



# **AWS Security for Developers & How to 10X your skills!**

by Ashish Rajan



# Overview of AWS

## Infrastructure

AWS provides a wide range of computing services and infrastructure to help businesses grow and scale.

## Services

AWS offers over 200 services, including compute, storage, databases, analytics, and machine learning.

## Global Reach

AWS operates in 25 regions around the world, enabling organizations to serve customers in different geographical locations.

## Market Leader

AWS is the market leader in cloud computing, providing reliable and secure cloud infrastructure and services since 2006.



# Importance of Security in



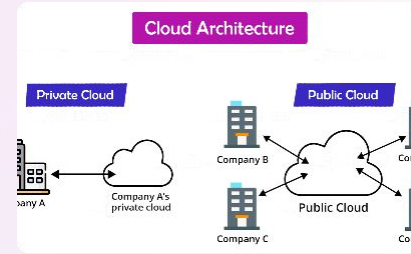
## Protect Sensitive Data

AWS provides services and tools to help businesses protect their sensitive data from unauthorized access, use, or disclosure.



## Compliance

AWS makes it easy for businesses to achieve compliance with industry standards and regulations.



## Cloud Architecture

Security in the cloud is a shared responsibility between AWS and the customer. AWS provides the necessary tools to build secure applications in the cloud



# AWS Shared Responsibility Model

1

## Responsibilities of AWS

AWS is responsible for security of the cloud including infrastructure, hardware, and software

2

## Responsibilities of Developers

Developers are responsible for security in the cloud including applications, data, and identity and access management.

3

## Explanation of Shared Responsibility Model

The shared responsibility model defines who is responsible for what in the AWS ecosystem. Understanding this model is crucial for building secure applications in the cloud.



# AWS Security Best Practices

1

## Secure Access Management

AWS Identity and Access Management (IAM) can be used to manage user accounts and permissions to AWS resources.

2

## Data Encryption

AWS Key Management Service (KMS) allows you to encrypt your data stored in AWS and control the encryption keys.

3

## Network Security

AWS offers several tools and services to secure your network, such as Amazon VPC, Security Groups, and Network ACLs.

4

## Incident Response and Monitoring

AWS Inspector and AWS Config can be used to monitor your AWS resources for security issues and compliance violations.



# AWS Security Tools

## **AWS Identity & Access Management (IAM)**

IAM enables you to manage access to AWS services and resources securely. You can create and manage users, groups, and permissions as required.

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

KMS is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data.

## **AWS Inspector**

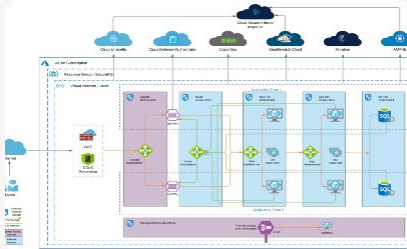
Inspector is an automated security assessment service that helps improve the security and compliance of your application deployed on AWS.

## **AWS Config**

AWS Config provides a detailed inventory of your AWS resources and associated metadata to enable compliance auditing, and troubleshooting.



# Conclusion



## Recap of Key Points

AWS provides a wide range of tools and services to help developers build secure applications in the cloud. The shared responsibility model defines who is responsible for security in the cloud.



## Importance of Prioritizing Security

By prioritizing security in AWS development, businesses can protect their sensitive data, achieve compliance, and build secure and scalable applications in the cloud.



## Collaboration

Collaboration between AWS and developers is essential for building secure applications in the cloud. With AWS, developers can build secure and scalable applications.





# Let's 10X this!

ChatGPT Custom Agent



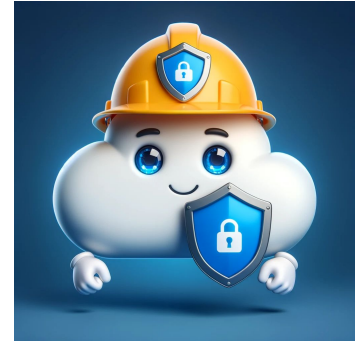




# ChatGPT Custom Agents

Announced Nov 6, 2023 at OpenAI Dev Day.  
An AI agent that can be configured to learn what you wanted to learn.

# Introducing Cloud Guardian



AI based Cybersecurity Assistant with deep knowledge for Cloud Security in Public & Hybrid Cloud environments.

# Demo?



## Cloud Guardian


I'm an AI based Cybersecurity Assistant with deep knowledge for Cloud Security in Public & Hybrid Cloud environments.

How do I secure my cloud application?

Best practices for AWS cloud security?

Tell me about the latest in cloud security

Explain public cloud vulnerabilities

 Message Cloud Guardian...



ChatGPT can make mistakes. Consider checking important information.

# AI Action = Github Actions for AI

Using Zapier

# Zapier Integration for AI



**AWS Lambda Integrations**  
Amazon, Developer Tools



**Azure DevOps Integrations**  
Developer Tools, Microsoft



**GitHub Integrations**  
Developer Tools



**tiktok**



**TikTok Conversions**



**Vookmark**



**TikTok Lead Generation**



**Instagram**



**YouTube**



Product ▾

Solutions ▾

Resources & Support ▾

Pricing

Free Google Ads Zaps through De

## Sort Apps By

Top 100 Apps

Premium

Beta

Recently Launched

[Expand all](#)

## App Categories

▾ App Families

▾ Artificial Intelligence

▾ Business Intelligence

▾ Commerce

🔍 github|



GitHub



Reddit



PSOhub



GitScrum



sproof



Redbooth



mailfloss



GitLab

# What Knowledge?

Not the one that finished in April,2023

## Github Knowledge

<https://github.com/hashishrajan/CloudGuardian/>

PR Please!

# Questions?

Cloud Security Podcast: [www.cloudsecuritypodcast.tv](http://www.cloudsecuritypodcast.tv)

Cloud Guardian - Training Data: <https://github.com/hashishrajan/CloudGuardian/tree/main>

Cloud Guardian AI Agent - <https://chat.openai.com/g/g-VQihKqtCa-cloud-guardian>