Cloud Security Playbook Overview

December 18, 2024

The ***Cloud Security Playbook, Volumes 1 & 2*** describes the most important actions for Mission Owners to implement in order to secure their systems in a cloud. It includes numerous references to documents that provide details. Implementing all these plays will significantly enhance cybersecurity, reduce risk, and accelerate the Authorization to Operate (ATO) process. This document provides a brief overview of the *Cloud Security Playbook, Volumes 1 & 2*; more information can be found in those two documents.

Volume 1 Shared Responsibility

Cloud Service Providers (CSPs) are responsible for the physical security of their datacenters. They are also responsible for providing secure services. But cybersecurity in a cloud is a shared responsibility between the CSP and the Mission Owner (MO). For example, the MO is responsible for properly configuring the cloud services that their systems use, including enabling encryption and logging. The MO is also responsible for the cybersecurity of any software they host in the cloud.

Individuals and organizations across the country rely on cloud services every day, and the security of this technology has never been more important. Nation-state actors continue to grow more sophisticated in their ability to compromise cloud service systems.

Secretary of Homeland Security, April 2024

U.S. Department of Defense

Cloud Security Playbook Overview

Prepare the Organization

Implement cloud governance, including cloud cost management. Create a Cloud Migration Strategy and a Cloud Exit Strategy.

Select an Appropriate Cloud

Select a cloud with the Proper Impact Level (IL) and a DoD Provisional Authorization (PA).

Establish Secure Network Access

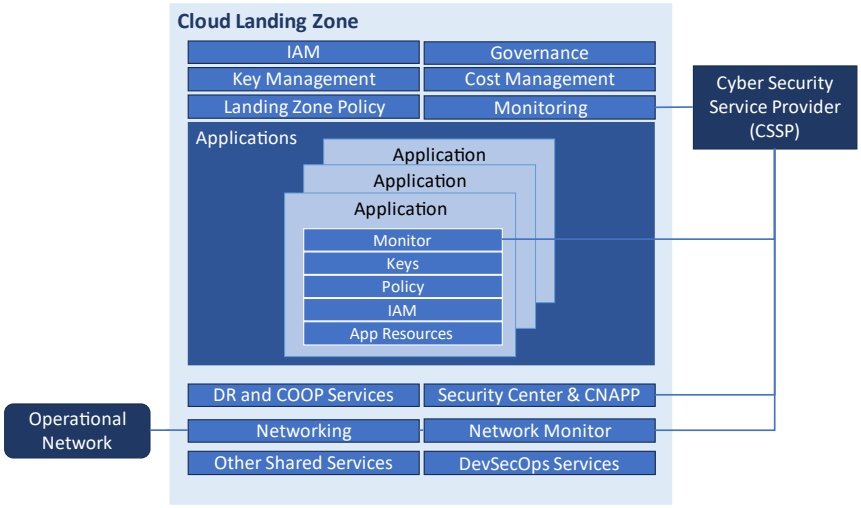
Cloud services for IL 4/5 must connect through the DISN Enterprise CAP or through a Component CAP approved by the DoD CIO. Register with the System Network Approval Process (SNAP).

Deploy with Infrastructure as Code

Infrastructure as Code (IaC) files are human and machine-readable text files that specify the intended state of the service they are instantiating. All the service parameters are set in these files, which are placed under version control and treated as immutable artifacts. Start with the DoD Cloud IaC templates.

Implement Secure Identity, Credential and Access Management (ICAM)

Implement the Principle of Least Privilege (PoLP).



Select or create an ICAM Solution in accordance with Department of Defense Instruction (DoDI) 8520.03, *Identity Authentication for Information Systems*.

Define or Identify a Cloud Landing Zone

Create a cloud landing zone. Integrate a Cybersecurity Service Provider (CSSP) and provide it with access to cloud monitoring capabilities. Create a Disaster Recovery (DR) plan and a Continuity of Operations (COOP) plan and test them.

Use a Cloud-Native Application Protection Platform (CNAPP)

A CNAPP is an integrated set of security and compliance capabilities to secure and protect cloud-native applications across development and production. Do not confuse a CNAPP with a Cloud Native Access Point (CNAP).

Implement Policy as Code (PaC)

Define policies in a machine-readable format and implement PaC. In tandem, enable automation that uses these policies to check for compliance. Also implement Configuration as Code.

Set up Logging and Manage the Logs

Defending applications hosted in a cloud requires creating and maintaining good logs with the proper level of detail to enable cyber defense. The logs must be protected so that malicious actors cannot alter the logs, even when they act as system administrators.

To manage logs, use Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), or Extended Detection and Response (XDR) tools.

Employ Defensive Cyberspace Operations (DCO)

Engage a DoD-approved CSSP. Establish and document which organization is responsible for which parts of incident detection and response. Ensure that all CSP-logged data is available to the CSSP. Perform Penetration Testing. Set up Intrusion Detection. Use Defensive Cybersecurity Artificial Intelligence (AI) tools.

Encrypt Data at Rest and in Transit

Enable encryption-in-transit. Enable encryption-at-rest. Enable encryption in IaC templates. Use approved CSP-provided encryption and Key Management Service (KMS). Use approved encryption algorithms.

Use Secure Cloud Secrets Management Practices

Manage secrets (e.g., keys) both for person entities (PEs) and non-person entities (NPEs). Use CSP tools to manage secrets.

Deploy User and Entity Behavior Analytics

Deploy User and Entity Behavior Analytics (UEBA) to detect anomalous behavior. This is typically implemented with a tool provided by the CSP. The CSSP should monitor the resulting analytics.

Apply Network Segmentation

Implement macro-segmentation to establish a secure cloud perimeter. Configure separate virtual private cloud (VPC) or virtual network (VNet) instances to isolate mission critical systems that are hosted in a cloud. Implement micro segmentation to further isolate cloud workloads by function. Implement out-of-band networks to separate data and control planes, enabling management of cloud workloads through approved connections.

Implement Cyber Resiliency

Create a cyber resilience plan. Enable automatic scaling for the software system. Deploy immutable artifacts. Set up automated backups. Restrict write-access to backups. Provision separate backup management accounts for administrators who require access to the backups. Implement a DR plan and test it. Enable COOP and test it.

Account for Complexities of Hybrid Cloud and Multi-Cloud Environments

Use IaC to deploy infrastructure resources from a centralized location. Use a centralized solution to aggregate logs and facilitate active monitoring and threat hunting.

Volume 2

Move Towards Zero Trust (ZT)

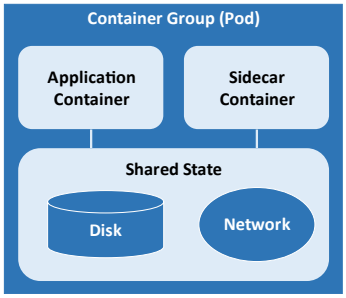
Implement ZT for the mission application. Consider CSP-provided ZT solutions.

Mitigate Third Party Risk

Secure the Software Supply Chain. Enable automatic creation of a Software Bill of Materials (SBOM) for software produced. Perform Software Composition Analysis (SCA) to help mitigate risk to the software supply chain. Consider using a DoD software factory with a Continuous Authorization to Operate (cATO), which incorporates tools to help secure the software supply chain.

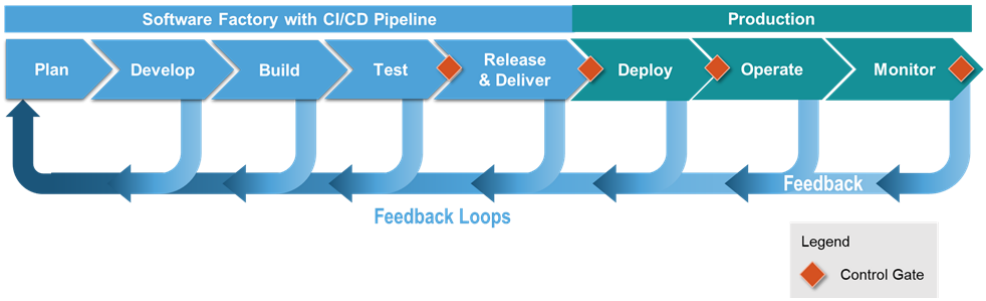
Cloud Security Playbook Overview

Secure Containers and Microservices



Package software in the form of containers. All containers must be Open Container Initiative (OCI) compliant. Scan containers for cybersecurity issues. Harden containers to improve cybersecurity. Use immutable containers. Create an artifact repository for hardened containers and their assessments. Ensure that only vetted, tested, validated, and digitally signed images are allowed to be uploaded to the registry. Implement the use of CNCF Kubernetes to orchestrate and manage containers. Use or create a sidecar security container or use an ambient mesh. Use Kubernetes to deploy the sidecar security container with each container it deploys.

Defend DevSecOps Pipelines



DevSecOps pipelines produce multiple applications and services, so they are prime targets for Malicious Cyber Actors (MCAs). Use a zero-trust approach. Assume no user, endpoint device or process is fully trusted. Minimize use of long-term credentials. To authenticate people, use identity federation and phishing-resistant security tokens to obtain temporary keys. Implement secure code signing to establish trust within the pipeline. Use two-person rules for code, at least one other developer must approve code before it can be promoted to the main branch. Implement least-privilege policies for access to the pipeline. Integrate security testing into the pipeline. Keep audit logs. Use a DoD software factory with a Continuous Authorization to Operate (cATO).

Secure Artificial Intelligence (AI) Systems

Manage deployment environment governance. Validate the AI system before and during use. Secure exposed APIs. Actively monitor model behavior. Protect model weights.

Secure Application Programming Interfaces (APIs)

Enable an API gateway to help manage and secure APIs.

Developing software using DevSecOps and a DoD Software Factory with a cATO both improves cybersecurity and achieves rapid authorization

---

Download the full *Cloud Security Playbook, Volumes 1 & 2* from the DoD CIO Library