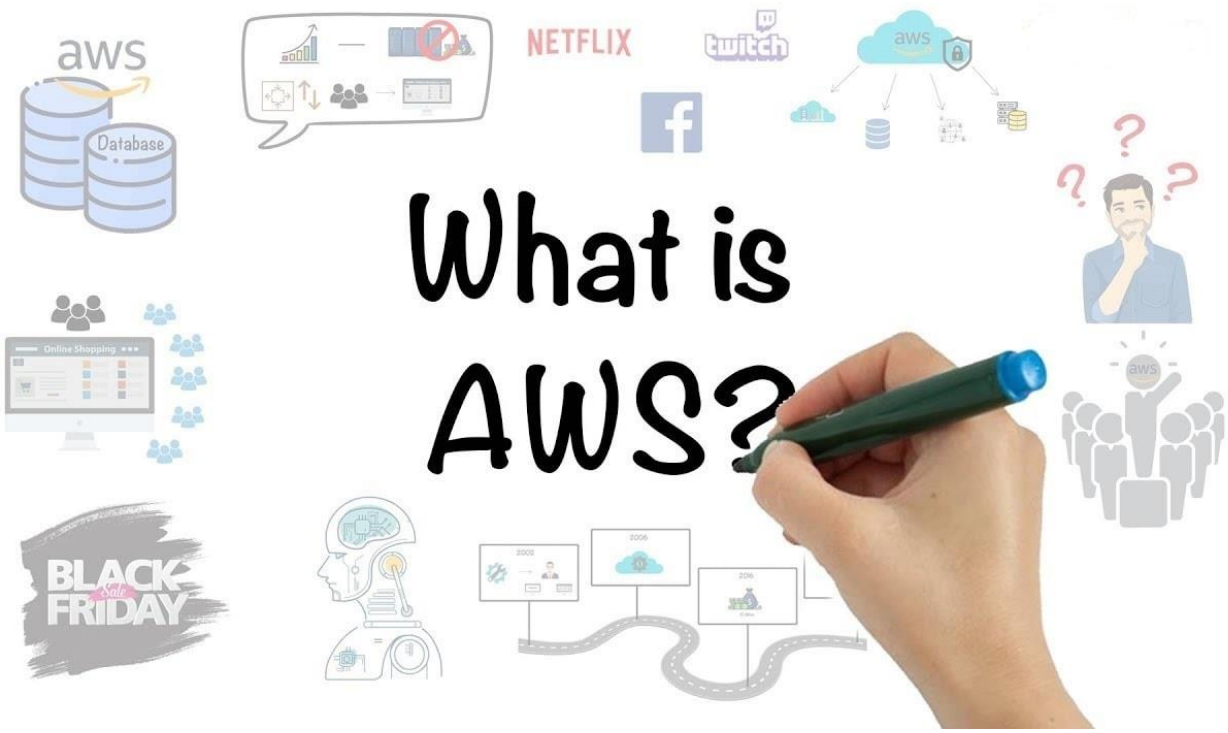
AWS Security Services and It's Parameters

Most of the enterprises are moving towards the cloud and expanding their infrastructure. Cloud helps companies to share their data anywhere around the globe. As a result, **cloud security** can't be compromised. Cloud security consists of a bunch of regulations and procedures that work together to protect cloud-based systems. AWS is a giant cloud and helping industries with a wide variety of services.

What exactly is AWS?

Amazon Web Services (AWS) is formed from many various cloud computing products and services. With pay-as-you-go pricing, Amazon Web Services provides a wide range of worldwide cloud-based products, including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and business applications. These products are available on demand and may be used in a matter of seconds. In Q2 2022, one independent analyst reports AWS has over a 3rd of the market at 34%, with Azure following behind at 21%, and Google Cloud at 11%.



Key Takeaways of AWS

- According to reports Amazon Web Services (AWS) is the primary profit driver for Amazon.
- Amazon Web Service (AWS) provides servers, storage, networking, remote computing, email, mobile development, and security.
- AWS now contributes **14%** of Amazon's total revenue.

- Amazon controls quite a 3rd of the cloud market, almost twice its next closest competitor.

Availability of AWS

Availability (also referred to as service availability) is both a commonly used metric to quantitatively measure resiliency, as well as a target resiliency objective. AWS features a global infrastructure to supply a high availability for cloud workloads.

- Availability is that the percentage of your time that a workload is out there to be used.
- This percentage is calculated over a period of time, like a month, year, or trailing three years. Applying the strictest possible interpretation, availability is reduced anytime that the application isn't operating normally, including both scheduled and unscheduled interruptions. We define availability as follows:

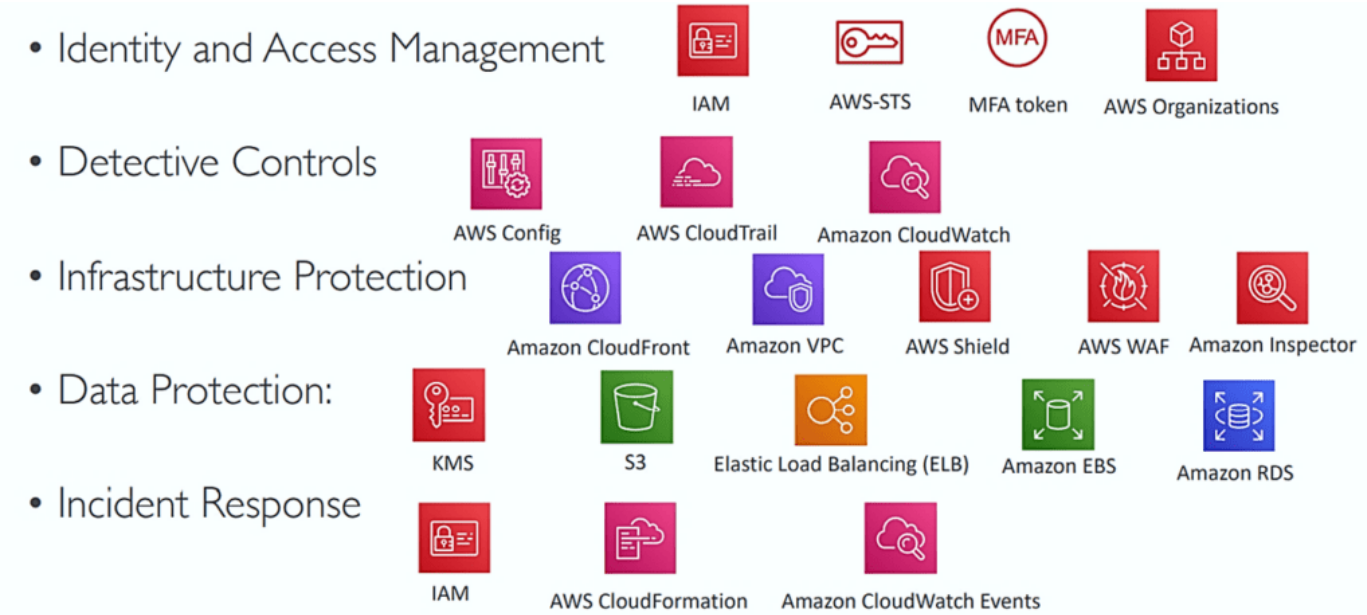
$$Availability = \frac{Available\ for\ Use\ Time}{Total\ Time}$$

- Availability is a percentage uptime (such as 99.9%) over a period of time (commonly a month or year).
- Common short-hand refers only to the "number of nines"; for instance, "five nines" translates to being 99.999% available.

Also Check: Our blog post on **AWS Auto Scaling**.

How Security Parameter is achieved on AWS?

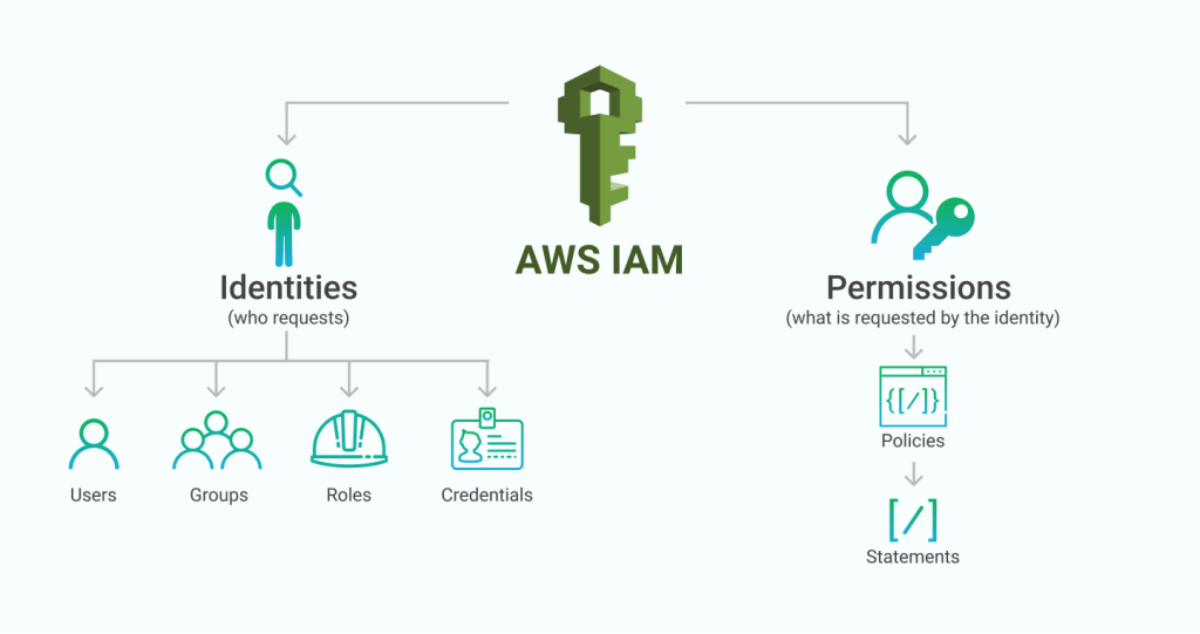
As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations. In the cloud, you don't have to manage physical servers or storage devices.



Identity and Access Management in AWS

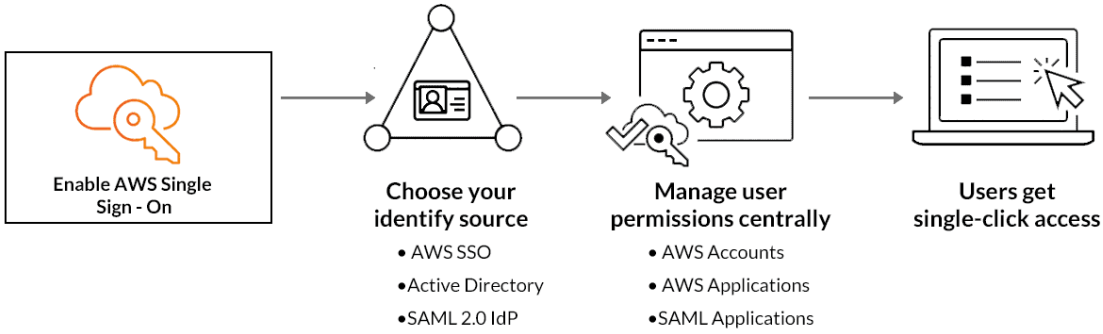
Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With IAM in the workplace, Information Technology (IT) managers can control user access to critical information within their organizations. Some of the Identity and Access Management Services are mentioned below

- **IAM:** AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. By using IAM, you'll create and manage AWS users, groups and use permissions to permit and deny their access to AWS resources. IAM is a feature offered at no additional charge.

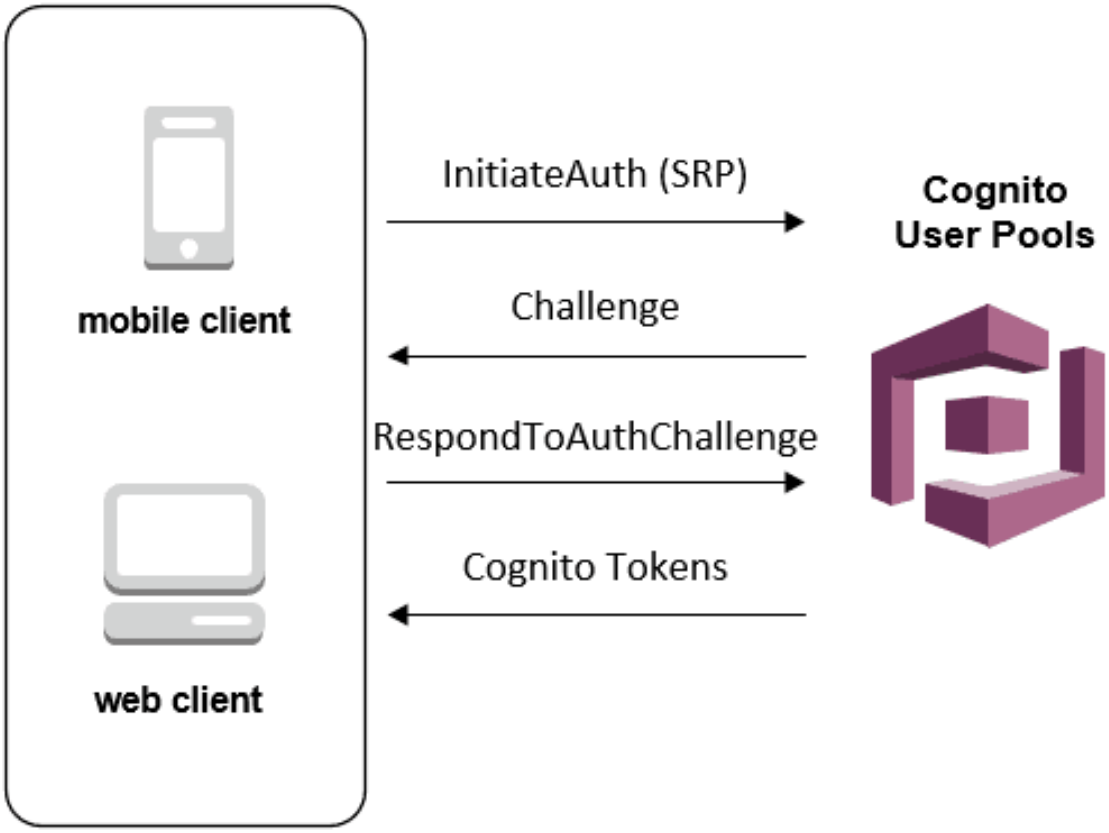


- **AWS Single Sign-on (SSO):** It makes it easier to centrally manage and access multiple AWS accounts and business applications. It enables you to provide users with single sign-on

access to all their assigned accounts and applications.

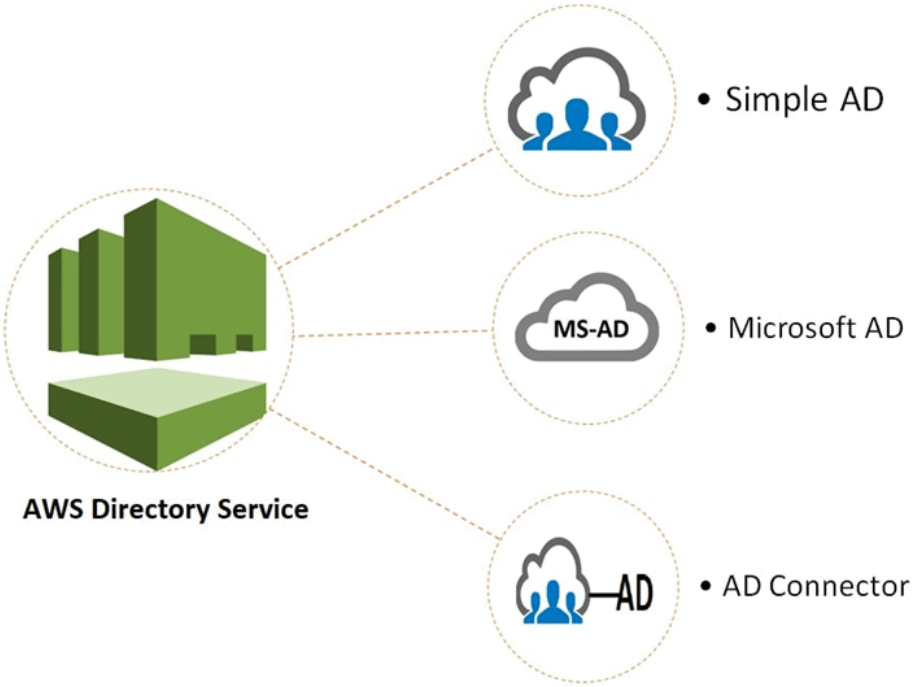


- **Amazon Cognito:** It is a service used for authentication, authorization, and user management for web or mobile applications. It allows customers to sign in through social identity providers such as Google, Facebook, Amazon and through enterprise identity providers such as Microsoft Active Directory via SAML.

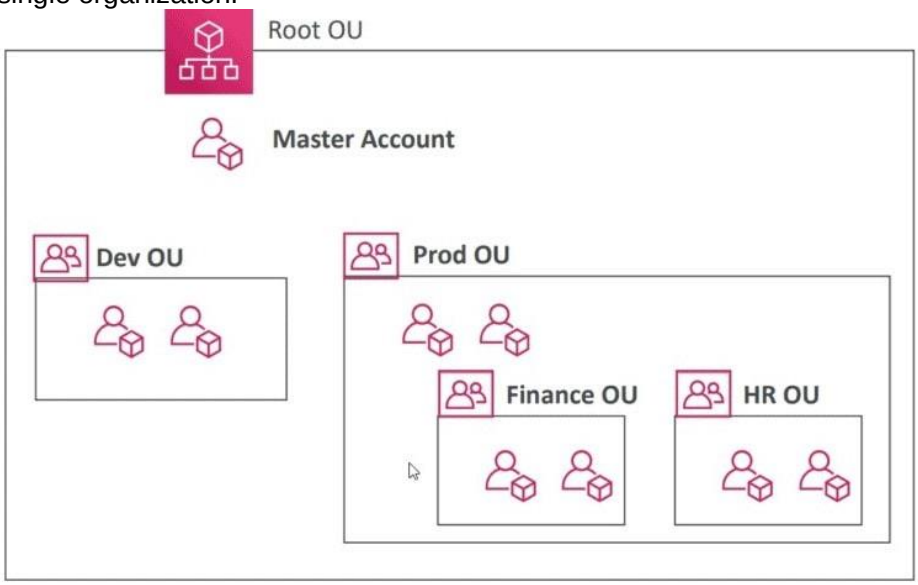


- **AWS Directory Service:** It is also known as AWS Managed Microsoft Active Directory (AD) and also enables multiple ways to use Microsoft Active Directory (AD) with other AWS services. By using AWS Managed Microsoft AD, it becomes easy to migrate Active Directory-

dependent applications and Windows workloads to AWS.



- **AWS Organizations:** It is a service that allows users to manage multiple AWS accounts grouped into a single organization.



Also Check: Our blog post on AWS Organizations

Detective Controls in AWS

Amazon Detective Controls **analyzes trillions of events and actions from multiple data sources such as AWS CloudTrail logs, Amazon GuardDuty, AWS Config, and AWS Inspector findings** and automatically creates a graph model that provides us with a unified and interactive view of the resources, users, and the interactions between them over the time. Some of the

Detective Controls Services are mentioned below

AWS Config

Record and evaluation configurations of your AWS resources

Amazon GuardDuty

Automatically detect threats

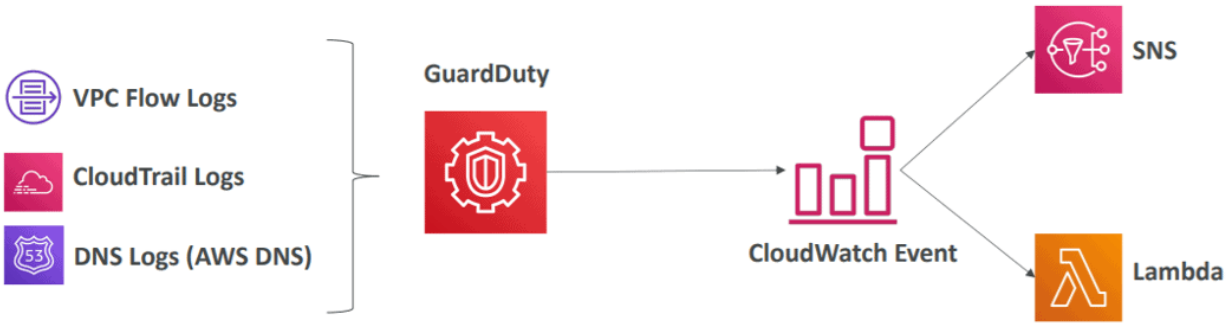
AWS CloudTrail

Track use activity and API usage

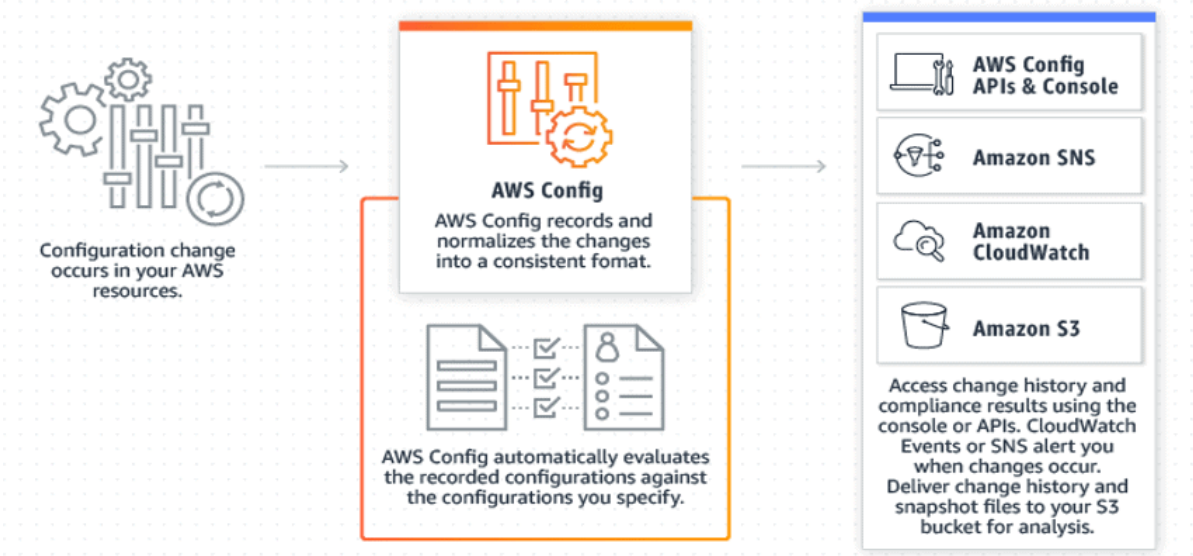
- **Amazon CloudTrail:** It is a service that gets enabled when the AWS account helps to enable compliance and auditing of the AWS account. It offers to view, analyze and respond to the activity across the AWS infrastructure. It records actions as an event by an IAM user, role, or

AWS service.

- **AWS GuardDuty:** It is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect our AWS Account, Workloads, and data stored in the S3.



- **Amazon Config:** It is a service that allows users to determine the quality of a resource's configuration in the AWS account.



Infrastructure Protection in AWS

The AWS infrastructure has been architected to be one of the most **flexible and secure cloud computing environments** available in today's cloud environment. It is designed to provide an extremely scalable and highly reliable platform that enables customers to deploy applications and data quickly and securely. Some of the Infrastructure Protection Services are mentioned below

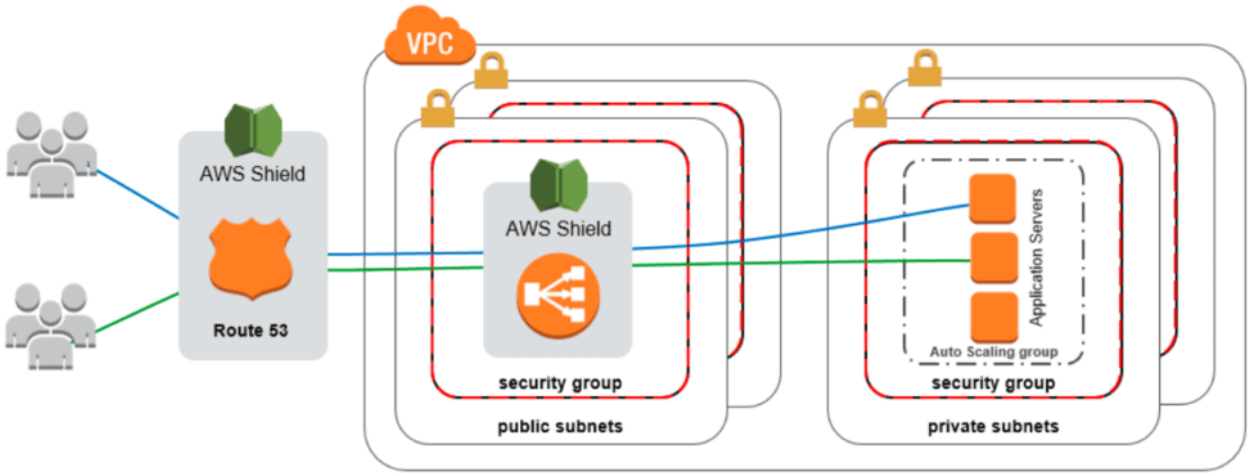
AWS Shield
Denial of service protection

AWS Firewall Manager
Centrally manage firewall rules

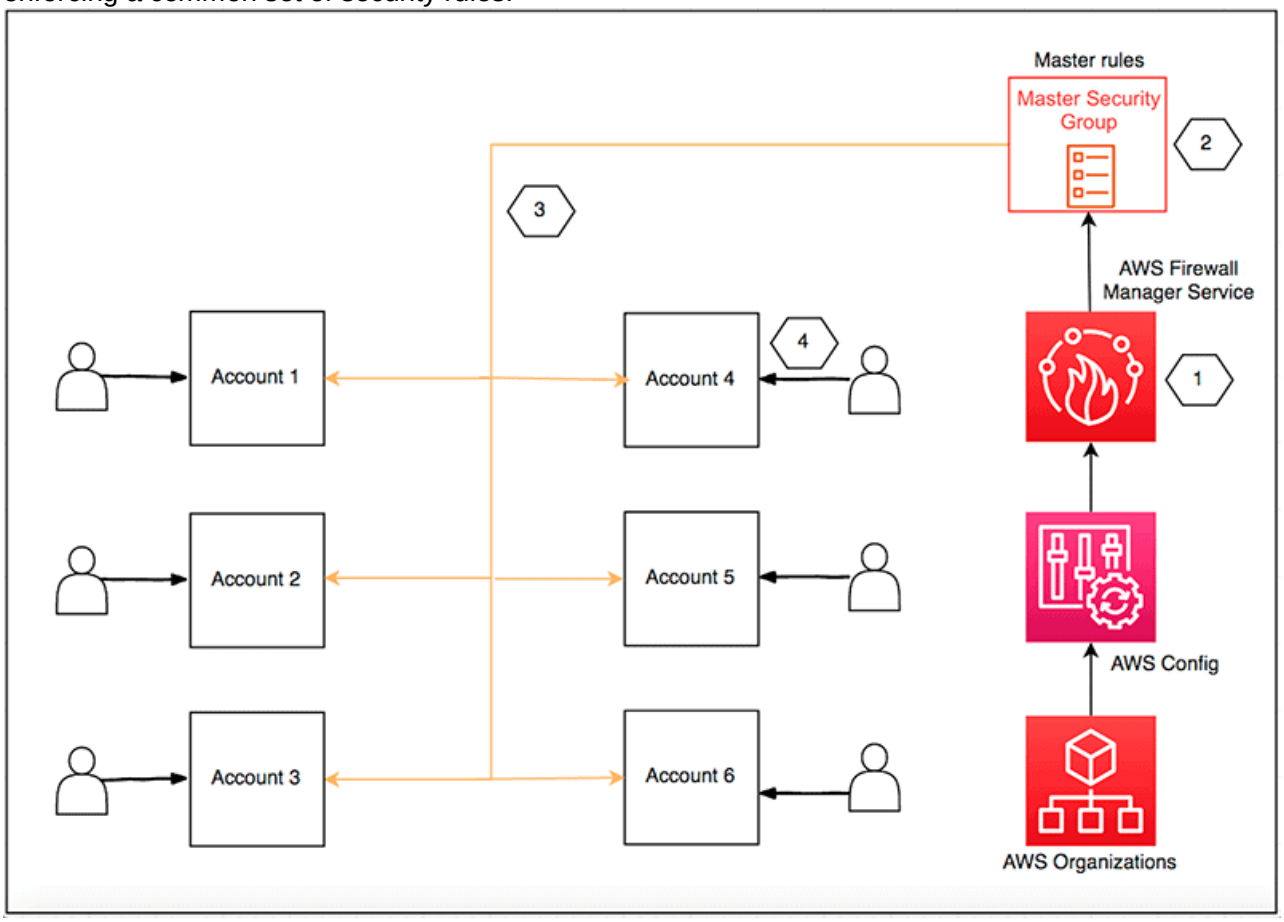
AWS Web Application
Firewall
Filter malicious website traffic

- **AWS Shield:** It is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two types of AWS Shield –

Standard and Advanced.

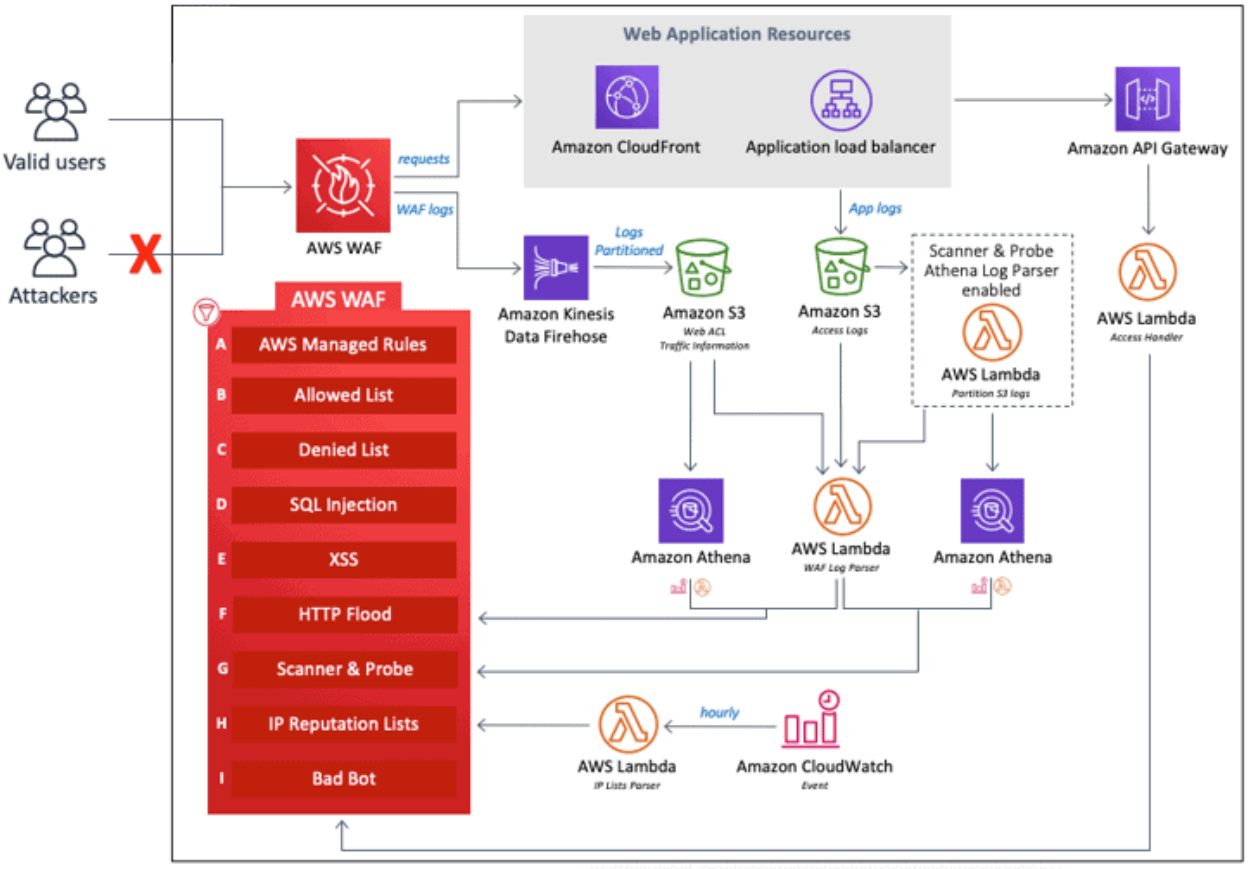


- **Amazon Firewall Manager:** It is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations. It makes it easy to bring new applications and resources into compliance by enforcing a common set of security rules.



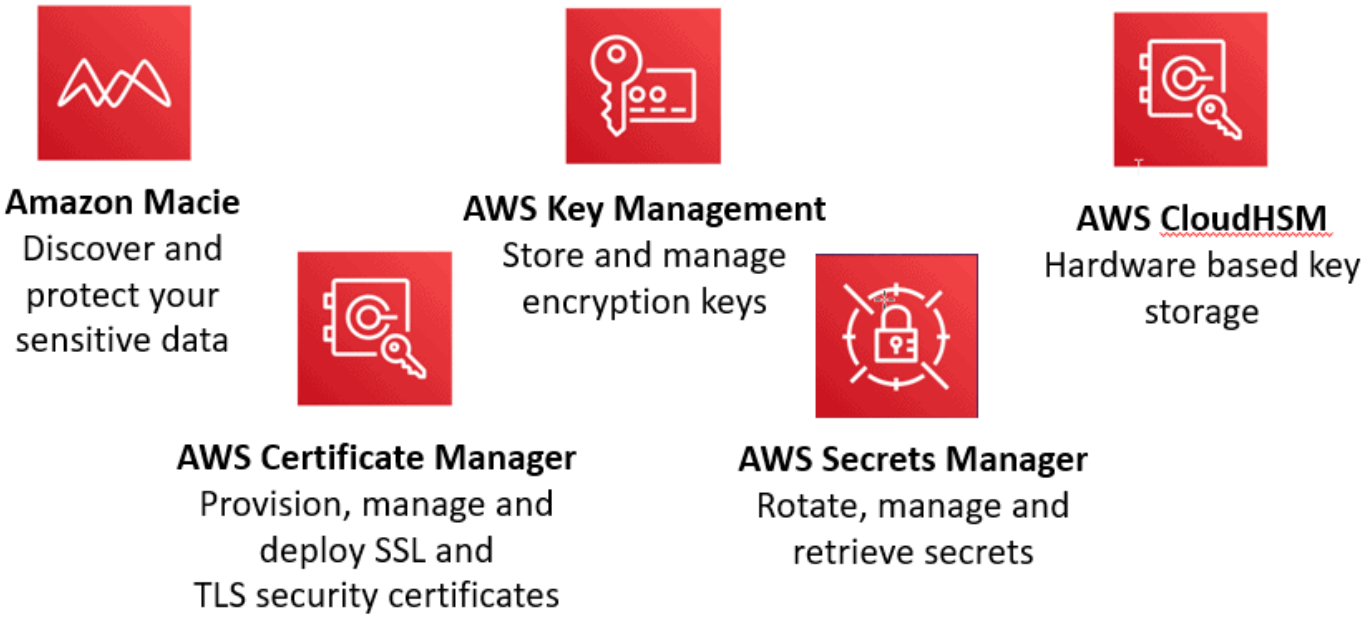
- **AWS Web Application Firewall (WAF):** It is a web application firewall that helps to protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security or consume excessive resources. AWS WAF gives you control over how the traffic reaches your applications by enabling you to create the security rules that control bot traffic and block some common attack patterns, such as SQL injection or

cross-site scripting.

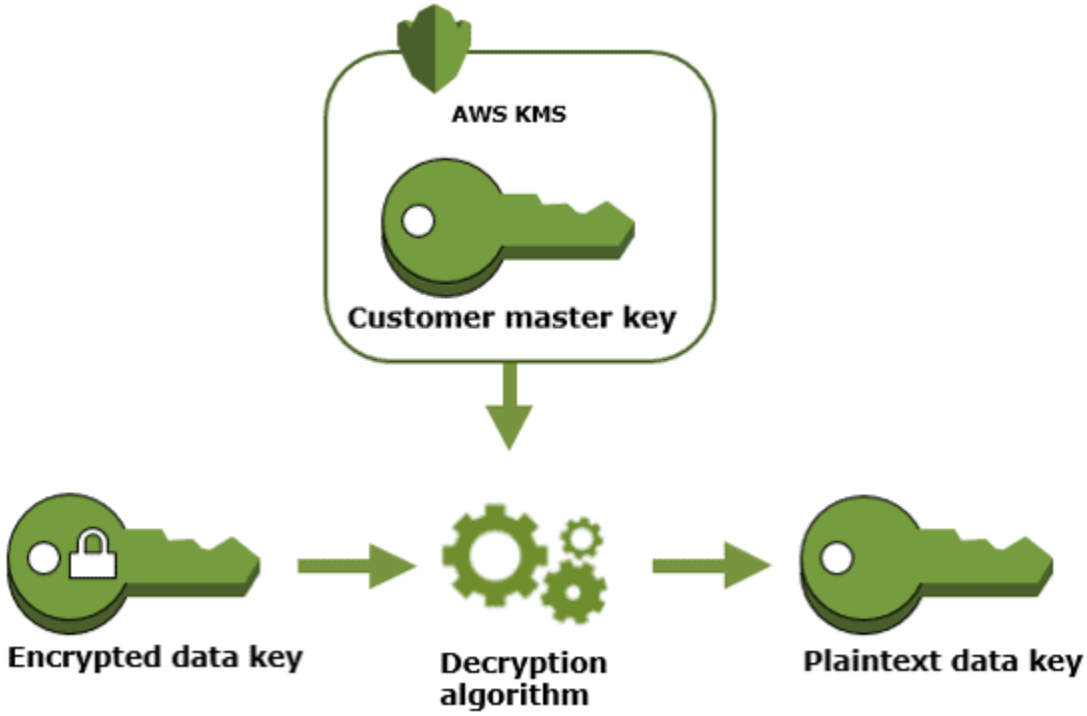


Data Protection in AWS

In AWS, you can manage the privacy of your data, control how your data is used, who has access to the data and how it is being encrypted. Some of the Data Protection Services are mentioned below



- **AWS KMS:** AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their uses across a wide range of AWS services. AWS KMS is integrated with AWS CloudTrail to provide you with the logs of all key usage to help you meet your regulatory and compliance needs.



- **AWS Certificate Manager:** It is a service that allows you to easily provision, manage and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates to use with AWS services and your internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of internet

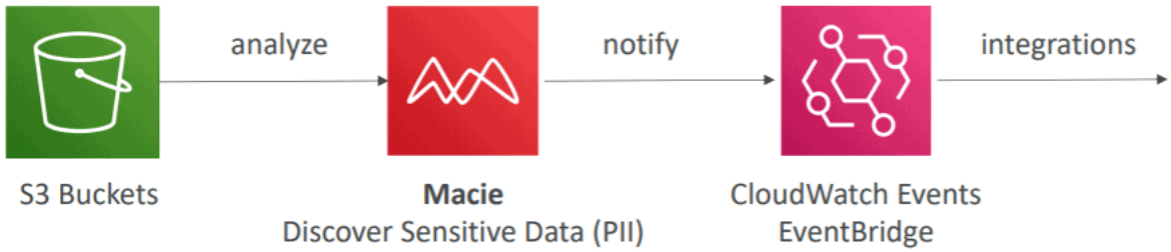
websites over the web and also as resources on private networks.

Certificate manager

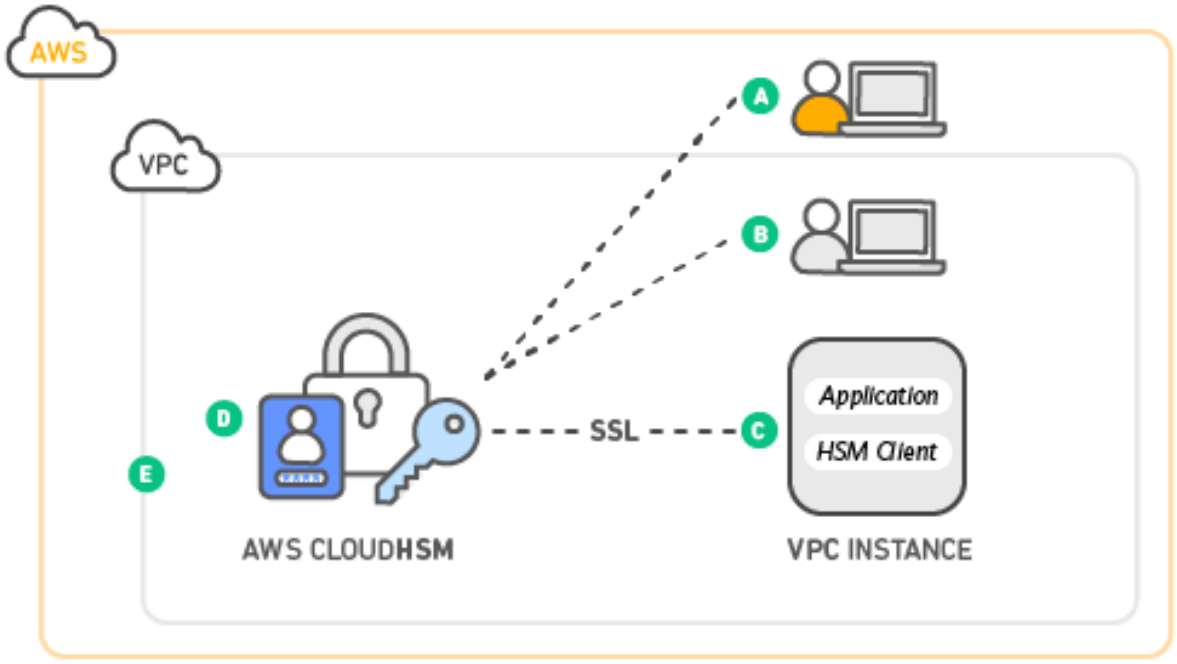
- **AWS Secret Manager:** It helps you to guard the secrets needed to access your applications, services, and IT resources. The service enables you to simply rotate, manage, and retrieve database credentials, API keys, and a few other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the necessity to hardcode sensitive information within the plain text.

- **Amazon Macie:** It is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS Environment. Amazon Macie automates the invention of sensitive data at scales up and

lowers the cost of protecting your data.



- **AWS CloudHSM:** It is a cloud-based hardware security module (HSM) that enables you to generate and use your own encryption keys on the AWS Cloud. It is a fully managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, high availability, and backups. CloudHSM also enables you to scale quickly by adding and removing HSM capacity on-demand, with no up-front costs.

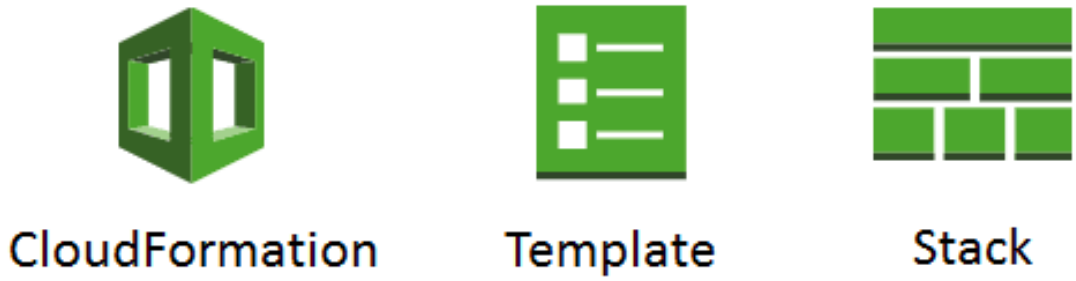


Incident Response in AWS

It focuses on an overview of cloud security and incident response concepts and identifies cloud capabilities, services, and all the mechanisms that are available to customers who are responding to security issues. Some of the Data Protection Services are mentioned below

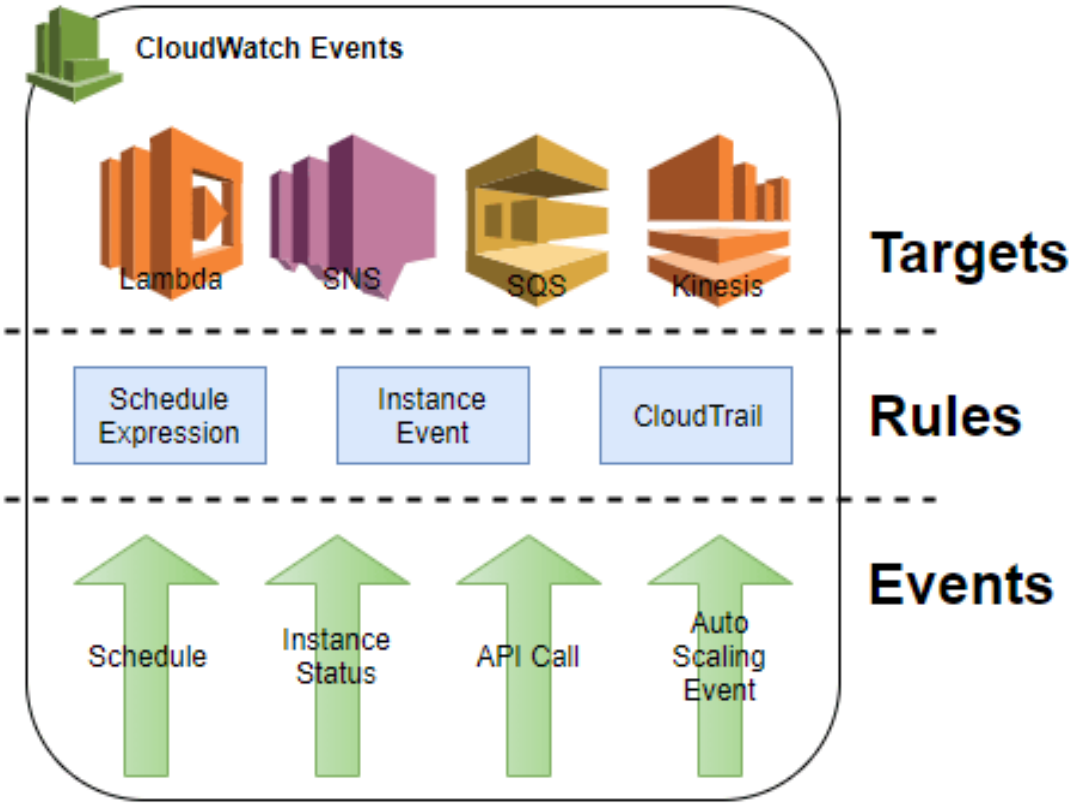
- **CloudFormation:** It gives you a simple way to prepare a model for a set of related AWS and third-party resources, provision them quickly, and consistently and manage them throughout their lifecycles, by treating infrastructure as code. You'll use a template to create, update, and delete a whole stack as a single unit, as often as you need to, instead of managing resources

individually.



Also Read: Our blog post on Introduction to AWS CloudFormation, Click here

- **Amazon CloudWatch Events:** It delivers a near real-time stream of system events that describe changes in Amazon Web Services (AWS) resources. Using simple rules that can be quickly set up, we can match events and route them to one or more target functions or streams.



.

Benefits of AWS Security

- **Keep Your Data Safe:** AWS infrastructure puts strong safeguards in place to help protect your privacy. All data is stored in highly secure Amazon Web Services 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.