AWS Security Services

- AWS manages security **OF** the cloud; you are responsible for security **IN** the cloud.

Benefits of AWS Security

- **Keep Your Data Safe** – the AWS infrastructure puts strong safeguards in place to help.
- **Protect your privacy** – All data is stored in highly secure AWS data centers.
- **Meet Compliance Requirements** – AWS manages dozens of compliance programs in its infrastructure. This means that segments of your compliance have already been completed.
- **Save Money** – cut costs by using AWS data centers. Maintain the highest standard of security without having to manage your own facility.
- **Scale Quickly** – security scales with your AWS Cloud usage. No matter the size of your business, the AWS infrastructure is designed to keep your data safe.

Compliance

AWS Cloud Compliance enables you to understand the robust controls in place at AWS to maintain security and data protection in the cloud.

As systems are built on top of AWS Cloud infrastructure, compliance responsibilities will be shared.

Compliance programs include:

- Certifications / attestations.
- Laws, regulations, and privacy.
- Alignments / frameworks.

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to you.

It provides on-demand access to AWS' security and compliance reports and select online agreements.

Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Amazon GuardDuty

Amazon GuardDuty offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Detects account compromise, instance compromise, malicious reconnaissance, and bucket compromise.

AWS WAF & AWS Shield

WAF:

- AWS WAF is a web application firewall.
- Protects against common exploits that could compromise application availability, compromise security, or consume excessive resources.

Shield:

- AWS Shield is a managed Distributed Denial of Service (DDoS) protection service.
- Safeguards web application running on AWS with always-on detection and automatic inline mitigations.
- Helps to minimize application downtime and latency.
- Two tiers – Standard and Advanced.

AWS Key Management Service (AWS KMS)

AWS Key Management Service gives you centralized control over the encryption keys used to protect your data.

You can create, import, rotate, disable, delete, define usage policies for, and audit the use of encryption keys used to encrypt your data.

AWS KMS is integrated with AWS CloudTrail which provides you the ability to audit who used which keys, on which resources, and when.

AWS KMS enables developers to easily encrypt data, whether through 1-click encryption in the AWS Management Console or using the AWS SDK to easily add encryption in their application code.