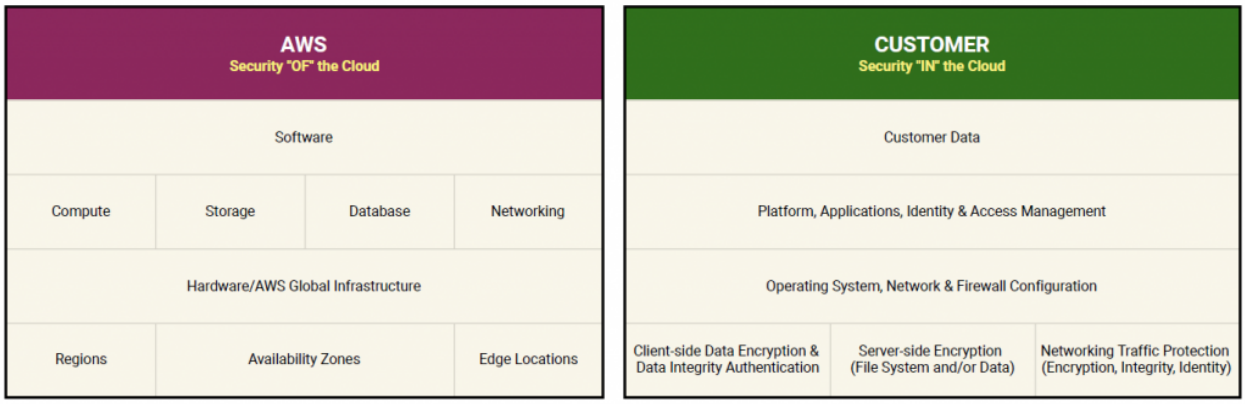
AWS Shared Responsibility Model

When using cloud services, it is important to understand the responsibilities of both the provider and the customer for the various components of the solution. The Shared Responsibility Model in Amazon Web Services outlines these responsibilities, specifying what AWS is responsible for and what the customer is responsible for. Additionally, it includes IT controls that are managed by either party or jointly, ensuring security and compliance throughout the cloud infrastructure.

AWS is responsible for the security “of” the cloud, while the customer is responsible for the security “in” the cloud. The distinction between “of” and “in” is significant because it defines the scope of responsibility for both AWS and the customer. The table below shows how AWS is in charge of securing the cloud infrastructure, while the customer is in charge of securing their usage and data within the cloud.



- Security “of” the Cloud – AWS manages, operates, and controls the host operating system, virtualization layer, as well as the physical security of its data centers. These data centers are physical facilities that house all the resources, and they require security measures to protect the IT assets inside, as customer data is stored in the storage volumes within the data center or across multiple availability zones. Additionally, AWS is responsible for maintaining the physical servers, including tasks such as applying OS patches, installing firmware updates, and implementing physical and environmental controls for its data centers to guarantee the availability, reliability, and scalability of its cloud service.
- Security “in” the Cloud – the customer is responsible for configuring the AWS-provided security group and virtual firewall, as well as managing the guest OS and related applications. Take note that the level of responsibility for cloud security and maintenance varies depending on the type of service used by the customer, such as Infrastructure as a Service (IaaS) or abstracted services. For example, Amazon EC2 is classified as IaaS, which means you must perform all the necessary

security configuration and management tasks. However, for abstracted services such as Amazon S3 and DynamoDB, AWS handles almost everything from the infrastructure layer, and you are only responsible for managing the data, classifying their assets, and applying the fine-grained permissions using IAM tools to meet the compliance requirements.

Furthermore, the AWS-customer shared responsibility applies to IT controls as well, with both managing, operating, and verifying them. Examples of controls managed by AWS, customers, and both include:

- Inherited Controls – the customer fully inherits certain items from AWS, such as the physical and environmental controls of the data centers and their related assets.
- Shared Controls – applies to both the AWS infrastructure and the customer layers. AWS provides the core infrastructure, and customers can add their own set of controls to AWS services. The following are examples of shared controls:
    - Patch Management – AWS is responsible for patching the host OS and resolving issues within the AWS infrastructure, while the customer is responsible for patching the guest OS and their applications.
    - Configuration Management – AWS manages the configuration of its infrastructure devices and servers, while the customer is responsible for configuring their guest OS, databases, and custom applications.
    - Awareness & Training – AWS trains its employees, while customers are responsible for training their own employees.
- Customer Specific – the customer is responsible for securing the deployed application in the AWS cloud, including zone security, where they can modify routes to resources or filter traffic to control access to cloud resources and data.