
# Introduction to AWS Security

***July 2015***

# Table of Contents

# Introduction

Amazon Web Services (AWS) delivers a scalable cloud computing platform designed for high availability and dependability, providing the tools that enable you to run a wide range of applications. Helping to protect the confidentiality, integrity, and availability of your systems and data is of the utmost importance to AWS, as is maintaining your trust and confidence. This document is intended to provide an introduction to AWS's approach to security, including the controls in the AWS environment and some of the products and features that AWS makes available to customers to meet your security objectives.

## Security of the AWS Infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24x7. AWS ensures that these controls are replicated in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient infrastructure, designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads you deploy in AWS (see Figure 1). This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public.

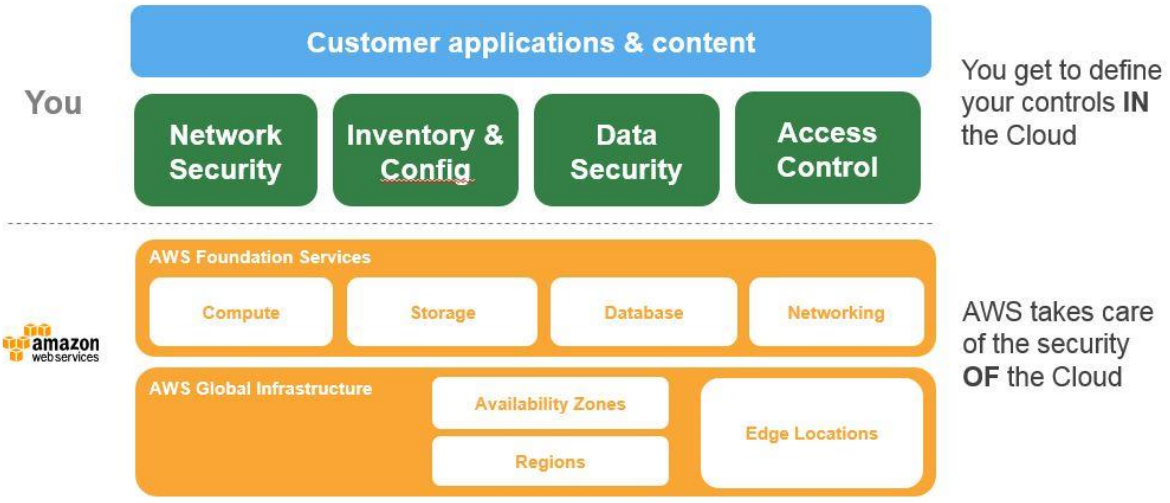


**Figure 1. AWS Shared Security Responsibility Model**

## Security Products and Features

AWS and its partners offer a wide range of tools and features to help you to meet your security objectives. These tools mirror the familiar controls you deploy within your on-premises environments. AWS provides security-specific tools and features across network security, configuration management, access control and data security. In addition, AWS provides monitoring and logging tools to can provide full visibility into what is happening in your environment.

### Network Security

AWS provides several security capabilities and services to increase privacy and control network access. These include:

- Built-in firewalls that allow you to create private networks within AWS, and control network access to your instances and subnets
- Encryption in transit with TLS across all services
- Connectivity options that enable private, or dedicated, connections from your office or on-premises environment
- DDoS mitigation technologies as part of your auto-scaling or content delivery strategy

### Inventory and Configuration Management

AWS offers a range of tools to allow you to move fast, while still enabling you to ensure that your cloud resources comply with organizational standards and best practices. These include:

- Deployment tools to manage the creation and decommissioning of AWS resources according to organization standards
- Inventory and configuration management tools to identify AWS resources and then track and manage changes to those resources over time
- Template definition and management tools to create standard, preconfigured, hardened virtual machines for EC2 instances

### Data Encryption

AWS offers you the ability to add a layer of security to your data at rest in the cloud, providing scalable and efficient encryption features. These include:

- Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift
- Flexible key management options that allow you to choose whether to have AWS manage the encryption keys or maintain complete control over your keys
- Dedicated, hardware-based cryptographic key storage options for customers to help satisfy compliance requirements

In addition, AWS provides APIs for you to integrate encryption and data protection with any of the services you develop or deploy in an AWS environment.

### Access Control

AWS offers you capabilities to define, enforce, and manage user access policies across AWS services. These include:

- Identity and access management capabilities to define individual user accounts with permissions across AWS resources
- Multifactor authentication for privileged accounts, including options for hardware-based authenticators
- Integration, and federation, with corporate directories to reduce administrative overhead and improve end-user experience

AWS provides native identity and access management integration across many of its services, plus API integration with any of your own applications or services.

### Monitoring and Logging

AWS provides tools and features that enable you to see what's happening in your AWS environment. These include:

- Deep visibility into API calls, including who, what, when, and from where calls were made
- Log aggregation and options, streamlining investigations and compliance reporting
- Alert notifications when specific events occur or thresholds are exceeded

These tools and features give you the visibility you need to spot issues before they impact the business and allow you to improve security posture, and reduce the risk profile, of your environment.

### AWS Marketplace

The AWS Marketplace offers hundreds of industry leading partner products that are equivalent, identical to, or integrate with existing controls in your on-premises environments, including anti-malware, web application firewalls, and intrusion protection.

These products complement the tools and features offered by AWS to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.

## Security Guidance

AWS provides customers with guidance and expertise through online tools, resources, support, and professional services provided by AWS and its partners.

**AWS Trusted Advisor** is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.

**AWS Account Teams** provide a first point of contact, guiding you through your deployment and implementation, and pointing you toward the right resources to resolve security issues you may encounter.

**AWS Enterprise Support** provides 15-minute response time and is available 24×7 by phone, chat, or email; along with a dedicated Technical Account Manager. This concierge service ensures that customers' issues are addressed as swiftly as possible.

**AWS Professional Services and AWS Partner Network** both help customers develop security policies and procedures based on well-proven designs, and help to ensure that customers' security design meets internal and external

compliance requirements. The AWS Partner Network has hundreds of certified AWS Consulting Partners worldwide to help customers with their security and compliance needs.

**AWS Advisories and Bulletins.** AWS provides advisories around current vulnerabilities and threats, and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing.

## Compliance

AWS computing environments are continuously audited, with certifications from accreditation bodies across geographies and verticals, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS.[i] Additionally AWS also has assurance programs that provide templates and control mappings to help customers establish the compliance of their environments running on AWS against 20+ standards, including the HIPAA, CESG (UK), and Singapore Multi-tier Cloud Security (MTCS) standards.

AWS is also fully compliant with applicable EU data protection laws, and the AWS Data Processing Agreement incorporates the Article 29 Working Party Model Clauses. This means that AWS customers wishing to transfer personal data from the European Economic Area (EEA) to other countries can do so knowing that their content in AWS will be given the same high level of protection it receives in the EEA.

By operating in an accredited environment, customers reduce the scope and cost of audits they need to perform. AWS continuously undergoes assessments of its underlying infrastructure—including the physical and environmental security of its hardware and data centers—so customers can take advantage of those certifications and simply inherent those controls.

In a traditional data center, common compliance activities are often manual, periodic activities. These activities include verifying asset configurations and reporting on administrative activities. Moreover, the resulting reports are out of date before they are even published. Operating in an AWS environment allows customers to take advantage of embedded, automated tools like AWS Config and AWS CloudTrail for validating compliance. These tools reduce the effort needed to perform audits, since these tasks become routine, ongoing, and automated. By spending less time on manual activities, you can help evolve the role of compliance in your company from one of a necessary administrative burden, to one that manages your risk and improves your security posture.

# Where can I learn more?

AWS has several whitepapers available that offer detailed descriptions of the security measures in place at AWS.

To learn more about AWS Security Practices and product features, download the AWS Security Processes Overview document at http://d0.awsstatic.com/whitepapers/Security/AWS Security Whitepaper.pdf

To learn more about the specific controls in place at AWS, and how to integrate AWS into your existing control framework download the AWS Risk and Compliance Whitepaper document at https://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

For best practices guidance on how to deploy security controls within an AWS environment download the AWS Security Best Practices document at http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

[i] For more information about the nature of AWS Compliance programs go to http://aws.amazon.com/compliance