



AWS Shared Responsibility Model

© 2025 Amazon Web Services, Inc. or its affiliates. All rights reserved.

DO NOT COPY
bufetekaye.22@gmail.com

What you will learn


At the core of the lesson

You will learn how to:

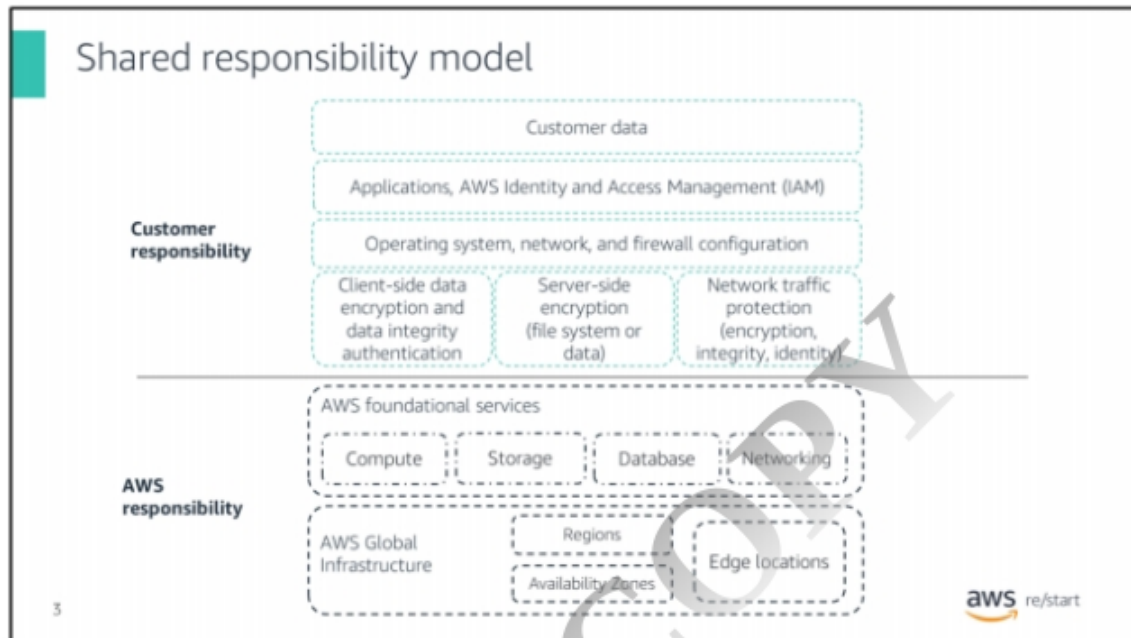
- Describe AWS Cloud security and the shared responsibility model
- Identify the security responsibilities of AWS versus the security responsibilities of the customer

2

aws re/start



This module provides an introduction to the AWS shared responsibility model.



Security is the highest priority at AWS. AWS delivers a scalable cloud computing environment that's designed for high availability and dependability, while 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 critical to AWS, and so is maintaining customer trust and confidence. This module provides an introduction to the AWS approach to security. You will learn about controls in the AWS environment, and some of the products and features that AWS offers to customers so that they can meet their security objectives.

AWS provides the same approach to security that companies have been using for decades, and also enables customers to take advantage of the flexibility and low cost of cloud computing. It's not inherently inconsistent to provide on-demand infrastructure while also providing the security isolation that companies expect in their existing, privately owned environments.

After the customer starts using AWS, Amazon shares the responsibility of securing the customer's data in the AWS Cloud with its customers, making AWS security a shared responsibility. This concept is known as the *shared responsibility model*.

Next, you will learn who is responsible for which aspects of security in the shared responsibility model.



AWS is responsible for security *of* the cloud. But what does that mean?

Under the shared responsibility model, AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities where the services operate. It means that AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud, which include AWS Regions, Availability Zones, and edge locations.

AWS handles the security of the physical infrastructure that hosts your resources, which include:

- **Physical security of data centers** with controlled, need-based access, located in nondescript facilities; 24/7 security guards; two-factor authentication; access logging and review; video surveillance; and disk degaussing and destruction.
- **Hardware infrastructure** including servers, storage devices, and other appliances that AWS services rely on.
- **Software infrastructure** that hosts operating systems, service applications, and virtualization software.
- **Network infrastructure** including routers, switches, load balancers, firewalls, and cabling. This includes nearly continuous network monitoring at external boundaries, secure access points, and redundant infrastructure with intrusion detection.
- **Virtualization** infrastructure including instance isolation.


Protecting this infrastructure is the number one priority for AWS. You can't visit AWS data centers or offices to experience this protection firsthand. However, Amazon provides several reports from third-party auditors who have verified AWS compliance with various computer security standards and regulations.

DO NOT COPY
bufetekaye.22@gmail.com

Customer security responsibilities: Security **IN** the cloud

Security in the cloud

- Amazon Elastic Compute Cloud (Amazon EC2) instance OS
 - Including patching, maintenance
- Applications
 - Passwords, role-based access, and others
- Security group configuration
- OS-based or host-based firewalls
 - Including intrusion detection or prevention systems
- Network configurations
- Account management
 - Login and permission settings for each user



The diagram illustrates the layers of customer responsibility in the cloud. It consists of several stacked boxes. The top box is labeled 'Customer data'. Below it is 'Applications, IAM'. The next box is 'OS, network, and firewall configuration'. Below this are three separate boxes: 'Client-side data encryption and data integrity authentication', 'Server-side encryption (file system or data)', and 'Network traffic protection (encryption, integrity, identity)'. A large arrow points from the top of the diagram down to the bottom, indicating the flow of responsibility. The AWS logo and 're/start' are at the bottom right.

5

Though the cloud infrastructure is secured and maintained by AWS, customers are responsible for security of everything they put in the cloud. The customer is responsible for what they implement by using AWS, and for the applications that connect to AWS. The security steps that a customer must take depend on the services that they use and the complexity of their system.

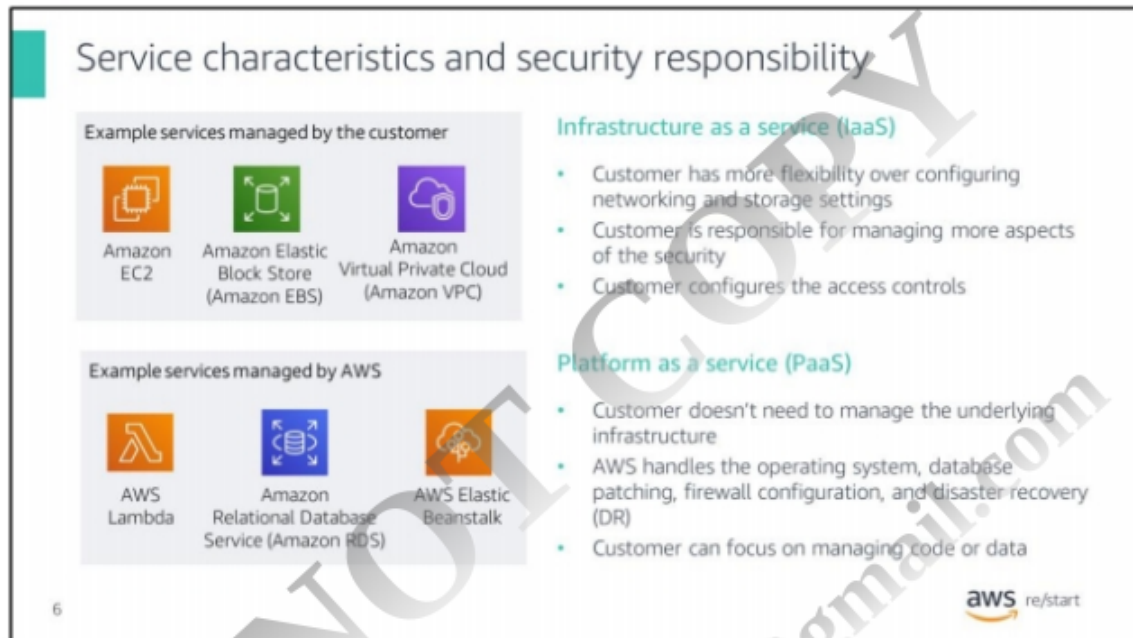
These steps selecting the instance OS; securing the application; configuring security groups and firewalls; and managing the network configuration and user accounts.

When customers use AWS services, they maintain complete control over their content. Customers are responsible for managing critical content security requirements, including:

- What content they choose to store on AWS
- Which AWS services are used with the content
- Which country that content is stored in
- The format and structure of that content and whether it's masked, anonymized, or encrypted
- Who has access to that content and how those access rights are granted, managed, and revoked

Customers retain control of the security that they choose to implement to protect their own data, environment, applications, AWS Identity and Access Management (IAM) settings, and operating systems. Thus, the shared responsibility model changes depending on the AWS services that the customer uses.

DO NOT COPY
bufetekaye.22@gmail.com



Infrastructure as a service (IaaS) refers to services that provide basic building blocks for cloud IT. These building block typically include network configuration, computers (virtual or on dedicated hardware), and data storage space. Cloud services that can be characterized as IaaS **provide the customer with the highest level of flexibility and management control** over IT resources. IaaS services are most similar to existing on-premises computing resources that many IT departments are familiar with.

AWS services—such as **Amazon EC2**—can be categorized as **IaaS**. Thus, **the customer must perform all necessary security configuration and management tasks**. Customers who deploy EC2 instances are responsible for managing the guest OS (including updates and security patches), any application software that's installed on the instances, and configuring the security groups that were provided by AWS.

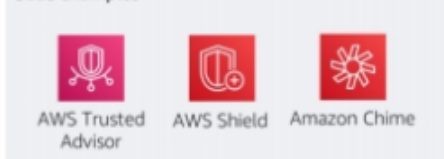
Platform as a service (PaaS) refers to services that reduce the customer's need to manage the underlying infrastructure (hardware, OS, and other resources). PaaS services enable the customer to focus on deploying and managing applications. Customers don't need to worry about resource procurement, capacity planning, software maintenance, or patching.

AWS services such as **AWS Lambda** and **Amazon RDS** can be categorized as **PaaS** because **AWS operates the infrastructure layer, the operating system, and platforms**. Customers only need to access the endpoints to store and retrieve data. With PaaS services, customers are responsible for managing their data, classifying their assets, and applying the appropriate permissions. However, these services act more like managed services, with AWS handling a larger portion of the security requirements. For these services, AWS handles basic security tasks—such as OS and database patching, firewall configuration, and disaster recovery (DR).

DO NOT COPY
bufetekaye.22@gmail.com

Service characteristics and security responsibility (continued)

SaaS examples



Software as a service (SaaS)

- Software is centrally hosted.
- Licensed on a subscription model or pay-as-you-go basis.
- Services are typically accessed through a web browser, mobile app, or application programming interface (API)
- Customers don't need to manage the infrastructure that supports the service

Software as a service (SaaS) refers to services that provide centrally hosted software that's typically accessible through a web browser, mobile app, or application programming interface (API). The licensing model for SaaS offerings is generally subscription or pay as you go. With SaaS offerings, customers don't need to manage the infrastructure that supports the service. Some AWS services—such as **AWS Trusted Advisor**, **AWS Shield**, and **Amazon Chime**—could be categorized as SaaS offerings, given their characteristics.

AWS Trusted Advisor is an online tool that analyzes your AWS environment and provides real-time guidance and recommendations to help you provision your resources by following AWS best practices. The Trusted Advisor service is offered as part of your AWS Support plan. Some of the Trusted Advisor features are free to all accounts, but Business Support and Enterprise Support customers have access to the full set of Trusted Advisor checks and recommendations.

AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards applications that run on AWS. It provides always-on detection and automatic inline mitigations that minimize application downtime and latency. Thus, customers don't need to engage AWS Support to benefit from DDoS protection. AWS Shield Advanced is available to all customers. However, to contact the DDoS Response Team, customers must have either Enterprise Support or Business Support from AWS Support.