

Introduction to AWS Security

January 2020



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

- Security of the AWS Infrastructure..... 1
- Security Products and Features.....2
 - Infrastructure Security2
 - Inventory and Configuration Management2
 - Data Encryption.....3
 - Identity and Access Control3
 - Monitoring and Logging4
 - Security Products in AWS Marketplace.....4
- Security Guidance4
- Compliance6
- Further Reading.....7
- Document Revisions.....8

Abstract

Amazon Web Services (AWS) delivers a scalable cloud computing platform designed for high availability and dependability, providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is of the utmost importance to AWS, as is maintaining your trust and confidence. This document is intended to provide an introduction to AWS's approach to security, including the controls in the AWS environment and some of the products and features that AWS makes available to customers to meet your security objectives.

Security of the AWS Infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. AWS ensures that these controls are replicated in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient infrastructure, designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads you deploy in AWS (*Figure 1*). This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public.

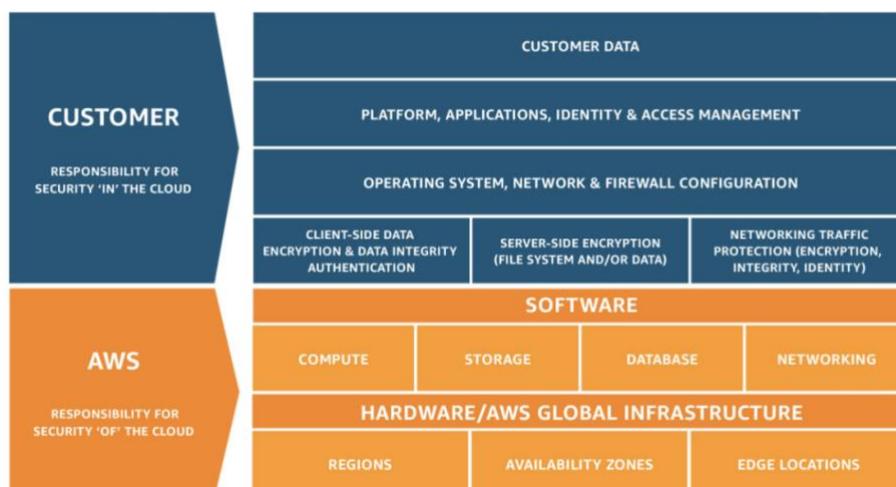


Figure 1: AWS Shared Security Responsibility Model

Security Products and Features

AWS and its partners offer a wide range of tools and features to help you to meet your security objectives. These tools mirror the familiar controls you deploy within your on-premises environments. AWS provides security-specific tools and features across network security, configuration management, access control and data security. In addition, AWS provides monitoring and logging tools to can provide full visibility into what is happening in your environment.

Infrastructure Security

AWS provides several security capabilities and services to increase privacy and control network access. These include:

- Network firewalls built into Amazon VPC let you create private networks and control access to your instances or applications. Customers can control encryption in transit with TLS across AWS services.
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment.
- DDoS mitigation technologies that apply at layer 3 or 4 as well as layer 7. These can be applied as part of application and content delivery strategies.
- Automatic encryption of all traffic on the AWS global and regional networks between AWS secured facilities.

Inventory and Configuration Management

AWS offers a range of tools to allow you to move fast, while still enabling you to ensure that your cloud resources comply with organizational standards and best practices. These include:

- Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards.
- Inventory and configuration management tools to identify AWS resources and then track and manage changes to those resources over time.
- Template definition and management tools to create standard, preconfigured, hardened virtual machines for EC2 instances.

Data Encryption

AWS offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data at rest encryption capabilities available in most AWS services, such as Amazon EBS, Amazon S3, Amazon RDS, Amazon Redshift, Amazon ElastiCache, AWS Lambda, and Amazon SageMaker
- Flexible key management options, including AWS Key Management Service, that allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your own keys
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to help satisfy your compliance requirements
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

Identity and Access Control

AWS offers you capabilities to define, enforce, and manage user access policies across AWS services. These include:

- [AWS Identity and Access Management \(IAM\)](#) lets you define individual user accounts with permissions across AWS resources AWS Multi-Factor Authentication for privileged accounts, including options for software- and hardware-based authenticators. IAM can be used to grant your employees and applications [federated access](#) to the AWS Management Console and AWS service APIs, using your existing identity systems, such as Microsoft Active Directory or other partner offering.
- [AWS Directory Service](#) allows you to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience.
- [AWS Single Sign-On \(AWS SSO\)](#) allows you to manage SSO access and user permissions to all of your accounts in AWS Organizations, centrally.

AWS provides native identity and access management integration across many of its services, plus API integration with any of your own applications or services.

Monitoring and Logging

AWS provides tools and features that enable you to see what's happening in your AWS environment. These include:

- With [AWS CloudTrail](#), you can monitor your AWS deployments in the cloud by getting a history of AWS API calls for your account, including API calls made via the AWS Management Console, the AWS SDKs, the command line tools, and higher-level AWS services. You can also identify which users and accounts called AWS APIs for services that support CloudTrail, the source IP address the calls were made from, and when the calls occurred.
- [Amazon CloudWatch](#) provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.
- [Amazon GuardDuty](#) is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Amazon GuardDuty exposes notifications via Amazon CloudWatch so you can trigger an automated response or notify a human.

These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment.

Security Products in AWS Marketplace

Moving production workloads to AWS can enable organizations to improve agility, scalability, innovation, and cost savings — while maintaining a secure environment. [AWS Marketplace](#) offers security industry-leading products that are equivalent, identical to, or integrate with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

Security Guidance

AWS provides customers with guidance and expertise through online tools, resources, support, and professional services provided by AWS and its partners.

AWS Trusted Advisor is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.

AWS Account Teams provide a first point of contact, guiding you through your deployment and implementation, and pointing you toward the right resources to resolve security issues you may encounter.

AWS Enterprise Support provides 15-minute response time and is available 24x7 by phone, chat, or email; along with a dedicated Technical Account Manager. This concierge service ensures that customers' issues are addressed as swiftly as possible.

AWS Partner Network offers [hundreds of industry-leading products](#) that are equivalent, identical to, or integrated with existing controls in your on-premises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.

AWS Professional Services houses a Security, Risk and Compliance specialty practice to help you develop confidence and technical capability when migrating your most sensitive workloads to the AWS Cloud. [AWS Professional Services](#) helps customers develop security policies and practices based on well-proven designs, and helps ensure that customers' security design meets internal and external compliance requirements.

AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it easy to find, test, buy, and deploy software that runs on AWS. [AWS Marketplace Security products](#) complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

AWS Security Bulletins provides [security bulletins](#) around current vulnerabilities and threats, and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing. We also have online resources for [vulnerability reporting](#).

AWS Security Documentation [shows how to configure AWS services](#) to meet your security and compliance objectives. AWS customers benefit from a data center and

network architecture that are built to meet the requirements of the most security-sensitive organizations.

AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. The [AWS Well-Architected Framework](#) includes a security pillar that focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. Customers can use the Well Architected service from the console or engage the services of one of the APN partners to assist them.

AWS Well Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. This free tool is available in the AWS Management Console, and after answering a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization. The [AWS Well-Architected Tool](#) then provides a plan on how to architect for the cloud using established best practices.

Compliance

AWS Compliance empowers customers to understand the robust controls in place at AWS to maintain security and data protection in the AWS Cloud. When systems are built in the AWS Cloud, AWS and customers share compliance responsibilities. AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 9001 / ISO 27001, FedRAMP, DoD SRG, and PCI DSS Level 1.i Additionally, AWS also has assurance programs that provide templates and control mappings to help customers establish the compliance of their environments running on AWS, for a full list of programs, see [AWS Compliance Programs](#).

We can confirm that all AWS services can be used in compliance with the GDPR. This means that, in addition to benefiting from all of the measures that AWS already takes to maintain services security, customers can deploy AWS services as a part of their GDPR compliance plans. AWS offers a GDPR-compliant Data Processing Addendum (GDPR DPA), enabling you to comply with GDPR contractual obligations. The AWS GDPR DPA is incorporated into the AWS Service Terms and applies automatically to all customers globally who require it to comply with the GDPR. Amazon.com, Inc. is certified under the EU-US Privacy Shield and AWS is covered under this certification. This helps

customers who choose to transfer personal data to the US to meet their data protection obligations. Amazon.com Inc.'s certification can be found on the EU-US Privacy Shield website: <https://www.privacyshield.gov/list>

By operating in an accredited environment, customers reduce the scope and cost of audits they need to perform. AWS continuously undergoes assessments of its underlying infrastructure—including the physical and environmental security of its hardware and data centers—so customers can take advantage of those certifications and simply inherit those controls.

In a traditional data center, common compliance activities are often manual, periodic activities. These activities include verifying asset configurations and reporting on administrative activities. Moreover, the resulting reports are out of date before they are even published. Operating in an AWS environment allows customers to take advantage of embedded, automated tools like AWS Security Hub, AWS Config and AWS CloudTrail for validating compliance. These tools reduce the effort needed to perform audits, since these tasks become routine, ongoing, and automated. By spending less time on manual activities, you can help evolve the role of compliance in your company from one of a necessary administrative burden, to one that manages your risk and improves your security posture.

Further Reading

For additional information, see the following resources:

For information on ...	See
Key topics, research areas, and training opportunities for cloud security on AWS	AWS Cloud Security Learning
The AWS Cloud Adoption Framework which organizes guidance into six areas of focus: Business, People, Governance, Platform, Security, and Operations	AWS Cloud Adoption Framework
Specific controls in place at AWS; how to integrate AWS into your existing framework	Amazon Web Services: Risk and Compliance
Best practices guidance on how to deploy security controls within an AWS environment	AWS Security Best Practices

For information on ...	See
AWS Well-Architected Framework, security pillar	AWS Well-Architected Framework Security Pillar

Document Revisions

Date	Description
January 2020	Updated for latest services, resources, and technologies.
July 2015	First publication.
