CloudHealth® by vmware®

The 3 Recommendations for Cloud Security

INTRODUCTION TO CLOUD SECURITY

Regardless of whether your data resides on-premises, in the cloud, or a combination of both, you are vulnerable to security threats, data breaches, data loss, and more. Security is often cited as a concern for organizations who are migrating to the public cloud, but the belief that the public cloud is not secure is a myth. In fact, the leading public cloud service providers have built rigorous security capabilities to ensure that your applications, assets, and services are protected. Security in the public cloud is now becoming a driver for many organizations, but in a rapidly evolving multicloud environment, you must keep up with changes that might impact your security posture.

This eBook outlines the three core recommendations for cloud security across Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

SHARING RESPONSIBILITY

It's a common misconception that it's the sole responsibility of public cloud service providers to safeguard your data and information. According to Gartner, through 2022, at least 95% of cloud security failures will be the customer's fault.[1] Let that sink in for a moment, and think about your cloud environment. Ensuring the security of one cloud can be a challenge, and if you are a multicloud user, that challenge becomes exponentially more difficult.

In order to best plan and execute on a security strategy, you must understand who is responsible. Cloud service providers, such as Amazon Web Services, have published Shared Responsibility Models to outline the protections that each party is responsible for. The AWS Shared Responsibility Model is broken into two categories; security of the cloud which is owned by AWS, and security in the cloud which is owned by customers. To put it simply, the cloud provider is responsible for protecting the infrastructure (e.g. hardware, software, facilities), and in turn, the customer is responsible for the applications, service configuration, and identity and access management.[2]

Prior to deploying new services and developing applications, it's recommended you outline which security requirements your organization is responsible for. If you're not a Chief Information Security Officer or security leader, perhaps it would be valuable to discuss this with them. The last thing you want is to become part of that 95% statistic.

[1] *Gartner, Clouds Are Secure: Are You Using Them Securely?, Jay Heiser, 31 January 2018*

[2] *"Shared Responsibility Model - Amazon Web Services (AWS)." Amazon, aws.amazon.com/compliance/shared-responsibility-model/.*

CENTER FOR INTERNET SECURITY BENCHMARKS DEFINED

The Center for Internet Security (CIS) is a non-profit organization that publishes standards and best practices for securing IT systems and data. One type of publication that they provide is a Benchmark, which is a security configuration guideline that has been tested and proven by experienced IT professionals.[3] CIS is a trusted third-party and organizations worldwide rely on the 100+ CIS Benchmarks to safeguard their cloud environments.

Three of these Benchmarks have been created for Amazon Web Services Foundations, Microsoft Azure Foundations, and Google Cloud Platform Foundation. Although each of these cloud service providers have unique recommendations (e.g. Security Center for Azure, and Kubernetes Engine for Google Cloud Platform etc.), they have three core recommendations in common: identity and access management, logging and monitoring, and networking. Within each recommendation, there are a set of controls that are given a profile level. A Level 1 Profile is a foundational control and shouldn't impact business functionality. A Level 2 Profile is for more in-depth security controls that could have a negative impact if not implemented properly. To perform an audit of your cloud infrastructure, you can use the cloud service provider management console, run a series of commands via the Command Line Interface, or leverage a cloud management solution to perform an audit on your behalf.

[3] Center for Internet Security, www.cisecurity.org/.

1 IDENTITY AND ACCESS MANAGEMENT

Cloud security starts with properly managing users and access controls. Without proper identity and access management, users can intentionally or unintentionally create security flaws with serious implications. The Identity and Access Management controls take a proactive approach by validating that you have properly and securely configured access to your cloud environment.

The controls help you stay ahead of breaches by monitoring for leading indicators such as:

- Misconfigured users (i.e., users not in a group)
- Users with too broad of a span of control
- Users with vulnerable accounts (i.e., multi-factor authentication disabled, etc.)
- Inactive users (i.e., IAM user with access keys that are not being used, etc.)

While it's always best to catch security vulnerabilities before they are exploited, it's prudent to also monitor for events that could turn into security incidents, or lagging indicators, such as:

- Suspicious activity (e.g., a large volume of instances are launched outside of normal usage patterns, etc.)
- Changes to security groups or users (e.g., new IAM group or user recently created or changed, etc.)

SAMPLE AWS CONTROL[4]

1.3 Ensure credentials unused for 90 days or greater are disabled (Scored)

RATIONALE:

Disabling or removing unnecessary credentials will reduce the window of opportunity for credentials associated with a compromised or abandoned account to be used.

[4] *CIS Benchmarks, Amazon Web Services Foundations v1.2.0, May 23, 2018.*

2 LOGGING AND MONITORING

Without proper audit trails and logs in place, it can be extremely challenging to identify security incidents, policy violations, fraudulent activity, and operational problems. In short, root cause analysis and troubleshooting are greatly helped by log management. To further assist with monitoring and responding to account activities, controls must be in place for log metric-filters and alarms. The Logging and Monitoring controls ensure that logs are collected, stored securely for the proper amount of time, and are available for analysis when needed.

SAMPLE GOOGLE CLOUD PLATFORM CONTROL[5]

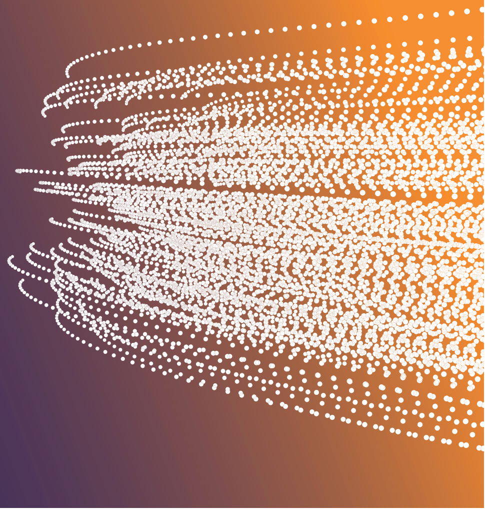
2.10 Ensure log metric filter and alerts exists for Cloud Storage IAM permission changes (Scored)

RATIONALE:

Monitoring changes to Cloud Storage bucket permissions may reduce time to detect and correct permissions on sensitive Cloud Storage bucket and objects inside the bucket.

[5] *CIS Benchmarks, Google Cloud Platform Foundation v1.0.0, September 05, 2018.*

3 NETWORKING



Maintaining a secure perimeter to allow only legitimate traffic onto the network is critical in both the data center and the cloud. Hacking and phishing are just a few examples of network security breaches. As organizations continue to move towards a multicloud model it becomes harder and harder to tell the difference between legitimate and malicious traffic. The Networking controls are designed to monitor for security group and network protocol misconfigurations, such as when a Security Group has too large of an ingress port range. Beyond measuring for Security Group configurations, you may also want to be notified when a new Security Group is created, or if a Security Group isn't being used. Since a single instance can have many different Security Groups applied to it, it's also important to monitor for instances associated with a large number of Groups.

SAMPLE AZURE CONTROL[6]

6.2 Ensure that SSH access is restricted from the internet (Scored)

RATIONALE:

The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure.

[6] *CIS Benchmarks, Amazon Web Services Foundations v1.0.0, February 20, 2018*

ADDITIONAL SECURITY CONSIDERATIONS

Although the CIS Foundations Benchmarks do not have resiliency called out in its own recommendation section, the ability to recover operations and data after an outage or data loss event is a key component of world-class security best practices. Business continuity can span from making sure critical systems have backups replicated in another region to checking that critical assets are stored on highly available and redundant infrastructure. Most organizations will segment their applications and downstream dependent assets by business criticality, typically onto four levels: mission critical, business critical, business important, business supporting. Each tier will have a defined recovery time objective (RTO), recovery point objective (RPO), and availability SLA. Having a data resiliency strategy is imperative, and in many cases organizations choose to backup and recover data between multiple cloud service providers. For example, if AWS is the primary cloud, an organization may recover to Azure, or Google Cloud Platform. A multicloud strategy hinges on data and application availability, resiliency, and security.

CONCLUSION

Ensuring the security of your public cloud environment is challenging, and ensuring the security of your multicloud environment can be even more difficult. Learn how the CloudHealth cloud management platform can help you mitigate security risks across your multicloud environment, by visiting **www.cloudhealthtech.com.**