Logical Separation

An evaluation of the U.S. Department of Defense Cloud Security Requirements for Sensitive Workloads

May 2018

[AWS Government Handbook Series]

Notices

This document is provided for informational purposes only. It represents AWS' current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Purpose

This paper examines the logical separation security equivalence for customers using Amazon Web Services (AWS) Infrastructure as a Service (IaaS) to meet the separation requirements set forth in the Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG). The paper discusses a three-pronged approach — leveraging virtualization, encryption, and deploying compute to dedicated hardware — that governments worldwide can leverage to confidently migrate sensitive (*e.g.*, high impact) unclassified workloads to the cloud without the need for a physically-dedicated infrastructure.

Introduction

Cloud technology takes advantage of transformative techniques in information technology (IT). Customers leveraging the cloud can benefit from a data center and network architecture built to meet the most security-sensitive organizations in the world. New operational models and new abstractions provided by cloud technologies contribute to creating a more secure IT environment. Cloud Service Providers (CSPs) like AWS use the cloud to innovate, delivering customers new and enhanced security features. AWS provides readily available services and supports both "defense-in-depth" and "defense-in-breadth" capabilities with security mechanisms intrinsic to cloud service designs and operations.

AWS gives customers ownership and control over their content by design through tools that allow customers to determine where their content will be stored. AWS features provide customers the ability to secure their content in transit and at rest, and to manage access to AWS services and resources for their users. AWS customers maintain full control over access to their content which prevents unauthorized users and customers from accessing other customer accounts. AWS provides multi-tenant services with industry-best tenant separation security. This logical separation between customer environments provided by AWS provides more effective and more reliable security as that of dedicated physical infrastructure.

Background

In December 2011, the U.S. Federal Chief Information Officer established a government-wide policy mandating federal agencies to use the Federal Risk and Authorization Management Program (FedRAMP) — a standardized, federal-wide program for the security authorization of cloud services. FedRAMP's "do once, use many times" approach was designed to offer significant benefits, such as increasing consistency and reliability in the evaluation of security controls, reducing costs for service providers and agency customers, and streamlining duplicative authorization assessments across agencies acquiring the same service. The primary governance and decision-making body for FedRAMP is the Joint Authorization Board (JAB), which consists of the Chief Information Officers (CIOs) of the General Services Administration, Department of Homeland Security, and DoD.

FedRAMP currently has three standardized security baselines — Low, Moderate, and High impact — based on Federal Information Processing Standards Publication (FIPS) 199 categorizations. These baselines were developed through the collaboration of cybersecurity experts across private industry and the U.S. Government (including the DoD). While the DoD has established reciprocity with the FedRAMP Moderate baseline, it has not established reciprocity with the FedRAMP High baseline. Instead, the DoD has developed and implemented what is effectively a "FedRAMP plus" set of security controls and requirements via the DoD Cloud Computing Security Requirements Guide (SRG).

In particular, DoD through the SRG requires separation between DoD and Federal government tenants/ missions either via physical or logical means. More specifically, the SRG provides that "CSPs must provide

evidence of strong virtual separation controls and monitoring, and the ability to meet 'search and seizure' requests without the release of DoD information and data." Even further, for Impact Level 5 systems (IL5),[1] DoD requires "physical separation (e.g. dedicated infrastructure) from non-DoD/non-Federal Government tenants." These DoD requirements are focused on DoD concerns regarding the co-mingling of DoD data with other tenant data from data leakage or spillage and the unauthorized access or tampering of DoD data by a non-DoD tenant.

To implement an outcome-focused best practice, the SRG acknowledged the use of logical separation as a viable approach to meet DoD IL5 separation requirements:

> *"A CSP may offer alternate solutions that provide equivalent security to the stated requirements. Approval will be assessed on a case by case basis during the PA [provisional authorization] assessment process."*

---

1 5.2.2.2 Impact Level 5 Location and Separation Requirements

Information that must be processed and stored at Impact Level 5 can only be processed in a dedicated infrastructure, on-premises or off-premises in any cloud deployment model that restricts the physical location of the information as described in section 5.2.1, "Jurisdiction/ Location Requirements." This excludes public service offerings.

The following applies:

- Only DoD private, DoD community or Federal Government community clouds are eligible for Impact Level 5.
- Each deployment model may support multiple missions or tenants / missions from each customer organization.
- Virtual/logical separation between DoD and Federal Government tenants / missions is permitted.
- Virtual/logical separation between tenant/mission systems is minimally required.
- Physical separation (e.g. Dedicated Infrastructure) from non-DoD/non-Federal Government tenants is required.

NOTE: A CSP may offer alternate solutions that provide equivalent security to the stated requirements. Approval will be assessed on a case by case basis during the PA assessment process.

https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

What are the shortcomings of physical separation requirements?

Requirements of physically dedicated cloud offerings are primarily driven by concerns about third-party or other unauthorized access to applications, content or data, including compelled law enforcement access and unauthorized third party access. However, for systems that are accessible over a network or the Internet, physical separation of those systems, such as placing them in a locked cage or a separate data center facility, does not provide added security or control over access. Simply put, all access controls for connected systems is managed via logical access controls, permission management, network traffic routing and encryption. AWS addresses any physical separation concerns through the logical security capabilities we provide to all of our customers and the security controls we have in place to protect customer data, described further in the three-pronged logical separation approach below.

Smaller, physically separated environments don't have parity with generally-available cloud environments; hence any physical separation requirement can limit or delay a customer's ability to leverage innovative investments (including security feature innovations) made on behalf of all customers using AWS services. Disadvantages also include higher cost structure and lower utilization resulting from less efficient use of space as well as limited redundancy options and features compared with the geo-diversity of commercial data center regions.

How is logical separation more effective than physical separation?

Customers can leverage the three-pronged approach below to successfully meet the security outcomes equivalent to physical separation, as required for DoD IL5.

1. Virtual Private Cloud (VPC) — Sufficient demonstration that VPC creates the equivalent of completely separate network domains for each tenant;
2. Encrypting data at-rest and in-transit — Leveraging either user-provided or intrinsic data encryption capabilities of AWS cloud services such as EBS, S3, and DynamoDB, with encryption keys generated and stored by AWS Key Management Service (KMS) and/or AWS Cloud Hardware Security Module (CloudHSM); and
3. Dedicated Hosts, Dedicated Instances, and Bare Metal — DoD mission owners can provision entire AWS physical hosts to process both hypervised and non-hypervised machine instances they assign and the associated workloads.

1. Virtual Private Cloud (VPC)

AWS VPC enables the creation of a logically separate network enclave within the AWS Elastic Cloud Compute (Amazon EC2) network that can house compute and storage resources. This environment can be connected to a customer's existing infrastructure through a virtual private network (VPN) connection over the Internet, or through AWS Direct Connect, a service that provide private connectivity into the AWS cloud. Use of a VPC provides mission owners with flexibility, security, and complete control of their network presence in the cloud. It allows a controlled transition to the cloud using a customer's existing data center model and management scheme. The customer controls the private environment including IP addresses, subnets, network access control lists, security groups, operating system firewalls, route tables, VPNs, and/or Internet gateways. Amazon VPC provides robust logical isolation of all customer resources. For example, every packet flow on the network is individually authorized to validate the correct source and destination before it is transmitted and delivered. It is not possible for information to pass between multiple tenants without specifically being authorized by both the transmitting and receiving customers. If a packet is being routed to a destination without a rule that matches it, the packet is dropped. Moreover, while Address Resolution Protocol (ARP) packets trigger an authenticated database look-up, ARP packets never hit the network as they are not needed for discovery of the virtual network topology, so ARP spoofing is impossible. Also, promiscuous mode does not reveal any traffic other than that bound to and from the customer operating system. These precise sets of rules for traffic ingress and egress set by the customer not only allow for increased connectivity flexibility, but enable more customer control over traffic segmentation and routing.

For instance, VPC[2] connectivity options include the ability for the customer to:

- Connect to the Internet using Network Address Translation (private subnets) — Private subnets can be used for instances that should not have direct access to or from the Internet. Instances in a private subnet can access the Internet without exposing their private IP address by routing their traffic through a Network Address Translation (NAT) gateway in a public subnet.
- Connect securely to your corporate datacenter — All traffic to and from instances in your VPC can be routed to your corporate datacenter over an industry standard, encrypted IPsec hardware VPN connection.
- Connect privately to other VPCs — Peer VPCs together to share resources across multiple virtual networks owned by your AWS accounts.
- Privately connect your internal services across different accounts and VPCs within your own organizations, significantly simplifying your internal network architecture.

---

2 Note: The use of VPC with a private gateway to an approved Cloud Access Point (CAP) or DoD Secure Cloud Computing Architecture (SCCA) solution is mandatory for all customers using SRG IL5 workloads in the AWS US GovCloud Region unless waived for special circumstances by the DoD CIO.

2. Encrypting data at-rest and in-transit

For data that mission owners are storing on AWS storage services or transiting on our networks, we strongly recommend encryption for data-at-rest and in-transit. In order to make it easy and secure for our customers, we provide a number of tools and features that allow them to encrypt data as well as several encryption key management infrastructure options. These encryption and data access control features are already built into foundational service offerings such as Amazon Simple Storage Service (Amazon S3), a highly scalable object storage service, Amazon Elastic Block Store (Amazon EBS), which provides network-attached storage to EC2 instances, and Amazon Relational Database Service (Amazon RDS), which provides managed database engines. These features are turn-key and provide a wealth of documentation to help customers understand how their data is being protected and the configuration options they can control to customize who can access the systems. AWS's native services have evolving security capabilities that, in legacy environments, were only achievable through an aggregation of third party vendors. Now these capabilities are increasingly available letting customers focus on service innovation.

The combination of AWS Key Management Service (KMS) and AWS CloudHSM are the centerpiece of a rigorous encryption solution. AWS KMS is a fully managed, highly available regional service using FIPS 140-2 Level 3 validated (physical security) hardware security modules (HSMs)[3] at its base, with sophisticated scale-out software that can handle hundreds of thousands of API requests per second. It gives customers the ability to perform key management functions in a way that is deeply integrated with other AWS services. AWS CloudHSM provides a dedicated, FIPS 140-2 Level 3 (overall) HSM under your exclusive control, directly in your Amazon Virtual Private Cloud (VPC).[4] The CloudHSM service provides automated availability, replication, and backup of the dedicated, single-customer HSMs across availability zones. It integrates into customer-owned applications using industry-standard crypto APIs. Though applicable in different contexts, both services work to ensure that the encryption algorithm is sufficiently robust to render data unintelligible and the keys sufficiently protected so the ciphertext will be unreadable by unauthorized persons. In other words, the storage of appropriately encrypted data with properly managed and secured keys can provide assurance of fully protected data. This approach is equally relevant, applicable, and effective regardless of whether it is deployed in a physically isolated or a logically isolated commercial cloud environment.

With encryption, the confidentiality of mission owner cryptographic keys is crucial. Security depends upon where the data was encrypted and who has access to and is protecting the keys. If the data is encrypted by the mission owner prior to being ingested into the cloud, there is no reason for the CSP to have access to the keys — the mission owner has full control and responsibility. On the other hand, if the data is encrypted using services that are native to the CSP, then both the CSP and the data owner would be in the chain of custody of the keys. AWS KMS is designed so that no one, including AWS employees, can retrieve your plaintext keys from the service. The service uses FIPS 140-2 validated HSMs to protect the confidentiality and integrity of your keys regardless of whether you request KMS to create keys on your behalf or you

3 https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3139

4 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/3108

import them into the service. Your plaintext keys are never written to disk and only ever used in volatile memory of the HSMs for the time needed to perform your requested cryptographic operation. KMS keys are never transmitted outside of the AWS regions in which they were created. Updates to the KMS HSM firmware is controlled by quorum-based access control that is audited and reviewed by an independent group within Amazon. These policies, processes and procedures have been independently audited and accredited under FedRAMP and by the DoD. The section below summarizes the capabilities of AWS KMS and AWS CloudHSM. Customers can refer to the embedded links for additional resources on AWS KMS and AWS CloudHSM.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) provides customers with centralized control over the encryption keys used to protect their data. Using AWS KMS, customers can create, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt customer data. AWS KMS is integrated with AWS services making it easy to encrypt data stored in these services with encryption keys that a customer manages (or via default encryption keys that an AWS service manages on behalf of the customer). This service is included along with five core services that were accredited to meet DoD IL5 requirements for enabling encryption of data at rest and in transit and provides a sufficient logical separation of DoD data transiting the AWS infrastructure and co-located on hardware with non-DoD customer data. For example, in the case of data at rest, the use of strong cryptographic algorithms for logical separation of customer data is the basis for establishing equivalency to physical separation of data at rest - a requirement of IL5.

The inner security boundary of AWS KMS is the Hardened Security Module (HSM). The HSM has a limited internal web-based API and no other active physical interfaces in its operational state. An operational HSM is configured and loaded with the appropriate cryptographic keys during initialization. Sensitive cryptographic materials of the HSM are only stored in volatile memory, and erased when the HSM moves out of the operational state, including intended or unintended shutdowns or resets. When in the operational state, no human operators can access the HSM. Only service hosts handling customer requests may make connections via the limited API. The HSM APIs are available over a mutually authenticated confidential session established by human operators (when not operational) or service hosts (when operational).

The system is designed so that multiple human operators using two-factor authentication are required via a quorum-based process to update firmware or software configuration on any KMS HSM but even then only after it is placed in a non-operational state and contains no key material.

> **Note:** AWS Key Management Service (KMS) now uses FIPS 140-2 validated hardware security modules (HSM) and supports FIPS 140-2 validated endpoints, which provide independent assurances about the confidentiality and integrity of your keys.

AWS Cloud HSM

AWS CloudHSM offers effective hardware key management at cloud scale for sensitive and regulated workloads. CloudHSM allows mission owners to provision and leverage cryptographic keys to encrypt their data within the AWS services and their resident applications. With CloudHSM, customers manage their own encryption keys using a FIPS 140-2 Level 3 validated HSM, and affords the flexibility of integrating with their applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries. It is also standards-compliant and enables mission owners to export all keys to most other commercially-available HSMs. CloudHSM is a managed service that automates time-consuming administrative tasks, such as hardware provisioning, software patching, high-availability, and backups. To protect and isolate your CloudHSM from other Amazon customers, CloudHSM must be provisioned inside a VPC.

Separation of duties and role-based access control is inherent in the design of CloudHSM. AWS has a limited access to the HSM that permits us to monitor and maintain the health and availability of the HSM, take encrypted backups, and to extract and publish audit logs to your CloudWatch Logs. AWS is unable to see, access or use your keys, or cause your HSM to perform any cryptographic operation using your keys.

3. Dedicated Hosts, Dedicated Instances, and Bare Metal

In addition to providing highly secure, logically isolated, multi-tenant compute services, AWS also provides three means of deploying compute to dedicated hardware using Dedicated Instances, Dedicated Hosts, and Bare Metal. These deployment options can be used to launch Amazon EC2 instances onto physical servers that are dedicated for your use. Dedicated Instances are hypervised Amazon EC2 instances that run in a virtual private cloud (VPC) on hardware that's dedicated to a single customer. Dedicated Instances are physically isolated at the host hardware level from instances that belong to other AWS accounts. Dedicated Instances may share hardware with other instances from the same AWS account that are not Dedicated Instances. A Dedicated Host is also a physical server that's dedicated for your use. With a Dedicated Host, you have visibility and control over how hypervised instances are placed on the server. Bare metal instances are non-hypervised host hardware devices. Using the AWS Nitro technology for network and storage offload, as well as the Nitro security chip to eliminate the risks associated with serial single-tenancy on bare metal, customers have direct access to Amazon EC2 hardware. These bare metal instances are full-fledged members of the Amazon EC2 service and have access to services such as Amazon VPC and Amazon Elastic Block Store (EBS).[5]

5 Currently, Amazon EC2 Bare Metal can be experienced on the I3 instance family in the form of the i3.metal instance type.

There are no performance, security, or physical differences between Dedicated Instances and instances deployed on Dedicated Hosts. However, Dedicated Hosts give mission owners additional control over how instances are placed on a physical server and how that server is utilized. When you use Dedicated Hosts, you have control over instance placement on the host using the Host Affinity and Instance Auto-placement settings. If your organization wants to use AWS, and has an existing software license that requires that the software be run on a particular piece of hardware for some minimum amount of time. Dedicated Hosts allow visibility into the host's hardware, enabling you to meet those licensing requirements.

How does multi-tenant cloud support law enforcement requests for data without releasing DoD data?

AWS complies with legal law enforcement requests for data. While on-premises systems typically allow authorities to directly seize or access physical hardware from the data owner, cloud computing introduces a different model since the data is hosted in a multi-tenant environment. Physically seizing or accessing physical hardware in AWS is not possible since data for one customer is spread across different physical devices, forcing all requests for data to go through an approved and authorized logical retrieval process. Through our FedRAMP accreditation, AWS complies with NIST 800-53's controls comprising the FedRAMP Moderate baseline, including "Information Handling and Retention" and "System and Information Integrity" security controls. This means, among other things, that the AWS services delineate between the boundaries of different customer accounts, prevent against any cross-mingling of customer accounts, and result in customers having full control over the contents and operations of their individual AWS accounts. DoD customers, like all customers, can rest-assured that any lawful law enforcement request will apply only to data within the account of a customer subject to the request. We also comply with, "System and Information Integrity" controls, which require that compliant CSPs provide customers access to their data and mandates that compliant agencies maintain their own data consistent with applicable laws. Additionally, "Audit and Accountability" controls require organizations to retain audit records to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Customers can retrieve cloud audit logs and reports by leveraging CloudTrail and CloudWatch Logs, which they can then provide to the appropriate authorities. These solutions enable DoD to respond directly to inspector general or law enforcement requests for information, enabling government officials to have direct access to information that they might require without seizing hardware.

AWS also applies strong policies and controls around sanitization and destruction. For instance, AWS tracks, documents, and verifies media sanitization and disposal actions. At no time does a customer have physical access to the media mapped to their logical volume or object. All media removal and disposal is performed by designated AWS personnel. Content on drives is treated at the highest level of classification pursuant to AWS's data classification policy. All media is rendered unreadable and destroyed at the end of the media lifecycle prior to leaving an AWS datacenter room in accordance with AWS's security standards as part of the decommissioning process.

How does multi-tenant cloud protect against unauthorized third party access, including CSP employee access, to DoD data?

A related concern to the breadth of law enforcement's ability to lawfully request customer data is the potential for unauthorized third party access to customer content and the adequacy of access control measures to prevent unauthorized access by CSP personnel. We do not access or use customer content for any purpose other than as legally required and for maintaining the AWS services and providing them to our customers and their end users.

Employee access to AWS systems are allocated based on least privilege, approved by an authorized individual prior to access provisioning, and supervised by an AWS employee. Duties and areas of responsibility (for example, access request and approval, change management request and approval, etc.) must be segregated across different individuals to reduce opportunities for an unauthorized or unintentional modification or misuse of AWS systems. AWS personnel with a business need to access the management plane are required to first use multi-factor authentication, distinct from their normal corporate Amazon credentials, to gain access to purpose-built administrative hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked. AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.

Customers manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (such as AWS CloudTrail, CloudWatch, CloudHSM, and AWS KMS as described above).

What are AWS' recommendations to governments considering physical separation requirements?

Through DoD's cloud computing SRG authorization process, AWS demonstrated the sufficiency of logical separation to meet the intent behind a request for dedicated, physically isolated infrastructure for DoD's most sensitive unclassified workloads. Our approach confirms that multi-tenant logically separated environments that meet robust security controls can provide a level of security superior to dedicated private cloud deployments, while providing significant advantages in availability, scalability, and lower cost. Modern cloud technology from established providers offers novel solutions that can meet the objective of traditional technology security as long as accreditation approaches are flexible enough to accommodate alternative implementations.

While reviewing security controls can be valuable for demonstrating compliance, our experience has shown that organizations that focus primarily (and in some instances exclusively) on traditional controls implementation can inadvertently limit their access to best-in-class security solutions. As governments evaluate whether CSPs meet requirements based on legacy concepts, they should clearly articulate the desired security outcome and allow CSPs to develop the optimal techniques for meeting (if not exceeding) those outcomes. Focusing on the desired security objective behind a specific requirement can help federal agencies rightly focus on outcomes they want to achieve rather than implementation details.

As security assurance programs mature and scale to keep up with the rapid pace of cloud feature and security innovation, control implementation details will become increasingly irrelevant relative to the capabilities CSPs have in place. The desired end-state – robust cloud security, based on a framework defined by customer security outcomes and CSP-determined security techniques to meet those outcomes – can only come about as a result of continuous dialogue across the cloud assurance stakeholder community. We believe this approach would provide significant improvements in maintaining assurance of a CSP's security posture.

In addition to providing a logically-equivalent alternative solution, AWS utilized an end-to-end approach and engaged in deep dive sessions to fully address DoD's top of mind security concerns. Beginning with the customer's needs manifested in the DoD Cloud Computing SRG, AWS held several knowledge sessions to educate DoD on how our three-pronged approach met the intent of the physical separation requirement. The third party assessor that validated our services also participated in these sessions to attest to the accuracy of our assertions and offer their risk-based assessment. These collaborative sessions served as a valuable and efficient means to ensure security assurance, accelerate accreditation, and ultimately, advance DoD's IT modernization goals.

We are encouraged by the DoD's evolution towards accepting innovative, cloud-adaptive solutions to achieve the intent behind physical separation requirements in the cloud. We are committed to ongoing collaboration with governments worldwide that are evaluating the merits and best practices from DoD's logical separation equivalency approach.