ARYATECHNO

AWS Shared Responsibility

Topics : AWS
Written on December 09, 2023

The concept of shared responsibility is a fundamental aspect of cloud computing security, and it defines the division of responsibilities between the cloud service provider (CSP), such as AWS, and the customer. The shared responsibility model is designed to ensure a secure cloud environment while clearly outlining the responsibilities of each party. In the context of AWS, the shared responsibility model can be summarized as follows:

1. **AWS Responsibility ("Security of the Cloud"):**
   - AWS is responsible for the security of the underlying cloud infrastructure. This includes the physical facilities, hardware, software, networking, and facilities that run AWS services.
   - AWS ensures the availability, reliability, and operational excellence of the infrastructure.
   - AWS provides global data center security measures, DDoS protection, and compliance certifications for its services.
2. **Customer Responsibility ("Security in the Cloud"):**
   - Customers are responsible for securing their data, applications, identity, and configurations within the AWS cloud.
   - This includes configuring access controls, managing user identities and permissions using AWS Identity and Access Management (IAM), securing data in transit and at rest, and implementing network security measures within their virtual private cloud (VPC).
   - Customers are responsible for setting up proper encryption, applying security patches to their instances, and managing configurations securely.
3. **IAM (Identity and Access Management):**
   - AWS IAM is a key component of the shared responsibility model. Customers are responsible for defining and managing IAM policies, roles, and permissions.
   - This includes creating strong password policies, using multi-factor authentication (MFA), and ensuring the principle of least privilege for user access.
4. **Data Encryption:**
   - Customers are responsible for encrypting their data, both in transit and at rest. AWS provides encryption tools and services such as AWS Key Management Service (KMS), but customers must configure and manage encryption settings.
   - Properly configuring encryption for data at rest (e.g., using Amazon S3 server-side encryption) and data in transit (e.g., using HTTPS) is the customer's responsibility.

5. **Networking and Firewall Configuration:**
   - Customers are responsible for configuring their network security within AWS. This includes setting up security groups, network access control lists (NACLs), and configuring Virtual Private Cloud (VPC) settings.
   - Implementing secure networking practices to control traffic and protect against unauthorized access is part of the customer's responsibility.
6. **Operating System and Application Security:**
   - Customers are responsible for securing their operating systems, applications, and middleware running on AWS instances.
   - This includes applying security patches, using secure configurations, and implementing security best practices for the specific applications and services deployed.
7. **Compliance and Governance:**
   - While AWS maintains various compliance certifications for its infrastructure, customers are responsible for ensuring that their applications and data comply with industry-specific regulations.
   - Customers are responsible for governance, risk management, and compliance (GRC) activities related to their use of AWS services.