SANS Institute
InfoSec Reading Room

Protecting Data To, From and In the Cloud

Attackers have adapted their strategies to the cloud and will likely continue to focus on this threat surface.
In this spotlight paper, SANS offers some guidance and recommendations for improving cloud service visibility,
data protection, threat protection, access control and reporting.

SANS

A SANS Spotlight

Protecting Data To, From and In the Cloud

Written by **Dave Shackleford**

December 2018

Sponsored by:

Symantec

Introduction

Adoption of cloud computing in all forms continues to grow. Many organizations are making use of SaaS applications like Microsoft Office 365, Salesforce and workforce applications such as Dropbox and similar cloud storage and collaboration tools. In the SANS cloud security survey from 2016, 55 percent of respondents were using SaaS, and 14 percent planned to implement it in the next 12 months.[1] 2017 saw growth all the way around as well—as many as 70 percent of all organizations have at least one application in the cloud, and some expect annual global spending on cloud services to increase by 19.4 percent on average by 2019.[2]

The 2017 SANS Cloud Security survey found close to 50 percent of respondents indicated they would be increasing the number of mission-critical applications in the cloud (versus those less important).[3] This trend changes the sense of urgency for security teams to implement sound controls and processes to help protect enterprise users and data in the cloud.

[1] Security and Accountability in the Cloud Data Center: A SANS Survey, www.sans.org/reading-room/whitepapers/cloud/security-accountability-cloud-data-center-survey-37327

[2] https://apiumhub.com/tech-blog-barcelona/cloud-computing

[3] Cloud Security: Defense in Detail If Not in Depth, www.sans.org/reading-room/whitepapers/analyst/cloud-security-defense-detail-in-depth-38120

Along with increased adoption of cloud computing and mission-critical applications in the cloud, organizations are storing sensitive and confidential information there. In the past two years, according to the survey referenced earlier, SANS found organizations consistently willing to store employee records, intellectual property, financial data and more in cloud-based applications and systems. Further, 2017 also saw increases in storage of healthcare records, business intelligence, customer personal data and payment card data in the cloud, and this trend will likely accelerate.

Figure 1. Common Cloud Problems and Their Effects

All of these issues indicate we've brought a lot of our traditional security challenges to the cloud and are not isolating cloud assets and controlling them effectively. Use of cloud applications isn't being governed and monitored carefully either, which likely reflects some common issues in organizations today, as shown in Figure 1.

For these reasons, controlling the use of cloud applications and interaction with hybrid cloud assets in platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) deployments is paramount. Attackers have adapted their strategies to the cloud and will likely continue to focus on this threat surface. In the following, SANS offers some guidance and recommendations for improving cloud service visibility, data protection, threat protection, access control and reporting.

Shifting to Cloud Security-as-a-Service

As users become increasingly mobile, it's vital to ensure traditional network security controls are in place and effective no matter where they go. To achieve this, an "access anywhere" model can be implemented to integrate with user endpoint devices to safely direct users' cloud application traffic to and through a secure cloud network service. While some organizations have traditionally tried to "backhaul" user traffic to the on-premises network, more progressive approaches can be implemented to direct users through a cloud security layer regardless of where they're connecting from. This enhances security by ensuring consistent controls are applied at all times and also provides the benefit of improving users' application performance.

Cloud network security should also include strong traffic encryption and decryption to allow for improved inspection and intrusion prevention control. SSL/TLS termination and inspection should be considered a mandatory feature for a cloud security service, and ideally these services will operate robust infrastructure controls to prevent any loss of performance along the way. Inspection of user traffic is vital for handling all manner of network security controls, ranging from data loss prevention (DLP) to malware sandboxing and more. Email security for cloud-based services such as Office 365 are also best handled this way, with controls for phishing prevention, malware prevention and DLP.

Cloud security services traditionally focused primarily on both monitoring cloud usage and protecting data sent via the cloud, but they are now rapidly emerging to become more fully featured platforms that offer preventive, detective and response network controls. Organizations can benefit from improved visibility into cloud service use, detection and prevention of malicious activity such as account hijacking, malware, insider threats and protection of data through techniques like encryption.

For data protection, organizations first need a sense of what cloud applications are in use, as well as the types of data being sent to the cloud. Within the enterprise, monitoring for specific types of sensitive data has been largely handled by DLP solutions that can identify specific patterns of data and then perform policy-based actions such as blocking data movement, encrypting data and alerting security teams to information security and compliance violations.

Choosing a cloud security service to help to protect users wherever they are and whatever device they are using is a critical element of any organization's security strategy.

In the cloud, this process has traditionally proven difficult due to lack of cohesion between on-premises DLP and cloud-based options that can integrate existing policies and work with numerous cloud service provider offerings. Fortunately, in recent years, more SaaS providers have created APIs allowing DLP policies to be effective for cloud storage and other scenarios. At the same time, enterprise DLP platforms have now been better adapted into PaaS and IaaS environments.

The good news is that more organizations are aware they need to adapt their security controls to the cloud. Companies are more willing to look at security controls offered as services that handle a wide variety of functions and would be challenging to adequately manage if deployed on-premises. Given the shift to moving critical apps and workloads and sensitive data into the cloud, choosing to adopt a cloud-delivered security service that can help to control and monitor data and user activity is a logical choice.

Cloud-delivered network security services are Security-as-a-Service (SecaaS) cloud offerings that inspect network traffic destined to the web and cloud, including both SaaS applications like Office 365 and home-grown applications deployed in PaaS and IaaS environments. These services inspect network traffic to determine whether sensitive data is being transmitted to the cloud and apply various policies and security controls to protect the data or prevent it from being transmitted in the first place. They also inspect cloud and web traffic coming back into the organization to block threat and malware.

Evaluating Cloud Network Security Services

The most effective way to implement cloud network security is by provisioning a "cloud mesh network" that users are connected into regardless of where they are. Traffic is routed to this security network through an in-house device such as an SD-WAN or agents deployed on endpoints that can re-direct traffic. When you're looking to procure and implement cloud network security services, there are several features that you should expect to have.

Cloud Network Traffic Visibility and Access Control. Cloud network security services should include a secure web gateway proxy connecting users to both cloud applications and services, as well as for general web browsing protection. As more users work remotely and need protection regardless of location or device (many of which may be owned by them in bring-your-own-device environments), having secure access to enforce acceptable use policies and filter content uploads and downloads can help security teams centrally control how their users access the web and cloud application services.

Data Protection. Encryption is the most common type of data protection control available, and some security services providers give you the capability to encrypt sensitive data when it leaves your environment. Enterprises should carefully evaluate key management capabilities and practices if they intend to implement encryption and decryption of data. Also, DLP is a critical capability many organizations should adopt, especially if there are sensitive data assets they do not want in the cloud for compliance reasons.

Network Threat Protection. Analyzing users' network traffic to detect malicious content, sandbox encrypted traffic to perform malware detonation and analysis, and monitor traffic destinations for reputation and known command and control patterns can significantly enhance network security for users accessing the web and cloud. With cloud network security services these capabilities come pre-packaged in an integrated solution, making them simpler to deploy and use and more effective overall.

Performance. For users who need access to large files and quantities of content online, caching and performance shaping services and tools for network traffic are important. Much of this functionality can be lost when moving to a cloud-delivered network security infrastructure. Look for a cloud network security service that has options for performance acceleration such as content peering and performance policy application for quality of service, because they will enable users to enjoy much faster cloud application use.

Dashboard Metrics and Reporting. All cloud network security tools should provide an easy to use dashboard that offers a variety of reporting options. Providers should offer a set of "canned" reports that detail user activity, data detected and/or protected and malicious traffic detected and blocked.

While not ubiquitous, some SecaaS offerings can also provide:

Web Browser Isolation Capabilities. Some services include the latest in threat prevention technology—web browser isolation. Isolation prevents malware and phishing threats targeting users' web browsers by executing web sessions away from endpoint devices. Because only safe rendering information is sent to a browser, any website delivered zero-day malware cannot be infected from reaching your users devices.

Ability to Deploy in a "Hybrid" Environment. Some organizations have one foot in the cloud and the other still on-premises. In this sort of an environment, you will want to consider having some of your network security stack in the cloud and some on-premises as well. Some vendors offer flexibility to deploy network security in on-premises appliances or as a full cloud service, which is useful to meet hybrid requirements. In this case, look for a solution that has a single management interface allowing you to perform policy and monitoring administrative tasks across the entire hybrid environment.

In-house Threat Intelligence Teams. Some providers offer additional threat intelligence services and data feeds to augment the core data and user monitoring capabilities. Enterprises interested in this threat intelligence data should expect the vendor to maintain an in-house intelligence team to continuously update the threat intelligence provided to customers.

SANS recommends...

When evaluating cloud network security services, organizations should focus on:

- Using a comprehensive set of the service's capabilities
- Ensuring the services offer broad threat prevention and information security controls
- Ensuring the services meet performance expectations, especially when working with applications such as Office 365
- Looking for solutions that provide flexible ways to provide and deploy simple connection methods that can support all device types

Implementing a cloud network security service should not require a major architecture overhaul, nor should it require significant manpower to maintain. Configuration of policies and tuning can take some time, however, so the "starter" threat prevention and data security policies that some vendors provide may prove useful to some. Organizations looking to implement these services should expect to dedicate one or more full-time security resources during planning and implementation.

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:

Last Updated: January 21st, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Las Vegas 2019	Las Vegas, NVUS	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LAUS	Feb 02, 2019 - Feb 09, 2019	Live Event
SANS SEC504 Stuttgart February 2019	Stuttgart, DE	Feb 04, 2019 - Feb 09, 2019	Live Event
SANS Anaheim 2019	Anaheim, CAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Northern VA Spring- Tysons 2019	Tysons, VAUS	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, GB	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS FOR610 Madrid February 2019 (in Spanish)	Madrid, ES	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Dallas 2019	Dallas, TXUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZUS	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, JP	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Zurich February 2019	Zurich, CH	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Riyadh February 2019	Riyadh, SA	Feb 23, 2019 - Feb 28, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VAUS	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NVUS	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Brussels February 2019	Brussels, BE	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MDUS	Mar 02, 2019 - Mar 09, 2019	Live Event
SANS Training at RSA Conference 2019	San Francisco, CAUS	Mar 03, 2019 - Mar 04, 2019	Live Event
SANS Secure India 2019	Bangalore, IN	Mar 04, 2019 - Mar 09, 2019	Live Event
SANS St. Louis 2019	St. Louis, MOUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, SG	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CAUS	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS London March 2019	London, GB	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, FR	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, DE	Mar 18, 2019 - Mar 23, 2019	Live Event
ICS Security Summit & Training 2019	Orlando, FLUS	Mar 18, 2019 - Mar 25, 2019	Live Event
SANS Secure Canberra 2019	Canberra, AU	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Norfolk 2019	Norfolk, VAUS	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Doha March 2019	Doha, QA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Jeddah March 2019	Jeddah, SA	Mar 23, 2019 - Mar 28, 2019	Live Event
SANS Madrid March 2019	Madrid, ES	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, FR	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS Dubai January 2019	OnlineAE	Jan 26, 2019 - Jan 31, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced