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	

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS
PCI DSS COMPLIANT
LEVEL 1 SERVICE PROVIDER
ISO
AICPA Service Organization Control Reports
AICPA
SOC
aicpa.org/soc
Formerly SAS 70 Reports
HIPAA
FISMA
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FIPS 140-2
FIPS
CRYPTOGRAPHY
International Traffic in Arms Regulations Compliant
ITAR
auditwerx
ISAE 3402
TYPE 2

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

Users

Groups

Roles

Policies

Summary

Physical Access

Security Certification

Shared Responsibility

Security Capabilities

IAM