AWS Certified Cloud Practitioner Training Bootcamp

Introduction to AWS Security

Introduction to AWS Security

- AWS delivers a scalable cloud computing platform designed for high availability and dependability
- Security is AWS's top priority; AWS helps you to protect the confidentiality, integrity and availability of your systems and data
- AWS architecture has been built following two key principles: flexibility and security, providing an extremely scalable and flexible cloud platform

Introduction to AWS Security

- AWS uses redundant and multi-layer controls, continuous validation and testing, with built-in automation, that helps monitoring and keeping customers safe and secure

- The same level of automation and security is contained and replicated in any AWS DC (AZ, remember ?)

- With AWS, you get a resilient, fault-tolerant architecture, designed for security, able to satisfy the requirements of even the most security-sensitive customers

AWS Shared Responsibility Model Overview

- Security and Compliance is a shared responsibility between AWS and the customer

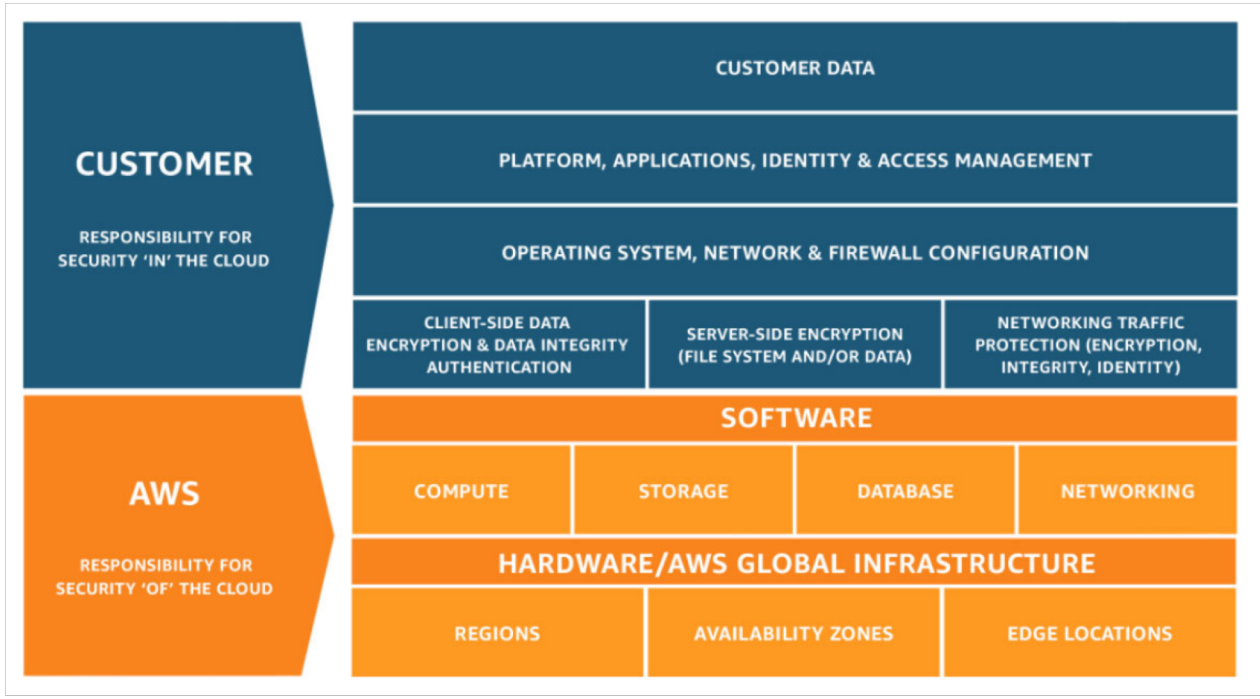
- The customer assumes responsibility and management of the guest operating system (including updates and security patches), as well as the configuration of the AWS provided security group firewall, while AWS takes care of the cloud

- This differentiation of responsibility is also know as Security "of" the Cloud versus Security "in" the Cloud

AWS Responsibility for Security OF the Cloud

- AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

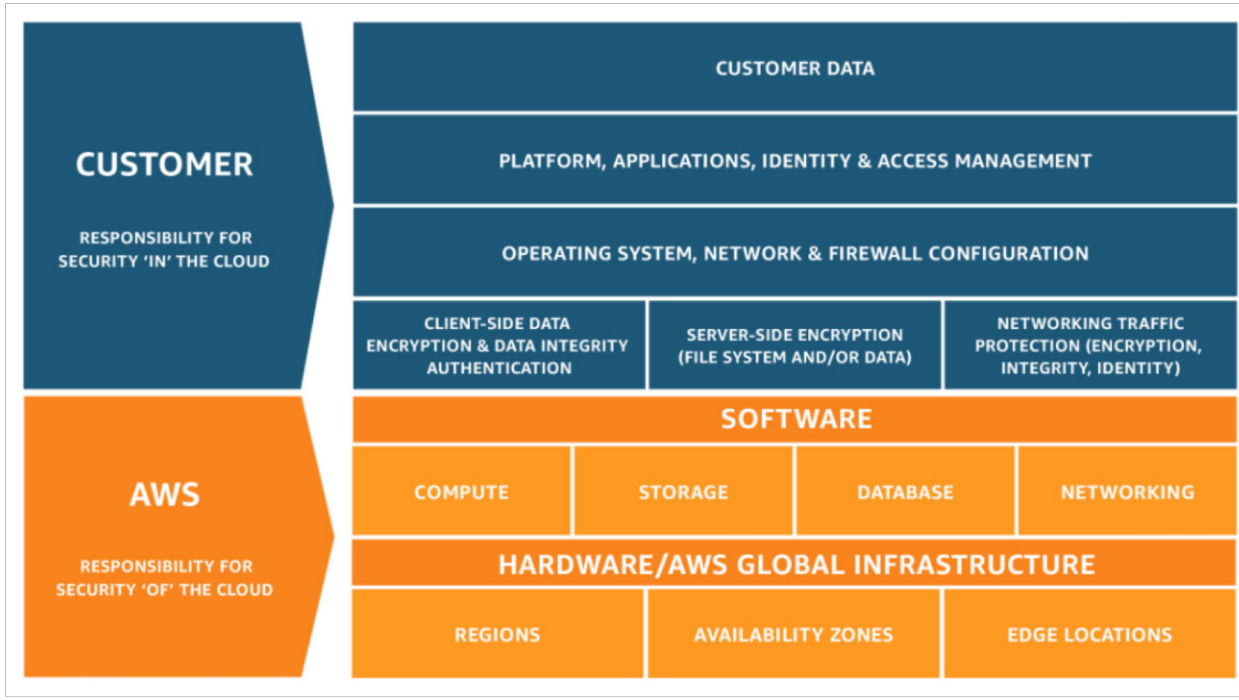
- This infrastructure is composed of the hardware, software, networking and facilities that run AWS Cloud services



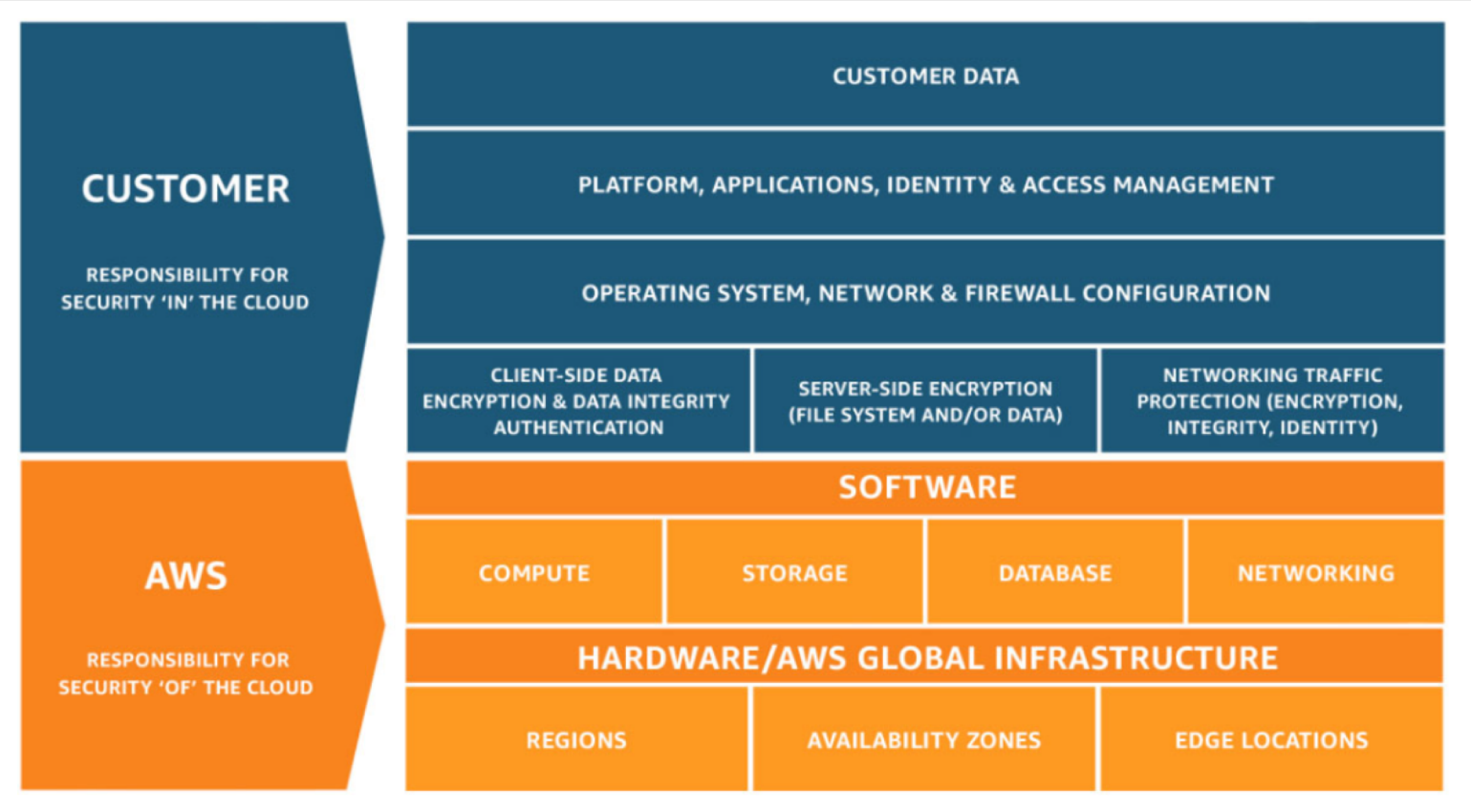
Customer Responsibility for Security IN Cloud

- 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



AWS Shared Responsibility Model



- https://aws.amazon.com/compliance/shared-responsibility-model/

Security Products and Features

- AWS offers a lot of tools and features that can help you meet you security objectives

- AWS provides security-specific tools and features across:
  - Network security
  - Configuration Management
  - Data Encryption
  - Access Control
  - Monitoring & Logging

AWS Network Security

- AWS provides security capabilities and services that can help you secure and protect your data:
  - Built-in firewalls (security groups) – control access to your instances and subnets
  - Encryption in transit using TLS
  - VPNs, for dedicated private connections
  - DDoS mitigation technologies

Inventory and Configuration Management

- AWS offers several tools that you can make use of:
  - Deployment tools for creation and decommissioning of AWS services and resources
  - Inventory tools – dashboards
  - Template definition in order to create custom EC2 instances (specific config that you can replicate)

Data Encryption

- AWS offers the possibility to define encryption at-rest for your data:
  - Data encryption capabilities available for AWS Storage and DB services
  - Flexible KMS (AWS or you manage the encryption keys)
  - Hardware based cryptographic key storage options (sensitive customers)

Access Control

- AWS gives you full control over access to AWS services:
  - IAM to define individual user accounts with custom permissions
  - MFA
  - Integration and Federation with corporate directories

Monitoring and Logging

- AWS provides multiple tools that can help you with monitoring and logging:
  - Deep visibility - CloudTrail
  - Log aggregation – CloudWatch
  - Notifications through alerts (emails)

AWS Security Guidance

- AWS provides customers with guidance and expertise through both online tools and AWS personnel
  - AWS Enterprise Support - 15 min. SLA, 24x7 availability, dedicated TAM
  - AWS Trusted Advisor
  - AWS Professional Services

AWS Compliance Program

- AWS computing environments are continuously audited, with certifications from accreditation entities across geographies and verticals (i.e. ISO 27001, PCI DSS, etc.)

- In a traditional data center, common compliance activities are often manual, periodic activities and include verifying asset configurations and reporting on administrative activities. Moreover, the resulting reports are out of date before they are even published ☺

- https://aws.amazon.com/compliance/programs/

AWS Certified Cloud Practitioner Training Bootcamp

Thank you