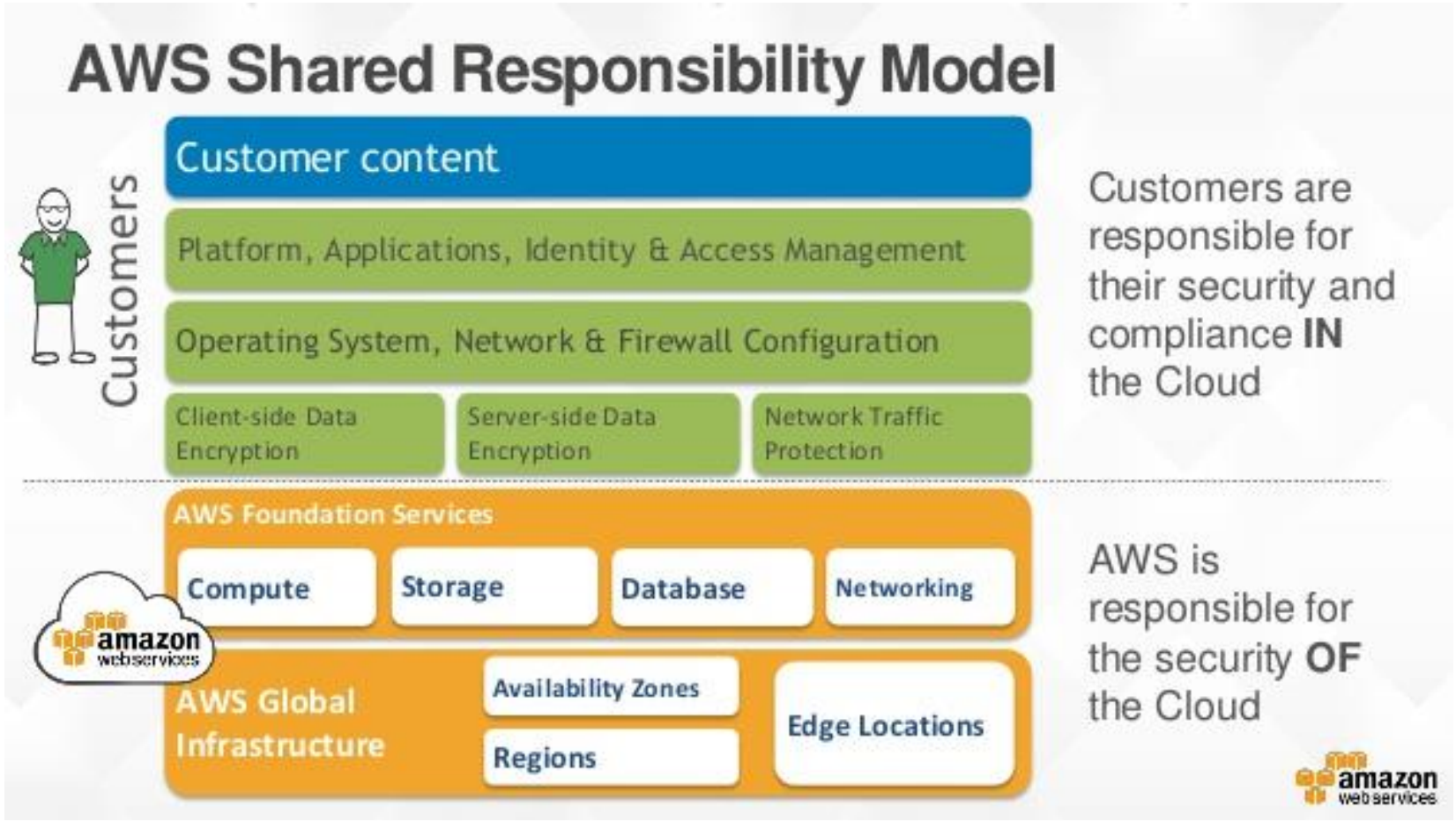
AWS Shared Responsibility Security Model

By

Keshav Kummari

AWS Shared Responsibility Model



Shared Security Responsibility Model

AWS is responsible for portions of the cloud, and you as the customer have portions of the cloud that you are responsible for, thus creating shared security responsibility.

Your Responsibility:

- IAM
- Multi-factor authentication
- Password/Key Rotation
- Access Advisor
- Trusted Advisor
- Security Groups
- Resource-Based Policies
- Access Control Lists
- VPC
- Port scanning is against the rules even on your own environment (ask AWS if you want to do this)
- Operating system level patches

AWS's Responsibility:

- Physical server level and below
- Physical Environment security and protection (fire/power/climate/management)
- Storage device decommissioning according to industry standards
- Personnel security
- Network Device Security and ACLs
- AWS API endpoints - SSL
- DDOS protection
- EC2 Instances and spoofing protection (Ingress/Egress filtering)
- EC2 Instance hypervisor isolation:
  - Instances on the same physical device are still independent

Service Differences

- AWS Lambda:
  - Generally, operating system patches are your responsibility
  - AWS Lambda is a fully-managed service that lets AWS handle responsibility for the OS
- Other managed services:
  - Some AWS managed services take on additional responsibility for you
  - Evaluate those services independently

Terminology

High Availability:
Refers to systems that are durable and likely to operate continuously without failure for a long time. In practice, this means making sure your AWS applications are always available when a user/customer tries to access them.

Fault Tolerance:
Is the property that enables a system to continue operating properly in the event of the failure of one or more of its components. An example of a fault tolerant application would be one that is resilient to the failure of one of its web servers. It would still be able to serve traffic to visitors and ever repair itself.

Scalability:
The ability of a system to easily increase in size and capacity in a cost-effective way (usually based on usage demand).

Cost Efficient:
Choosing the correct options to make a system as inexpensive as possible.

Secure:
Following proper security guidelines and practices to secure a system.

AWS Best Practices:
A set of guidelines outlined by AWS that should be followed when provisioning and using their services.