AWS and AWS Partner Network (APN) Partners offer a wide range of tools and features to help you to meet your security objectives. These tools mirror the familiar controls that you deploy in your on-premises environments. AWS provides security-specific tools and features across network security, configuration management, access control, and data security.

To learn more, see: Security Products and Features

You can use AWS Identity and Access Management (IAM) to manage access to AWS services and resources securely. By using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.

To learn more, see:

Security best practices in IAM
What is IAM?

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a virtual private cloud (VPC), you can assign up to five security groups to the instance. Security groups act at the instance level, not the subnet level. Therefore, each instance in a subnet in your VPC can be assigned to a different set of security groups.

To learn more, see: Security groups for your VPC

A network access control list (network ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules that are similar to your security groups to add an additional layer of security to your VPC.

To learn more, see: Network ACLs

Your VPC has an implicit router, and you use route tables to control where network traffic is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table).

To learn more, see: Route tables for your VPC

Data at rest represents any data that you persist in non-volatile storage for any duration in your workload. This includes block storage, object storage, databases, archives, Internet of Things (IoT) devices, and any other storage medium where data is persisted. Protecting your data at rest reduces the risk of unauthorized access, when encryption and appropriate access controls are implemented.

To learn more, see: Protecting Data at Rest

Data in transit is any data that is sent from one system to another. This includes communication between resources within your workload, and communication between other services and your end users. By providing the appropriate level of protection for your data in transit, you protect the confidentiality and integrity of your workload's data.

To learn more, see: Protecting Data in Transit

AWS recommends encryption as an additional access control to complement the identity, resource, and network-oriented access controls that were already described. AWS provides a number of features that customers can use to encrypt data and manage keys. All AWS services offer the ability to encrypt data at rest and in transit. AWS Key Management Service (AWS KMS) integrates with the majority of AWS services. With AWS KMS, customers can control the lifecycle of and permissions on the keys that are used to encrypt data on their behalf.

To learn more, see: Encrypting Data-at-Rest and -in-Transit

Data classification provides a way to categorize organizational data based on criticality and sensitivity to help you determine appropriate protection and retention controls.

To learn more, see: Data Classification

AWS KMS keys can be divided into two general types: AWS managed and customer managed. An AWS managed key is created when you choose to enable server-side encryption of an AWS resource under the AWS managed key for that service for the first time. The AWS managed key is unique to your AWS account and the Region where it's used. An AWS managed key can only be used to protect resources within the specific AWS service for which it's created. It does not provide the level of granular control that a customer managed key provides.

Note: AWS KMS is replacing the term customer master key (CMK) with AWS KMS key and KMS key. The concept has not changed. Also, the AWS-managed CMK is now known as the AWS managed key, and the customer-managed CMK is now known as the customer managed key. The following documentation link uses the previous terminology.

To learn more, see: AWS-managed and Customer-managed CMKs