Cloud Solution Brief

About Sungard Availability Services
Sungard Availability Services provides disaster recovery services, managed IT services, information availability consulting services and business continuity management software.

To learn more, visit www.sungardas.com
or call 1-888-270-3657

Trademark information
Sungard Availability Services is a trademark of SunGard Data Systems Inc. or its affiliate used under license. All other trade names are trademarks or registered trademarks of their respective holders.

Connect with Us