Security Fundamentals

Immersion Day

Tim Robinson

April 2019

Security Foundations

What are your perceptions on cloud security?

At AWS, cloud security is the highest priority!

Whitepaper:

Introduction to AWS Security

AWS Security Center

Comprehensive security portal to provide a variety of security notifications, information and documentation.

Security Whitepapers

- Overview of Security Process
- AWS Risk and Compliance
- AWS Security Best Practices

Security Bulletin

Security Resources

Vulnerability Reporting

Penetration Testing

Requests

Report Suspicious Emails

http://aws.amazon.com/security

Security Resources

Developer Information, Articles and Tutorials, Security Products, and Whitepapers

http://aws.amazon.com/security/security-resources/

Security Blog

Subscribe to the blog – it's a great way to stay up-to-date on AWS security and compliance.

http://blogs.aws.amazon.com/security/

Video Resources

The AWS Shared Responsibility Model in Detail	https://youtu.be/RwUSPkIR24M
IAM Recommended Practices	https://youtu.be/R-PyVnhxx-U
Encryption Options on AWS	https://youtu.be/9bn7p2tdym0
Compliance, Logging, Analysis and Alerting	https://www.youtube.com/watch?v=bFMkxIAhFv8
Securing Serverless Architectures	https://www.youtube.com/watch?v=lKVp8d45HSU
Account Separation and Mandatory Access Control	https://youtu.be/42-1xpT-s6U

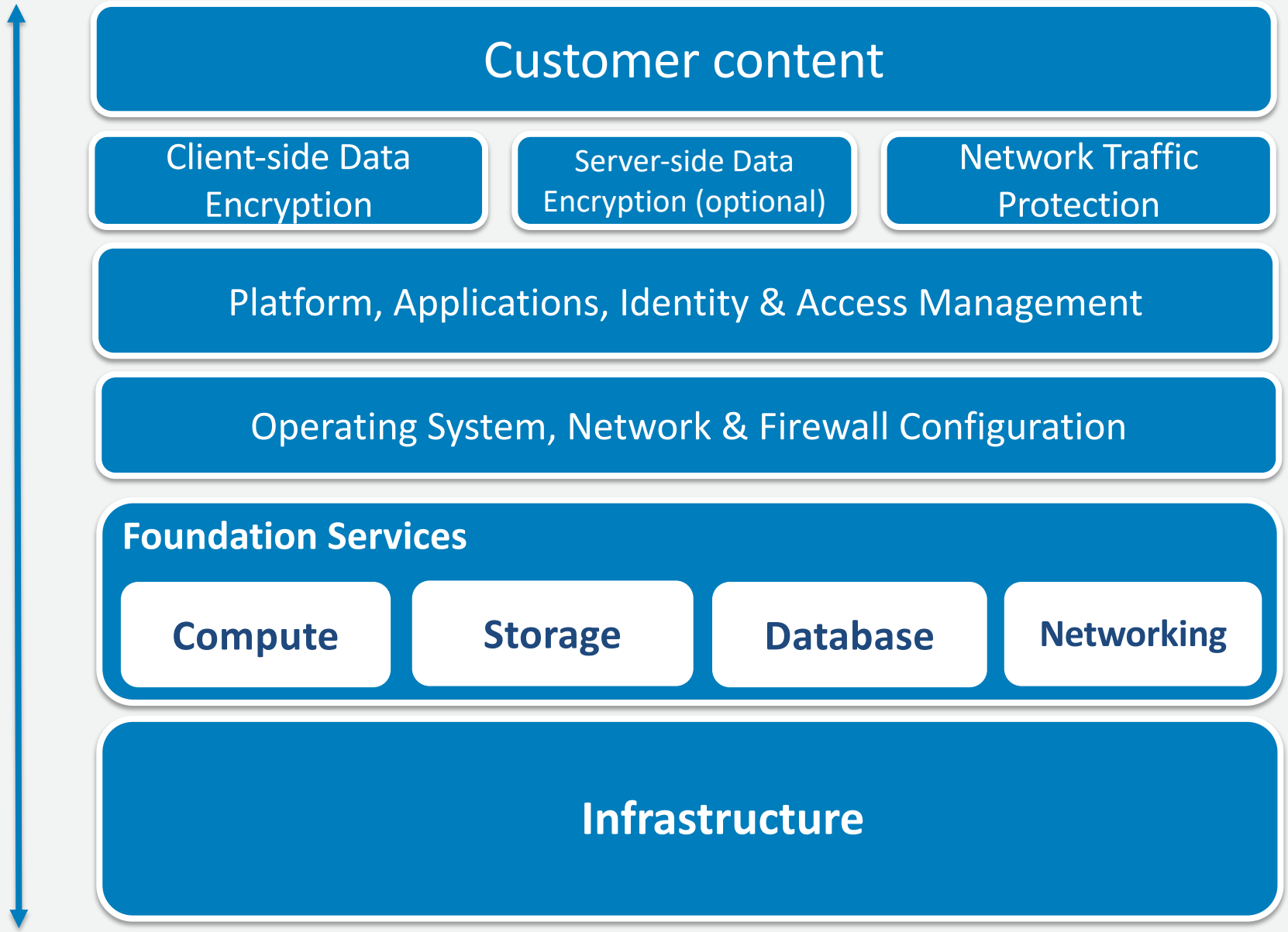
Shared Responsibility Model

“Security OF the Cloud” - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

“Security IN the Cloud” - Customer responsibility will be determined by the AWS Cloud services that a customer selects.

Traditional On-Premises Security Model

Customers are responsible for end-to-end security in their on-premises data centers



AWS Security Model when using Infrastructure Services

Customer's responsibility

AWS takes over responsibility from customers

Customer content

Client-side Data Encryption

Server-side Data Encryption (optional)

Network Traffic Protection

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Customer IAM

AWS IAM

Mgmt Protocols

API Endpoints

API Calls

aws

AWS Security Model when using Container Services

Customer's responsibility

AWS takes over responsibility from customers

Customer content

Client-side Data Encryption

Server-side Data Encryption (optional)

Network Traffic Protection

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Customer IAM

Mgmt Protocols

AWS IAM

API Endpoints

API Calls

aws

AWS Security Model when using Abstracted Services

Customer's responsibility

AWS takes over responsibility from customers

Customer content

Client-side Data Encryption

Server-side Data Encryption (optional)

Network Traffic Protection

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

Compute | **Storage** | **Database** | **Networking**

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

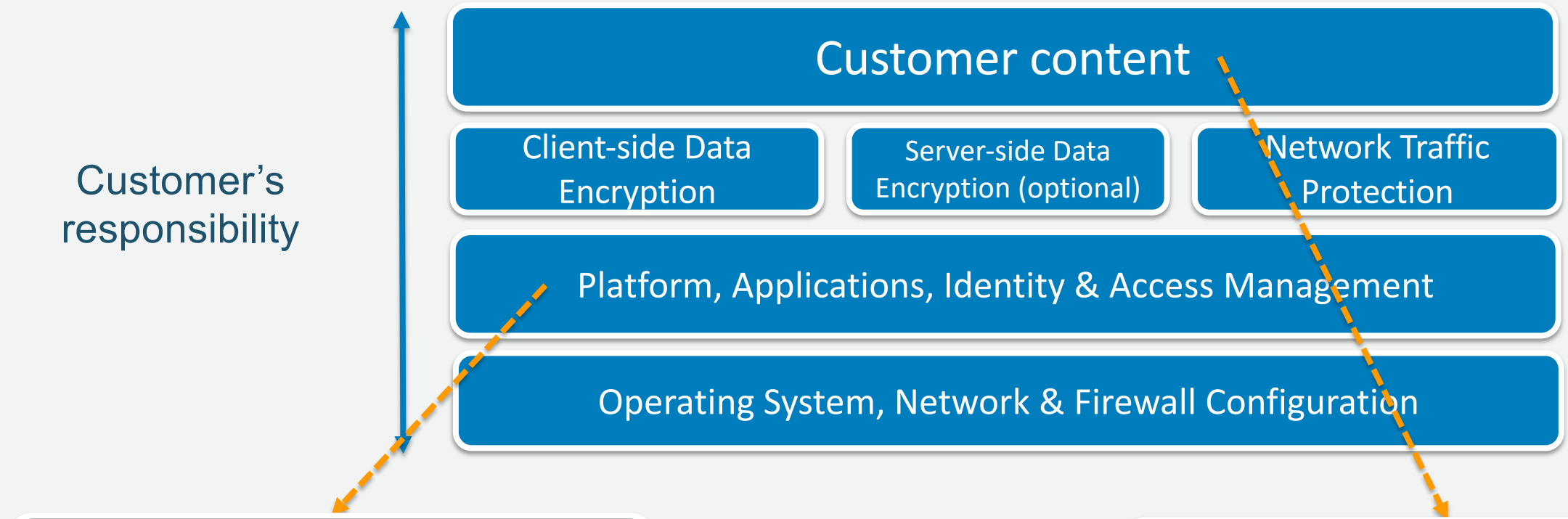
AWS IAM

API Endpoints

API Calls

aws

More details for customer responsibility



Leave S3 Buckets public (open for read/write)

What helps?

Amazon Macie

AWS Config

Commit Secret Credentials to GitHub

What helps?

Amazon GuardDuty

Customer applications & Compliance

Customer Applications

Your own accreditation

Your own certifications

Your own external audits

AWS Services

Applications built on top of AWS services, **are not implicitly compliant** to security controls (that AWS services are complaint with).

Customers need to **certify applications separately** by engaging with external auditors.

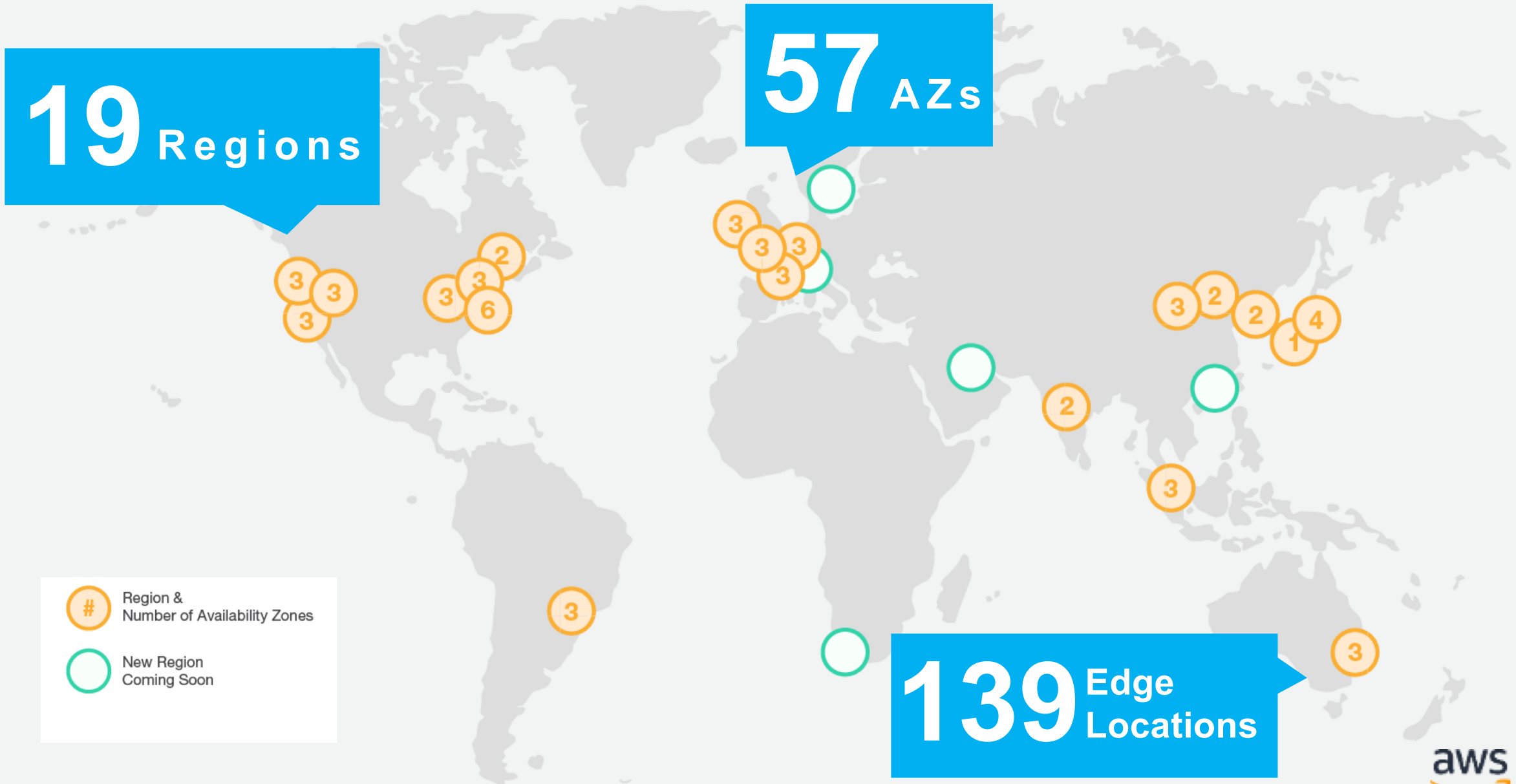
AWS Compliance

List of compliance, assurance programs and resources: http://aws.amazon.com/compliance/

Available Reports

Australian Prudential Regulation Authority CPG 234 Workbook	Cloud Computing Compliance Controls Catalogue (C5)	FedRAMP Partner Package	Global Financial Services Regulatory Principles	Government of Canada Partner Package	Hong Kong Monetary Authority TM-G-1 Workbook	IRAP Package
ISO 27001:2013 Certification and Statement of Applicability (SoA)	ISO 27017:2015 Certification and Statement of Applicability (SoA)	ISO 27018:2014 Certification and Statement of Applicability (SoA)	ISO 9001:2015 Certification	MAS TRM Guidelines Workbook	MTSC Certification and Self-Disclosure Form	PCI DSS Attestation of Compliance (AOC) and Responsibility Summary
PSN Connection Compliance Certificate (CoCo)	PSN Service Provision Compliance Certificate	Quality Management System Overview	Service Organization Controls (SOC) 1 Report	Service Organization Controls (SOC) 2 Report	Service Organization Controls (SOC) 3 Report	SOC Continued Operations Letter

AWS Global Infrastructure



Our Data Centers

Our data centers provide protection at every layer:

- ✓ Perimeter Layer
- ✓ Infrastructure Layer
- ✓ Data Layer
- ✓ Environmental Layer

Take a virtual tour:

https://aws.amazon.com/compliance/data-center/data-centers/

Perimeter Layer

- ACCESS IS SCRUTINIZED
- ENTRY IS CONTROLLED AND MONITORED
- AWS DATA CENTER WORKERS ARE SCRUTINIZED, TOO
- MONITORING FOR UNAUTHORIZED ENTRY
- AWS SECURITY OPERATIONS CENTERS MONITORS GLOBAL SECURITY

Infrastructure Layer

- LAYER-BY-LAYER ACCESS REVIEW
- MAINTAINING EQUIPMENT IS A PART OF REGULAR OPERATIONS
- EMERGENCY-READY BACKUP EQUIPMENT

Data Layer

- TECHNOLOGY AND PEOPLE WORK TOGETHER FOR ADDED SECURITY
- PREVENTING PHYSICAL AND TECHNOLOGICAL INTRUSION
- SERVERS AND MEDIA RECEIVE EXACTING ATTENTION
- THIRD-PARTY AUDITORS VERIFY OUR PROCEDURES AND SYSTEMS

Environmental Layer

- PREPARED FOR THE UNEXPECTED
- HIGH AVAILABILITY THROUGH MULTIPLE AVAILABILITY ZONES
- SIMULATING DISRUPTIONS & MEASURING OUR RESPONSE
- GREENER IN THE AWS CLOUD

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the AWS datacenters

Toggling on the Server-side encryption feature for S3 buckets

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for S3 buckets

Preventing packet sniffing at the hypervisor level

Securing the internal network inside the AWS datacenters

Questions so far?