K7

# Cloud Security Hardening Checklist (AWS / Azure / GCP)

3 pages • CyberK7 Whitepaper

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



CyberK7 | Delhi, India | cyberk7.com

## 1. Identity & Access Management

Enforce least-privilege IAM roles. Enable MFA on all privileged and root/owner accounts without exception.

## 2. Storage & Data Protection

Audit all storage buckets for public access. Encrypt data at rest and in transit by default.

## 3. Logging & Monitoring

Enable native logging across all accounts and regions, centralized into a SIEM.

## 4. Network Security

Review security groups quarterly — testing configurations have a way of becoming permanent.

## About CyberK7

CyberK7's Cloud Security team helps secure AWS, Azure and GCP environments. Contact 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 |

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