

Cloud Security

Find the misconfigurations and access paths in your AWS, Azure and Google Cloud environments

Moving to the cloud changes who is responsible for what. Your provider secures the infrastructure underneath, and you remain responsible for everything you configure on top of it: identities, permissions, storage, networks and the workloads you deploy.

Most cloud breaches start with a misconfiguration rather than a software flaw. A public storage bucket, an over-privileged IAM role, an access key committed to a code repository or a management port open to the internet can expose an entire environment.

SentryArk's cloud security assessment reviews your configuration against best practice, then tests it the way an attacker would, so you know which issues can actually be exploited.

CONFIGURATION REVIEW AND CLOUD PENETRATION TESTING

We start with an authenticated, read-only review of your accounts, subscriptions and projects against the CIS Benchmarks and each provider's security best practice. We then test from an attacker's starting point, such as a leaked credential, a compromised workload or a low-privileged user, and show how far they could escalate.

- | | | |
|-----------------------------|------------------------------|-----------------------------|
| ■ AWS | ■ Microsoft Azure | ■ Google Cloud |
| ■ Kubernetes and containers | ■ Microsoft 365 and Entra ID | ■ Serverless and IaC review |

IDENTITY AND ACCESS ATTACK PATHS

In the cloud, permissions decide what an attacker can reach. We map IAM roles, policies, service accounts and trust relationships to find privilege escalation paths, cross-account access and dormant keys. Findings are grouped by the attack path they enable, so your team can fix the root cause in one change.

All testing stays within each provider's penetration testing policy and the scope you approve, and nothing is changed in your environment without your agreement.

ASSESSMENT DETAILS AND METHODOLOGY

Our cloud methodology combines automated configuration analysis with manual testing by engineers who work in AWS, Azure and Google Cloud. It follows the CIS Benchmarks, each provider's security best practice and the shared responsibility model, and covers single accounts through to multi-account organisations.

Planning and access	01	Accounts, subscriptions and services in scope are agreed, and you grant read-only audit access for the configuration review.
Configuration review	02	Identity, logging, storage, networking, encryption and compute settings are checked against the CIS Benchmarks and provider best practice.
Attack path analysis	03	IAM policies, roles and trust relationships are mapped to find privilege escalation and lateral movement paths across accounts and services.
Exploitation	04	From agreed starting points such as a leaked key or a compromised container, we safely exploit findings to show the real impact on your data and workloads.
Reporting and retest	05	Findings come with risk ratings and fix steps for the console, CLI and infrastructure as code, and a free retest once you've patched.

The assessment includes

- Executive summary
- Misconfigurations and risk ratings
- Remediation steps for console, CLI and IaC
- CIS Benchmark compliance scorecard
- IAM attack path analysis
- Retest report confirming fixes

ABOUT SENTRYARK

SentryArk is a team of security engineers and offensive security specialists. Our consultants hold OSCE, CRYPTO and CEH certifications. We have secured 20+ organisations, assessed 8K+ devices and 30+ applications, and reported 250+ vulnerabilities. Our focus is offensive security that shows the real-world risk to your business.