Securing the Hybrid Cloud: Traditional vs. New Tools and Strategies A SANS Whitepaper

This paper takes a look at the current state of cloud security and offers specific recommendations for security best practices, including how to use some traditional security tools and emerging solutions, while taking into account typical staffing, technology and other resource issues.
Introduction

As organizations move more workloads into cloud environments, security professionals are wondering why cloud security seems so difficult. They face challenges with visibility and attribution that arise from trying to validate and measure security posture in an environment where they have little to no control.

This is not a new problem. We’ve been outsourcing and using co-location providers and other third-party arrangements for years. Now, however, we have a highly scalable and dynamic service infrastructure, and in most cases, we share resources with other organizations. The good news is that today, there are many more options for security controls in the cloud, ranging from vendor solutions to cloud-native offerings from the providers themselves.

This paper takes a look at the current state of cloud security and offers specific recommendations for security best practices, including how to use some traditional security tools and emerging solutions, while taking into account typical staffing, technology and other resource issues.
Moving to Cloud Often Means a Hybrid Cloud Model

Most organizations are using some form of hybrid cloud, where some assets are maintained internally and other assets are moving into more public cloud provider environments. This model is becoming much more common as organizations look to migrate certain assets into the cloud to save money and realize some efficiencies. In fact, this cloud model is often the result when an organization decides to take its first step into cloud computing, not realizing that allowing interfaces between internal resources and external clouds creates a hybrid model that warrants specific security measures and analysis.

Migrating to a public cloud can be challenging, both in porting systems and applications into cloud-based environments, as well as in simply offloading large quantities of data into cloud storage. These problems are compounded when organizations employ a multi-cloud strategy, where they are using multiple cloud providers for different architectural functional reasons. To complicate matters, many cloud provider APIs and components are not interoperable, forcing organizations to maintain multiple management interfaces and learn entirely new skills for each. These circumstances force security teams to need development skills more commonly today, because security tools may need custom integration to normalize, sanitize and correlate data in order for security controls and processes to adapt. Most security teams lack the staff, budget or skills available to perform this level of development today. Additionally, different vendor products may only be available in one or another cloud environment, making multi-cloud even more challenging.

There are many examples of cloud provider security and availability failures, as well. At the end of 2009, the Zeus botnet was rampant in the wild, and Amazon Web Services (AWS) hosted numerous instances of Zeus botnet Command and Control (C2) servers at the time. Code Spaces, a code hosting and sharing service hosted in Amazon, was breached by an attacker in June 2014. In February 2017, an AWS employee accidentally typed a command that took out a large number of their Simple Storage Service (S3) systems. The outage caused many failures across the US East region in AWS, and even the AWS Alarms dashboard was crippled.

What Happened in the Code Spaces Breach?

In 2014, an attacker broke into Amazon-hosted Code Spaces by guessing credentials for the management login page and then demanded a ransom. When Code Spaces refused to pay (and tried to delete the attacker account), the hacker retaliated by deleting all the information they had obtained.

---

1 “Hackers find a home in Amazon’s EC2 cloud,” www.infoworld.com/article/2629005/hacking/hackers-find-a-home-in-amazon-s-ec2-cloud.html
3 “Here’s Why Amazon’s Cloud Suffered a Meltdown This Week,” http://fortune.com/2017/03/02/amazon-cloud-outage/
Mapping Internal Security Controls to Cloud

As more organizations adopt a hybrid cloud model, they’ll need to adapt their internal security controls and processes to public cloud service provider environments. To begin, risk assessment and analysis practices should be updated to continually review the items featured in Figure 1.

After risk reviews, and keeping the “shared responsibility” model in mind (meaning cloud providers and consumers share responsibility for security at different layers of the stack), security teams should have a better understanding of what controls they currently have. Teams should also have a greater understanding of what controls they will have to modify to successfully operate in the cloud, and what the most pressing concerns are (as they change).

It’s almost guaranteed that some security controls won’t operate the way they did in-house or won’t be available in cloud service provider environments. Looking at core security and IT controls, security teams will quickly realize that some controls are made easier in the cloud, while others will need to be modified in order to meet requirements. For example, system inventory is actually easier to maintain and monitor within a public cloud environment. Because all systems are linked to a cloud provider console and customer account, administrators can leverage the graphic console or provider APIs (via scripting) to query the current inventory at any time.

Let’s review several common areas within IT security operations to get a better sense of how they may adapt to cloud.

Figure 1. Items for Ongoing Review in Risk Assessment Process

It’s almost guaranteed that some security controls won’t operate the way they did in-house or won’t be available in cloud service provider environments.
Configuration and Patch Assessment

For all cloud-based systems, organizations need to determine a set of configuration items they want or need to develop and maintain. Typical items are shown in Figure 2.

Most organizations are free to develop their own internal standards that meet policies and compliance guidelines, whereas others (such as federal agencies) may be required to adhere to standards like the DISA STIGs or CIS secure configuration guides. Using an agent-based and/or agentless technology, organizations will need to apply the configuration standard to systems in the cloud and then begin assessing the new configuration for changes to or deviations from policy.

Vulnerability Scanning and Assessment

Related to configuration and patch assessment is the larger scheme of vulnerability scanning and assessment. In many cloud environments, this process is best accomplished in one of two ways. First, some traditional vulnerability scanning vendors have adapted their products to work within cloud provider environments, often relying on APIs to avoid manual requests to perform more intrusive scans on a scheduled or ad hoc basis.

The second option is to rely on host-based agents that can scan their respective virtual machines continually or as needed. Ideally, systems will be scanned on a continuous basis, with reporting of any vulnerabilities noted during the life cycle of the instance. See Figure 3 for a checklist of typical vulnerabilities to include in a scan.

Security Monitoring

Infrastructure-as-a-service (IaaS) environments are complex, almost always virtualized, multi-tenant platforms that do not lend themselves to simple monitoring for attacks on a per-customer basis. Monitoring virtual infrastructure happens at one of several places: the VM/container, the virtual switch, the hypervisor or the physical network.

In almost all cloud environments, the only place we can truly tap into is the VM/container or software-defined network offered by the cloud provider. Host-based tools...
can be installed on some PaaS platforms and most IaaS instances, with the agent reporting to a management server (either in the cloud or in your enterprise network). Considerations on how to architect monitoring tools include network bandwidth, dedicated connection(s) in place, and data aggregation/analysis methods.

Logs and events generated by services, applications, and operating systems within cloud instances should be automatically collected and sent to a central collection platform. Automated and remote logging is something many security teams are already comfortable with, so organizations implementing robust cloud security designs really just need to ensure they are collecting the appropriate logs, sending them to secure central logging services or cloud-based event management platforms, and monitoring them closely using SIEM and/or analytics tools. If data will be correlated with SIEM tools, events will need to be sent back via VPN or other encrypted tunnel, or sent to SIEM services running in the cloud themselves.

Security teams will want to monitor many types of events and activities within cloud environments. Common types of events and areas of focus will include the following:

- Unusual user logins or login failures
- Large data imports or exports to and from the cloud environment
- Privileged user activities
- Changes to approved system images
- Access and changes to encryption keys
- Changes to privileges and identity configuration
- Changes to logging and monitoring configurations
- Cloud provider and third-party threat intelligence

Regardless of controls, as organizations move to the cloud, finding some homogeneity across tools and consolidating systems will prove invaluable in maintaining system security and patch levels over time, especially in a dynamic cloud-driven architecture.

New “Cloud Native” Security Tools and Controls

As we just discussed, some controls like vulnerability scanners, patch and configuration management, and event and network monitoring may be adapted from existing in-house controls and processes to work in public cloud provider environments. However, as we move toward more software-based implementation of systems and networking, we’ll find that not all controls will work in a “security as code” model, where automated configurations can be defined and updated (more on this shortly when we discuss DevOps and automation).

As more organizations move assets into the cloud, security professionals are realizing the need for new and modified security controls within the cloud provider environments and as distinct service offerings. In other words, the types of controls we
used to have, such as network security appliances and heavy-handed agents running on endpoints and servers, are dying out as we move workloads into highly virtualized multi-tenant environments.

To make things even more complex, we’re moving data into SaaS and PaaS environments as fast as we can, and we’re finding that these types of providers may not offer many (if any) of the native security controls we’re used to. A new model for implementing security controls is starting to emerge, however, and that model is entirely driven by the use of security-oriented APIs developed specifically for cloud environments.

Most cloud operations today can make use of available APIs from the cloud providers, including configuration management and provisioning with tools such as Chef and Puppet; development and code promotion into platforms such as Amazon CodeCommit; security monitoring and management of identity data (via identity-as-a-service, or IDaaS, solutions), data protection and control with DLP and encryption; and network monitoring and traffic control, as well.

Most security-as-a-service (SecaaS) offerings make heavy use of APIs. In some cases, this approach may very well be the only way to integrate with SaaS and PaaS providers such as Salesforce and Office 365 to perform most functions related to data protection. For example, many CASB providers can monitor data being sent to cloud provider environments, and also provide DLP and policy enforcement actions for the use of cloud services. Without deep API integration, none of this could occur.

Most large cloud providers offer native APIs to developers and operations teams alike, many with some related security functionality or advantages. One example is Amazon Web Services’ CloudTrail logging and event capture and retention service. Amazon has published a detailed set of APIs for CloudTrail that allows security and operations teams to query events, list users associated with events, start and stop logging, and perform numerous additional functions.

For security teams looking to build and maintain a DevSecOps workflow and supporting processes with development and operations teams, integrating into existing orchestration and automation design will require learning and understanding the APIs available and how they’re being used.

**DevOps and Automation**

While simply adapting existing security controls and using the same tools in the cloud seems to make sense for cloud deployments and operational cloud environments, an emerging paradigm called *shift left* security looks to implement more effective controls as early in the development and deployment pipeline as possible. In other words, security is truly embedded with development and operations practices and infrastructure (a practice sometimes called *SecDevOps* or *DevSecOps*). Security and DevOps teams should define and publish IT organizational standards for a number of

**What Is the Cloud Security Open API Working Group?**

The use of APIs to govern and control security functionality in the cloud has led the Cloud Security Alliance (CSA) to start up a Cloud Security Open API Working Group in an attempt to universalize cloud use and define “protocols and best practices for implementing cloud data security” as a part of a framework for cloud access security brokers. The working group is focused on developing vendor-neutral guidelines to facilitate the growth of cloud access security brokers (CASBs). The CSA Open API Working Group charter is to help enterprises evaluate and integrate with cloud APIs via CASBs and other cloud security services, using open standards and definitions everyone can assess and understand.
areas, including application libraries and OS configurations that are approved for use. Any cloud applications and instances should be as locked down as possible, running a minimum of services, and configuration requirements should be revisited to ensure any cloud-based infrastructure is as resilient as possible.

In a true shift left model, security teams need to integrate with the developers promoting code to cloud-based applications. Security teams can impress upon development and operations that they bring a series of tests and “quality conditions” to bear on any production code push without slowing the process. Security teams should work with QA and development to define certain parameters and key qualifiers that must be met before any code can be promoted. To help shift the culture toward one that is more collaborative, security engineers and architects should be embedded full-time into the development and operational teams building and deploying cloud workloads. Figure 4 illustrates the components of a shifting left approach.

In addition, security teams need to determine which tools they have in operations that can integrate into a DevSecOps environment, as well as processes and controls that may need to be updated or adapted to work in a continuous integration and/or continuous deployment model.

Examples of automated controls that security teams need to implement for each phase of the DevOps pipeline include the following:

- Static scanning as development and code check-in is performed
- Dynamic scanning and testing during the building and testing phases
- Configuration implementation with approved templates and “infrastructure as code” definitions
- Monitoring of deployed instances through installed agents or continuous scanning within the cloud environment
- Assessment of container images in the registry and as promoted/launched in production

It’s likely that new standards for many security prevention, detection and response capabilities should be revisited, as well. These standards include areas such as encryption, privileged user management, network security access controls and filtering, event management, and logging standards.

The key for all of these various controls to be effective is Security working with DevOps teams to integrate security throughout the entire pipeline, not coming in after the fact to apply security and possibly slow down deployment.

**DevOps and Container Security**

Containers are really “OS level virtualization.” One OS instance is deployed in the cloud, and then multiple isolated usermode instances are created on top, with binaries and libraries and content—but no OS in the instance. This means that essentially a single OS kernel is now shared by multiple small application instances on the same platform, and the OS kernel (and sometimes binaries and libraries) are shared for efficiency. There are many uses for container technology today, primarily the deployment of...
lightweight application stacks and platforms. DevOps teams, in particular, like the use of containers due to the lightweight deployment options, growing maturity of automation and orchestration tools like Docker Swarm and Kubernetes, and the customization and scalability that containers offer.

Containers require access to code repositories to install and configure software packages. There are many known concerns and issues with trust validation and security for repositories and software distribution, particularly in open source environments. All container images should ideally be validated at various stages of the CI/CD pipeline. Security of containers should include hardening (configuration), patching and monitoring. The Center for Internet Security (CIS) has a set of excellent guides available for Docker, and security teams should evaluate tools that assess container builds against standards like CIS’s or vendor-recommended controls. Tools that can scan container environments are rapidly becoming requirements for security teams, and these tools may also include other features such as testing the container daemon and its configuration, validating the containers running on the container host and reviewing the container security operations. The key for any container security configuration and scanning tool is to be as lightweight as possible while scaling across many containers deployed simultaneously.

Avoiding Silos and “Point Solutions”

One major headache for organizations moving to cloud is the potential to create “silos” of controls or point solutions with a single vendor or cloud-native option that does not offer flexibility across different providers and environments. Some vendor products will work only in specific environments, and most cloud providers’ built-in services will work only on their own platforms. Such siloing can lead to major headaches when business needs drive organizations to a multi-cloud strategy, necessitating the revisitation of security controls that meet requirements. This situation is not ideal—more time and money will be lost having to reevaluate the specific capabilities of the provider.

Many organizations may want to investigate security-as-a-service (SecaaS) options to help augment or implement controls they need in the cloud. Many SecaaS providers offer lightweight embedded agents and service options tightly integrated with leading cloud provider APIs that can lower cost and complexity for a number of different control areas. SecaaS options are also ideally suited for automation and continuous development and deployment strategies, making them attractive to DevSecOps teams.

SecaaS may also be ideal for multiple cloud environments, because the service model is external to the cloud and can integrate into many major provider environments such as AWS, Microsoft Azure, Google Cloud and more.

TAKEAWAY
When looking at cloud-compatible security products and services (both SecaaS and tools that integrate directly to cloud environments), it’s important to consider maturity in the security products available as well as the vendors themselves. While there are some great emerging security tools and products for the cloud, mature vendors have adapted some of the same products you may already be familiar with (and those you’re already using) to many types of cloud environments. Using tools that are familiar and uniform across both internal and cloud environments may greatly simplify management and operations related to these tools.
Conclusion

The major security considerations for hybrid cloud largely revolve around secure data transfer and storage, controlling and monitoring user activity, and looking for compatibility and capabilities in the cloud from trusted security vendors and service providers. Adopting a shift left strategy also means formally defining configuration standards and application security criteria that are baked into the deployment workflows much earlier than ever before, and then monitored in an ongoing fashion.

Determine the code promotion and QA processes in place at your organization today and decide where security team members can best integrate into the code development and promotion life cycle for evaluating and analyzing current practices. Also, work with business unit leaders to understand their goals as they relate to rapid development, and learn how operations and security teams can better work with programmers throughout the SDLC to facilitate, not hinder, these goals.

Evaluate operations collaboration with development and see where the major gaps are related to communication and ongoing management and maintenance. Record these, have conversations with all relevant teams to understand where roadblocks are, and determine what actions might help overcome obstacles. Security teams can be valuable team players in the DevOps movement. However, they need to adapt to more rapid changes, more flexibility, and the willingness to concede “perfect security” for business benefits, with advanced monitoring and awareness after the fact.

Those organizations moving to a hybrid cloud model need to complete a thorough review of all existing controls and processes before deploying the public cloud assets, if possible. This will give them the opportunity to adequately protect the data involved, as well as look for equivalent security capabilities in public cloud environments. Look for tools that can help you manage both in-house and cloud assets in one place, because security and operations teams are usually spread too thin to manage multiple management and monitoring tools across one or more cloud provider environments.
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.

SANS would like to thank this paper’s sponsor:

Qualys®
Continuous Security
<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Zurich 2018</td>
<td>Zurich, CH</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Spring 2018</td>
<td>Baltimore, MDUS</td>
<td>Apr 21, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Seattle Spring 2018</td>
<td>Seattle, WAUS</td>
<td>Apr 23, 2018 - Apr 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training 2018</td>
<td>Louisville, KYUS</td>
<td>Apr 23, 2018 - Apr 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh April 2018</td>
<td>Riyadh, SA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha 2018</td>
<td>Doha, QA</td>
<td>Apr 28, 2018 - May 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta Two</td>
<td>Crystal City, VAUS</td>
<td>Apr 30, 2018 - May 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Automotive Cybersecurity Summit &amp; Training 2018</td>
<td>Chicago, ILUS</td>
<td>May 01, 2018 - May 08, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC504 in Thai 2018</td>
<td>Bangkok, TH</td>
<td>May 07, 2018 - May 12, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2018</td>
<td>San Diego, CAUS</td>
<td>May 11, 2018 - May 18, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2018</td>
<td>Melbourne, AU</td>
<td>May 14, 2018 - May 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Reston Spring 2018</td>
<td>Reston, VAUS</td>
<td>May 20, 2018 - May 25, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam May 2018</td>
<td>Amsterdam, NL</td>
<td>May 28, 2018 - Jun 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Atlanta 2018</td>
<td>Atlanta, GAUS</td>
<td>May 29, 2018 - Jun 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rocky Mountain 2018</td>
<td>Denver, COUS</td>
<td>Jun 04, 2018 - Jun 09, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>DFIR Summit &amp; Training 2018</td>
<td>Austin, TXUS</td>
<td>Jun 07, 2018 - Jun 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Milan June 2018</td>
<td>Milan, IT</td>
<td>Jun 11, 2018 - Jun 16, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2018</td>
<td>Manila, PH</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo June 2018</td>
<td>Oslo, NO</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit and Training 2018</td>
<td>Munich, DE</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Crystal City 2018</td>
<td>Arlington, VAUS</td>
<td>Jun 18, 2018 - Jun 23, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cyber Defence Canberra 2018</td>
<td>Canberra, AU</td>
<td>Jun 25, 2018 - Jul 07, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vancouver 2018</td>
<td>Vancouver, BCCA</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2018</td>
<td>Minneapolis, MNUS</td>
<td>Jun 25, 2018 - Jun 30, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Charlotte 2018</td>
<td>Charlotte, NCUS</td>
<td>Jul 09, 2018 - Jul 14, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London April 2018</td>
<td>OnlineGB</td>
<td>Apr 16, 2018 - Apr 21, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>