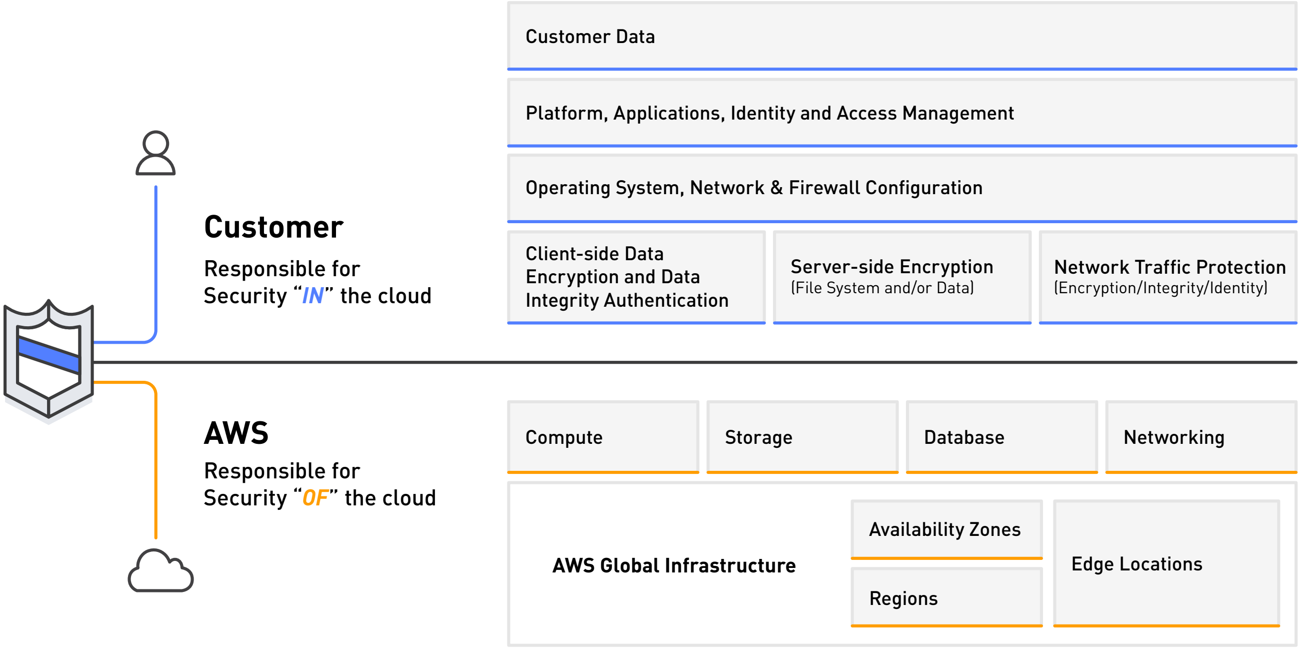
Security

Network Protection for Advanced Threats & Malware

AWS Shared Responsibility Model

Deploying workloads on Amazon Web Services (AWS) helps streamline time-to-market, increase business efficiency, and enhance user performance for many organizations. But as you capitalize on this strategy, it is important to understand your role in securing your AWS environment. As the AWS Shared Responsibility Model illustrates (see figure below), AWS provides a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations, while you are responsible for securing services built on top of this infrastructure, notably including network traffic from remote networks.



Customer

Responsible for Security "*IN*" the cloud

Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network & Firewall Configuration

Client-side Data Encryption and Data Integrity Authentication

Server-side Encryption (File System and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

AWS

Responsible for Security "*OF*" the cloud

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

AWS Solution

When leveraging the AWS Cloud, customers can choose a security solution that is suitable to protect their organization's content, platform, applications, systems and networks, while also meeting their business needs. AWS offers a wide range of tools and features that help organizations increase privacy and control network access so they can more easily meet their needs within the AWS Shared Responsibility Model.

Amazon Virtual Private Cloud (VPC) enables you to create an isolated portion of the AWS Cloud, from which you can launch Amazon EC2 instances in a virtual network that you define. Security groups allow you to define a virtual firewall around your EC2 instances, which contains rules that control the inbound and outbound traffic to your instances. Network Access Control lists (ACLs) provide an optional layer that allows you to control traffic in and out of one or more subnets in your VPC.

Protect Workloads from Suspicious Traffic

Protecting network traffic in your AWS environment can be extended by leveraging infrastructure security offerings available from software vendors in AWS Marketplace. Infrastructure security offerings help increase visibility and protect against cyber-attacks, while also controlling authorization and access for compliance. Amongst targeted and automated attacks, four common threats these software applications help secure against are **malware, distributed denial of service (DDoS) attacks, cross-site scripting**, and **SQL injections**.

- Enforce **malware** protection to help your organization keep it's networks and users safe from malicious attacks, such as bots, worms, spyware, rootkits and Trojan horses.
- Prevent **DDoS** attacks to limit downtime and ensure availability of websites and applications.
- Secure applications from **cross-site scripting** to stop attackers from bypassing access controls in an attempt to penetrate sensitive data.
- Protect against **SQL injections** to help prevent attackers from abstracting sensitive data, such as credit card numbers, from private databases.

Threat Prevention for your AWS Environment

Infrastructure security solutions can be integrated with your AWS environment to help strengthen your security posture and provide multi-layer threat protection. Three common solutions to help with this initiative are traditional **firewalls, next-generation firewalls**, and **web-application firewalls.**

Firewall

While AWS provides complete firewall solutions, many organizations purchase and deploy third-party firewalls from software vendors in AWS Marketplace to supplement their environment and gain additional security controls. Based on the AWS Shared Responsibility Model, you are responsible for setting firewall rules to implement your desired security controls to help restrict suspicious traffic.

Next-Generation Firewall (NGFW)

NGFWs provide much of same protections as standard firewalls, while also adding application-level inspection, intrusion prevention, and full-stack visibility. NGFWs are often accompanied by highly scalable and granular management and reporting consoles. Leveraging a NGFW gives organizations the option to help secure workloads on AWS by enforcing security policies at the application and port and protocol levels. These added features enable organizations to better inspect data payloads and distinguish different types of network traffic.

Web Application Firewall (WAF)

Many AWS customers supplement network firewalls with a third-party WAF to protect the highest layers of the computing stack. In particular, WAFs secure the application layer by protecting web-facing applications from automated and targeted attacks. Securing applications against these exploits helps ensure application availability and minimizes the risk of an attacker using your application as an entry point into your entire system. WAFs enable users to filter common attack patterns, such as SQL injections or cross-site scripting. They can also detect cookie, session, or parameter tampering attacks and provide data loss prevention, stopping attackers from extracting sensitive data.

Get Started with Network Protection in AWS Marketplace

Find and deploy the solution you need in minutes

Save money with pay-as-you-go pricing

Scale globally across all AWS Regions