



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](#)



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



The screenshot shows the AWS Cloud Security homepage. At the top, there's a blue header with the AWS logo and the text "AWS Cloud Security". Below it, a sub-header says "Protect your data with cloud-powered security." A button labeled "I'd like Information about Security in the Cloud »" is present. The main content area has several sections: "Cloud Security", "Penetration Testing", "Security Bulletins", "Resources", "Compliance", and "Partners". In the "Cloud Security" section, text discusses AWS's security posture and cost-efficiency. In the "Resources" section, there's a quote from Richard Crowley of Slack: "The fact that we can rely on the AWS security posture to boost our own security is really important for our business. AWS does a much better job at security than we could ever do running a cage in a data center." The Slack logo is shown next to the quote. At the bottom, links are provided for "Security Careers »" and "Security Blog »".

<http://aws.amazon.com/security>



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



Security Resources

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

Cloud Security Resources

Find information about security in the cloud.

Cloud Security Penetration Testing Security Bulletins Resources Compliance Partners

Developer Documents

- AWS Security Credentials
- Using Encryption in S3
- List of Secure Endpoints
- Configuring EC2 Security Groups
- Server Access Logging in S3
- Signing AWS API Requests
- Turning on CloudTrail Logging
- EC2 Security and Networking
- Security in Your Virtual Private Cloud (VPC)
- Networking in Your VPC
- AWS Identity and Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Amazon S3 Bucket Logging



<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.

AWS Security Blog

How to Use New Advanced Security Features for Amazon Cognito User Pools
by Tim Hunt | on 19 Feb 2018 | in Amazon Cognito, Mobile Services | Permalink | 0 Comments | 0 Shares

Amazon Cognito lets you easily add user sign-up, sign-in, and access control to your mobile and web apps. You can use fully managed user directories, called Amazon Cognito user pools, to create accounts for your users, allow them to sign in, and update their profiles. Your users also can sign in by using external identity [...]

[Read More](#)

How to Patch Linux Workloads on AWS
by Bas van Wijngaarden | on 15 Feb 2018 | in Amazon EC2 Systems Manager | Permalink | 0 Comments | 0 Shares

Most malware tries to compromise your systems by using a known vulnerability that the owning system maker has already patched. As best practices to help prevent malware from affecting your systems, you should apply all operating system patches and actively monitor your systems for missing patches. In this blog post, I show you how to [...]

[Read More](#)

How to Use Your Own Identity and Access Management Systems to Control Access to AWS IoT Resources
by Balazs Molnarvergyo | on 14 Feb 2018 | in AWS IoT, Partners, Identity & Access | Permalink | 0 Comments | 0 Shares

AWS IoT is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices by using the Message Queuing Telemetry Transport (MQTT) protocol, HTTP, and the MQTT over the WebSocket protocol. Every connected device must authenticate to AWS IoT, and AWS IoT must authorize all requests to determine [...]

[Read More](#)

Join Us for AWS Security Week February 20-23 in San Francisco
by Doug Lippert | on 13 Feb 2018 | in Training, Identity & Compliance | Permalink | 0 Comments | 0 Shares

Join us for AWS Security Week, February 20-23 at the AWS Pop-up Loft in San Francisco, where you can participate in four days of themed content that will help you secure your workloads on AWS. Each day will highlight a different security and compliance topic, and will include an overview session, a customer or partner speaker, [...]

[Read More](#)

New Available: Encryption at Rest for Amazon DynamoDB
by Nitin Goyal | on 09 Feb 2018 | in Amazon DynamoDB, AWS Key Management Service | Permalink | 0 Comments | 0 Shares

Today, AWS announced Amazon DynamoDB encryption at rest, a new DynamoDB feature that gives you enhanced security of your data at rest by encrypting it using your associated AWS Key Management Service encryption keys. Encryption at rest can help you meet your security requirements for regulatory compliance. You now can create an encrypted DynamoDB table anytime with a single click [...]

[Read More](#)



<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=bFMkxlAhFv8>

Securing Serverless Architectures

<https://www.youtube.com/watch?v=IKVp8d45HSU>

Account Separation and Mandatory Access Control

<https://youtu.be/42-1xpT-s6U>



Shared Responsibility Model



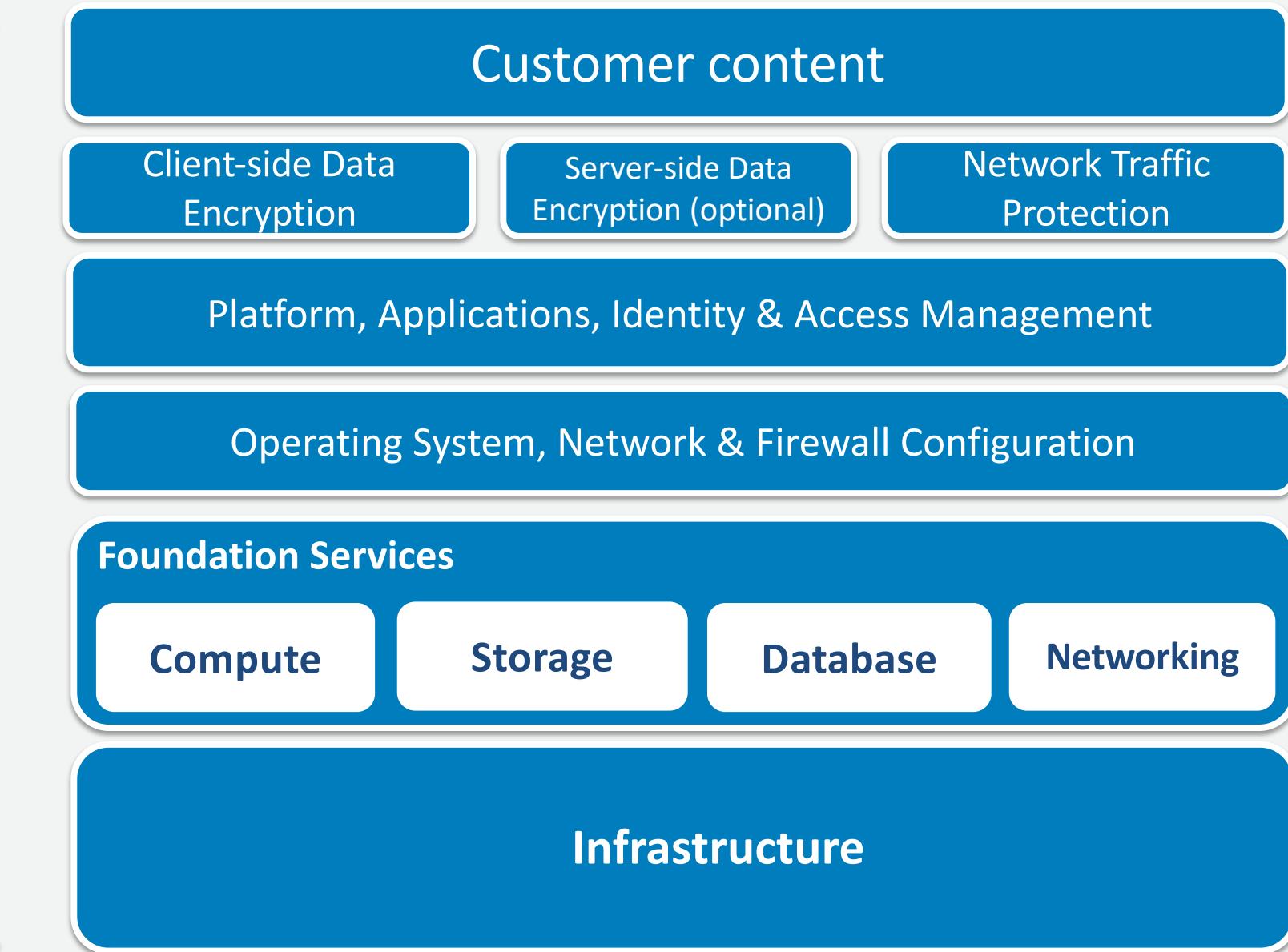
“Security OF the Cloud” - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud.

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

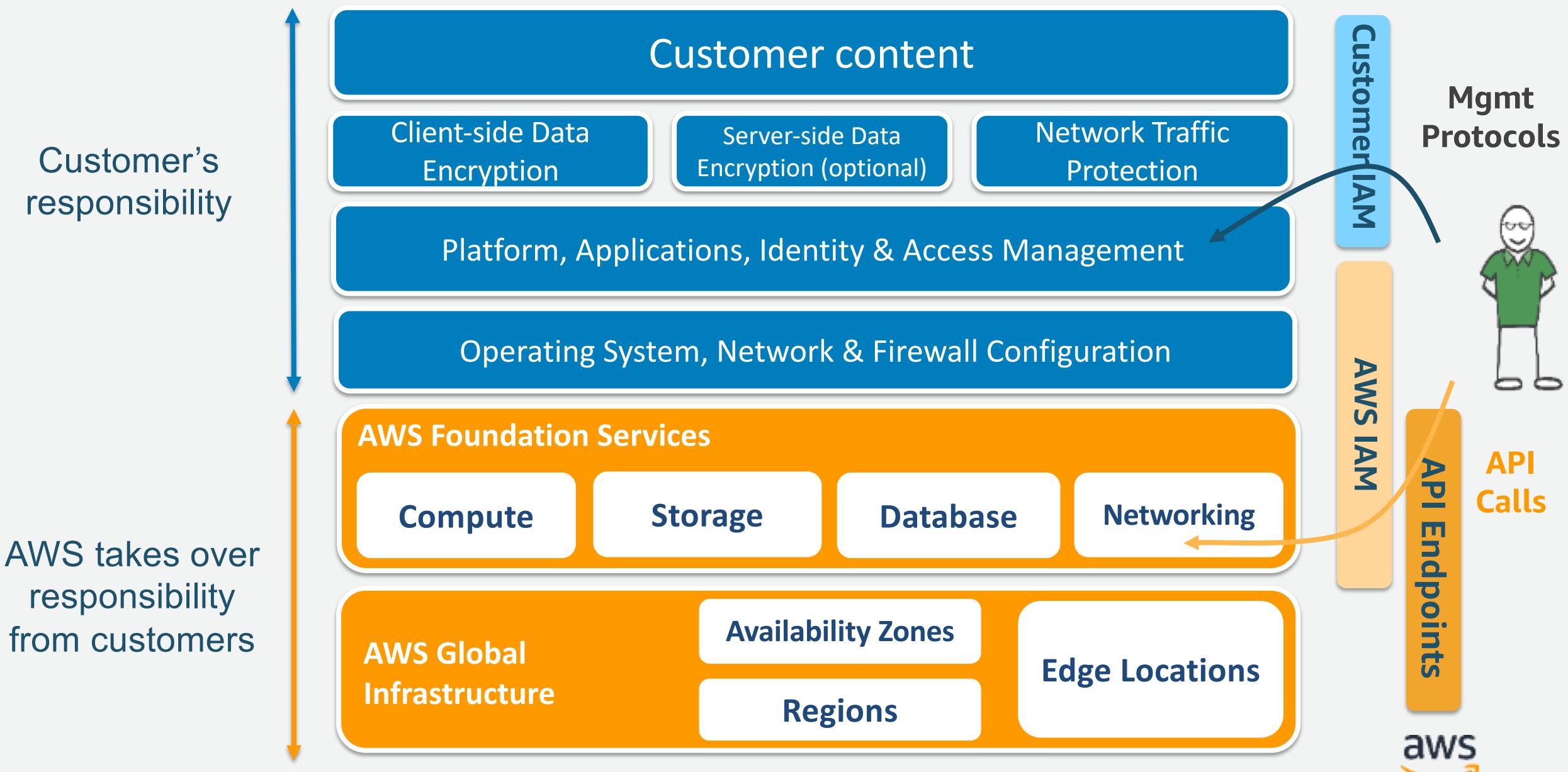


Traditional On-Premises Security Model

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



AWS Security Model when using Infrastructure Services



AWS Security Model when using Container Services

Customer's responsibility

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 takes over responsibility from customers

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Customer IAM

Mgmt Protocols

AWS IAM

API Endpoints

API Calls



AWS Security Model when using Abstracted Services

Customer's responsibility

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 takes over responsibility from customers

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

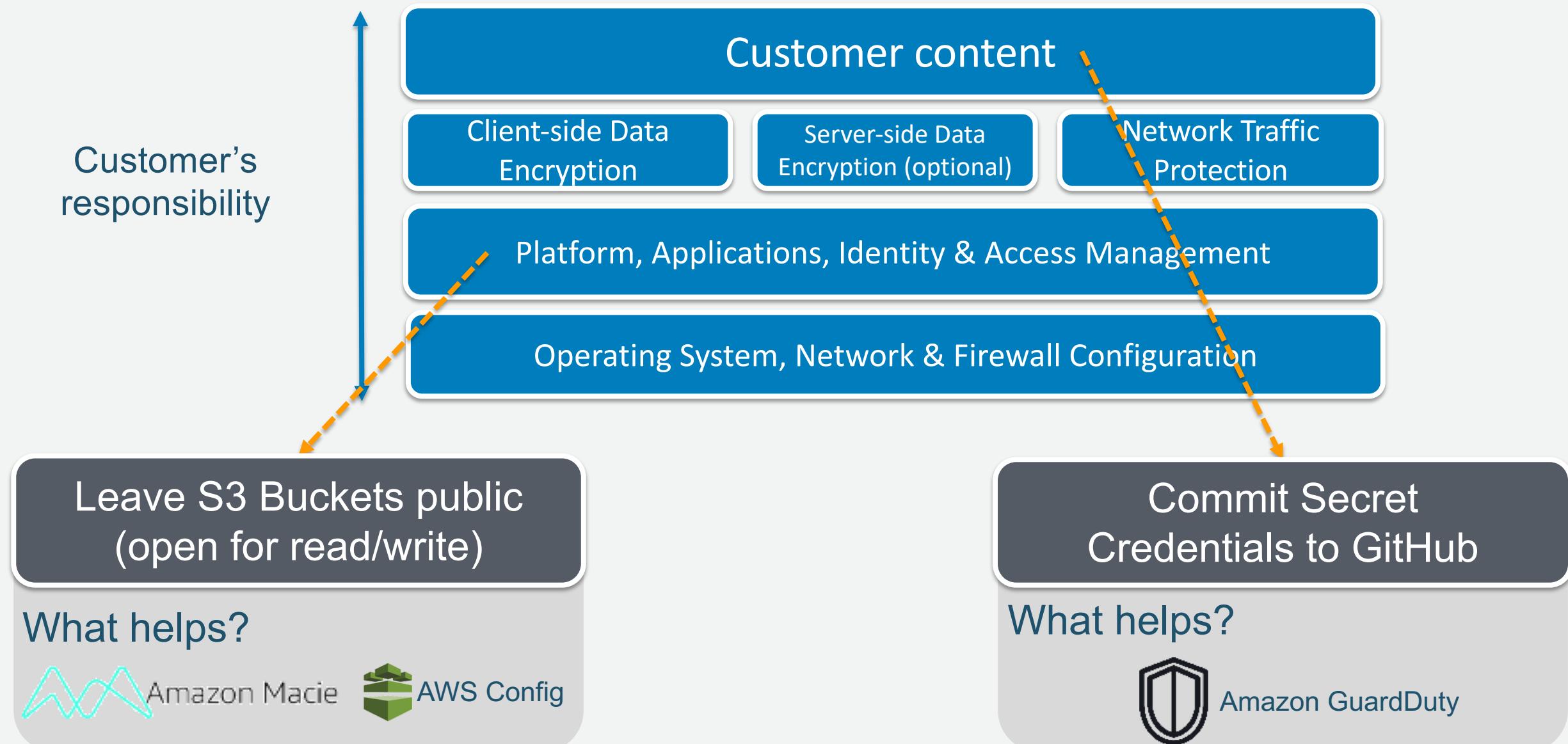
AWS IAM

API Endpoints

API Calls



More details for customer responsibility



Customer Applications

Your own accreditation

Your own certifications

Your own external audits

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

AWS Services



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/>



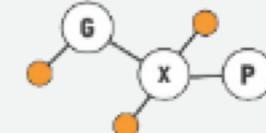
FedRAMP



NIST



FIEC



irap



FFIEC



FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT

ISO
International Organization for Standardization



PCI Security Standards Council
PARTICIPATING ORGANIZATION™

AICPA SOC
Soc for Service Organizations



TÜV AUSTRIA



aws



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

19 Regions

57 AZs

139 Edge Locations

Region & Number of Availability Zones

New Region Coming Soon



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/>





- 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



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



- 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



- 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

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical 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

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets



Questions so far?

