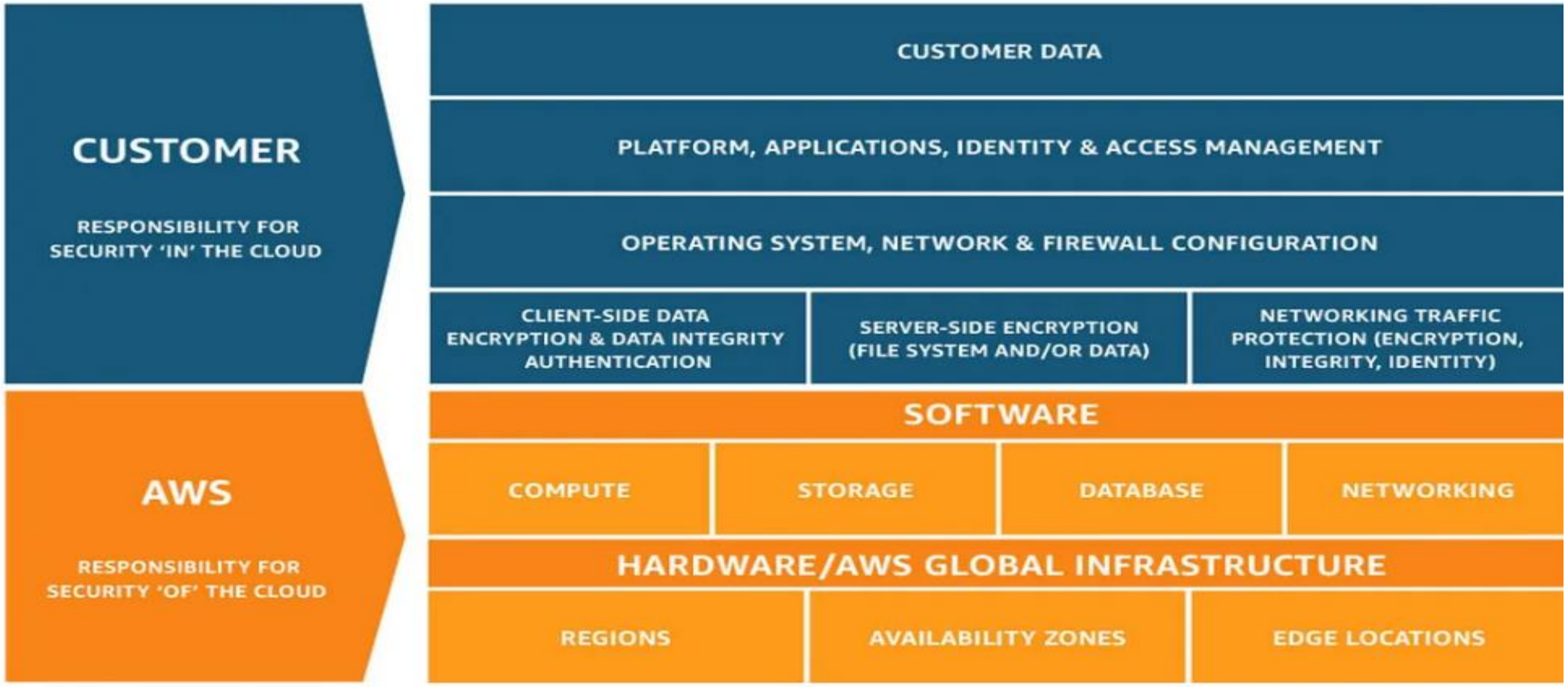
Shared Responsibility Model

OW

Overview

- AWS follows a shared responsibility model, wherein both AWS and its customers collaborate to maintain a secure cloud environment.
- This comprehensive guide explores the AWS shared responsibility model, covering essential points and best practices for implementing effective security measures, including IAM (Identity and Access Management) and data encryption.
- Amazon Web Services (AWS) has enabled businesses to harness the power of the cloud.

Responsibility: Between Aws and Customers



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

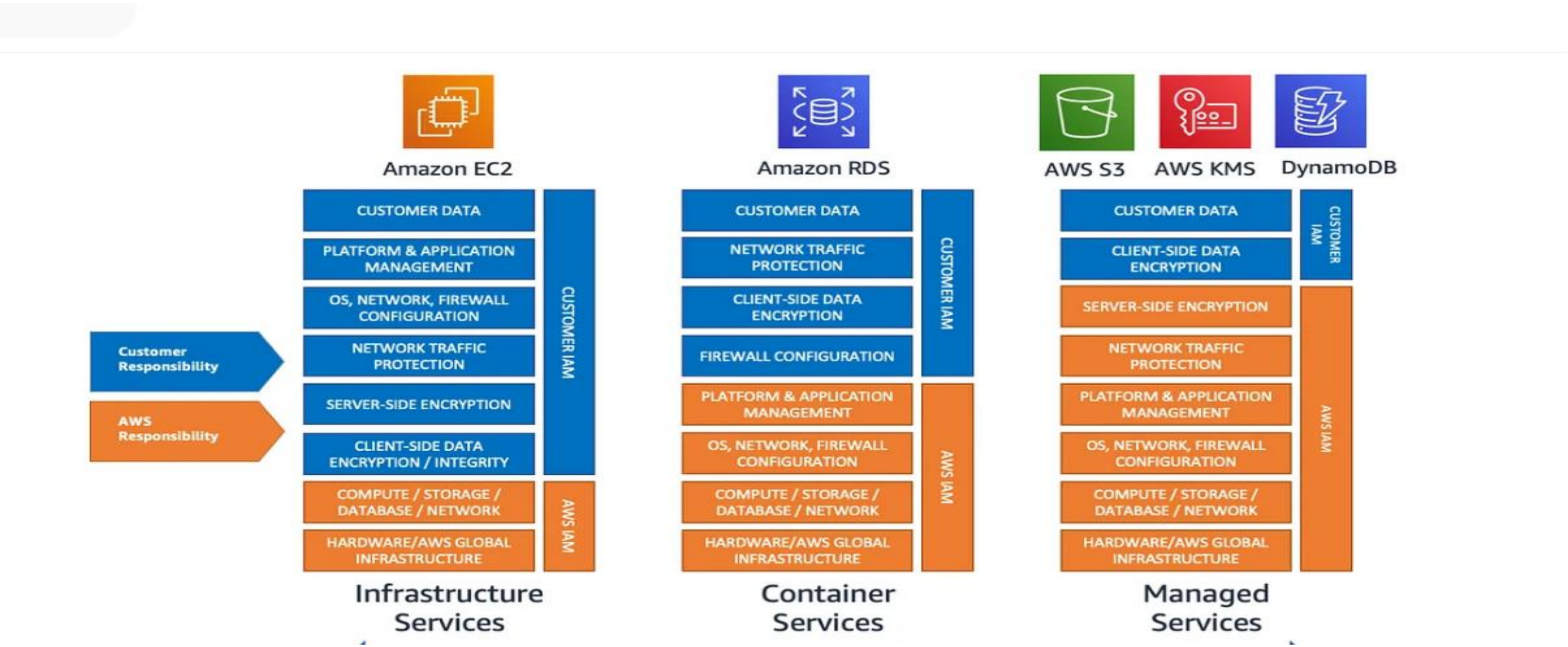
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

..


Amazon EC2
CUSTOMER DATA
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
NETWORK TRAFFIC PROTECTION
SERVER-SIDE ENCRYPTION
CLIENT-SIDE DATA ENCRYPTION / INTEGRITY
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Infrastructure Services
Customer Responsibility
AWS Responsibility
Amazon RDS
CUSTOMER DATA
NETWORK TRAFFIC PROTECTION
CLIENT-SIDE DATA ENCRYPTION
FIREWALL CONFIGURATION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Container Services
AWS S3
AWS KMS
DynamoDB
CUSTOMER DATA
CLIENT-SIDE DATA ENCRYPTION
SERVER-SIDE ENCRYPTION
NETWORK TRAFFIC PROTECTION
PLATFORM & APPLICATION MANAGEMENT
OS, NETWORK, FIREWALL CONFIGURATION
COMPUTE / STORAGE / DATABASE / NETWORK
HARDWARE/AWS GLOBAL INFRASTRUCTURE
CUSTOMER IAM
AWS IAM
Managed Services

Aws Responsibility

- AWS takes responsibility for securing its global infrastructure, including data centers, networking, and the virtualization layer. This includes measures to protect against common security threats
- **Physical Infrastructure:** AWS is responsible for securing the physical infrastructure, data centers, and networking equipment that form the backbone of their cloud services. This includes implementing physical security measures to prevent unauthorized access to data centers and protecting against environmental hazards.

..

- **Hypervisor and Virtualization:**AWS manages the hypervisor and virtualization layer that enables the creation and management of virtual instances, ensuring the segregation of customer data and workloads.
- **Managed Services:**AWS takes responsibility for securing and managing the underlying infrastructure of managed services, such as Amazon RDS, Amazon DynamoDB, and AWS Lambda. This includes patching, monitoring, and maintaining the service’s availability and security.

..

- **Global Network Backbone:** AWS operates a global network backbone that securely routes data between AWS regions and availability zones. This ensures data transmission reliability and protection against network-related security threats.

- **Compliance and Auditing:** AWS maintains compliance certifications and undergoes regular audits to meet industry standards and regulatory requirements. AWS customers can access compliance reports to verify the security and compliance of AWS services

Customer Responsibility

- Customers using AWS services are responsible for securing their data, applications, and user access within the AWS environment. This includes the following responsibilities:
- **Data Protection and Encryption:** Customers are responsible for selecting appropriate encryption methods to protect sensitive data at rest and in transit. AWS provides encryption options, and customers must choose the appropriate level of protection based on their data’s sensitivity.

..

- **IAM and Access Management:** Customers are responsible for managing access to AWS resources using IAM. This includes creating IAM users, groups, and roles, and assigning appropriate permissions to control access to AWS services.
- **Operating System and Applications:** Customers are responsible for securing the operating systems and applications running on their EC2 instances and other compute services. This includes implementing security patches and updates to protect against known vulnerabilities.

..

- **Network Security:** Customers are responsible for configuring network security measures such as security groups, network access control lists (ACLs), and firewalls to control inbound and outbound traffic to their resources.
- **Application-Level Security:** Customers are responsible for securing their applications, including authentication, authorization, and application-level encryption.
- **Data Backup and Recovery:** Customers are responsible for implementing data backup and recovery solutions to ensure data resilience and availability.