Top 10 AWS Security *best practices for financial services*

ClickIT
DevOps & Software Development

In a Cloud Platform like AWS, there are services used for multiple purposes like storing data, accessing productivity tools, and deploying IT infrastructure. In all these use-cases, cloud services allow organizations to move faster. However, the use of any cloud service or AWS comes with challenges and risks of data security.

ClickIT
DevOps & Software Development

Cloud Security practices consist of some general best practices that organizations should follow to secure the application environment. These guidelines also show you **how to successfully lift, shift and operate your business on the cloud.**

ClickIT
DevOps & Software Development

1 *DevSecOps Adoption*

DevSecOps is a relatively new term. It is about introducing security in the Software Development Life Cycle (SDLC). DevSecOps is a **collaboration between Development and Operations teams in DevOps to include security teams** as well. In short, DevSecOps is a shared responsibility, and everyone involved in Software Development has a role to play in building security into the DevOps workflow.

2 Amazon Web application Firewall

AWS WAF is a Web Application Firewall that helps to **protect applications hosted on AWS Cloud** against the common web threats that can affect the applications' availability, security, and can also consume infrastructure resources and lead to slowness and increased resource usage.

3 *Amazon Security Groups*

Security Group acts as a **virtual firewall for EC2 instances on AWS Cloud** to control inbound and outbound traffic flow and provides Cloud Security. Security Groups operate at the instance level, and **each instance can have up to five security groups attached to it.** You can not block incoming traffic but only allow it on a particular port or a range of ports.

4 *Threat detection system like Amazon Guard Duty*

This does not provide security but continuously monitors malicious activity and unauthorized behavior to detect threats and protect accounts, workloads, and data stored in Amazon S3 buckets. Guard Duty **is an intelligent and cost-effective option** for continuous threat detection on AWS Cloud. Guard Duty uses machine learning, anomaly detection, and integrated threat intelligence to **identify and prioritize potential threats.**

5 *Amazon Inspector*

AWS Inspector is an automated security assessment service. It helps to **improve the compliance and security of the applications** deployed on the AWS Cloud and achieve Cloud Security.
It **automatically assesses applications for vulnerabilities**, exposure, and deviations and produces a detailed report of security findings prioritized by severity level.

6 *CloudTrail and CloudWatch to monitor AWS resources*

CloudTrail:

CloudTrail **simplifies compliance audits** by automatically recording and storing event logs for actions made within the AWS account and increasing visibility into your resource and user activity. Cloud trail enables compliance, governance, operational auditing, and risk auditing of the AWS account. It **simplifies functional analysis and troubleshooting.**

CloudWatch:

The Cloudwatch service provided by AWS can achieve monitoring and observability. It **provides data to monitor applications deployed in the AWS account.** The same monitoring data can optimize resource utilization and get an insight into the application’s health. Y**ou can use Cloudwatch to set alarms**, get alerted, visualize logs and metrics, take automated actions, and discover insights to keep your applications running smoothly.

7 Key management system for accessing API, Database, Application, Compute, etc. (Amazon KMS)

To perform any kind of encryption, a cryptographic key is needed. Managing this key is again a challenging task. AWS KMS(Key Management Service) makes it easy to create and manage these cryptographic keys. It also **controls its use across various AWS services and applications.**

8 Cloud Security Frameworks

Till now, we have seen challenges, risks, and a few of the AWS Security Best Practices. However, there are specific policies, tools, rules, configurations needed to manage the security of a cloud platform. Cloud Security Frameworks outline these security standards and organizational guidelines.

9 End-to-end encryption (TDE) 256-bit encryption

End-to-End encryption is a method to encrypt the communication and secure it from third parties. TDE, Transparent Data Encryption, encrypts stored data on DB instances and is supported by AWS RDS for SQL Server (SQL Server Enterprise Edition) and Oracle (Oracle Advanced Security option in Oracle Enterprise Edition). TDE **encrypts data automatically before it is written to database** or storage and decrypts when it is read from the database or storage.

10 Penetration Testing on AWS

AWS permits its users to carry out Penetration Tests on certain services(8 Services as of June 21, 2021) in their accounts. The user must abide by the policies set by AWS for such tests. You can carry out pen-tests on your AWS account by following the policies and guidelines at Penetration Testing. You **don’t need any approval from AWS to carry out pen-tests against your account.** Also, contracted third parties can perform security assessments that do not violate the policy defined by AWS.

Security is a shared responsibility between AWS and its customers. **You can trust AWS as it has proven itself to be a strong Cloud partner**. However, you should verify. Also, by following AWS Security Best Practices and Cloud Security Standards, you can build a more secure environment to host your applications. Most of the time, misconfiguration and improper access practices are responsible for data breaches and illegitimate access.

ClickIT
DevOps & Software Development

What is your best AWS Security practice?

Comment below!

ClickIT
DevOps & Software Development