HC3: Analyst Note

August 9, 2022 TLP: White Report: 202208091700

Cloud Security

Executive Summary

When we refer to the cloud or cloud computing what we are really talking about is a server(s) that is accessed over the internet. Majority of these servers are stored through third party cloud service providers (CSP) at data centers which can be located anywhere in the world. Through this, companies can reduce their cost because they do not have to physically manage the servers or software for them. By using a CSP, providers and customer enter a shared responsibility for security. When it comes to cloud security, we usually refer to a set of policies, controls, and technologies that are working together to protect an infrastructure. Threats facing the cloud can vary, but the biggest concerns exist with internal threats such as human error, external threats from malicious actors, and the infrastructure itself. Since the cloud exist off-site the conventional methods of protection aren't always effective. When protecting the cloud, we are attempting to secure the network, recover data, minimize human error, and reduce the overall impact of a compromise.

What is Cloud Security?

Cloud security is an area of cyber security that focus' on protecting cloud computing-based systems. Properly securing cloud services begins with understanding what is being secured along with the system that is managing it. It is the combination of technology, protocols, and practices that protect these environments and applications operating in the cloud. Together they protect the system, data, and infrastructure. Securing this is a team effort between the cloud provider and their clients regardless of whether it's a small or large business. These security measures are configured with the intent to protect data and customer privacy as well as setting up proper authentication rules for the individual users and devices. Through this, cloud security can be configured to meet the specific needs of a business. Since these rules can be configured and managed in one place, teams have increased availability to focus on other needs in their department.

What is the Goal of Cloud Security?

Cloud security measures are almost always working to achieve one or more of the following:

- Recover data in the event of data loss
- Ensuring the privacy of data across networks
- Protect networks against malicious activity
- Minimize human error that could cause data loss
- Reduce the overall impact of compromises

The Shared Responsibility Model

Most organizations use a third-party cloud service provider to host their data and applications. Because of this cloud security becomes a shared responsibility between provider and customer. The security responsibility for each party is based off which cloud service they are using: Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

HC3: Analyst Note

August 9, 2022 TLP: White Report: 202208091700

Service Type	Vendor Responsibility	User Responsibility
SaaS	Application security	Endpoints, user and network security; misconfigurations, workloads and data
PaaS	Platform security, including all hardware and software	Security of applications developed on the platform Endpoints, user and network security, and workloads
IaaS	Security of all infrastructure components	Security of any application installed on the infrastructure (e.g. OS, applications, middleware) Endpoints, user and network security, workloads, and data

Source: Crowdstrike

Cloud Security Risk

Many cyber security threats that exist today apply to the cloud as well. Vulnerabilities with insider risk, data breaches, phishing, and malware are all a real possibility. Weak cloud security can expose users and providers to all types of cyber related threats such as concerns with the infrastructure and incompatible frameworks, internal threats from human error, and external threats from malicious actors.

Misconfiguration

The NSA believes that cloud misconfiguration is a leading vulnerability in many environments and according to a Gartner survey, 80% of data breaches are caused by a misconfiguration in the cloud. Some of the common misconfigurations include:

- Unrestricted inbound/outbound ports
- Disabled monitor/logging capabilities
- Unsecure API keys
- Internet Control Message Protocol left open

Cloud Credentials and Phishing

Threat actors commonly use cloud applications and environments in their phishing attacks. With the growing use of cloud-based email and document sharing services people have grown accustomed to receiving emails with links to confirm their identity.
This change in the way we operate has benefited cybercriminals and increased their phishing attempts for an employee's credentials. Subsequently, the accidental exposure of cloud credentials should be a concern for organizations since it endangers the privacy and security of their data and resources.

Shadow IT

Shadow IT is the use of information technology services, software, or devices that aren't approved by an IT department for use. Shadow IT has risen over the years through the use of public cloud services and as employees saw the short term benefit versus the long term security impacts. If a department is unaware of an application, then they won't have the ability to secure it properly. Organizations can educate users and mimize their risk from Shadow IT.

Additional Cloud Risk

Cloud Hijacking: Where cyber criminals take over your account.
Identity and access management (IAM): Is referring to the accessibility given to user accounts. Access controls are critical to restrict accounts for authorized and malicious users alike.

Lack of cloud visibility: Gaining full visibility over a cloud environment is difficult and faces complications of its own with:

- Limited control over the traffic since the infrastructure is off-site
- Blind spots can result in a failure to alert on security incidents
- Limited security if alerts are not investigated

Cloud compliance: Maintaining the practices and procedures that use specific security and privacy standards.

Protecting the Cloud

The cloud provides plenty of advantages to an organization, but these benefits also come with their own security challenges. Cloud-based infrastructure is simply just different when compared to an on-site data center. Evaluating the geographic location is an important consideration when choosing a CSP. The main goal with cloud security is maintaining the integrity of the files and preventing unauthorized access, but traditional tools and strategies are not always capable of accomplishing this.
Knowing some of the best practices for securing the cloud is an important factor in safekeeping your organizations data.

- Use a cloud service provider that encrypts
- Conduct compliance audits
- Implement a Zero Trust model
- Set up your privacy settings
- Use a Two-Factor Authentication
- Establish and enforce security policies
- Maintain cloud visibility
- Understand cloud compliance, requirements, and regulations
- Install updates to your operating system
- Avoid using public Wi-Fi

Most organizations today are using the cloud and it's important to choose the best CSP for your organization and to understand what security controls they offer.

References:

- Acronis. "What is cloud-based security and how does it work?" January 12, 2021. https://www.acronis.com/en-us/blog/posts/cloud-based-security/?utm_content=sfdc%3A7011T000001pnQK%3A7011T000001pnQU&gclid=EAIaIQobChMIxOibwrXn-AIVH3RvBB0bUAKBEAAYASAAEgLNd_D_BwE
- Box. "What is Cloud Security?" https://www.box.com/resources/what-is-cloud-security
- CheckPoint. "Top 15 Cloud Security Issues, Threats, and Concerns"https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
- CheckPoint. "What is Cloud Security?" https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

- CloudFare. “What is the Cloud|Cloud definition” https://www.cloudflare.com/learning/cloud/what-is-the-cloud/
- ForcePoint. “What is Cloud Security?” https://www.forcepoint.com/cyber-edu/cloud-security
- Froehlich, Andrew. Shea, Sharon. Cole, Ben. “cloud security” February, 2021. https://www.techtarget.com/searchsecurity/definition/cloud-security
- IBM. “What is cloud security?” https://www.ibm.com/topics/cloud-security#:~:text=Cloud%20security%20is%20a%20collection,as%20part%20of%20their%20infrastructure
- Kaspersky. “What is Cloud Security” https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security
- NetApp. “Cloud Visibility: 3 Critical Challenges and Solutions” March 22, 2021. https://cloud.netapp.com/blog/blg-cloud-visibility-3-critical-challenges-and-solutions
- Puzas, David. “Cloud Security Risk, Threats, and Challenges” CrowdStrike. June 17, 2021. https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-security-risks-threats-challenges/
- Sukianto, Axel. “Common Cloud Misconfigurations and How to Avoid Them” UpGuard. May 01, 2022. https://www.upguard.com/blog/cloud-misconfiguration#:~:text=Cloud%20misconfiguration%20refers%20to%20any,vulnerabilities%20to%20access%20your%20network.
- Norton. NortonLifeLock Employee. “How to secure your information in the cloud” Norton. https://us.norton.com/internetsecurity-how-to-secure-your-info-in-the-cloud.html
- Alvarenga, Gui. “What is Cloud Security?” Crowdstrike. 04 Feb, 2022. https://www.crowdstrike.com/cybersecurity-101/cloud-security/?utm_campaign=cloudsecurity&utm_content=c4c_cloud_us_en_nb_low&utm_medium=sem&utm_source=goog&utm_term=what%20is%20cloud%20security&gclid=EAIaIQobChMIq7rsruT4-AIVkMmUCR0yog8-EAAYBCAAEgLhH_D_BwE

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback