Security in AWS Notes

Amazon Shared Responsibility Model

Security and compliance are shared responsibilities between us and the customer. This shared model can help relieve a customer's operational burden because we operate, manage, and control the components from the host operating system and virtualization layer down to the physical security of the facilities where the service operates. The customer is responsible for--and manages--the guest operating system (including updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall. Customers should carefully consider the services that they choose because their responsibilities will vary depending on the services that they use, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. This differentiation of responsibility is commonly referred to as Security *of* the Cloud versus Security *in* the Cloud.

AWS responsibility

Security of the Cloud: We are responsible for protecting the infrastructure that runs all of the services that are offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility

Security in the Cloud: Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

For more details about the Shared Responsibility Model, see: https://aws.amazon.com/compliance/shared-responsibility-model/