AWS Shared Responsibility Model: Security in Partnership

Security in the cloud requires a partnership between AWS and its customers. This presentation explores how the AWS Shared Responsibility Model defines and clarifies these crucial security boundaries, helping organizations better protect their cloud workloads through clear responsibility allocation.

AWS Responsibilities: Security OF the Cloud

AWS takes responsibility for protecting the infrastructure that runs all services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS Cloud services.

Global Infrastructure

Physical security of 30+ regions, 99+ availability zones, and 400+ edge locations worldwide

Virtualization Infrastructure

Hypervisor management, instance isolation, and storage service encryption

Network Security

DDoS protection, automatic encryption of traffic between AWS facilities, and intrusion detection

AWS implements rigorous third-party audits for over 50 compliance programs to validate the security controls that protect their infrastructure.

Customer Responsibilities: Security IN the Cloud

Customers maintain complete control—and responsibility—over their content and how they secure it within AWS services.

Data Protection

Customers must implement appropriate data classification, encryption at rest and in transit, and backup strategies. This includes managing AWS KMS keys and client-side encryption options.

Identity & Access

Creating IAM users, implementing MFA, rotating credentials, applying least privilege principles, and configuring service-specific access policies are customer responsibilities.

Network Controls

Customers must configure VPCs, subnets, security groups, network ACLs, and implement proper network segmentation according to security requirements.

The degree of customer responsibility varies depending on the specific AWS services used, but customers always retain control over their data.

Service Types and Shifting Responsibilities

1

Infrastructure as a Service (IaaS)

With services like EC2, EBS, and VPC, customers manage guest OS, applications, data, and most security configurations. AWS only manages the underlying physical infrastructure.

Examples: EC2, EBS, VPC

2

Platform as a Service (PaaS)

AWS manages more components including OS, middleware, and runtime environment. Customers focus on application code and data.

Examples: RDS, Elastic Beanstalk, EMR

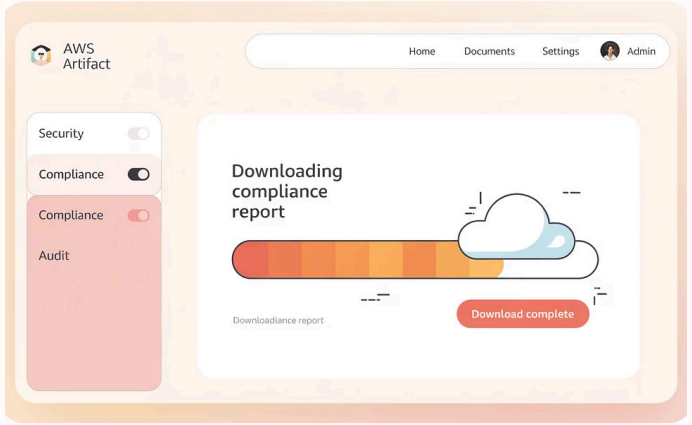
3

Software as a Service (SaaS)

Customers primarily manage data and access within the application. AWS handles virtually all infrastructure and application management.

Examples: Amazon WorkMail, Amazon Chime, Amazon Connect

Compliance Tools and Frameworks

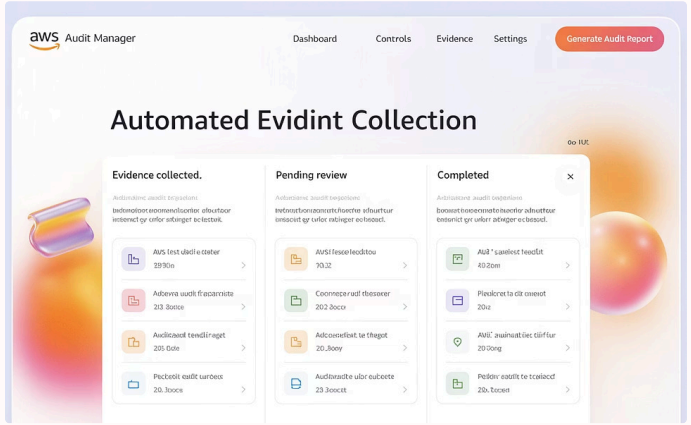


AWS Artifact

Self-service portal providing on-demand access to AWS' compliance reports. Download SOC reports, PCI certifications, and ISO certifications to support your own compliance requirements.

AWS Config

Continuously monitors and records AWS resource configurations, allowing assessment against desired configurations and compliance rules. Automates remediation for non-compliant resources.



AWS Audit Manager

Continuously collects evidence relevant to your compliance requirements, mapping AWS resource data to specific controls. Simplifies audit preparation and reduces manual effort.

These tools help customers demonstrate compliance with various regulatory standards including HIPAA, GDPR, PCI-DSS, FedRAMP, and many others.

Case Study: Financial Services Firm Implements Shared Responsibility

Challenge

A mid-sized financial services company needed to migrate core banking applications to AWS while maintaining strict compliance with financial regulations.

Approach

Assessment

Mapped all regulatory requirements to specific AWS and customer responsibilities

Implementation

Deployed AWS Config, CloudTrail, and GuardDuty for continuous compliance monitoring

Automation

Created automated remediation for common compliance violations

Results

60%

Reduction in compliance overhead

90%

Automated security controls

40%

Decrease in audit duration

Best Practices for Effective Responsibility Management

Map Responsibilities

Create a detailed matrix mapping each compliance requirement and security control to either AWS or your organization. Update this map as you adopt new services or face new regulatory requirements.

Implement Controls

Deploy technical controls using services like AWS Config Rules, GuardDuty, Security Hub, and CloudTrail. Establish administrative controls through documented policies and procedures.

Automate Everywhere

Implement Infrastructure as Code, automated compliance checking, and auto-remediation for common issues. Use AWS Security Hub to centralize security findings and automate responses.

Monitor & Improve

Continuously monitor your security posture with CloudWatch, Config, and third-party tools. Regularly review and update your security strategy based on new AWS capabilities and evolving threats.

Conclusion: Leveraging the Shared Responsibility Model

Key Takeaways

- The Shared Responsibility Model clearly delineates security duties between AWS and customers
- Customer responsibilities shift depending on service type (IaaS, PaaS, SaaS)
- AWS provides robust tools to help manage your security responsibilities
- Security is a continuous journey requiring regular assessment and improvement

Next Steps

- Conduct a responsibility mapping exercise for your specific AWS environment
- Explore AWS security services that can help automate your responsibilities
- Consider AWS Security Hub for centralized security management

Learn More | Try Free Test

> "Security is a shared responsibility between AWS and you. When you clearly understand your security responsibilities, you can build more secure applications and achieve better compliance outcomes."