AWS Security Services And Compliance

mazon Web Services (AWS) is a cloud giant that helps industries with a wide variety of services. **AWS Security Services** and **Compliance** are used to elevate **Security**, **Confidentiality**, **Integrity**, and **Data availability** in the cloud.

Overview of AWS Security

Security is a crucial concern for all who want to grow their footprint in the cloud. It could be an enterprise, startup, or small business. AWS Security tools help protect your data, accounts, applications, and infrastructure from unauthorized access. It enables the creation of the most secure cloud infrastructure to manage data flow and encrypt confidential information. AWS Automation cloud security helps securely build and deploy applications faster from developer and operation teams.

AWS Compliance

AWS Compliance allows you to understand the strong controls in AWS to keep security and data protection in the cloud. AWS manages several compliance programs in its infrastructure. The partial list of assurance services for which AWS complies mentioned below:

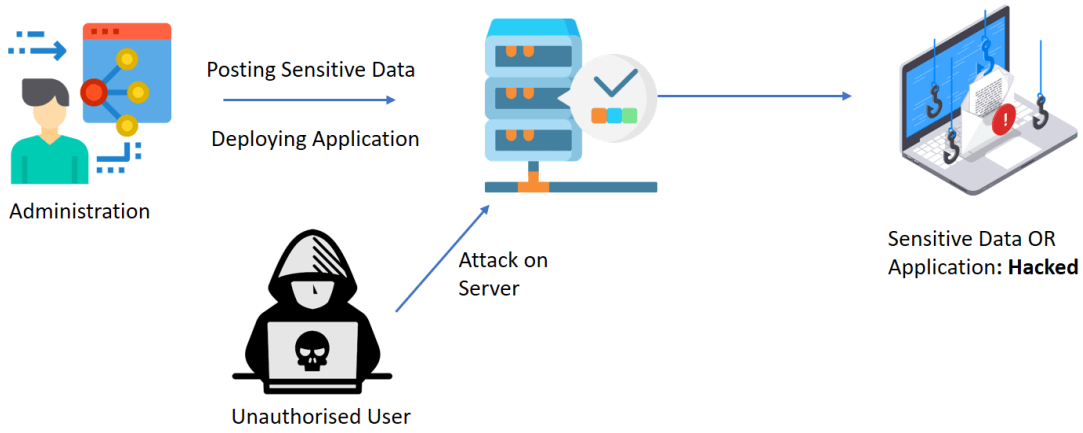
- SOC 1/ISAE 3402, SOC 2, SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 9001, ISO 27001, ISO 27017, ISO 27018

Check Out: How to Set Up MFA for AWS.

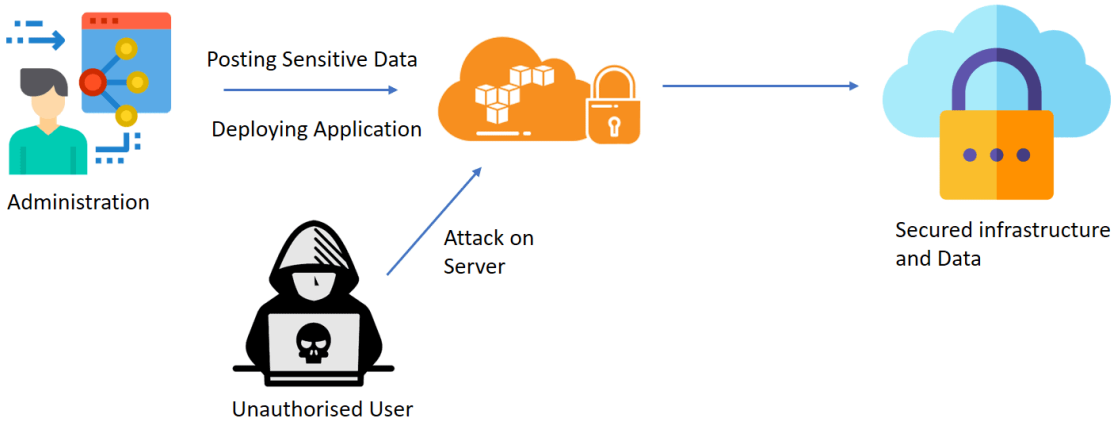
Why Cloud Security & Compliance?

No one knew the breach's seriousness when Dropbox, a cloud-based file-sharing service, revealed it in 2012. Hackers gained access to over 68 million user accounts, including passwords. According to reports, hackers sold stolen credentials on the dark web.

In another example, LinkedIn suffered when 6 million user passwords were stolen and published on a Russian forum. In addition to changing their passwords, LinkedIn implemented two-way authentication, which worked out in a great way. Hence to prevent a big loss of sensitive data, we use security techniques to establish the most secure atmosphere in the cloud.

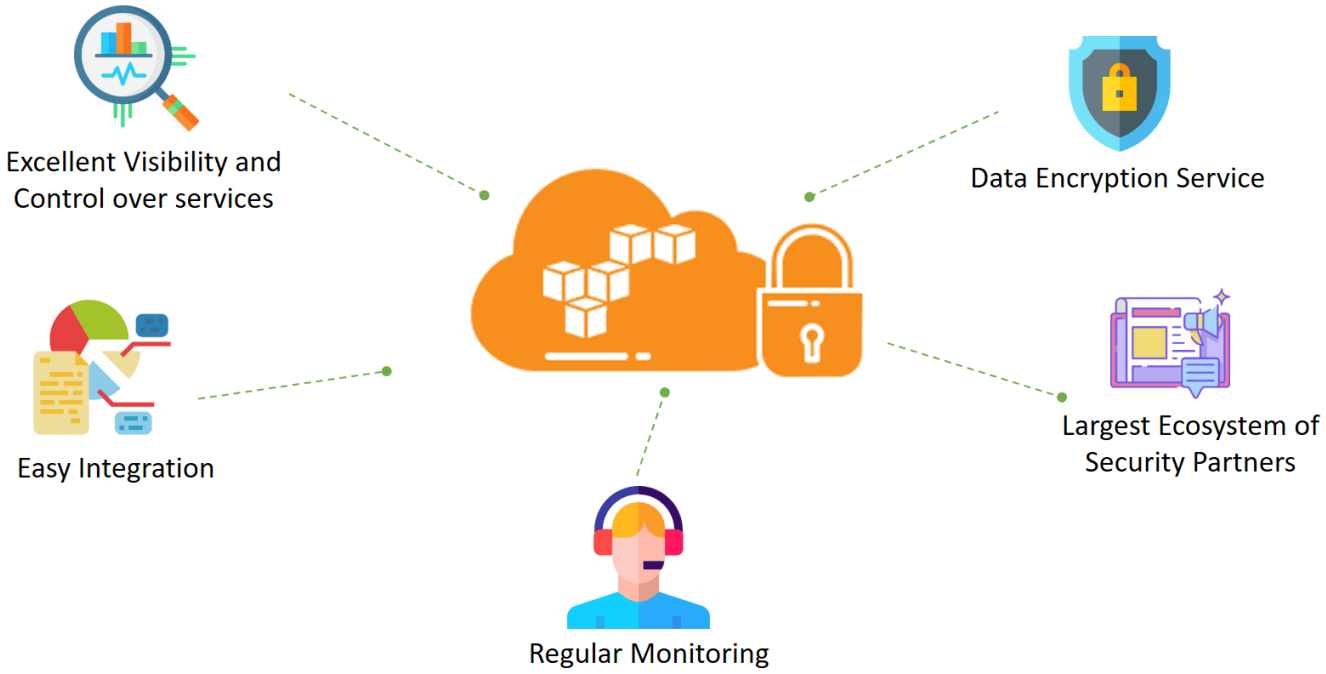


So security is a big concern for running a business on the cloud. AWS Provides reliable and secure services that help companies to store sensitive data, applications, and authentication more securely.



Benefits of AWS Security Services & Compliance

Security is critical for companies making the transition to the cloud. Cloud computing is no less vulnerable than an on-premise system to security threats continually changing and becoming more sophisticated. For this reason, it is vital to work with a cloud provider that offers best-in-class security that has been customized for your needs.



.

AWS Cloud Security offers various benefits:

Excellent Visibility and Control over services: AWS helps you track stored data with accessibility and resources consumed by your applications. Also, it provides identity and access control, combined with continuous security information monitoring in real time. It ensures that the right resources have proper suitable access, regardless of where the data is stored.
Easy Integration: By this, you can integrate AWS services with your current solution to help existing workflows, streamline your processes, and simplify compliance reporting.
Regular Monitoring: AWS ensures that they have a world-class team of security experts monitoring services and systems over time to protect your application and data.
Data Encryption Service: Data encryption is just a one-step process in AWS. Key Management service encrypts the data and manages the keys for you.
Largest Ecosystem of Security Partners: Get benefits of AWS security technology by consulting services from familiar solution providers you already know and trust.

AWS Security Services & Compliance

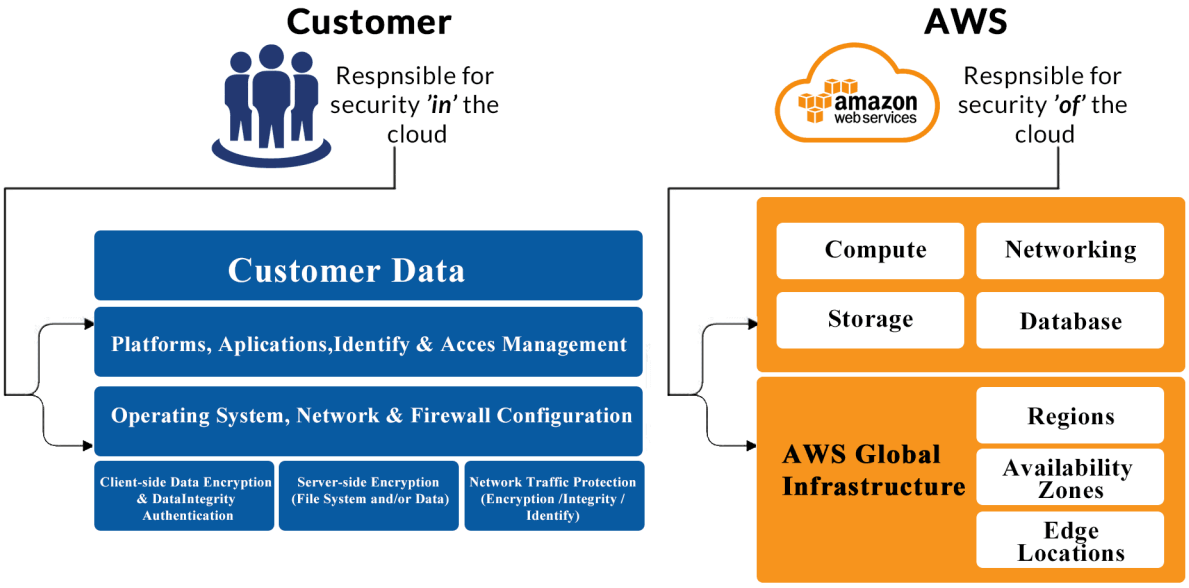
AWS provides services that help protect your sensitive data and accounts from unauthorized access. Let's have a look at those Essential security services mentioned below.

- **Identity & Access Management (IAM):** IAM helps you restrict who and what can access your AWS resources; through the use of identities, permissions, and a set of authentication and authorization methods.
- **Amazon Inspector:** Amazon Inspector is an automated security assessment service that helps you find security vulnerabilities within EC2 instances. Also, it improves the security and compliance of AWS-hosted applications.
- **AWS Certificate Manager:** The certificate Manager handles the planning and managing of **SSL** (Secure Sockets Layer)**/TLS**(Transport Layer Security) certificates.
- **AWS Directory Service:** AWS Directory Service allows your directory-aware resources and workloads to use managed **Active Directory (AD)** within your environment. Without the AWS Directory Service, both AD and AWS would be siloed to their own resources and would have to be managed separately.
- **AWS WAF & Shield:** The WAF service helps prevent websites and applications from being maliciously attacked by web attack patterns, such as SQL injection and cross-site scripting. The shield protects web applications from Distributed Denial of Service (DDoS) attacks.
- **AWS Artifact Portal:** Artifact provides on-demand access to security and compliance reports and select online agreements. Although the following two services do not fall within the same console category as the ones above, these are also critical services for encrypting your data.
- **AWS Key Management Service (KMS):** Key Management Service provides easy control access to your data using managed encryption. It is essential to have sensitive data that unauthorized users must not access. It makes the services highly available with full auditing functions to encrypt data at AWS and within your applications.
- **AWS Cloud HSM:** Hardware Security Module (HSM) is another encryption service that encrypts your data with protected keys. Therefore with this dedicated appliance, you control the HSM's encryption keys and cryptographic operations.

Here are some essential services that we have discussed. Now let's have a look at AWS Shared Security Responsibility Model.

Shared Security Responsibility Model

AWS has security rights starting from infrastructure, Regions, and Availability zones. These zones are physical data centers and are a group of 2 or more. In the Shared Security Responsibility Model, AWS is responsible for securing infrastructure, and customers are responsible for anything they put on the cloud or connect to the cloud.



However, the implementation of cloud security processes should be a shared responsibility between the customer and the solution provider (AWS). So AWS has a Shared security Responsibility model.

.

AWS Responsibility: For securing the underlying infrastructure, Regions, and Availability Zones.

- Amazon web service is responsible for defending the infrastructure that runs all of the AWS services in the cloud. The infrastructure is involved in physical centers, software, networks, and facilities that run services inside the AWS portal.
- AWS provides several feedback from third-party auditors who have verified their compliance with various compute security standards and regulations.
- AWS is responsible for the security configuration of its products and services like RDS, and DynamoDB.
- For Managed Services, AWS handles basic security tasks like guest OS and database patching, firewall configuration, and disaster recovery.

Customers' Responsibility

- AWS IaaS products like EC2, VPC, S3, etc., are entirely under your (customer) control and require you to perform all of the necessary security configuration and management tasks.
- Customers are responsible for managing the guest OS, including updates and security patches, application software, and the configuration of the AWS-provided firewall on each instance.
- In most of the AWS services, customers only have to protect the account credentials and configure logical access controls for the resources.

Case Study

Security is one of the major factors while doing operations on the cloud. AWS services help in Healthcare, Financial Services, Education, Government, and many other fields. Some of them are as follows:

Healthcare

MedStar Health: MedStar Health is a non-profit healthcare organization. It operates more than ten hospitals and 110 other healthcare entities. Using AWS has made it possible to engage their patients more directly—and offer them a reliable and efficient experience.

Financial Services

Intuit®: Intuit Inc. is an American company that concentrates on financial software. Through Intuit's partnership with AWS, they instantly and frequently provision the servers required to simulate the targeted user traffic.

Many more entities trust AWS to achieve great heights in their journey to the cloud.