



Mid-Atlantic CIO Forum

Agenda

- Security of the Cloud
- Security In the Cloud
- Your Product and Services Roadmap (innovation)
- AWS and Cloud Services
- Growth and Expansion at AWS
- Questions & Discussion

Shared Responsibility

What about security **OF** the cloud?

Security Shared Responsibility Model



AWS is responsible for the security **OF** the cloud

Auditing - Comparison

on-prem vs on AWS

- Start with **bare concrete**
- Functionally **optional** – you can build a secure system without it
- Audits done by an **in-house** team
- Accountable to **yourself**
- Typically check **once a year**
- **Workload-specific** compliance checks
- Must keep pace and **invest in security** innovation

on-prem

- Start on base of **accredited services**
- Functionally necessary – **high watermark** of requirements
- Audits done by **third party** experts
- Accountable to **everyone**
- **Continuous** monitoring
- Compliance approach based on **all workload** scenarios
- **Security innovation** drives broad compliance

on AWS

What this means

- 📦 You benefit from an environment built for the most security sensitive organizations
- 📦 AWS manages 1,800+ security controls **so you don't have to**
- 📦 You get to define the right security controls for your workload sensitivity
- 📦 You always have full ownership and control of your data

AWS Assurance Programs



Meet your own security objectives



Customers

Your own accreditation



Your own certifications



Your own external audits



Customer scope and effort is **reduced**

Better results through **focused efforts**

AWS Foundation Services

Compute

Storage

Database

Networking

Built on AWS **consistent** baseline controls

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations



Navigating Shared Responsibility

Achieving **accreditation** or **certification** on AWS is **possible** but how can we help?

Industry Best Practices for Securing AWS Resources



Center for
Internet Security®

CIS Amazon Web Services Foundations

- Architecture agnostic set of security configuration best practices
- provides set-by-step implementation and assessment procedures

2.4 Ensure CloudTrail trails are integrated with CloudWatch Logs (Scored)

Profile Applicability:

- Level 1

Remediation:

Perform the following to establish the prescribed state:

Via the AWS management Console

- Sign in to the AWS Management Console and open the CloudTrail console at <https://console.aws.amazon.com/cloudtrail/>
- Under All Buckets, click on the target bucket you wish to evaluate
- Click Properties on the top right of the console
- Click Trails in the left menu
- Click on each trail where no CloudWatch Logs are defined
- Go to the CloudWatch Logs section and click on Configure
- Define a new or select an existing log group
- Click on Continue
- Configure IAM Role which will deliver CloudTrail events to CloudWatch Logs
 - Create/Select an IAM Role and Policy Name
 - Click Allow to continue

Via the CLI

```
aws cloudtrail update-trail --name <name> --cloudwatch-logs-log-group-arn <group_arn> --cloudwatch-logs-role-arn <role_arn>
```

Industry Best Practices for Securing AWS Resources



Center for
Internet Security®

- 📦 Benchmarks for AWS Marketplace
- 📦 O.S images hardened according to the trusted secure configuration baselines prescribed by CIS



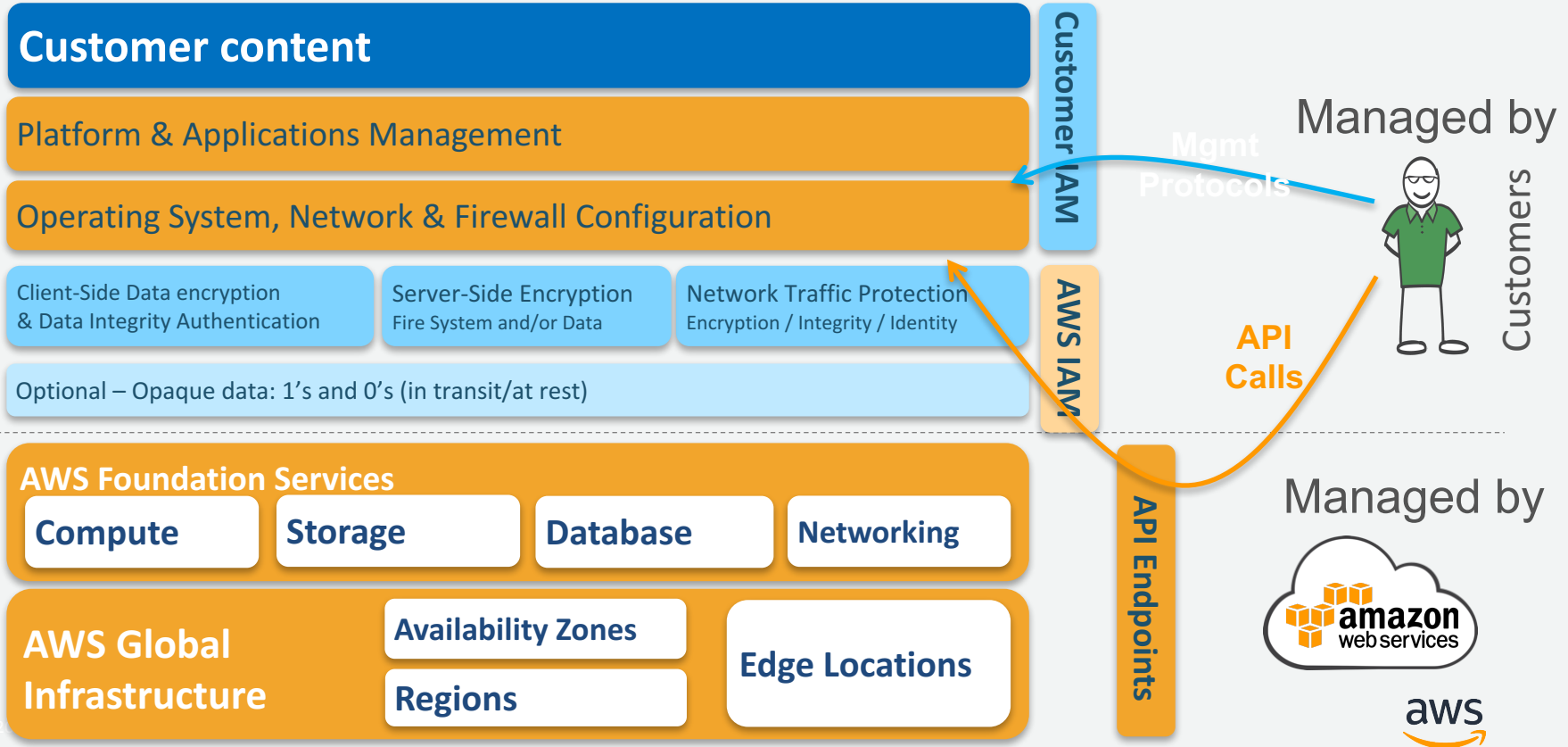
The screenshot displays three AWS Marketplace listings for CIS hardened Amazon Machine Images (AMIs). Each listing includes the Center for Internet Security logo, the product name, version, and seller information. The first listing is for CIS Amazon Linux 2015.03 x64 - v1.1.0 (HVM), version 1.1.0-1, sold by Center for Internet Security, with a rating of 4 stars. The second listing is for CIS Microsoft Windows Server 2012 R2 Benchmark v2.1.0.5 64-bit Level 1 on Windows, version 2.1.0.6, sold by Center for Internet Security, priced at \$0.02/hr for software plus EC2 and AWS usage fees. The third listing is for CIS CentOS Linux 7 x64 - v1.1.0 (HVM), version 1.1.0-1, sold by Center for Internet Security, also priced at \$0.02/hr for software plus AWS usage fees. All listings describe the AMIs as being hardened according to trusted secure configuration baselines prescribed by CIS.

Center for Internet Security **CIS Amazon Linux 2015.03 x64 - v1.1.0 (HVM)**
★★★★☆ (1) | Version 1.1.0-1 | Sold by [Center for Internet Security](#)

Center for Internet Security **CIS Microsoft Windows Server 2012 R2 Benchmark v2.1.0.5 64-bit Level 1 on Windows**
Version 2.1.0.6 | Sold by [Center for Internet Security](#)
\$0.02/hr for software + Charges for EC2 with Windows + AWS usage fees
The ability to launch instances hardened according to the trusted secure configuration baselines prescribed by the Center for Internet Security's (CIS) expert consensus ...
Windows, Windows Server 2012 R2 2012 R2 | 64-bit Amazon Machine Image (AMI)

Center for Internet Security **CIS CentOS Linux 7 x64 - v1.1.0 (HVM)**
Version 1.1.0-1 | Sold by [Center for Internet Security](#)
\$0.02/hr for software + AWS usage fees
The ability to launch instances hardened according to the trusted secure configuration baselines prescribed by the Center for Internet Security's (CIS) expert consensus ...
Linux/Unix, CentOS 7 x64 | 64-bit Amazon Machine Image (AMI)

AWS Shared Responsibility Model: for Infrastructure Services



Infrastructure Service

Example – EC2

- Foundation Services — Networking, Compute, Storage
- AWS Global Infrastructure
- AWS API Endpoints



AWS

RESPONSIBILITIES

Customers



- Customer Data
- Customer Application
- Operating System
- Network & Firewall
- Customer IAM (Corporate Directory Service)
- High Availability, Scaling
- Instance Management
- Data Protection (Transit, Rest, Backup)
- AWS IAM (Users, Groups, Roles, Policies)

AWS Shared Responsibility Model: for Container Services

Customer content

Client-Side Data encryption
& Data Integrity Authentication

Network Traffic Protection
Encryption / Integrity / Identity

Optional – Opaque data: 1's and 0's (in transit/at rest)

Firewall
Configuration

Customer IAM

AWS IAM

API Endpoints

Platform & Applications Management

Operating System, Network Configuration

AWS Foundation Services

Compute

Storage

Database

Networking

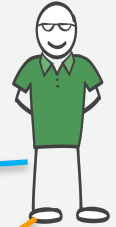
AWS Global
Infrastructure

Availability Zones

Regions

Edge Locations

Managed by



Customers

Mgmt
Protocols

API
Calls

Managed by



aws

Infrastructure Service

Example – RDS

- Foundational Services – Networking, Compute, Storage
- AWS Global Infrastructure
- AWS API Endpoints
- Operating System
- Platform / Application



AWS

RESPONSIBILITIES

Customers



- Customer Data
- Firewall (VPC)
- Customer IAM (DB Users, Table Permissions)
- AWS IAM (Users, Groups, Roles, Policies)
- High Availability
- Data Protection (Transit, Rest, Backup)
- Scaling

AWS Shared Responsibility Model: for Abstract Services

Customer content

(optional)
Opaque Data: 1's and 0's
(in flight / at rest)

Client-Side Data Encryption
& Data Integrity Authentication

Data Protection by the Platform
Protection of Data at Rest

Network Traffic Protection by the Platform
Protection of Data at in Transit

AWS IAM

Platform & Applications Management

Operating System, Network & Firewall Configuration

AWS Foundation Services

- Compute
- Storage
- Database
- Networking

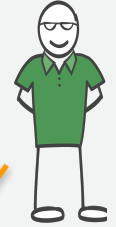
AWS Global Infrastructure

- Availability Zones
- Regions
- Edge Locations

API Endpoints

API Calls

Managed by



Customers

Managed by



Infrastructure Service

Example – S3

- Foundational Services
- AWS Global Infrastructure
- AWS API Endpoints
- Operating System
- Platform / Application
- Data Protection (Rest - SSE, Transit)
- High Availability / Scaling



AWS

Customers



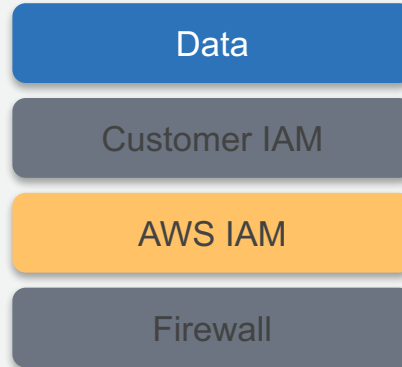
- Customer Data
- Data Protection (Rest – CSE)
- AWS IAM (Users, Groups, Roles, Policies)

Summary of Customer Responsibility in the Cloud

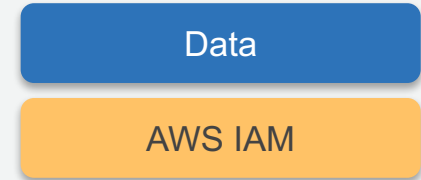
Infrastructure Services



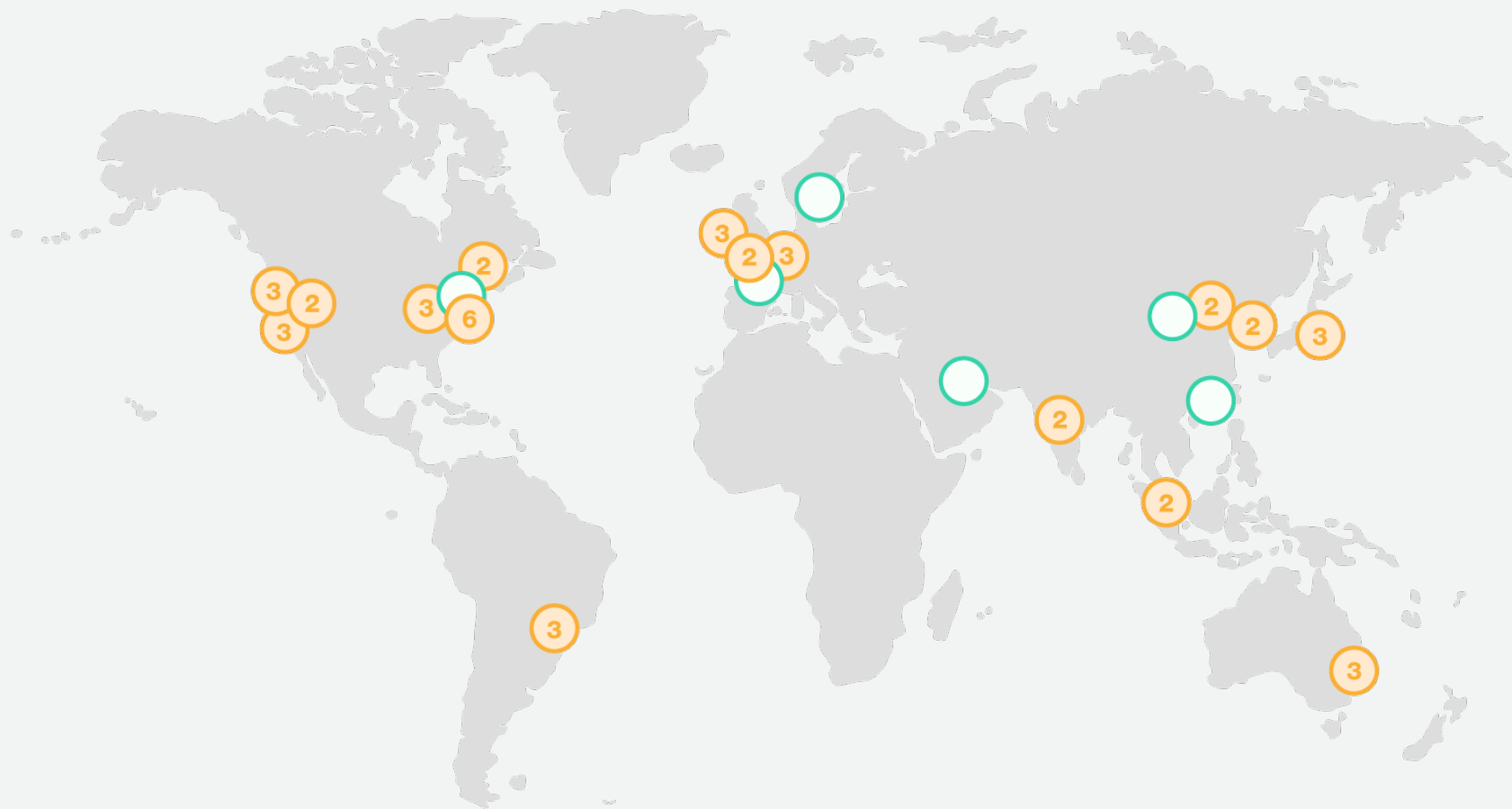
Container Services



Abstract Services

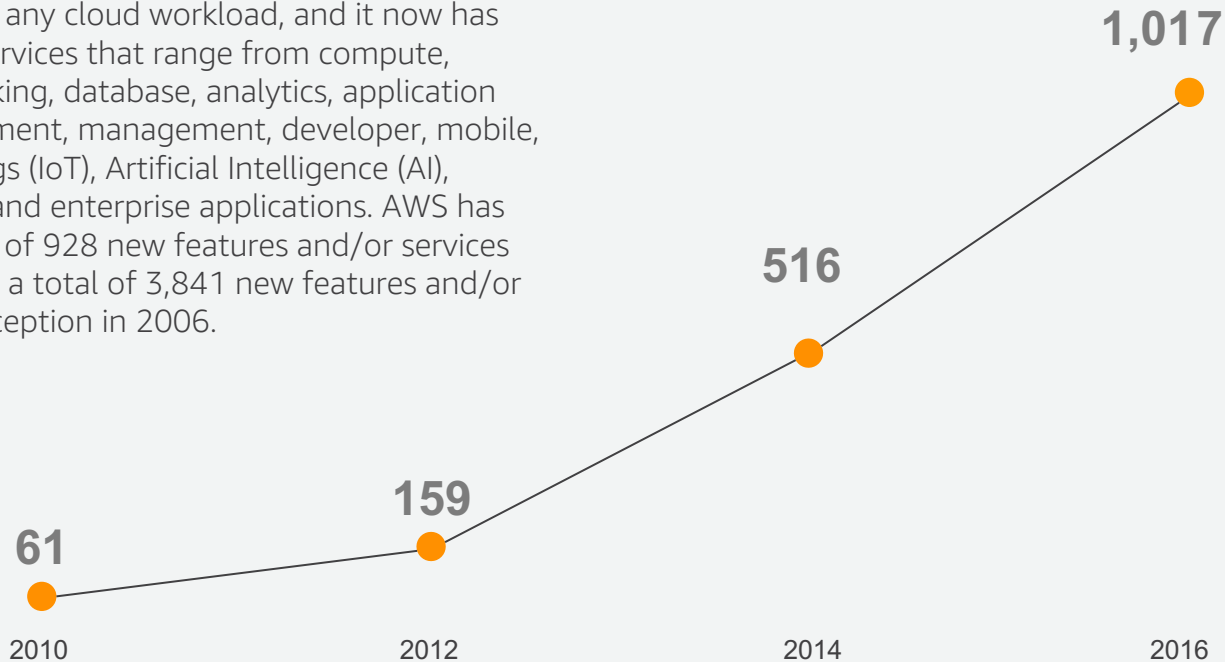


Global Infrastructure



AWS Pace of Innovation

AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 90 services that range from compute, storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid and enterprise applications. AWS has launched a total of 928 new features and/or services year to date* for a total of 3,841 new features and/or services since inception in 2006.



Thank You!