

A Quick Overview of the Amazon Web Services Shared Responsibility Model



Understanding Your Security Responsibilities with AWS

AWS security features are robust enough for the most risk-sensitive organizations, including public sector organizations at all levels.



6,500+

Government, education, nonprofit, and healthcare organizations using AWS



200

Services to accelerate digital transformation



Strongest Security Rating

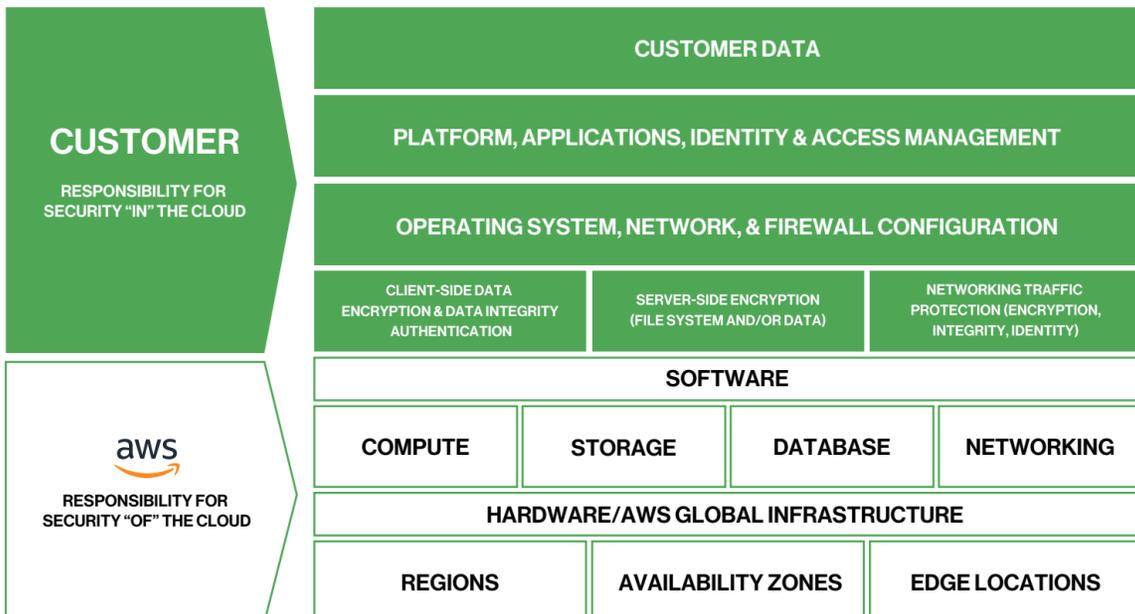
Of public cloud and infrastructure platform services (CIPS) providers, according to Gartner's 2021 Magic Quadrant

AWS's high degree of security is only one reason why public sector organizations rely on AWS – another is control. Customers of AWS always retain control over their data, what they upload to the network, and how they manage and access their content. The government of Quebec, for instance, entrusts citizen data with AWS, knowing that the data is encrypted, safe, and only accessible to its owners.

Understanding the Amazon Web Services Shared Responsibility Model

While this enhanced degree of control enables more flexibility and manageability, it also requires that you, as an AWS customer, are required to oversee some of that security. These security responsibilities are delegated through a shared responsibility model (SRM).

In this model, AWS manages the security of the cloud, while you and a qualified AWS cloud provider manage security in the cloud. Your choices and responsibilities are clearly delineated, which enables you to implement end-to-end security more quickly, efficiently, and effectively. Understanding this model is critical to taking full advantage of the benefits AWS has to offer.



Benefits of Sharing Amazon Web Services Security

Sharing your AWS security responsibilities with AWS and your AWS-partnered cloud provider enables you to keep your data safe, meet compliance requirements, lower costs, and scale confidently. The benefits of sharing security responsibilities with the right partner include:



Flexibility

AWS cloud and security grows with you, allowing you to scale at your own pace, securely, and with confidence.



Clarity

The AWS SRM clearly defines your responsibilities, choices, roles, and duties, which improves predictability and removes ambiguity.



Visibility

AWS's robust toolbox of security features provides key security information, such as where your data is stored, who can access it, and what resources your organization is consuming.



Control

Even in the AWS cloud, you always retain control over your data, applications, infrastructure, and security.

Stay Secure on Amazon Web Services with



Optimization



Implementation



Consulting



Management

Maximize and extend the security benefits of AWS by sharing your security responsibilities. Leverage our expertise to simplify complexity, stay compliant, and minimize risk, while making the most of your cloud investment. Partner with us today to receive a security-focused solution tailored to your specific AWS environment, workloads, use cases, and business needs.

Understand the Amazon Web Services Share Responsibility Model now with

Take the first step in your journey to the AWS cloud. An experienced AWS partner, will provide you with hands-on support every step of the way, from assessment to planning to execution to optimization.

Contact us today to schedule a free consultation.

