

# Understanding AWS Security

---



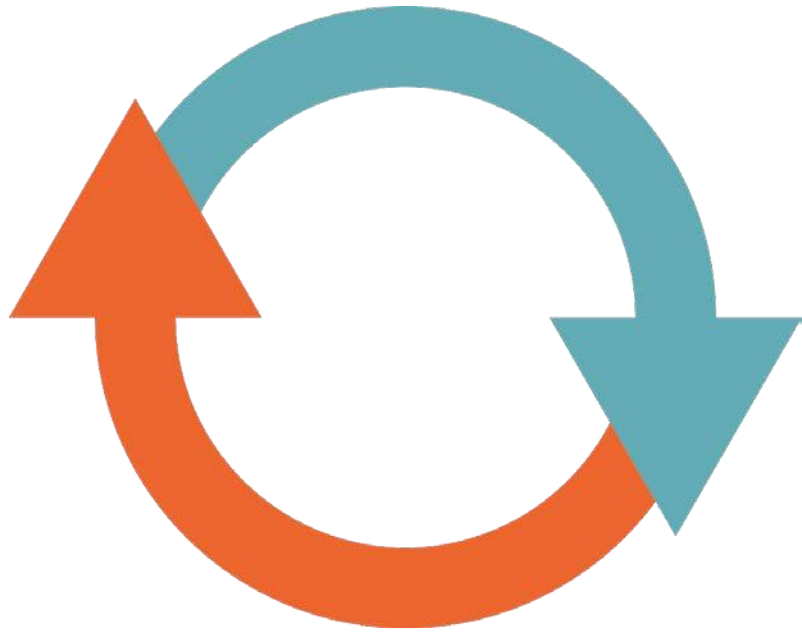


Secret locations

Controlled physical access

Best in class datacenter  
security

Video surveillance



Hardware refresh cycle to avoid  
component failure

Properly decommissioned  
storage

Always on monitoring system

# Security Certifications and Compliance

AWS	
HIPAA	FIPS 140-2
SOC 1/SSAE 16/ISAE 3402	CSA
SOC 2	MPAA
SOC 3	
PCI DSS Level 1	
ISO 27001	
FedRAMP(SM)	
DIACAP and FISMA	
ITAR	



AWS Compliance:

<http://aws.amazon.com/compliance/>

# Shared Security Responsibility

## AWS Responsibility

Virtual host security

Storage security

Network security

Data center security

Database security

## Our Responsibility

AWS account security (MFA, API)

Operating system

Database

Applications

Data encryption

Authentication

Network integrity

# Security Methods and Connectivity

Virtual Private  
Cloud (VPC)

Dedicated  
Connectivity

Encryption

Web Application  
Firewalls (WAF)

DDoS Mitigation

Dedicated Servers

# Security Methods and Connectivity

Inventory and  
Configuration

Monitoring and  
Logging

Penetration Testing

# Identity and Access Management (IAM)



User and service  
management



Controls access  
to AWS  
resources



Multi-factor  
authentication



API access

AWS IAM:

<http://aws.amazon.com/iam/>



# Users, Groups, Roles, and Policies



A diagram consisting of four colored squares arranged in a 2x2 grid. The top-left square is blue and contains the word 'Users'. The top-right square is maroon and contains the word 'Groups'. The bottom-left square is gray and contains the word 'Roles'. The bottom-right square is green and contains the word 'Policies'.

Users

Groups

Roles

Policies

# Summary



Physical Access

Security Certification

Shared Responsibility

Security Capabilities

IAM

