National Security Agency | Cybersecurity Information

NSA’s Top Ten Cloud Security Mitigation Strategies

Executive summary

As organizations continue to migrate to using cloud environments, these environments are becoming increasingly valuable targets for malicious cyber actors (MCA). Many cloud breaches occur due to misconfigurations in cloud tenants. NSA’s Top Ten Cloud Security Mitigation Strategies inform cloud customers of the most important practices to improve the security posture of their cloud environments. As organizations shift their data to the cloud for ease of processing, storing, and sharing, they must take precautions to maintain parity with on-premises security and mitigate additional cloud-specific threats. The following sections outline NSA’s top ten recommended mitigation strategies that cloud customers should take to improve their security posture. Each strategy has an associated cybersecurity information sheet that describes it in more detail at the following:

1. **Uphold the Cloud Shared Responsibility Model**
2. **Use Secure Cloud Identity and Access Management Practices**
3. **Use Secure Cloud Key Management Practices**
4. **Implement Network Segmentation and Encryption in Cloud Environments**
5. **Secure Data in the Cloud**
6. **Defending Continuous Integration/Continuous Delivery (CI/CD) Environments**
7. **Enforce Secure Automated Deployment Practices through Infrastructure as Code**
8. **Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments**
9. **Mitigate Risks from Managed Service Providers in Cloud Environments**
10. **Manage Cloud Logs for Effective Threat Hunting**

1. Uphold the Cloud Shared Responsibility Model

Security gaps arise when customers assume that the cloud service provider (CSP) is securing something that is actually the customer’s responsibility. Customers must understand the CSP’s shared responsibility model (SRM), which identifies who is responsible for security based on the type of service acquired (SaaS, PaaS, or IaaS). The SRM will vary from service to service, and it may also vary by CSP, so close attention to documentation and best practice guides is essential. Direct engagement with the CSP may sometimes be necessary to understand their service models. Customers should hold the CSP accountable for its part, while the customers must dutifully fulfill their own tenant responsibilities.

2. Use Secure Cloud Identity and Access Management Practices

Proper identity and access management (IAM) are critical to securing cloud resources. Malicious actors can compromise accounts using phishing techniques, exposed credentials, or weak authentication practices to gain initial access into cloud tenants. They can also exploit overly broad access control policies to penetrate further into the environment, gaining access to sensitive resources. To prevent this, cloud users should use secure authentication methods such as phishing-resistant multifactor authentication (MFA) and properly managed temporary credentials. Access control policies should be carefully configured to ensure users are granted the least privileges necessary. Separation of duties should be implemented to protect especially sensitive operations and resources.

3. Use Secure Cloud Key Management Practices

CSPs offer a variety of methods for handling key management, ranging from full reliance on the cloud vendor for fully delegated server-side encryption, to a full client-side encryption method where the customer generates and manages the keys themselves and encrypts all data prior to uploading it. In most cases, organizations will rely on the CSP for a portion of key management, encryption, and decryption. However organizations handle this, it is vital that they understand the risks and benefits to each option and their roles and responsibilities for properly managing keys.

4. Implement Network Segmentation and Encryption in Cloud Environments

Organizations using cloud resources must implement controls in their tenant to prevent and detect MCA activities. Zero Trust (ZT) network security practices, such as evaluating identity information in all requests, micro segmentation, and end-to-end encryption, should be used to protect organizational data. Micro segmentation is a large part of the prevention effort by separating resources based on organizational team, application workflow, and data ingress/egress, as applicable. Restricting resources to only the communication paths necessary to support normal functionality greatly limits

MCAs with access to the tenant. End-to-end encryption of all data in transit to, from, and within the cloud is also key to protecting data in the cloud.

5. Secure Data in the Cloud

The cloud presents an attractive target to malicious actors for data theft and ransom. Organizations can secure their data by selecting appropriate cloud storage, preventing exposure over public IPs, enforcing least privilege, using object versioning, creating immutable backups with recovery plans, enabling encryption, and regularly reviewing data security measures. Organizations should understand CSP data retention policies and then choose the appropriate options for storing sensitive data. In addition, organizations should consider enabling "soft delete" features to mitigate the effects of accidental or malicious deletions.

6. Defending Continuous Integration/Continuous Delivery (CI/CD) Environments

An organization's development, security, and operations (DevSecOps) procedures are critical to the security of their environment. Continuous integration and continuous delivery (CI/CD) pipelines are a key part of this process and are frequently deployed in the cloud. These pipelines make valuable targets for MCAs as a successful compromise of a CI/CD pipeline could impact both infrastructure and applications. Organizations should follow best practices in securing their organization's CI/CD pipelines, such as strong IAM practices, keeping tools up to date, auditing logs, implementing security scanning, and properly handling secrets.

7. Enforce Secure Automated Deployment Practices through Infrastructure as Code (IaC)

Infrastructure as code (IaC) automates the deployment of cloud resources. The elimination of manual infrastructure deployment reduces the likelihood of misconfigurations and ghost assets introduced by human error. IaC allows organizations to quickly detect unauthorized changes to infrastructure. Policy as code codifies security and compliance best practices.

Prior to IaC deployment, organizations should create a threat model[1] to map attack vectors, determine if IaC templates will be declarative or imperative, complete static application security testing, and consider integrating existing CI/CD processes. After deployment, organizations should dynamically test deployed resources, ensure access and version controls are enabled, avoid manual changes, and continuously log and monitor resources.

8. Account for Complexities Introduced by Hybrid Cloud and Multi-Cloud Environments

Organizations should account for complexities that may arise when using hybrid cloud and multi-cloud environments. The use of hybrid and multi-cloud environments introduces operational silos and skill gaps, which may lead to configuration discrepancies, unnecessary data flows, insecure IAM, loss of visibility, and exploitable security gaps. Network, IAM, and logging best practices should be used to maintain secure cloud infrastructures. Standardizing cloud operations with vendor agnostic tools allows organizations to maintain and monitor multiple environments from a centralized location.

9. Mitigate Risks from Managed Service Providers in Cloud Environments

While managed service providers (MSPs) can provide useful technical support for administering, maintaining, and/or securing a cloud environment, using an MSP can increase an organization’s attack surface. Organizations should make security a priority when choosing an MSP in order to mitigate threats to the cloud tenant through the MSP. Organizations should select providers that comply with the security standards and practices important to the organization. In addition, organizations should audit MSP accounts and operations in the environment, prioritizing privileged accounts and activities. Organizations should also integrate MSP services into security operations, system recovery, and incident response processes.

[1] For more information on what a threat model is and how to go about writing one consider reviewing OWASP’s Threat Modeling resources: https://owasp.org/www-community/Threat_Modeling

10. Manage Cloud Logs for Effective Threat Hunting

Logs play a fundamental role in threat detection for cloud environments. Detecting and responding to security incidents require a thorough understanding of the system’s activity and behavior. Cloud systems involve many users accessing numerous shared resources and services. This commonly includes ephemeral resources, which create a complex and dynamic environment that can be difficult to visualize and monitor.

Organizations should collect and aggregate logs from all relevant sources, such as cloud services, operating systems, and applications. Cloud environments typically offer convenient log aggregation mechanisms for pulling log data into centralized services for better visualization and threat hunting. Default logging policies vary greatly between cloud services, so it is vital that security professionals configure these policies to ensure MCAs cannot freely operate within cloud tenants without being detected.

Security professionals can use tools, such as security information and event management (SIEM) systems, log analysis software, and anomaly detection services, to analyze the logs for indicators of compromise and abnormal activity, including unusual login attempts, network traffic patterns, and anomalous system events. This enables security teams to directly respond to threats identified in logs and sometimes even automate these actions to respond in real time.

Conclusion

As organizations continue to migrate more of their data and services to cloud environments, MCAs will increasingly attempt to compromise those environments. Misconfigured, unsecured, or unmonitored cloud systems will pose enticing targets. NSA recommends that organizations and cloud users follow these mitigation strategies to improve their cloud security posture.▪

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries or Customer Requests: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov