K7

# Cloud Security Hardening Checklist (AWS /

3 pages • CyberK7 Whitepaper

*A practical, provider-by-provider checklist covering IAM least-privilege, storage configuration, logging and network security group hardening.*

## 1. Identity & Access Management

Enforce least-privilege IAM roles across all accounts — audit existing roles quarterly and remove unused permissions. Enable multi-factor authentication on all privileged and root/owner accounts without exception.

## 2. Storage & Data Protection

Audit all storage buckets and containers for public access — this remains the single most common cause of cloud data exposure. Encrypt data at rest and in transit by default across every service, not as a manually-applied exception.

## 3. Logging & Monitoring

Enable native logging (CloudTrail, Azure Monitor, Cloud Audit Logs) across all accounts and regions. Centralize these logs into a SIEM for correlation — logs sitting unreviewed in native consoles provide little practical protection.

## 4. Network Security

Review security groups and network security groups quarterly. Testing-phase configurations have a tendency to become permanent if nobody actively reviews and removes them.

## 5. Containers & Kubernetes

Scan container images for known vulnerabilities before deployment, not after. Apply Kubernetes RBAC and network policies to prevent lateral movement between workloads sharing a cluster.

## About CyberK7

CyberK7 is a cybersecurity consulting firm based in Delhi, India, helping organizations build secure, resilient and compliant digital environments through GRC, VAPT, SOC monitoring, cloud security, IAM, EDR/XDR, backup & disaster recovery, and security awareness training.

Our consultants hold certifications including CISA and ISO 27001 Lead Auditor, with hands-on experience across banking, healthcare, manufacturing, education and fast-growing startups.

To discuss how this whitepaper applies to your organization, reach us at info@cyberk7.com or +91 98990 62199.

## Quick Reference

| Area | AWS | Azure | GCP |
|---|---|---|---|
| IAM Review Tool | IAM Access Analyzer | Azure AD Access Reviews | IAM Recommender |
| Logging Service | CloudTrail | Azure Monitor | Cloud Audit Logs |
| Storage Scan | S3 Public Access Block | Storage Firewall Rules | Bucket IAM Policies |
| Posture Management | AWS Security Hub | Microsoft Defender for Cloud | Security Command Center |

*For a tailored consultation, contact CyberK7 at info@cyberk7.com or +91 98990 62199.*