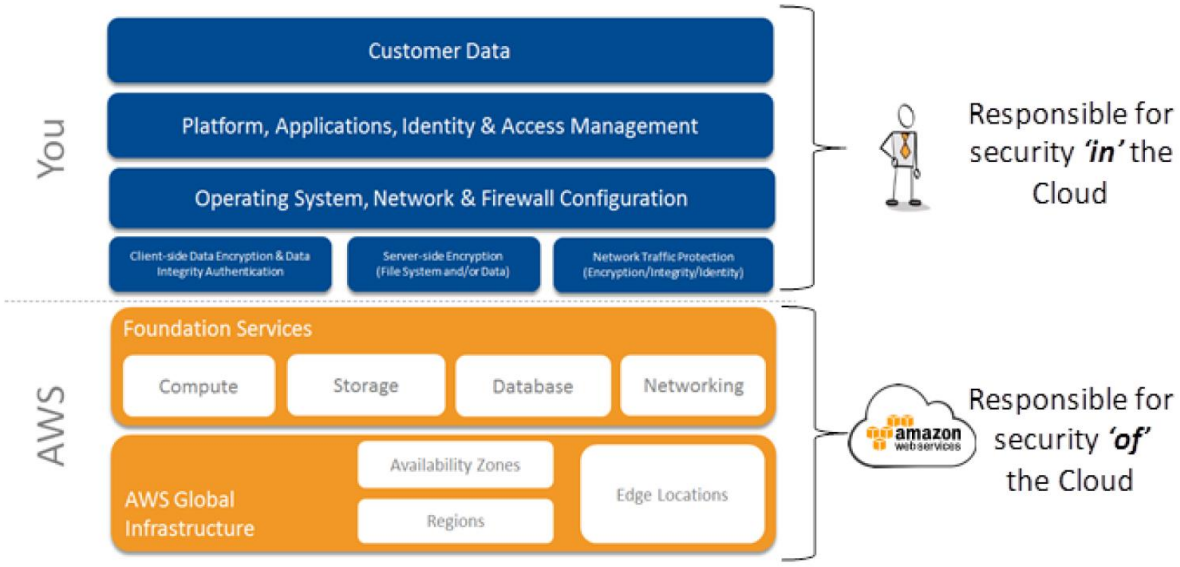
AWS Security Whitepaper

Shared Security Responsibility Model

In the Shared Security Responsibility Model, AWS is responsible for securing the underlying infrastructure that supports the cloud, and you're responsible for anything you put on the cloud or connect to the cloud.



AWS Security Responsibilities

- AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services.
- AWS provide several reports from third-party auditors who have verified their compliance with a variety of computer security standards and regulations
- AWS is responsible for the security configuration of its products that are considered managed services *for e.g. RDS, DynamoDB*
- For Managed Services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

Customer Security Responsibilities

- AWS Infrastructure as a Service (IaaS) products *for e.g. EC2, VPC, S3* are completely under your control and require you to perform all of the necessary security configuration and management tasks.
- Management of the guest OS (including updates and security patches), any application software or utilities installed on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance
- For most of these managed services, all you have to do is configure logical access controls for the resources and protect the account credentials

AWS Global Infrastructure Security

AWS Compliance Program

IT infrastructure that AWS provides to its customers is designed and managed in alignment with security best practices and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

And meet several industry-specific standards, including:

- Criminal Justice Information Services (CJIS)
- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Motion Picture Association of America (MPAA)

Physical and Environmental Security

Storage Decommissioning

- When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals.
- AWS uses the techniques detailed in DoD 5220.22-M (National Industrial Security Program Operating Manual) or NIST 800-88 (Guidelines for Media Sanitization) to destroy data as part of the decommissioning process.
- All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Network Security

Amazon Corporate Segregation

- AWS Production network is segregated from the Amazon Corporate network and requires a separate set of credentials for logical access.
- Amazon Corporate network relies on user IDs, passwords, and Kerberos, while the AWS Production network require SSH public-key authentication through a bastion host.

Networking Monitoring & Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

AWS network provides protection against traditional network security issues

1. **DDOS** – AWS uses proprietary DDoS mitigation techniques. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
2. **Man in the Middle attacks** – AWS APIs are available via SSL-protected endpoints which provide server authentication
3. **IP spoofing** – AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
4. **Port Scanning** – Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Penetration/Vulnerability testing can be performed only on your own instances, with mandatory prior approval, and must not violate the AWS Acceptable Use Policy.

5. **Packet Sniffing by other tenants** – It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic.

Secure Design Principles

AWS's development process follows :-

- Secure software development best practices, which include formal design reviews by the AWS Security Team, threat modeling, and completion of a risk assessment
- Static code analysis tools are run as a part of the standard build process
- Recurring penetration testing performed by carefully selected industry experts

AWS Account Security Features

AWS account security features includes credentials for access control, HTTPS endpoints for encrypted data transmission, the creation of separate IAM user accounts, user activity logging for security monitoring, and Trusted Advisor security checks

AWS Credentials

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWS SDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.
Key Pairs	• SSH login to EC2 instances • CloudFront signed URLs	A key pair is required to connect to an EC2 instance launched from a public AMI. The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have a key pair generated automatically for you when you launch the instance or you can upload your own.
X.509 Certificates	• Digitally signed SOAP requests to AWS APIs • SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Security Credentials page.

Individual User Accounts

Do not use the Root account, instead create an IAM User for each user and provide them with a unique set of Credentials and grant least privilege as required to perform their job function

Secure HTTPS Access Points

Use HTTPS, provided by all AWS services, for data transmissions, which uses public-key cryptography to prevent eavesdropping, tampering, and forgery

Security Logs

Use Amazon CloudTrail which provides logs of all requests for AWS resources within the account and captures information about every API call to every AWS resource you use, including sign-in events