HELECLOUD

10 best practices for ensuring your AWS Cloud Security

As more and more organisations adopt cloud computing services and migrate their data to Amazon Web Services (AWS), cloud security is becoming an increasingly important topic in today's cybersecurity. Although AWS has some of the best security features available to secure their infrastructure, each organisation still has its own responsibility due to the shared responsibility model. This article outlines the top 10 best practices for ensuring your AWS cloud security.

The shared responsibility model

Let's first dive into the AWS shared responsibility model. Security and Compliance is shared between AWS and the customer. AWS operates, manages, and controls the security of the host operating system, the virtualization layer and the physical security of the facilities in which the service operates. The customer is responsible for the management of guest operating system, other associated application software as well as the configuration of the AWS provided security group firewall. The difference between these types of responsibility is sometimes referred to as the security "of" the Cloud (i.e. AWS responsibility) versus security "in" the Cloud (i.e. the customers responsibility).

Put simply, AWS is responsible for the security of the Cloud and for protecting the infrastructure that runs all the services AWS is offering but the customer is responsible for the security in the Cloud; the degree of responsibility is largely dependent upon the AWS Cloud services the customer selects.

Learn more about the AWS shared responsibility model **here.**

Best practices

Now that the shared responsibility model has been explained let's examine the best practices.

1. Implement security as a part of your cloud strategy

It is important to make sure you implement security as a part of your cloud strategy to ensure it is integrated immediately. Later on, you can always evaluate how well it works for your overall cloud strategy and adjust it accordingly.

HELECLOUD

2. Apply security in every single layer

Once you have set up security as an integral part of your cloud strategy, ensure you apply security in every single layer. This is sometimes referred to as a 'defense in depth' approach with multiple mechanisms used to secure an environment. For example, define a web application firewall at the perimeter and then define additional controls at the VPC, load balancer, EC2 instance, operating system, application and code. This means that if one security control fails there are multiple others providing a second line of defense and protecting the environment. AWS provides many security related products and services that support a defense in depth approach and can apply security at every single layer.

3. Create policies around security and keep them up to date

As mentioned earlier, security is a shared responsibility between you and AWS. Although AWS is securing the Cloud and offers a rich eco-system of security features, you are still responsible for the policies that drive security in the cloud and protect your own infrastructure; for example advanced malware can still target your infrastructure. Ensure your policies clearly delineate your responsibilities (e.g. install anti-malware and keep the anti-viral signatures up to date) vs. Amazon's responsibilities and store them in a place where all individuals within your team can access the policies. Also make sure you involve your security team in setting up these policies and have the documents reviewed regularly for the latest security updates. This way, everyone within your organisation is aware of the security policies and most importantly, the policies are never outdated.

4. Monitor User access

Not monitoring user access is one of the most common mistakes made on AWS. However, AWS requires you to manage your own access control policies, so make sure you have them included in your security policies. The AWS Management Console allows you to manage and monitor user access to your resources and instances. By monitoring user access you ensure no unauthorized access is taking place. You must continuously work to define the least privilege necessary for persons or systems accessing data.

Hiring or firing? Also make sure that the person who has left the company no longer has access. When you're hiring, only give access to those resources and instances relevant to them.

5. Make use of well-integrated AWS security services

AWS offers well-integrated security services. It is highly recommended that you make use of these too. The services AWS offers around security are divided into identity & access management, detection, infrastructure protection, data protection, incident response and compliance.

HELECLOUD

For example, you can use Amazon Cognito for identity management for your applications or Amazon GuardDuty as a managed threat detection service. **Take a look here to learn more about AWS security offerings.**

6. Keep your AWS practices up to date

AWS is constantly evolving and launching new services. It can be challenging to keep up to date with AWS practices, but it is necessary to keep up to date to ensure cloud security. And don't forget to continually include new practices in your policy as discussed in point 3.

7. Backup data regularly

This is something that shouldn't need to be said and yet it's still something customers often overlook, so we will say it again: backup your data and do it regularly. AWS offers backup solutions to ensure you can backup your data regularly on the cloud. Through their solutions, you can manage and automate backups across AWS services.

8. Keep your SSL/TLS certificates updated

Renew your SSL/TLS certificates before they expire to avoid embarrassing security alerts in your client browsers or even better use the AWS Certificate Manager (ACM) to issue and automatically renew your certificates for you. Even better, certificates issued by ACM are totally free to AWS users! One less thing to worry about.

9. Encrypt information

Encrypting sensitive information and storing/retrieving encryption keys in AWS is rather easy thanks to Amazon Key Management Service (KMS). All AWS services that handle customer data, encrypt data in motion and provide options to encrypt data at rest. You can enable encryption in Amazon Elastic Block Search (EBS), in Amazon S3 and Amazon Relational Database Service (RDS).

10. Regularly carry out Security Posture Assessments (SPA) and/or Penetration (PEN) Tests

You can carry out security assessments or penetration tests against your AWS infrastructure without prior approval to identify weaknesses in your security posture.

Contact a recognized AWS partner like HeleCloud to conduct an AWS security posture assessment to ensure that your environment is configured against best practice to minimize the risk of compromise. Additionally, if you wish to determine if your environment is vulnerable to attack, then we recommend conducting a Penetration Test. An external Penetration test will

HELECLOUD

test your system against attacks launched from outside of your network perimeter whereas an internal Penetration test focuses upon testing attacks which would be carried out by an adversary who has already gained access to your network.

PEN testing is supported for the following 8 services:

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Beware, there are also activities that are prohibited by AWS:

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS (These are subject to the **DDoS Simulation Testing policy**)
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

The activities you carry out need to be aligned with AWS security policy.

Conclusion

Gartner predict that by 2025, 99% of cloud security failures will be the customer's fault. Security is a shared responsibility between AWS and you. Although AWS has the best security features, you still must ensure the security of your own infrastructure. Organisations can take advantage of AWS services to maximise their agility and by following security best practices.