CONNECT | MANAGE | PROTECT

# WHITE PAPER:

## Clouds Are Fluffy; Security Is Hard

*How to overcome security challenges and reap the business benefits of the cloud computing model.*

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

CybersecurityWP1218

## EXECUTIVE SUMMARY

Cloud computing has become a component of virtually every organization's IT strategy. According to a recent Spiceworks survey, 93 percent of organizations are using at least one cloud service, and 30 percent expect that more than half of their IT services will be cloud-based within two to three years. Email hosting, cloud storage and web-based productivity apps are among the most popular solutions, with cloud backup and recovery and Infrastructure-as-a-Service growing rapidly.

Cloud computing has mushroomed thanks to the significant business benefits it offers. Many organizations are attracted to the cloud because it minimizes capital investments in hardware and software, reduces ongoing maintenance and support costs, and accelerates the deployment of infrastructure for a new application. The cloud also delivers long-term value by enabling rapid rollout of IT services and the ability to scale up or down as needs dictate.

In the early days of the cloud, businesses moved cautiously due to concerns about security and data governance. Those concerns have largely evaporated. In the Spiceworks survey, 71 percent of respondents said that cost is the most important factor to consider when evaluating cloud services, followed by reliability at 58 percent. Security ranked a distant third at 41 percent.

Counter to the initial objections of cloud naysayers, cloud-based services can be more secure than on-premises systems. When compared to the IT support teams of small to midsize businesses, a cloud service provider is more likely to have the expertise, budget and operational processes to maintain a high level of security. Cloud also forces security controls at the host level, while many on-premises environments implement security controls at the network level. This results in a more "gooey middle" with open communications between systems.

Nevertheless, organizations must not become complacent. They should demand transparency from their cloud providers to confirm that appropriate measures are in place to ensure data confidentiality, integrity and availability. They should also review to make sure they understand which controls are their responsibility and not assume the service provider has covered the entire security program on their behalf.

Many service providers issue reports based upon the Statement on Standards for Attestation Engagements (SSAE) No. 16 and the Service Organization Controls (SOC) reporting framework. Organizations should carefully review this information, particularly the SOC 2 reports on the effectiveness of controls related to security, availability and processing integrity.

This whitepaper is designed to help organizations understand the security challenges that are unique to the cloud so they can maintain proper oversight of cloud service providers. It also offers recommendations for developing a cloud computing strategy and security policies that ensure effective protection of mission-critical data.

## A LOOK INSIDE THE CLOUD

In network diagrams, a cloud is commonly used to denote the Internet — hence the term "cloud computing." It's an appropriate symbol given that the Internet has no hard boundaries. It seems to be everywhere and nowhere, and is something of a mystery.

Cloud computing has a similarly amorphous quality. The cloud enables organizations to tap computing resources as needed, without purchasing or maintaining hardware and software. Those resources are generally unseen and unknown, and can expand and contract dynamically. As a result, the cloud brings levels of speed, efficiency, flexibility and scalability never before imagined.

In reality, however, the cloud is a very real thing. Servers, storage, applications and network infrastructure reside somewhere, in someone's data center. The difference between cloud infrastructure and the typical data center environment lies in the dynamic nature of cloud-based workloads.

Traditional server-based architectures are fully constrained by hardware. Moving a workload to another host requires that the application be shut down and the data physically transferred to the new machine. Virtualization breaks the one-to-one association between a workload and its host, allowing for scalability and movement. Nevertheless, virtualized workloads are still constrained by the physical resources available to them in the data center.

The cloud should eliminate those physical constraints. Server, storage, networking and other resources are "pooled" to enable seamless movement of workloads and near-infinite scalability. The physical location of those resources becomes irrelevant. A high degree of automation removes much of the human element so that common operational tasks are handled in real time.

As the name suggests, the public cloud consists of resources that are made available to the general public and shared among customers. A private cloud is operated solely for one organization, although it may be managed by a third party and hosted offsite. A hybrid cloud combines one or more public and one or more private clouds along with technology that enables workloads to be moved among them.

## Defining the Cloud

In October 2009, the National Institute of Standards and Technology (NIST) published a definition of cloud computing that remains relevant today. Peter Mell and Tim Grance, authors of the NIST definition, described cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." According to Mell and Grance, cloud services must have these characteristics:

- **On-demand Self-service.** A customer can provision cloud resources as needed without requiring human interaction with the service provider.
- **Broad Network Access.** Cloud services can be accessed over the network through standard mechanisms using a variety of devices.
- **Resource Pooling.** Cloud resources are pooled and dynamically assigned according to demand. The customer generally has no knowledge of, or control over, the location of the resources.
- **Rapid Elasticity.** Services can be rapidly provisioned, sometimes automatically, and quickly scaled up or down. To the customer, the available resources appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service.** Cloud systems automatically control and optimize resources through metering. Resource usage can be monitored and reported, providing transparency for both the service provider and customer..

## CLOUD SECURITY

As with any other IT infrastructure, the cloud environment must be properly managed, with robust security measures and access controls to prevent a data breach. However, the dynamic nature of the cloud introduces unique security challenges. The key is to ensure that the right security controls are applied as resources are dynamically deployed, moved and scaled.

There are various frameworks to utilize in building an all-encompassing security methodology that includes physical, virtual and cloud infrastructure, allowing protection of company data no matter the location or type of infrastructure. A framework helps ensure each security control is applied consistently across all areas, even with differences in tools. The Cloud Security Alliance Cloud Controls Matrix (CSA CCM) is an example of such a framework. The CSA CCM is based upon industry best practices and security standards and provides guidance across 16 domains, including physical security, data center operations, data protection, change controls, identity and access management, encryption, and application security.

Typical security frameworks, including ISO 27001/2, NIST 800-53, PCI, HIPAA and others, can and should be utilized to define controls across all data regardless of location. This can allow the development of a complete security program to cover on-premises, cloud and hybrid environments. The following is an analysis of key elements to look for in assessing the security of a cloud service provider.

## Firewalls and Unified Threat Management (UTM)

Physical firewalls have come a long way in recent years, with next-generation technology that integrates antivirus, intrusion prevention, threat monitoring, data loss prevention and other security controls. However, firewall rules have traditionally been based upon the physical location of resources and their specific function. The cloud requires a flexible, scalable firewall that provides stateful packet inspection and other UTM functions across a dynamic environment.

**SageNet Advice:** *Cloud network architectures should apply defense-in-depth techniques for detecting and responding to network-based attacks, particularly with regard to high-risk applications and data flows. Don't assume your cloud provider is handling your firewall and UTM services. Ensure your cloud environments are applying appropriate controls based upon the data residing in the cloud.*

## Data Loss Prevention (DLP)

DLP solutions identify sensitive data and prevent unauthorized copying or downloading. There are clear differences between traditional and cloud-based environments in the application of DLP. Robust platforms have the ability to discover, monitor and protect data stored in the cloud, and provide unified management and reporting that encompasses all cloud usage regardless of the user's location or device.

**SageNet Advice:** *Data should be classified and protected against unauthorized use, access, loss, destruction or falsification in accordance with corporate data governance requirements.*

## Host-Based Controls

Most security tools can be applied at the host level to supplement network-based controls. Host-based controls include security configuration management, patch management, antimalware scanning, application controls, file integrity monitoring, endpoint detection, host-based firewalls and physical device controls.

**SageNet Advice:** *Not all hosts within the DMZ should be treated equally. The application that is being run within a particular cloud workload should determine the security controls to be used. As applications are migrated to the cloud, this is the perfect opportunity to re-evaluate the host-based security controls applied to each host rather than transport network-based controls from on-premises systems.*

## Authentication

A federation or federation-like authentication architecture should be used to ensure only approved users have access to cloud systems. Administrator accounts should be restricted based upon the principle of least-privilege access and supported through technical controls such as multifactor authentication, audit trails and IP address filtering.

**SageNet Advice:** *In many cases, cloud environments don't carry the same access controls as corporate systems, and terminated users continue to have active accounts. User accounts should be added/ removed and roles changed using a centralized solution integrated with the user directory. This is one of the easiest and most common ways the SageNet ethical hacking team is able to breach cloud environments.*

### Logging

Unique user access should be logged across all systems, and log files reviewed regularly to detect potentially suspicious network behavior and/or file integrity anomalies. Logging also supports forensic investigations in the event of a security breach.

**SageNet Advice:** *The cloud service provider should ensure the protection, retention and full lifecycle management of audit logs. It is common to see typical infrastructure and security event logs for on-premises systems being fed to security monitoring solutions. However, cloud environments are often a complete gap. This results in zero monitoring of security controls in cloud environments, making hacking of these systems much easier and without reaction and response.*

### Incident Response, Forensics and E-Discovery

Policies and procedures should be established, and technical tools and processes implemented to ensure timely and thorough incident management. Proper forensic procedures, including chain of custody, are required for the presentation of evidence after a security incident.

**SageNet Advice:** *Access to physical disks in the cloud can be challenging, but service providers are becoming more accommodating. On-premises e-discovery and forensic suites can also run in the cloud. Because dynamic data acquisition will be required in some instances, advance planning and the use of technology that includes cloud acquisition capabilities is advisable.*

## DEVELOPING A CLOUD SECURITY STRATEGY

While cloud security frameworks provide guidance, organizations must build a cloud security strategy from the ground up, embracing the differences between traditional data center infrastructure and cloud architectures. This strategy should reflect existing security policies as well as any legal or regulatory requirements specific to the cloud. Once the right security controls are in place, organizations can begin moving workloads to the cloud where appropriate, recognizing that not all applications can be cloud-enabled.

Cloud security should be built using virtualized networking and security tools that are designed to work with automatic scaling technologies and support dynamic migration of workloads to new hosts. However, the cloud should not be an add-on — it should be integrated with, and made part of, the overall IT delivery strategy.

The easiest way to manage a hybrid security framework is to integrate cloud and on-premises controls using toolsets and processes that will apply to data regardless of its location. This is not always possible. For example, common on-premises DLP and IPS technologies don't always apply to the cloud in the same way due to differences in network infrastructure. The goal is to determine where existing controls can apply with tweaks to processes. Organizations may also need to supplement existing toolsets with alternatives that work with the cloud provider.

## CONCLUSION

Given the near-universal adoption of cloud computing, organizations must take steps to address cloud security concerns. The capabilities that distinguish the cloud from traditional data center infrastructure — resource pooling, dynamic workload movement and on-demand scalability — create a unique set of security challenges.

The largest risk SageNet commonly sees in cloud environments is the gray area between on-premises controls and what is covered by the cloud provider. Many organizations assume that controls are being managed by the cloud provider and simply file away the SSAE16 annual report without a review and validation that the cloud environment meets or exceeds the controls defined within their on-premises environments.

Cloud security frameworks provide a starting point for the development of an end-to-end cloud security strategy. Organizations should adapt these best practices to meet the specific business, legal and regulatory requirements associated with each cloud workload. In addition, the security controls implemented to protect cloud workloads and data should be integrated with on-premises frameworks, tools and processes.

## ABOUT SAGENET

SageNet is a relationship-driven leader in managed network and cybersecurity services. The company connects, manages and protects technologies and devices across the enterprise. SageNet delivers creative solutions built on an integrated cybersecurity framework and best-of-breed technology from industry-leading partners.

The company offers world-class service and support via its three US-based 24/7 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, three national data centers, and a nationwide field service organization.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation’s largest retail, healthcare, financial, utilities and energy organizations. SageNet manages communications at more than 160,000 locations. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.