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

aws

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

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

AWS Assurance Programs

aws

Meet your own security objectives

Customers

Your own accreditation

PCI DSS LEVEL 1 SERVICE PROVIDER

Your own certifications

CSA cloud security alliance®

Your own external audits

AICPA SOC aicpa.org/soc Formerly SAS 70 Reports

Customer scope and effort is **reduced**

Better results through **focused efforts**

Built on AWS **consistent** baseline controls

amazon web services

AWS Foundation Services

Compute | Storage | Database | Networking

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

aws

Navigating Shared Responsibility

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

aws

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

1. Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/
2. Under All Buckets, click on the target bucket you wish to evaluate
3. Click Properties on the top right of the console
4. Click `Trails` in the left menu
5. Click on each trail where no `CloudWatch Logs` are defined
6. Go to the `CloudWatch Logs` section and click on `Configure`
7. Define a new or select an existing log group
8. Click on `Continue`
9. Configure IAM Role which will deliver CloudTrail events to CloudWatch Logs
    1. Create/Select an `IAM Role` and `Policy Name`
    2. 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>
```

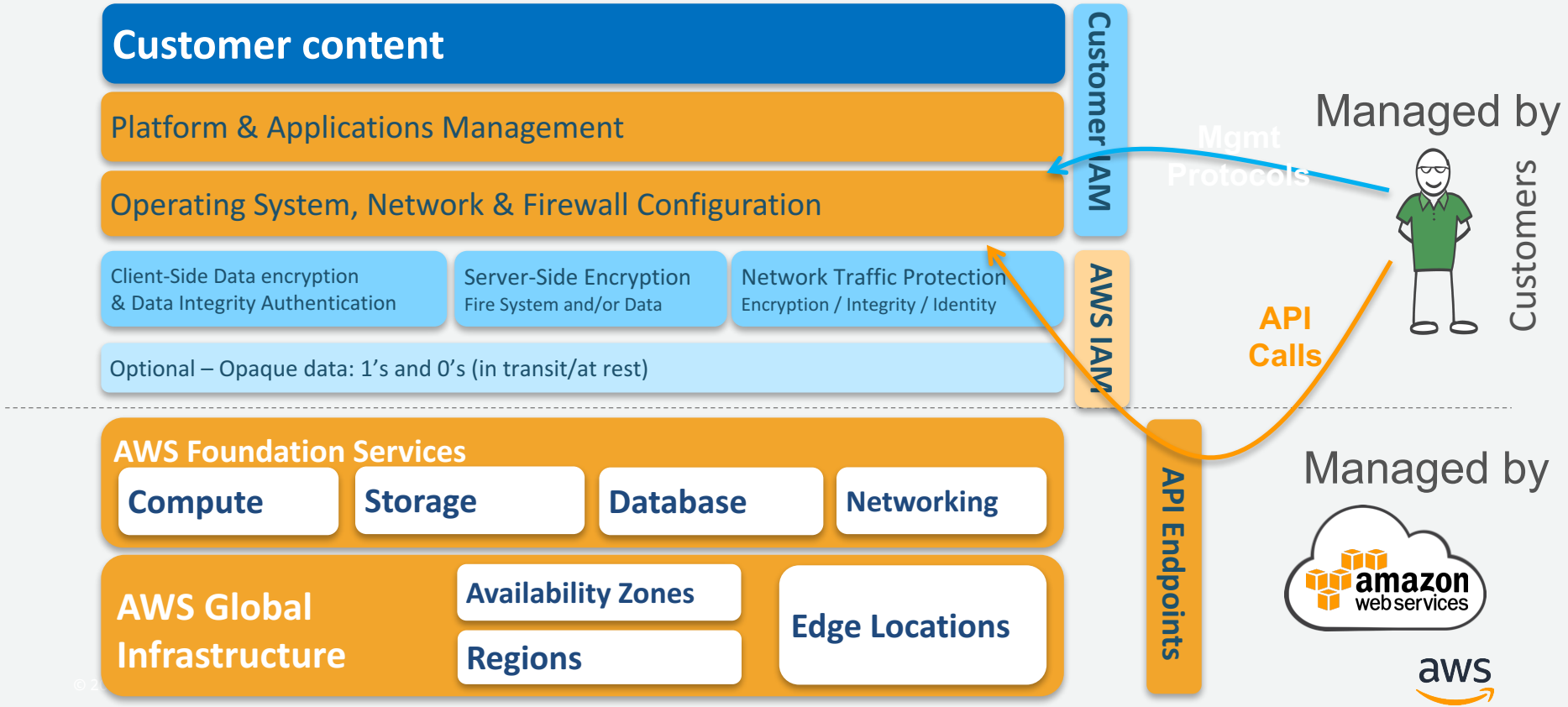
Industry Best Practices for
Securing AWS Resources

Center for Internet Security®

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

aws

AWS Shared Responsibility Model:
for Infrastructure Services



Infrastructure Service

Example – EC2

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

AWS

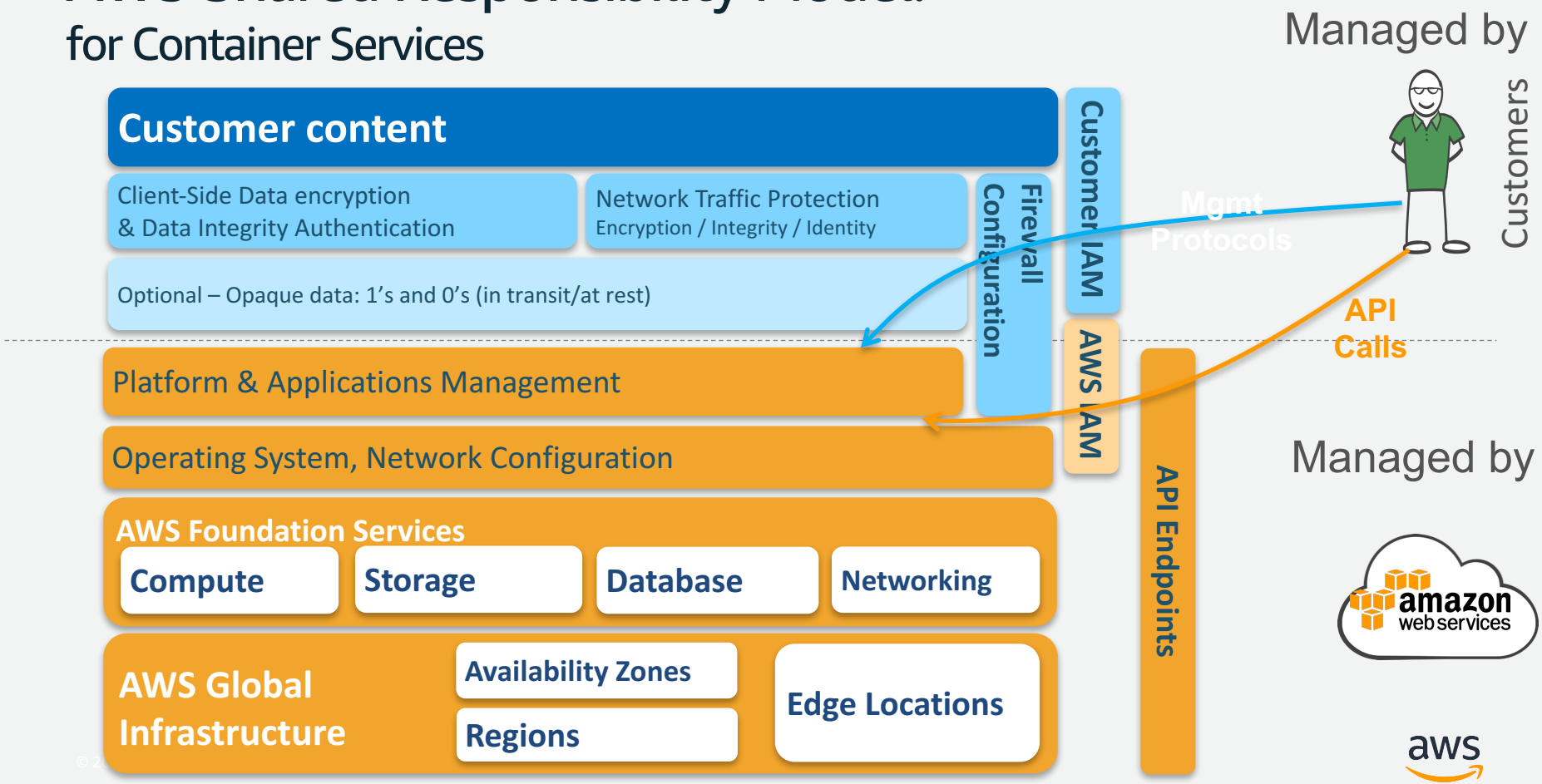
RESPONSIBILITIES

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



Infrastructure Service

Example – RDS

- Foundational Services – Networking, Compute, Storage
- AWS Global Infrastructure

- AWS API Endpoints
- Operating System
- Platform / Application

AWS

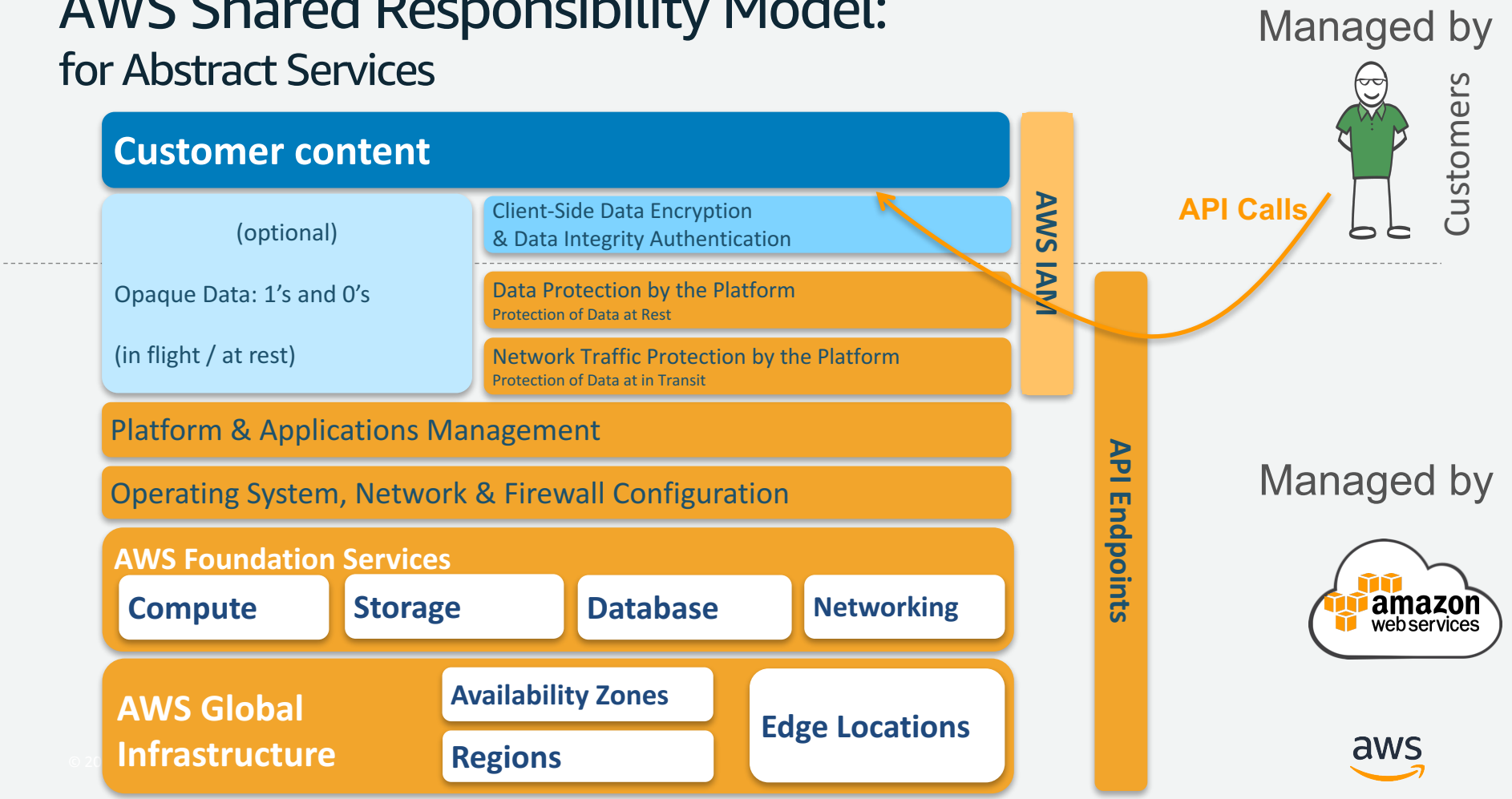
RESPONSIBILITIES

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



Infrastructure Service
Example – S3

- Foundational Services
- AWS Global Infrastructure
- AWS API Endpoints
- Operating System

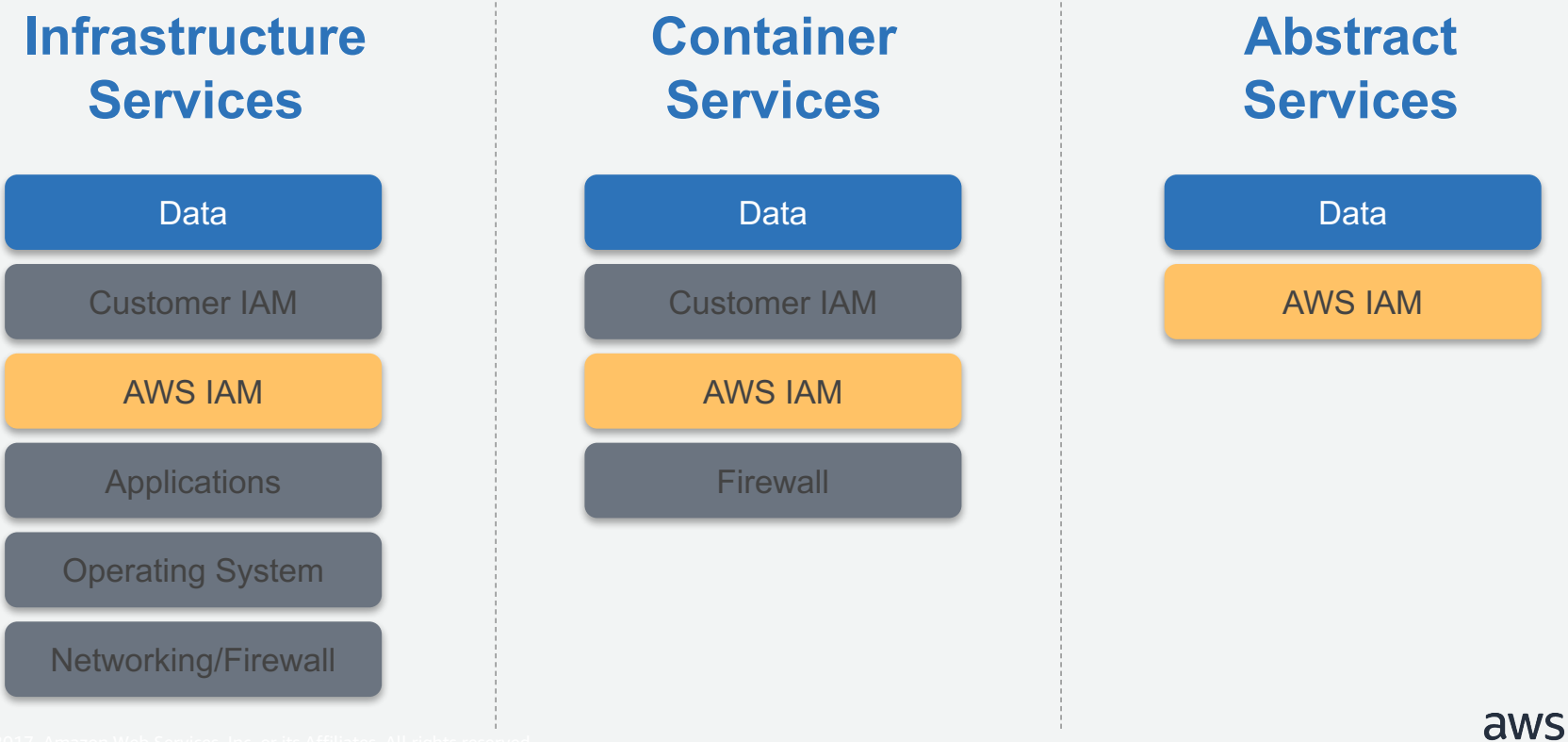
- Platform / Application
- Data Protection (Rest - SSE, Transit)
- High Availability / Scaling

AWS

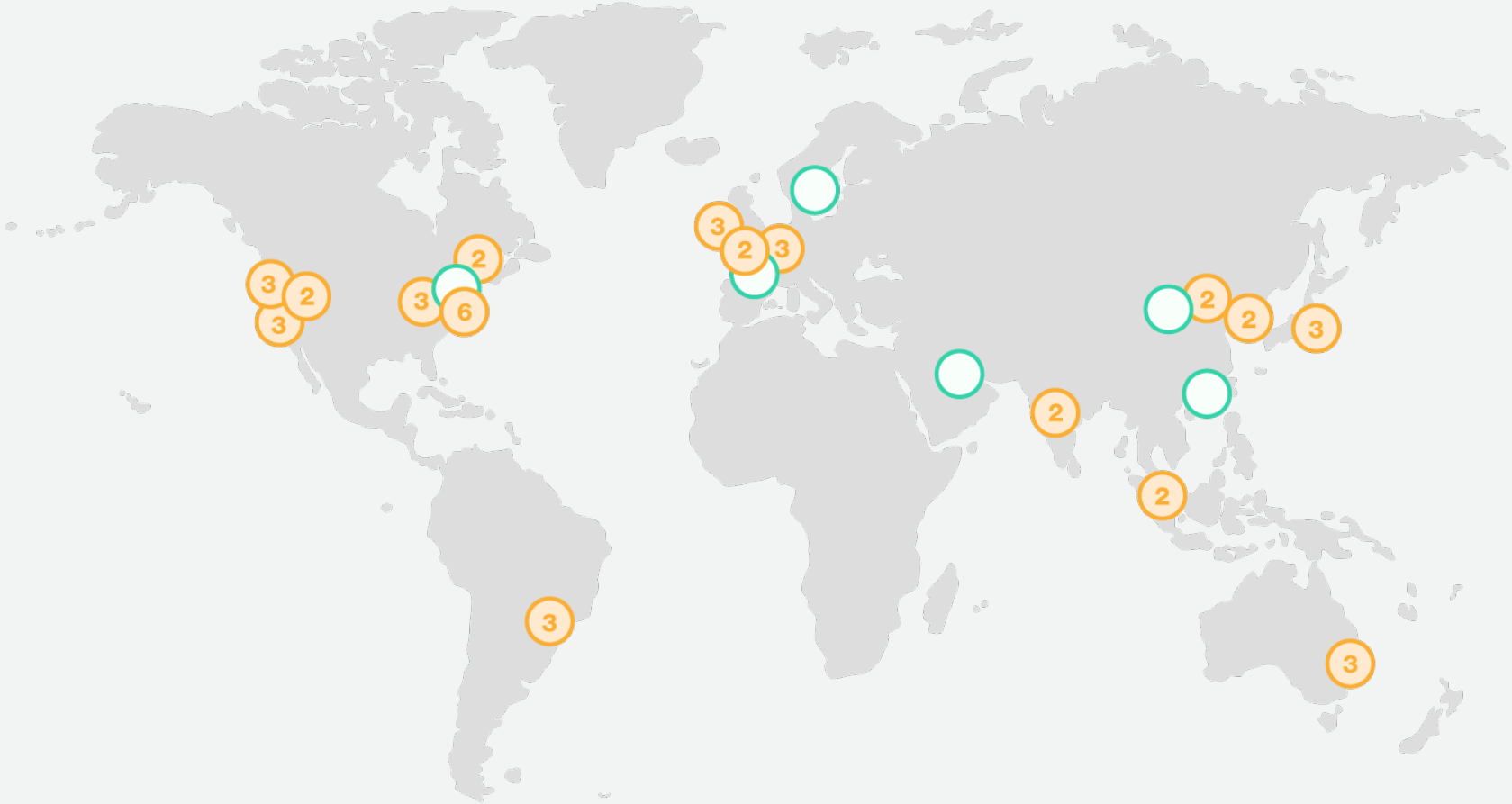
Customers

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

Summary of Customer Responsibility in the Cloud

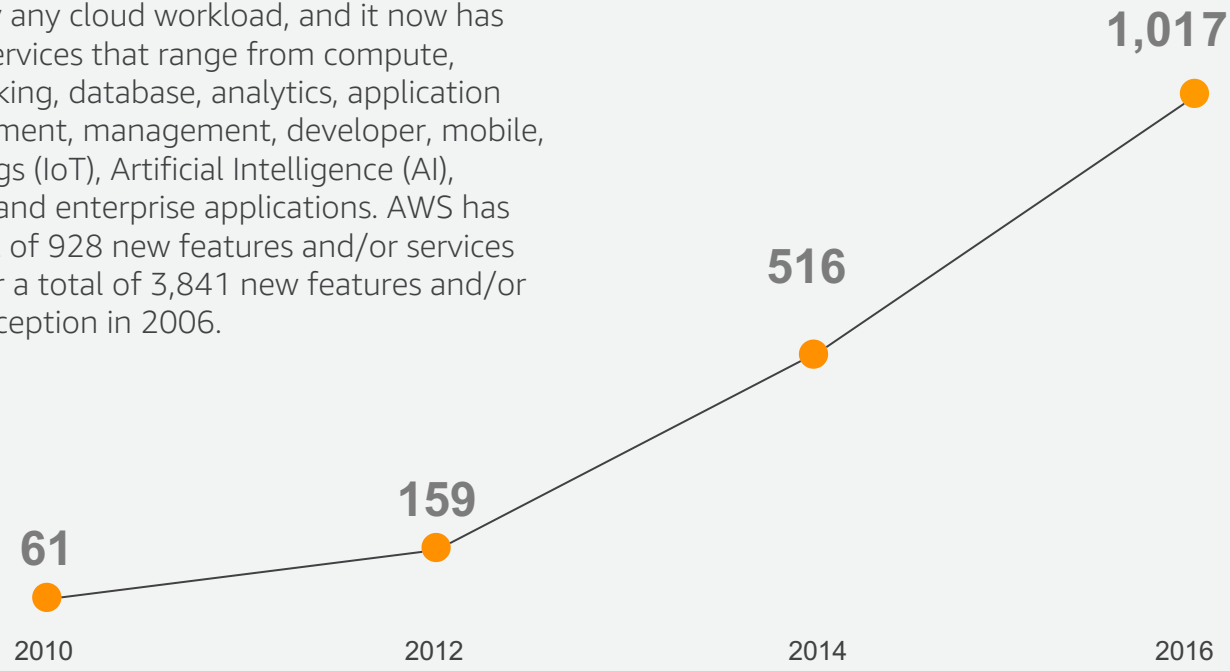


Global Infrastructure

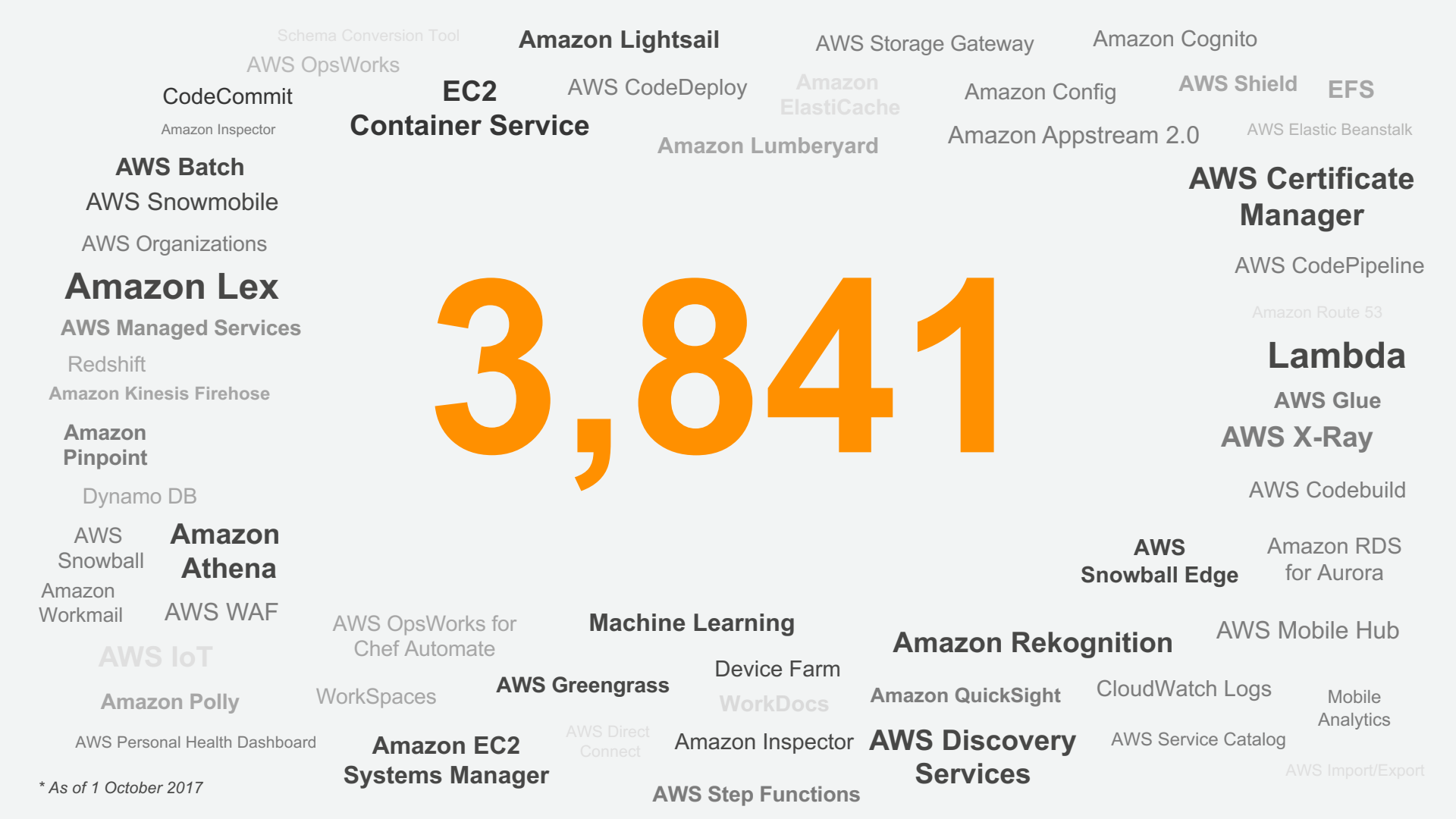


AWS Pace of Innovation

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.



** As of 1 October 2017*



** As of 1 October 2017*

Thank You!