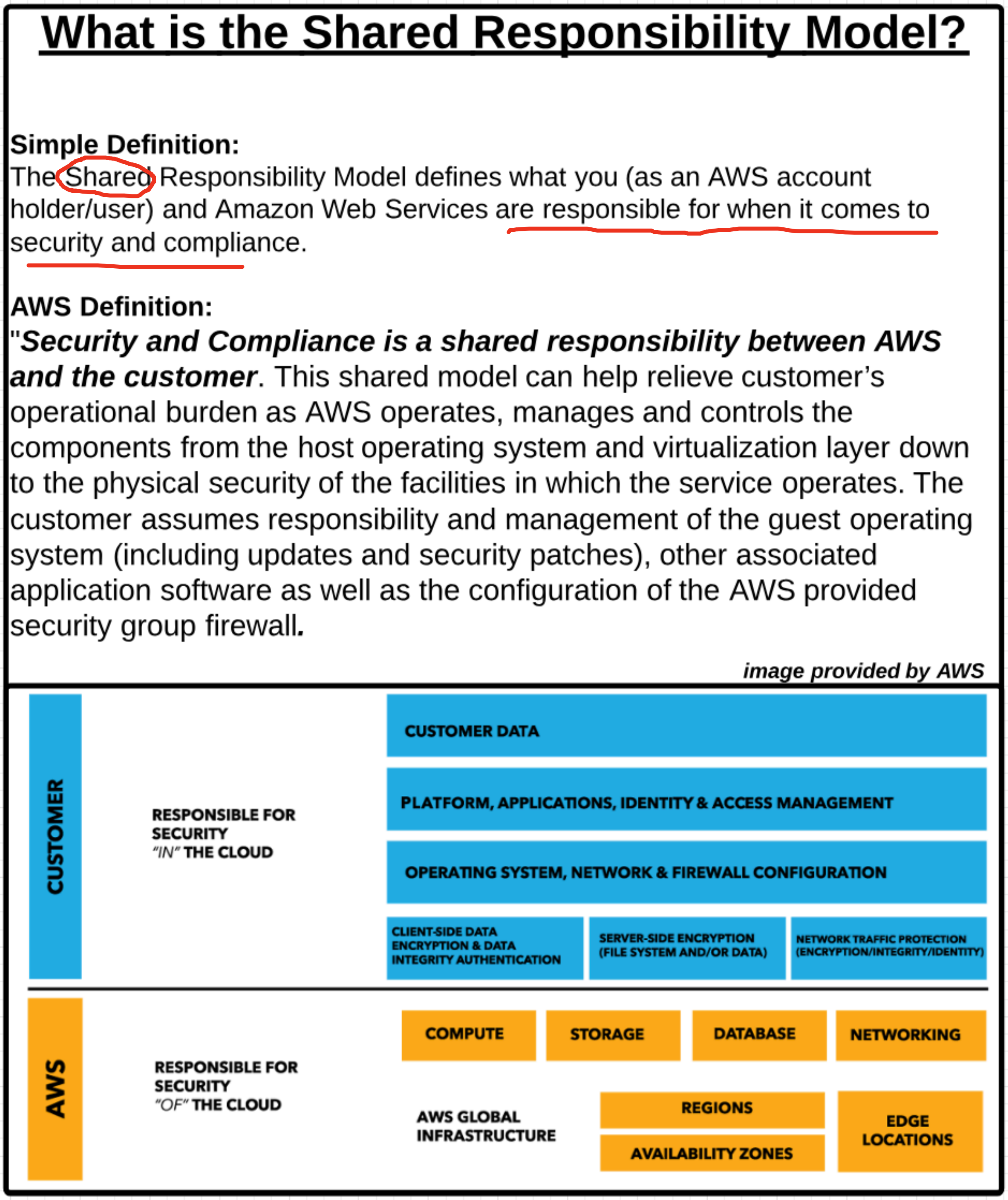
Shared Respon Model & DDOS

2019年2月10日 星期日　　下午1:46



What is the Shared Responsibility Model?

Simple Definition:
The Shared Responsibility Model defines what you (as an AWS account holder/user) and Amazon Web Services are responsible for when it comes to security and compliance.

AWS Definition:
"***Security and Compliance is a shared responsibility between AWS and the customer***. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall.

image provided by AWS

CUSTOMER

RESPONSIBLE 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)

NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)

AWS

RESPONSIBLE FOR SECURITY "OF" THE CLOUD

COMPUTE

STORAGE

DATABASE

NETWORKING

AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Shared Responsibilty Model Example:

Elastic Cloud Compute Shared Responsibility Model:

AWS is Responsible for:

(1) The setup and maintenance of the physical hardware located at each AWS data center.

(2) The physical security data centers (locks, keys, security guards, etc).

(3) The setup an maintenance of the host virtualization software.

You are responsible for:

(1) Network level security (NACLs, Security Group).

(2) Operating System patched and updates

(3) IAM user access management

(4) Client and server side data encryption

Note: This is not an all-inclusive list - just the most prominent examples

In addition to the Shared Responsibility Model, DDoS Protection is build-in/Mitigated by many core AWS Services. But what if you want to simulate an attack to test your applications security?

DDoS and Penetration Testing:

AWS Services with Built-In DDoS Protection/Mitigation:

(1) Route 53
(2) CloudFront
(3) WAF (web application firewall)
(4) Elastic Load Balancing
(5) VPCs and Security Groups

53 + CF
+ WAF + ELB
+ VPC

Penetration Testing:

Penetration testing is the practice of ***testing one's own application security for vulnerability*** by simulating an attack. AWS allows penetration testing, however ***you must request permission from AWS before doing and penetration testing***.

Penetration testing is allowed on the following AWS resources:
(1) EC2
(2) RDS
(3) Aurora
(4) CloudFront
(5) API Gateway
(6) Lambda
(7) LIghtsail
(8) DNS Zone Walking