**Module 6**

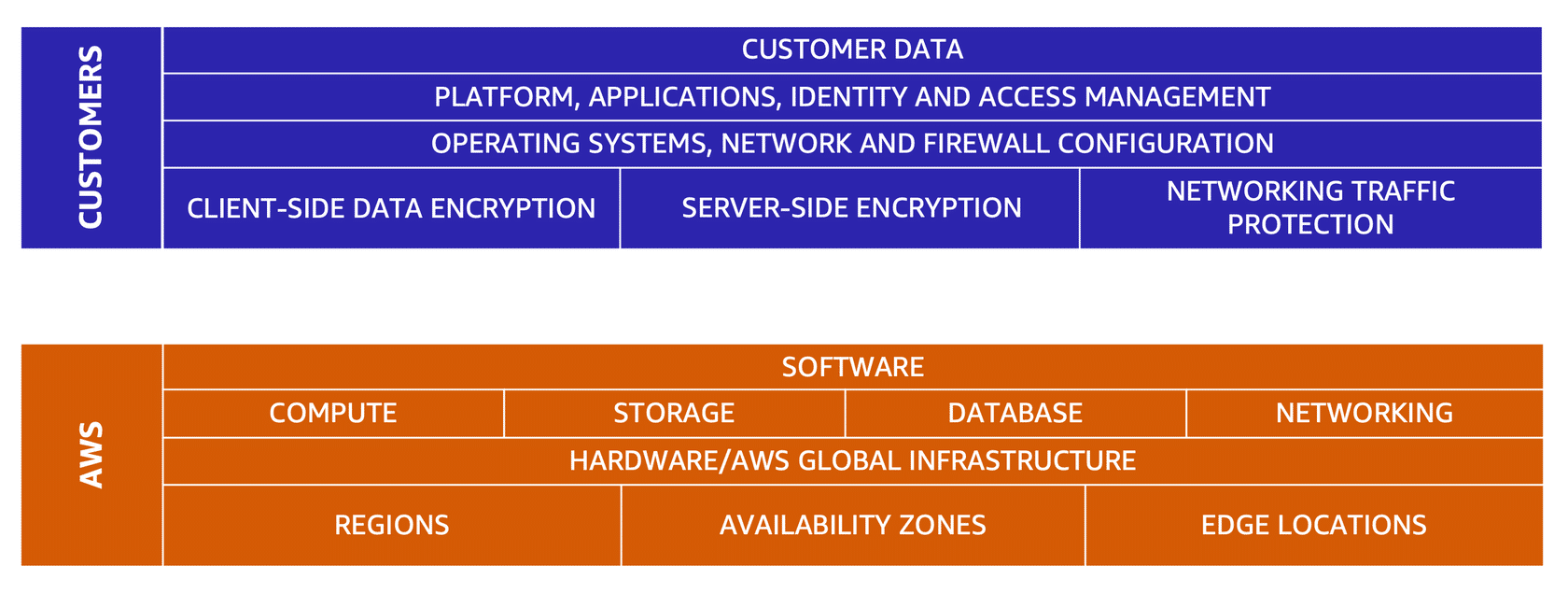
**Security**

**The AWS Shared responsibility model**

AWS is responsible for some parts of your environment as a collection of parts that build upon each other. AWS is responsible for some part of your environment, and you (the customer) are responsible for other parts.

* This concept is known as shared responsibility model

|  |  |
| --- | --- |
| Customer responsibility | AWS responsibility |
| Security in the cloud | Security of the cloud |
| Responsible for security of everything that they create and put in the AWS Cloud | AWS operates, manages, and controls the components at all layers of infrastructure. |
| You are responsible for managing security requirements for your content | Responsible for protecting the global infrastructure that runs all the services offered in the AWS Cloud.  E.g AWS Regions, Availability zones, and edge’s locations |
| You also control how access rights are granted, manage, and revoked | Manages the security of the cloud, specifically the physical infrastructure, that hosts your resources. |



**AWS Identity and Access Management (IAM)**

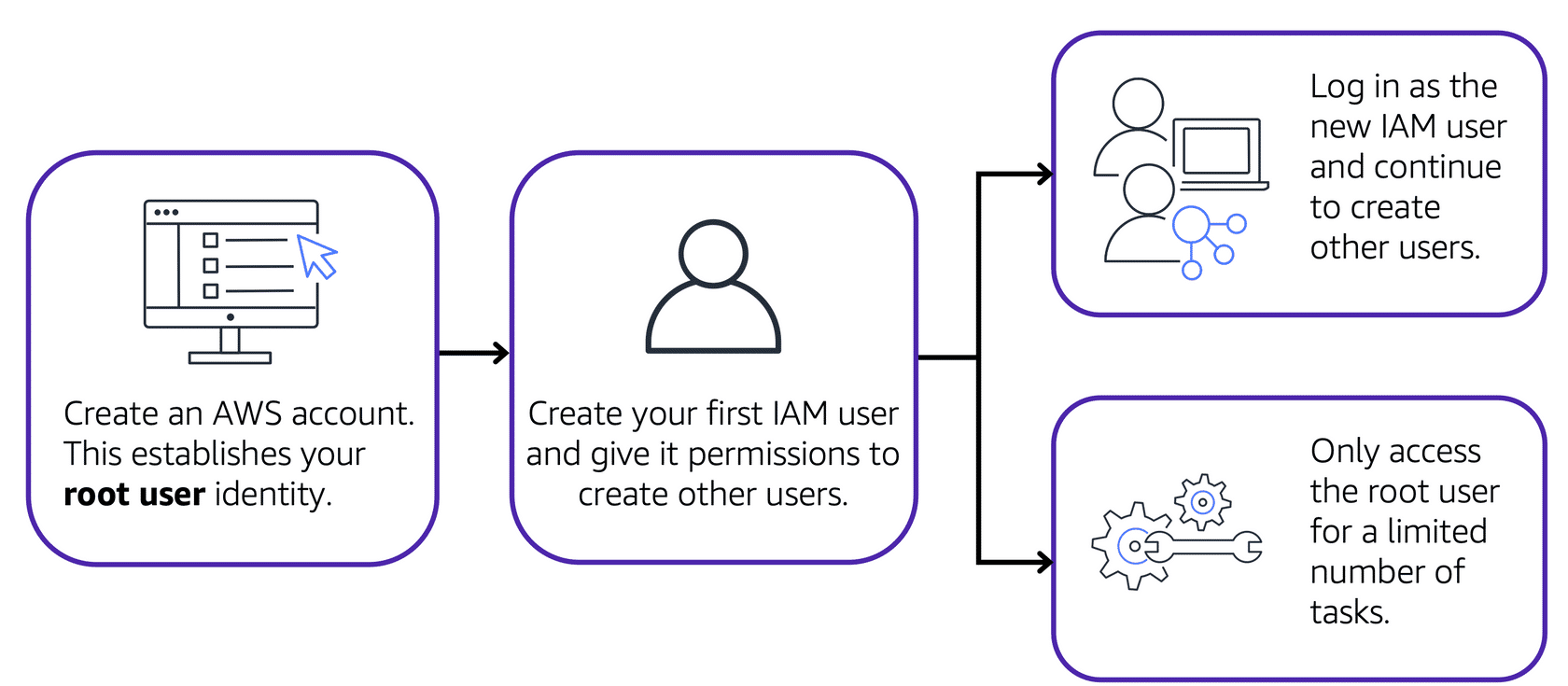
* Enables you to manage access to AWS services and resources securely
* Gives you the flexibility to configure access based on your company’s specific operational and security needs.

**IAM Features**

* IAM users, groups, and roles
* IAM policies
* Multi-factors authentication

**AWS account root user**

* When you first create an AWS account, you begin with a single sign in identity that has complete access to all AWS services and resources in the account. This identity is call root user.



**Best practises**

* Do not use the root user for everyday tasks
* Instead use the root user to create your first IAM user and assign it permission to create other users
* Create individual IAM users for each person who need access to AWS
* Follow the security principle of least privilege when granting permissions

**IAM users**

* Is identity that you create in AWS
* It represents the person or application that interacts with AWS services and resources

**IAM policies**

* Is a document that allows or denies permissions to AWS services
* Enables you to customize user’s level of access to resources.

**IAM Groups**

* Is a collection of IAM users
* When you assign an IAM policy to a group, all users in the group are granted permissions specified by the policy

**IAM Roles**

* Is an identity that you can assume to gain temporary access to permission
* Are ideal for situations in which access to services or resources needs to be temporarily, instead of long term.

**Multi-factor authentication**

* Provides extra layer of security for you AWS account

**AWS Organizations**

* Centrally manage your environment as you grow and scale your resources on AWS
* You can use service control policies to centrally control permissions on the AWS service, resources, and individual API actions that users and roles in each account can access
* You can group accounts into organizational units to make it easy to manage accounts with similar business or security requirements.

**Compliance**

**AWS Artifact**

* Is a service that provides on-demand access to AWS security and compliance report and select online agreements.

**Two main section of AWS Artifact**

|  |  |
| --- | --- |
| **AWS Artifact Agreements** | **AWS Artifact Reports** |
| You can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations. | Provide compliance reports from third-party auditors.  You can provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security control |
| Different types of agreements are offered to address the needs of customers who are subject to specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA). |  |

**Customer Compliance Centre**

* Contains resources to help you learn more about AWS compliance.
* You can read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges.

**You can also access compliance whitepapers and documentation on topics such as:**

* AWS answers to key compliance questions
* An overview of AWS risk and compliance
* An auditing security checklist

**Includes learning path** – the learning path is designed for individuals in auditing, compliance, and legal roles who want to learn more about how their internal operations can demonstrate compliance using AWS Cloud.

**Denial-of-service-attacks**

* Is a deliberate attempt to make a website or application unavailable to users.

**Distributed Denial-of-service-attacks**

* Multiple sources are used to start an attack that aims to make a website or application unavailable.
* This can come from a group of attackers, or even a single attacker.
* Bots – is a multiple of infected computers.

To help minimize the effect of DoS and DDoS attacks you can use **AWS Shield**

**AWS Shield**

* Is a service that protects application against DDoS attack. AWS Shield provides two level of protection: Standard and Advanced

|  |  |
| --- | --- |
| **AWS Shield Standard** | **AWS Shield Advanced** |
| Automatically protects all AWS customers at no cost. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks | Is a paid service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks |
| Uses a variety of analysis techniques to detect malicious traffic in real time and automatically | It integrates with other services such as Amazon CloudFront, Amazon Route 53 and Elastic Balancing.  You can integrate with AWS WAF by writing custom rules to mitigate complex DDoS attacks |

**AWS Key Management Service (AWS KMS)**

* Enables you to perform encryption operations using **cryptographic** keys.
* A **cryptographic** key is a random string of digits used for locking(encryption) and unlocking(decryption) data.
* AWS KMS is used to create, manage, and use cryptographic keys.

**AWS Web Application Firewall (AWS WAF)**

* Is a web application firewall that lets monitor network requests that come into your web applications.
* Works together with Amazon CloudFront and Application Load Balancer.
* AWS WAF works similar way as network access control list , to block or allow traffic it by using a web access control list (ACL).

How can you use WAF to allow and block specific requests?

Suppose that your application has been receiving malicious network requests from several IP addresses. You want to prevent these requests from continuing to access your application, but you also want to ensure that legitimate users can still access it

* You configure the web ACL to allow all request except those from IP address that you specified.

**Amazon Inspector**

* Performs automated security assessments
* Helps improve the security and compliance of applications by running automated security assessments.
* It checks apps for security vulnerabilities and deviations from security best practises

**Amazon GuardDuty**

* Is a service that provides intelligent threat detection for your AWS infrastructure and resources.
* It identifies threats by continuously monitoring the network activity and account behaviour within your AWS environment
* GuardDuty continuously analyses network and account activity from multiple AWS sources, including VPC Flow Logs and DNS logs
* GuardDuty intelligently detects threats
* Review detailed findings and take action.