UltraHeals

AWS Cloud Security Checklist

S.NO	AWS Cloud Security Checklist		Implemented	
			Yes	No
1	Identity and Access Management (IAM)	Use Strong Identity Foundations: Implement multi-factor authentication (MFA) for AWS accounts.	☐	☐
2	Identity and Access Management (IAM)	Least Privilege Principle: Ensure that permissions are given based on the minimum required for the role.	☐	☐
3	Identity and Access Management (IAM)	Use IAM Roles: Assign roles to services rather than permanent credentials.	☐	☐
4	Identity and Access Management (IAM)	Enable AWS IAM Access Analyzer: To review and monitor access to resources across accounts.	☐	☐
5	Data Protection	Encrypt Data at Rest: Use AWS Key Management Service (KMS) for encrypting data stored in S3, RDS, DynamoDB, and EBS.	☐	☐
6	Data Protection	Encrypt Data in Transit: Implement SSL/TLS for securing data communication in transit.	☐	☐
7	Data Protection	Backup and Restore: Ensure regular backups using AWS Backup and set recovery point objectives (RPO) and recovery time objectives (RTO).	☐	☐
8	Network Security	Use VPC: Segment your infrastructure into public and private subnets. Place sensitive resources in private subnets.	☐	☐
9	Network Security	Use Security Groups and NACLs: To control inbound and outbound traffic, apply least privilege access.	☐	☐
10	Network Security	Minimize Network I/O: Reduce unnecessary traffic between availability zones or regions to control costs and improve security.	☐	☐
12	Network Security	Use AWS Shield and AWS WAF: Protect against DDoS attacks and application-layer vulnerabilities.	☐	☐
13	Monitoring and Incident Response	Enable CloudTrail and GuardDuty: For logging, auditing, and detecting unusual activity in your environment.	☐	☐

S.NO	AWS Cloud Security Checklist		Implemented Yes	Implemented No
14	Monitoring and Incident Response	Enable Amazon CloudWatch: For monitoring logs, metrics, and setting up alarms on your infrastructure.	☐	☐
15	Monitoring and Incident Response	Incident Response: Continuously monitor systems for threats.	☐	☐
16	Infrastructure Protection	Multi-AZ Architecture: Ensure critical services (e.g., RDS, EC2) are deployed across multiple availability zones to ensure high availability.	☐	☐
17	Infrastructure Protection	Auto Recovery: Configure auto-scaling and auto-recovery for EC2 instances.	☐	☐
18	Infrastructure Protection	Protect Serverless Resources: Apply IAM roles for Lambda and API Gateway, and enable throttling to avoid overuse.	☐	☐
19	Infrastructure Protection	Use Bastion Hosts: For accessing instances in private subnets securely.	☐	☐
20	Regular Security Audits	Enable AWS Trusted Advisor: Regularly check security best practices, especially for permissions and data encryption.	☐	☐
21	Regular Security Audits	Security Reviews: Conduct regular internal audits and use AWS Security Hub for continuous monitoring and improving your security posture.	☐	☐

Business Advantages of Implementing a Cloud Security Checklist for SaaS Startups

Implementing this cloud security checklist in AWS enhances a SaaS startup's security posture, builds customer trust, and ensures regulatory compliance. By securing access, encrypting data, and automating monitoring, the startup minimizes the risk of breaches and downtime. This approach not only protects sensitive data but also ensures high service availability, improving customer satisfaction and reducing operational costs. Overall, it strengthens business resilience and supports long-term growth by reducing risks and maintaining a secure, efficient environment.

Get Free Demo

UltraHeals

Cyber Heals Ltd - UK
71-75, Shelton Street,
Covent Garden, London, WC2H 9JQ

sales@cyberheals.com