Cloud Security: Are You Ready?

As more midsize organizations move into the cloud, security professionals may wonder why cloud security seems difficult. More than likely, the real security challenge is the perceived loss of control. Numerous security best practices plus improved security products and services now exist. This short paper takes a look at some of the key elements and best practices for midsize enterprises looking to ensure security in their cloud implementations.

SANS

A SANS Spotlight

Cloud Security: Are You Ready?

Written by **Dave Shackleford**

June 2018

Sponsored by:

Symantec

Introduction

The cloud offers organizations of all sizes and types numerous advantages in terms of scalability, potential cost savings and innovative services that would likely be prohibitive to build internally. As more midsize organizations move workloads into cloud environments, security professionals may be wondering why cloud security seems so difficult. Is it because the cloud is inherently less secure than other models of computing?

More than likely, the real security challenge with cloud computing is the perceived loss of control, including challenges with visibility into the provider environment and possible incompatibility of security tools and controls in the cloud.

Fortunately, both cloud security tools and staff skills have evolved and there are numerous security best practices for cloud service and delivery models, as well as better and more capable security products and services of which organizations can take advantage. This short paper takes a look at some of the key elements and best practices for midsize enterprises looking to ensure security in their cloud implementations.

Shared Responsibilities

In the age of cloud computing, more companies will adopt a shared responsibility model for data and IT security. This means the cloud provider handles some aspects of security and your organization handles some controls. Who handles what is critically important to know before signing a contract! The nature of the shared responsibility model will differ depending on the model in play, which may be SaaS, platform-as-a-service (PaaS) or infrastructure-as-a-service (IaaS).

In SaaS models, for example, the consumer is responsible only for data, with the provider responsible for the operating system, application and infrastructure. In PaaS models, the consumer is responsible for data—that is, for the application layer—and likely some application components.

In contrast, in the IaaS model, the consumer is responsible for all layers of security in the cloud (also referred to as deployed assets), with the cloud service provider responsible for only the underlying "plumbing," or infrastructure (commonly referred to as the security of the cloud).

It's a guarantee that no cloud provider will take full ownership of all cyber security controls and requirements. Some security issues will be on you, and it's your responsibility to know what you can and can't control within the various cloud environments in which you'll be working. While this might be daunting for some organizations, some specific guidelines and recommendations can help.

Compliance Obligation, Data Classification and Accountability

Almost all organizations must now deal with one or more compliance issues, which means matching compliance requirements to cloud provider controls is critical. Following the shared responsibility model, you'll need to determine which controls the provider will maintain and attest to and those you're expected to implement and maintain, as well as the available options for those. Be sure your provider has at least SSAE 18 SOC 2 reports available, ideally along with ISO 27001 assessments, and can meet specific compliance regulation controls needed to ensure your compliance in its environment. If you are not yet familiar with SSAE 18, you can find more information here: https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard.

It's also critical to know what types of data are going to the cloud and be able to control that flow carefully. This can be especially difficult when users can sign up for cloud services without the organization's knowledge and many data loss prevention (DLP) tools can't cover cloud use from individual laptops or other endpoints. In these cases, it makes sense to integrate a cloud access security broker (CASB) service that can track cloud use, monitor user behavior and, ideally, prevent data loss or leakage.

What you need to know before embarking on a cloud-based security project, in a nutshell:

1. Know what security aspects you can—and cannot—control.
2. Make sure your provider provides compliance reports.
3. Protect your endpoints and automate when you can.
4. Manage access and use strong authentication.
5. Make security part of your DevOps.
6. Architect and implement cloud-specific network monitoring and controls.

Client and Endpoint Protection

Endpoints in the cloud will need the same level of protection as they would internally. The most important controls to implement for cloud instances include patching, configuration management and anti-malware capabilities. To scale in cloud environments, implementations of these controls need to be highly automated and, ideally, should align with your internal controls. It's also critical to make sure that anti-malware products are lightweight and don't affect performance significantly.

For security teams, the best approach to take is to implement all configuration controls and patches desired on a continuous basis, integrating these into a development and deployment workflow. Anti-malware technology should be installed within the same image. Once the image is approved, security teams will need to monitor the state of deployed instances to ensure the controls meet the organization's standards.

Any tools that can help unify endpoint and network security (covered shortly) should be given preference by smaller organizations and teams, which will need to centralize and simplify their security strategy wherever possible.

Identity and Access Management

The goal of identity management is to control access to computer resources, applications, data and services, and its importance in the cloud is growing. Identity management service providers can offer brokered identity access and translation/federation services to a number of cloud provider environments. Many of these can easily integrate into your existing on-premises directory services, such as Microsoft's Active Directory.

Authentication and authorization will change with a move from internal to external assets and environments, too. Ideally, look for multifactor authentication support for those products you are familiar with and ensure there are options for all types of users and devices that will interact with your cloud environment or applications.

Many cloud providers can also provide robust identity and access control services that align with your internal policies and standards. Be sure to look at single sign-on (SSO) and federated access models to control access to SaaS applications in use, as these can become unwieldy to manage over time if users have to authenticate to each individual application. This can often lead to "orphaned" accounts in cloud services.

Application-Level Control

Cloud applications are exposed to every sort of security threat. The Cloud Security Alliance (CSA) divides application security into different areas, including securing the software development life cycle in the cloud; authentication, authorization and compliance; identity management, application authorization management, application monitoring, application penetration testing; and risk management.

For cloud applications in general, it's important that security becomes more embedded in deployment pipelines with source code reviews, dynamic security testing with scanning tools, and monitoring of user accounts, privilege use and encryption keys. Once an application is running in the public cloud, it needs to be carefully scanned on a regular basis, ideally using an integrated scanning platform that resides in the same cloud environment.

Network Control

For hybrid cloud assets within the internal data center, very little changes for network security controls and processes other than an increase in the use of virtual appliances for firewalls, network intrusion detection and the like. Also, with virtual and software-defined networking, ensure that you carefully define roles and privileges for the virtualization, network, and security teams so that over-allocation of privileges doesn't occur.

For assets in the public cloud, implement a secure, dedicated connection using IPSec or a cloud provider circuit between internal and external environments, and implement any network access controls or intrusion detection via compatible products in the cloud provider's marketplace. Ideally, organizations can use the same products and vendors they are using in-house, but additional operational resources and time may be needed to architect and implement cloud-specific network monitoring and controls.

Unfortunately, there are many scenarios in which SaaS providers and other cloud services won't natively support secure connections and best-of-breed network intrusion detection. And they may not support additional technologies like malware sandboxing and network DLP for sensitive data either.

In these cases, and especially as your cloud use grows across more than one service, cloud brokering services and network proxies can help to monitor and control network traffic more effectively. Monitoring user behavior within SaaS accounts and dynamically protecting data when needed can also make cloud-compatible gateways and services vital for protecting users and data within services such as Office 365 and Salesforce.com. Increasingly, employees are working remotely and while traveling. This means more organizations are looking to facilitate safe and controlled access to their cloud services from any system or location. You should employ a cloud network access platform or cloud brokering service that integrates with providers to allow protection from both your premises and end-user equipment in the field.

Conclusion

The major security considerations for a cloud migration for any organization largely revolve around secure data transfer, controlling and monitoring user activity, and having compatibility and capabilities in the cloud from trusted security vendors and service providers. These requirements apply equally to midsize organizations looking to start a cloud project or make a more complete transition.

For organizations moving to a public cloud model, thoroughly review your existing controls and processes before deploying the public cloud assets, if possible. This will give you the opportunity to adequately protect the data involved and look for equivalent security capabilities in public cloud environments. If you're already using cloud services, your emphasis should be on leveraging cloud security controls to protect your users and data in the cloud and while people are using cloud services. Finding security products and services that provide broad coverage of many control areas can also help.

About the Author

Dave Shackleford, a SANS analyst, instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

Symantec™

Last Updated: July 17th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LAUS	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MDUS	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS Alaska Summit & Training 2018	Anchorage, AKUS	Sep 10, 2018 - Sep 15, 2018	Live Event
SANS Munich September 2018	Munich, DE	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, GB	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NVUS	Sep 23, 2018 - Sep 30, 2018	Live Event
SANS DFIR Prague Summit & Training 2018	Prague, CZ	Oct 01, 2018 - Oct 07, 2018	Live Event
Oil & Gas Cybersecurity Summit & Training 2018	Houston, TXUS	Oct 01, 2018 - Oct 06, 2018	Live Event
SANS Brussels October 2018	Brussels, BE	Oct 08, 2018 - Oct 13, 2018	Live Event
SANS Pen Test Berlin 2018	OnlineDE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced