How to Think About Data Security in the Cloud

Eric Docktor
Vice President, AWS Cryptography

Ken Beer
General Manager, AWS Key Management Service
What the Cloud Offers For Security

- Improves security for nearly all customers
- Delivers unprecedented visibility and control
- Simplifies the work of security and compliance
- Enables agility and speed through automation
Building blocks for your workload

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer
- Hardened service endpoints
- Rich API capabilities

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- Authentication & account management
- Authorization policies
In Cloud, Security Is a Shared Responsibility

Customers concentrate on their stack while cloud provider manages infrastructure.

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer
- Hardened service endpoints
- Rich API capabilities

+ 

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- Authentication & account management
- Authorization policies

= 

More secure and compliant systems than any single entity could normally achieve on its own

This allows your security team to focus on a subset of overall security needs that pertain directly to your data
Shared Responsibility Model - Infrastructure

Amazon Web Services (AWS) and its customers share responsibility for security, compliance, and operational controls within the AWS Cloud. AWS is responsible for the security of the cloud infrastructure that hosts customers’ applications and data, while customers are responsible for the security of the data they store and the configurations of the applications running on the AWS Cloud.

- **Infrastructure Managed by AWS**: This includes the physical hardware, networking, and software infrastructure that supports the AWS Cloud.

- **Applications Managed by Customers**: This includes applications, data, and workloads that are hosted and managed by customers within the AWS Cloud.

### AWS Services and Features

- **Compute**: AWS services like EC2, Lambda, and Fargate
- **Storage**: S3, EFS, and Glacier
- **Databases**: RDS, DynamoDB, and Redshift
- **Networking**: VPC, Route 53, and CloudFront

### Security and Compliance

- **Customer Data Security**: Including encryption and access controls.
- **Platform & Application Management**: Customers are responsible for managing their own applications and configurations.
- **Operating System, Network, & Firewall Configuration**: Customers manage the configurations and security of these aspects.

### Managing Responsibility

- **Managed by AWS Customers**: This area includes all aspects of the cloud infrastructure that are not directly managed by AWS, including the applications and data they host.

- **Managed by Amazon Web Services**: This encompasses the security and operational controls for the underlying infrastructure.

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Shared Responsibility – Platform Services

Managed by AWS Customers

Managed by Amazon Web Services
Global Compliance Schemes

FedRAMP

Department of Defense - United States of America

HIPAA

NIST

PCI Security Standards Council

CIS

C5

ITAR

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Global Compliance Schemes
Leverage the work your provider has already done

<table>
<thead>
<tr>
<th>Certifications / Attestations</th>
<th>Laws, Regulations, and Privacy</th>
<th>Alignments and Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>C5 [Germany]</td>
<td>CISPE</td>
<td>CIS</td>
</tr>
<tr>
<td>Cyber Essentials Plus [UK]</td>
<td>DNB [Netherlands]</td>
<td>CJIS</td>
</tr>
<tr>
<td>DoD SRG</td>
<td>EU Model Clauses</td>
<td>CSA</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>FERPA</td>
<td>ENS [Spain]</td>
</tr>
<tr>
<td>FIPS</td>
<td>GLBA</td>
<td>EU-US Privacy Shield</td>
</tr>
<tr>
<td>IRAP [Australia]</td>
<td>HIPAA</td>
<td>FISC [Japan]</td>
</tr>
<tr>
<td>ISO 9001</td>
<td>HITECH</td>
<td>FISMA</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>IRS 1075</td>
<td>G-Cloud [UK]</td>
</tr>
<tr>
<td>ISO 27017</td>
<td>ITAR</td>
<td>GxP (FDA CFR 21 Part 11)</td>
</tr>
<tr>
<td>ISO 27018</td>
<td>My Number Act [Japan]</td>
<td>ICREA</td>
</tr>
<tr>
<td>MTCS [Singapore]</td>
<td>VPAT / Section 508</td>
<td>MITA 3.0</td>
</tr>
<tr>
<td>PCI DSS Level 1</td>
<td>EU Data Protection Directive [EU]</td>
<td>MPAA</td>
</tr>
<tr>
<td>SEC Rule 17-a-4(f)</td>
<td>Privacy Act [Australia &amp; New Zealand]</td>
<td>NIST</td>
</tr>
<tr>
<td>SOC 1</td>
<td>PDPA - 2010 [Malaysia]</td>
<td>PHR</td>
</tr>
<tr>
<td>SOC 2</td>
<td>PDPA - 2012 [Singapore]</td>
<td>Uptime Institute Tiers</td>
</tr>
<tr>
<td>SOC 3</td>
<td>PIPEDA [Canada]</td>
<td>UK Cloud Security Principles</td>
</tr>
<tr>
<td>Spanish DPA Authorization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Applying the Shared Responsibility Model

Security of the cloud
- Security measures the provider implements and operates
- Provider’s security standards shown by certifications & attestations

Security in the cloud
- Security measures that the customer implements and operates
- Certifications and attestations can be used by customers when undertaking risk assessments or using frameworks
Security Controls You Define and Operate

Access Control
- You control who can do what to which resources under which conditions

Visibility-Audit-Remediation
- No hidden resources – everything discoverable via an API

Automate
- Security through code
- Enforce the use of templates – no cowboy code
Building Blocks: Starting Small

Compute

AI/ML

Is it secure?

Logging

Storage

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Building Blocks: Finished Application

Re-using secure blocks minimizes chance of data breach across the entire workload
Securing Your First Workload
Cloud Access Control – Expressing Policy

Identity
   Must be authenticated by provider, may be federated from your network

Effect
   Allow vs. Deny

Action/Scope
   API to create, read, update, or delete a resource

Resource
   Instance, storage, database, networking group, identity, encryption key, etc.

Condition
   SourceIP, time, MFA, custom metadata in API request, etc.
Cloud Access Control – Policy Requirements

- Human-readable
- Flexible semantics
- Consistent across cloud provider’s services
- Access control on access control
  - Only privileged users can create/edit policy
  - No escalation of privilege
Where Your Architecture Might Be Headed
Applying Access Control to A Sample Workload

Load Balancer and Web Front-End

Application/Compute Instances

Database

Object Store
Load Balancer and Web Front-End

You own:
- Routing rules
- Protocols/Ports
- Targets behind load balancer

Cloud Provider owns:
- Availability, throughput, host security

Your choice:
- TLS config
  - Generate/store certificates?
  - Automate certificate rotation?
Application/Compute Instances

You own:
- Protocols/Ports
- CPU/Memory/Storage size
- OS-level authentication
- Automatic scaling rules
- Application logs

Cloud Provider owns:
- Availability, IOPS, host security

Your choice:
- Operating system deployment/patching?
Data Storage

You own:
- Storage size
- Access rules

Cloud Provider owns:
- Availability, durability, host security, logs

Your choice:
- DB engine?
- Storage type (block, file, object)?
Sample Access Policy - Who Can Create Compute Resources

{"Statement":[
  "Identity": "ComputeAdministrator",
  "Effect": "Allow",
  "Action": [
    "CreateImage",
    "RunInstance",
    "CreateSnapshot"],
  "Resource": "instance/i-1234567890abcdef0",
  "Condition": {
    "StringEquals": {"ResourceTag": "ProjectName"}}}

When One Set of Access Controls Isn’t Enough

Encryption
Your cloud provider ensures the plaintext key(s) can only be used by identities you define.
Encryption/Decryption as Access Policy

Both policies must be true to grant access to run your workload.
Quis custodiet ipsos custodes?

1. You define the resource configuration and access policies.
2. Your cloud provider faithfully executes your configuration and access policies.
3. The cloud provider’s auditors ensure the cloud providers are faithfully executing your configuration and access policies and not looking at your data.
4. Your auditors ensure you define your resource configuration and access policies correctly.
5. GOTO 1
Automating Security Is The Only Way To Safely Scale

Security by Design allows you to automate deployment, configuration, audit, and remediation of your workloads.
Thank you!