Security by Design
Running Compliant workloads in AWS
Evolution of security & compliance at AWS

AWS certifications

Customer enabler docs

Workbook for PCI Compliance in the AWS Cloud

Customer case studies

Security by Design tech (SbD)

AWS IAM

AWS KMS

AWS CloudHSM

AWS CloudTrail

AWS Config
Security by Design (SbD) is a modern, security assurance approach that formalizes AWS account design, automates security controls, and streamlines auditing. It is a systematic approach to ensure security; instead of relying on after-the-fact auditing, SbD provides control insights throughout the IT management process.
Why - Security by Design

- Organizations continue to labor over demonstrating their alignment with security, compliance and audits assertions across regulated environments.

- Additionally, the majority of technology governance processes relies predominantly on administrative and operational security controls with Limited technology enforcement.

- Traditional Technology Governance isn’t working to reduce data breach's across regulated industries (e.g. Health, Finance and Public Sector)
Impact of Security by Design

• SbD - Scripting your governance policy
• Result: Reliable technical implementation of administrative controls
The SbD Approach

A Standardized Package Which:

• Automates implementation of system-specific security controls
• Deploys an infrastructure which supports multiple security requirements (e.g. FISMA, CJIS, HIPAA, PCI, FFIEC etc.)
• Provides a quick repeatable process for deploying and documenting baseline architectures for specific use cases
• Can be used as a organizationally defined standard which meets several security control requirements
Security by Design (SbD)

AWS Config Rules

AWS GoldBase

Amazon Inspector
Elements of a secure architecture

1. Create a Golden Environment
2. Enforce Service Catalog
3. Create Permissions to Use AWS Services
AWS GoldBase

Network Architectural Diagrams
Create a Golden Environment

Understand the configuration use of AWS services, for example:

<table>
<thead>
<tr>
<th>S3</th>
<th>EBS</th>
<th>Redshift</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force SSE</td>
<td>Define Volume type</td>
<td>Cluster Type (Single or Multi)</td>
</tr>
<tr>
<td>Turn on logging</td>
<td>Volume size limits</td>
<td>Encryption (KMS or HSM)</td>
</tr>
<tr>
<td>Specify retention</td>
<td>IOPS performance (Input/Output)</td>
<td>VPC location</td>
</tr>
<tr>
<td>Set Glacier archiving</td>
<td>Data location - regions</td>
<td>External Access (Yes/No)</td>
</tr>
<tr>
<td>Prevent external access</td>
<td>Snapshot (Backup) ID</td>
<td>Security Groups applied</td>
</tr>
<tr>
<td>Specify overriding permissions</td>
<td>Encryption requirements</td>
<td>Create SNS topic</td>
</tr>
<tr>
<td>Set event notifications</td>
<td></td>
<td>Enforce CloudWatch alarms</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S3</th>
<th>EBS</th>
<th>Redshift</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1. Create a Golden Environment</td>
</tr>
</tbody>
</table>
Enforce AWS Service Catalog

- Allows administrators to create and manage approved catalogs of resources (products) that end users can access via a personalized portal
- A Service Catalog **Product** is a deployable CloudFormation template

Provisioning Team creates and manages Service Catalog Products built from CloudFormation Templates
Create Permissions to Use AWS

Least Privilege Access -

• Gives workload owners permissions to deploy templates, nothing more
Additional Enterprise-wide Benefits

• Accelerates - The AWS learning process by providing complex example systems that conform to leading practices

• Decreases - The Level of Effort (LoE) in producing security related documentation through automation of reporting

• Enhances - Enterprise security through automation and integration with security tools (e.g. AWS Config Rules, Inspector, Evident.io and Splunk)

• Verifiable – Evidence gathering capability is enhanced by using AWS and external partners (e.g. Allgress and Veris Group)
SbD Operating Principles

- Separation of duties
- Different personnel across service lines
- Least privilege
SbD enables secure operational automation

Visibility through automation

Shrinking the protection boundaries

Ubiquitous encryption
SbD - Modernization of Technology Governance

*Construct, Implement and Run secure workloads through automation in the cloud*

AWS provides Governance, Risk, and Compliance teams:

1. The right SbD tech - AWS
2. SbD Whitepaper
3. AWS GoldBase
   1. Security controls implementation matrix
   2. Architecture diagrams
   3. AWS CloudFormation templates
      1. Industry compliance templates (PCI, NIST 800-53, HIPAA, FFIEC, and CJIS)
      4. User Guides and deployment instructions
4. AWS Config Rules – auditing
5. AWS Inspector – advanced in-host security and audit
6. Training
Thank You

awscompliance@amazon.com
aws.amazon.com/compliance