Security & Compliance in the AWS Cloud

Richard Busby  &  Stanley Chan
APAC Partner Solutions Architect  APAC Head of Technology Partners
Amazon Web Services
September 8, 2016
Our Culture

Simple Security Controls
Easy to Get Right
Easy to Audit
Easy to Enforce
Security is **Job Zero**

- **People & Process**
- **System**
- **Network**
- **Physical**

Familiar security model

Validated by security experts

Collaboration on Enhancements

Every Customer Benefits
AWS has been continually expanding its’ services to support virtually any cloud workload and now has more than 70 services that range from compute, storage, networking, database, analytics, application services, deployment, management and mobile.
SECURITY IS SHARED
Every customer gets exactly the same service from AWS

AWS Foundation Services

- Compute
- Storage
- Database
- Networking

AWS Global Infrastructure

- Availability Zones
- Regions
- Edge Locations

AWS is responsible for the security of the Cloud

GxP
ISO 13485
AS9100
ISO/TS 16949

AWS is responsible for the security of the Cloud...
Customers **decide how to implement** their own security policies

Customers have their choice of security configurations **IN** the Cloud

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

- **AWS Foundation Services**
  - Compute
  - Storage
  - Database
  - Networking

- **AWS Global Infrastructure**
  - Availability Zones
  - Edge Locations
  - Regions

- **Customer applications & content**
- Platform, Applications, Identity & Access Management
- Operating System, Network, & Firewall Configuration
- Client-side Data Encryption
- Server-side Data Encryption
- Network Traffic Protection
SECURITY IS VISIBILITY AND AUDITABILITY
How often do you map your network?

WHAT’S IN YOUR ENVIRONMENT RIGHT NOW?
You are making API calls...

On a growing set of services around the world...

AWS CloudTrail is continuously recording API calls...

And delivering log files to you

<table>
<thead>
<tr>
<th>User</th>
<th>Action</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tim</td>
<td>Created</td>
<td>1:30pm</td>
</tr>
<tr>
<td>Sue</td>
<td>Deleted</td>
<td>2:40pm</td>
</tr>
<tr>
<td>Kat</td>
<td>Created</td>
<td>3:30pm</td>
</tr>
</tbody>
</table>
SECURITY IS CONTROL
CONTROL ....

(USERS, RESOURCES, CONTENT)
Control access and segregate duties everywhere

With AWS Identity Access Management you get to control who can do what in your AWS environment and from where

Fine-grained control of your AWS cloud with two-factor authentication

Integrate with your existing corporate directory using SAML 2.0 and single sign-on

AWS account owner

Network management

Security management

Server management

Storage management
Your data stays where you put it

13 Regions
35 Availability Zones
59 Edge Locations
Create your **own private, isolated section** of the AWS cloud

**AWS Virtual Private Cloud**
- Provision a **logically isolated** section of the AWS cloud
- You choose a **private IP range** for your VPC
- Segment this into subnets to deploy your compute instances

**AWS network security**
- AWS network will **prevent spoofing** and other common layer 2 attacks
- You **cannot sniff** anything but your own EC2 host network interface
- **Control** all external routing and connectivity
You can connect resiliently and in private to your own datacenters
AWS Key Management Service

Encryption key management and compliance made easy

One-click Encryption
Centralized key management (create, delete, view, set policies)
Enforced automatic key rotation
Visibility into any changes via CloudTrail

PCI DSS SP L1 Compliant Under-going FIPS140-2
Integrated with AWS Services (e.g. S3, EBS, RDS, Redshift, CloudTrail, EMR)
Highly Available and durable
AUDIT EVERYTHING
Innovations Are For **Auditors** Too

**Auditing-centric services and features**

- AWS Config (Rules)
- AWS Key Management Service (AWS KMS)
- AWS Trusted Advisor checks
- Last AWS sign in

- AWS CloudTrail
- IAM Credential Reports
- IAM Access Advisor
- Policies versioning
Improved Governance

Fine-grained visibility and control for accounts, resources, data

Geographic data locality
Control over regional replication

Fine-grained access control
Policies, resource level permissions, temporary credentials

Visibility into resources and usage
Service Describe* APIs and AWS CloudWatch

In-depth logging
AWS CloudTrail and Config

Control over deployment
AWS CloudFormation
COMPLIANCE
More accreditations & certifications than anyone

<table>
<thead>
<tr>
<th>ISO 9001</th>
<th>SOC 1 / ISAE 3402</th>
<th>FedRAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 9001</td>
<td>SOC 2</td>
<td>ISO 27017</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>SOC 3</td>
<td>PCI DSS Level 1</td>
</tr>
<tr>
<td>GxP</td>
<td>HIPAA</td>
<td>FIPS 140-2</td>
</tr>
<tr>
<td>ITAR</td>
<td>CJIS</td>
<td>G-Cloud</td>
</tr>
<tr>
<td>FERPA</td>
<td>DoD SRG Levels 2 &amp; 4</td>
<td>IT-Grundschutz</td>
</tr>
<tr>
<td>Section 508 / VPAT</td>
<td>MLPS Level 3</td>
<td>MPAA</td>
</tr>
<tr>
<td>NIST</td>
<td>MTCS Tier 3</td>
<td>Cloud Security Alliance</td>
</tr>
<tr>
<td>FISMA, RMF, and DIACAP</td>
<td>IRAP</td>
<td>Cyber Essentials Plus</td>
</tr>
</tbody>
</table>
Get **evidence** you can audit

- Many compliance audits require access to the state of your systems at arbitrary times (i.e. PCI, HIPAA)
- A complete inventory of all resources and their configuration attributes is available for any point in time
Data Sovereignty & Privacy

- You retain control and ownership of your content
- Choose your AWS region and adhere to data sovereignty laws
- Compliant with ISO 27001, ISO 27017, ISO 27018
- Encrypt your data using AWS Services or using your own
Vibrant Partner Ecosystem

Infrastructure Security

Logging and Monitoring

Identity and Access Control

Configuration and Vulnerability Analysis

Data Protection

SaaS
Security is Job Zero

YOU ARE BETTER IN AWS THAN YOU ARE IN YOUR OWN ENVIRONMENT

– “Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own data centers.”
  - Tom Soderstrom, CTO, NASA JPL

– “We work closely with AWS to develop a security model, which we believe enables us to operate more securely in the public cloud than we can in our own data centers.”
  - Rob Alexander, CIO, Capital One
설문 조사 이벤트

• 설문조사를 작성하시는 분들에게, AWS 티셔츠를 드립니다!

CLOUDSEC PoC 신청 이벤트

• PoC를 신청하시는 분들에게, 무료 컨설팅과 보조 배터리를 드립니다!
In order to secure your valuable data, MEGAZONE is working together with its No.1 PARTNERS, AWS and TrendMicro, in providing diverse services.
THANK YOU