Secure Data in the Cloud

Executive summary

As organizations move more of their data into cloud environments, the prevention of unauthorized access to that data is extremely important. Data stored in the cloud can take many forms depending on the needs of the organization. For these reasons, organizations must understand the sensitivity of the data they store in the cloud, select the appropriate storage services, and apply pragmatic security methods to properly protect their data. The purpose of this cybersecurity information sheet is to provide an overview of what cloud storage is and common practices for properly securing and auditing cloud storage systems.

Cloud data types

The three main types of data storage that cloud service providers (CSP) offer are:

File, which stores data in a folder-based structure and allows for user access via protocols like network file system or server message block protocols.

Object, which stores data objects in a key-value data store. Users can access these objects by interacting with the Object storage application programming interface.

Block, which is typically used by cloud compute resources that need large amounts of hard drive space, ranging from Nonvolatile Memory Express (NVME), Solid State Drive (SSD), and Hard Disk Drive (HDD) speeds and sizes. [1], [2], [3]

File, Object, and Block storage systems are not only standalone systems, but also are used as the building blocks for cloud-specific platform as a service (PaaS) and software as a service (SaaS) offerings. PaaS instances are on-demand, comprehensive platforms used for deploying custom software in the cloud. SaaS instances are ready-to-use software, such as email, collaboration, or file sharing applications. Typically, when provisioning PaaS and SaaS offerings, the storage system is not hidden within the service, but instead is directly available and is managed alongside the PaaS or SaaS system.

Securing Data

The following sections describe common practices for properly securing cloud storage systems. They list several related MITRE ATT&CK® and MITRE D3FEND™ threat and defensive techniques. These are meant as representative examples, but are not intended to include all possible related techniques. [4], [5]

Encryption

Encryption at rest and in transit is an imperative for sensitive data. All interactions with cloud storage that include sensitive data should be encrypted using Commercial National Security Algorithm (CNSA) Suite 1.0 approved encryption mechanisms at minimum. CNSA Suite 2.0 standards should also be considered. [6] Sensitive data should never be accessed over insecure channels. Connections via the web should be encrypted with TLS1.2 or higher. Many individual storage offerings that CSPs provide include easy to integrate server and client-side encryption methods.

Many CSPs offer their own standalone key management services (KMSs) as well as provide integrations for data services with other KMSs. Depending on the implementation of the KMS, the service can easily generate keys or allow customers to bring their own. KMSs provide a secure storage solution for keys and the ability to rotate them. Organizations should consider hardware security modules (HSM) when there is a need for more security.

For more details on what to consider when choosing a key management solution and how to securely manage key material for cloud environments, see the joint Cybersecurity Information sheet (CSI): Use Secure Cloud Key Management Practices.

ATT&CK Tactic	Technique
Collection	Data from Cloud Storage [T1530]
Credential Access, Discovery	Network Sniffing [T1040]

ATT&CK Mitigation
Encrypt Sensitive Information [M1041]

D3FEND Tactic	Countermeasure
Platform Hardening	Disk Encryption [D3-DENCR]
Platform Hardening	File Encryption [D3-FE]
Network Isolation	Encrypted Tunnels [D3-ET]

Data access policies

CSPs have designed access systems around the role-based access control (RBAC) and attribute-based access control (ABAC) strategies. RBAC grants account permissions based on a given role. These can be built-in roles that are set up by the CSP or custom roles created by customers. ABAC assigns individual access attributes to a given user or role to limit access to storage devices and limit an account's ability to provision resources.

Both user and system accounts should only be given the minimal level of access needed to perform tasks by their cloud administrators. Overly permissive policies for data access can have large repercussions for cloud security incidents. Plan to implement roles and access in a scalable and easy-to-use way. Higher complexity around the process of assigning proper permissions may result in overly permissive access. Data access permissions should be granular, and the use of "wildcard" permissions should be severely limited. Consider utilizing a data tagging system or solution, where data is conditionally accessed via granular ABAC policies to protect data. It is also important to separate accounts that grant access to resources from those that manage them daily.

Most CSPs provide capabilities that can assist with the account permission auditing process. Additionally, commercial products are available to identify insecure permissions in cloud environments. These can help, especially in multi-cloud environments.

Organizations should also consider data loss prevention (DLP) systems, which can identify systems exposing data unnecessarily. DLP systems often offer both active and passive monitoring of data and automatic detection and remediation processes. Some CSPs offer features or policy systems that provide DLP capabilities. Organizations should evaluate the sensitivity levels of their data and implement a series of controls or policies to prevent accidental data spillage.

ATT&CK Tactic	Technique
Collection	Data from Cloud Storage [T1530]

ATT&CK Mitigation
User Account Management [M1018]
Restrict File and Directory Permissions [M1022]

Data Loss Prevention [M1057]

D3FEND Tactic	Countermeasure
Operational Activity Mapping	Access Modeling [D3-AM]
Platform Hardening	Local File Permissions [D3-LFP]

Limiting the attack surface

All cloud resources should be regularly audited by cloud administrators for improper exposure. Data storage services should never be placed into publicly accessible networks unless justified by a mission requirement that is periodically reassessed. Having a clearly defined cloud architecture will limit the possibility of accidental public exposure.

Object storage is one of the most exploited data storage methods because of its popularity and how easily it can be misconfigured. Applying proper access policies to Object storage will prevent unintentional data exposure. For example, major CSPs have access policies that can be deployed by cloud administrators enterprise wide to block publicly accessible Object storage by default and allow it only by exception.

ATT&CK Tactic	Technique
Discovery	Cloud Storage Object Discovery [T1619]

ATT&CK Mitigation
Limit Access to Resource Over Network [M1035]
Restrict File and Directory Permissions [M1022]

D3FEND Tactic	Countermeasure
Operational Activity Mapping	Access Modeling [D3-AM]
Network Mapping	Network Traffic Policy Mapping [D3-NTPM]
Platform Hardening	Local File Permissions [D3-LFP]
Network Isolation	Inbound Traffic Filtering [D3-ITF]

System recovery and backup

Regardless of size, all users of cloud environments supporting production systems must implement a recovery and backup solution. Many CSPs now provide a backup service, which can simplify the process and save backups as immutable. Immutability allows for a high amount of protection against malicious activity and ransomware. As well as implementing a recovery backup solution, it is important to properly identify all cloud

resources that need to be backed up, including resources that span multiple regions and availability zones. Account access to backups should be continuously evaluated and limited to administrators who directly maintain and test backups.

ATT&CK Tactic	Technique
Impact	Data Encrypted for Impact [T1486]
Impact	Data Destruction [T1485]

ATT&CK Mitigation
Data Backup [M1053]
Remote Data Storage [M1029]

D3FEND Tactic	Countermeasure
Asset Inventory	Data Inventory [D3-DI]
Restore Object	Restore File [D3-RF]

Understanding CSP data procedures

CSPs have created complex platforms that are designed for ease of access and convenience. However, cloud administrators often overlook policies for data storage and retention. Soft deletion is a feature that enables a deleted object to be recoverable for a certain period of time. NSA and CISA recommend organizations utilize soft delete features—when possible—to prevent accidental data loss. If soft delete features are enabled, it's important to understand how this aligns with data retention policies.

Deallocation of resources, such as allowing customers to control what resources are needed to run at specific times, is a signature feature of CSPs. The process of stopping or deallocating resources typically does not mean that the data is deleted or inaccessible. It is important to understand the specific resource that stores data and whether the data is truly deleted rather than stopped or deallocated. Depending on the data storage resources deployed, there may be a difference in the secure wiping of processes and the deallocation of resources. Resources that are truly meant to be deleted should go through the secure wipe or removal process outlined by the CSP. [7], [8]

Organizations should also carefully review cloud service agreements to understand the risk of data being stored outside of the United States. Depending on the agreement and the laws of the country where the data is physically located, the data could be subject to

seizure requests by foreign governments. For data that must reside outside the United States, customers can reduce risk by implementing solutions such as:

- On-premises or external key management solutions,
- Secure compute enclave environments, and
- Other data protection tools.

Organizations should understand that on-premises encryption methods can be a limiting factor to data processing in cloud environments especially when compared with secure compute environments in the cloud.

Best practices

The following is a summary of best practices for securing data in the cloud:

1. Obtain and retain a good understanding of the cloud storage offerings and choose storage types that make sense for the data being stored.
2. Use encryption for all data that is sensitive in nature. Manage these keys through either a KMS or HSM.
3. Have an understandable process of assigning permissions to users and service accounts. Always use the principal of least privilege when assigning permissions.
4. Properly audit and understand cloud data's attack surface. Especially look for those resources that are publicly exposed.
5. Use a backup solution and routinely test restoration of critical data and services.
6. Review individual cloud provider data retention policies with regards to deleting data. Be sure that systems that carry sensitive data are properly being deleted.

Further guidance

Supplementary NSA guidance on ensuring network environments are secure and defendable is available at NSA Cybersecurity Advisories & Guidance. Those of particular relevance are:

- Mitigating Cloud Vulnerabilities
- Top 10 Mitigation Strategies
- Identity and Access Management Recommended Best Practices for Administrators

Works cited

[1] Microsoft. What is Cloud Storage? 2024. https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-storage
[2] Amazon. What is Cloud Storage? 2024. https://aws.amazon.com/what-is/cloud-storage/
[3] Google. Product overview of Cloud Storage. 2024. https://cloud.google.com/storage/docs/introduction
[4] The MITRE Corporation. MITRE ATT&CK. 2024. https://attack.mitre.org
[5] The MITRE Corporation. MITRE D3FEND. 2023. https://d3fend.mitre.org
[6] NSA. Announcing the Commercial National Security Algorithm Suite 2.0. 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
[7] Google. Data deletion on Google Cloud. 2023. https://cloud.google.com/docs/security/deletion
[8] Microsoft, Data-bearing device destruction. 2024. https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-bearing-device-destruction

Disclaimer of endorsement

Trademarks

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their 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.

Contact

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk:
NSA: 443-634-0721, MediaRelations@nsa.gov
CISA: 703-235-2010, CISAMedia@cisa.dhs.gov