CLOUD SECURITY CHEAT SHEET

Misconfigurations & How to Fix Them (AWS + Azure)

Use this as a practical reference to secure your cloud environment during implementation or audits.

PUBLICLY ACCESSIBLE STORAGE

MISCONFIGURATION: Storage like S3 buckets or Azure Blob Containers are left open to the public.

BEST PRACTICE: Secure data with encryption & enforce private access only.

AWS

1. Block public access for all S3 buckets via S3 > Block Public Access Settings.
2. Enable S3 bucket policies to enforce IAM-controlled access.
3. Turn on S3 Server-Side Encryption (SSE) with KMS.

AZURE

1. Set public access level to "Private" in Blob container settings.
2. Use firewalls and virtual networks to restrict access.
3. Enable Storage Service Encryption (SSE) and Azure Key Vault integration.

OVERLY PERMISSIVE IAM POLICIES/ROLE TRUSTS

MISCONFIGURATION: Use of * in actions or resources; broad trust policies.

BEST PRACTICE: Implement least privilege access.

AWS

1. Use IAM Access Analyzer to detect overly broad permissions.
2. Replace * with specific actions and resources.
3. Use Service Control Policies (SCPs) in AWS Organizations.

AZURE

1. Use Azure Role-Based Access Control (RBAC) with fine-grained roles.
2. Audit roles via Privileged Identity Management.
3. Limit role assignments to specific resource scopes.

HARDCODED OR EXPOSED SECRETS

MISCONFIGURATION: Credentials stored in code, scripts, or GitHub.

BEST PRACTICE: Use secure credential management and protect secrets.

AWS

1. Store secrets in Secrets Manager or Systems Manager Parameter Store.
2. Rotate secrets automatically and regularly.
3. Scan repositories for hardcoded credentials using third-party tools.

AZURE

1. Store secrets in Key Vaults.
2. Set up Key Vault access policies and enable logging.
3. Scan repos with third party scanners.

UNRESTRICTED INBOUND NETWORK ACCESS

MISCONFIGURATION: Open ports (e.g., SSH/RDP) accessible from anywhere.

BEST PRACTICE: Use network segmentation and restrict inbound traffic.

AWS

1. Use Security Groups with strict inbound rules (limit to IP or CIDR).
2. Employ Network ACLs for added control.
3. Use Network Firewall or WAF for inspection and control.

AZURE

1. Use NSGs (Network Security Groups) with limited IP rules.
2. Enable Just-In-Time VM Access via Azure Security Center.
3. Use firewalls or DDoS Protection.

DISABLED/INCOMPLETE LOGGING & MONITORING

MISCONFIGURATION: No audit trail or alerting set up.

BEST PRACTICE: Enable logging, threat detection, and incident response.

AWS

1. Enable CloudTrail across all regions.
2. Set up AWS Config to track resource changes.
3. Use third party security tools for threat detection.

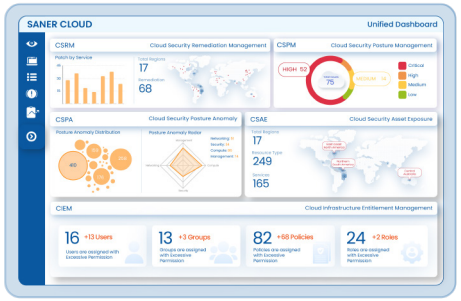
AZURE

1. Enable Azure Activity Logs and Diagnostic Logs.
2. Use Azure Monitor, Log Analytics, and Microsoft Defender for Cloud.
3. Set up SIEMs for incident response workflows.

KEY TAKEAWAY

By avoiding the top 5 misconfigurations & adopting the top 5 best practices, you reduce your cloud attack surface by 70–90%.

These measures help secure against data leaks, credential theft, ransomware, and more — making your cloud environment resilient and compliant.



ABOUT SECPOD

SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

www.secpod.com

secpod