



CLOUD PENETRATION TESTING

We target your cloud the way real adversaries do, across identity, infrastructure, and the applications running on top.

Your business runs on the cloud and your attackers know this. A cloud-focused penetration test goes further than reviewing settings. We actively exploit the misconfigurations, over-permissioned identities, and exposed applications in your environment to prove exactly how far an intruder can get. Whether your stack runs on Azure, AWS, or GCP, we test the full surface area, from the control plane down to the APIs and web apps on top. We won't provide just a configuration checklist, **we'll give you proven attack paths, and the fixes to close them.**

WHERE WE ATTACK

Cloud Control Plane & Config



We hunt the misconfigurations attackers love, like public storage and exposed management interfaces. These are the most common entry points for hackers.

Identity & Access Management (IAM)



Over-permissioned roles, stale keys, and weak trust relationships are the fastest route to full compromise. We escalate privileges and assume identities the way a real adversary would.

Web Applications



The apps in your cloud, from COTS applications to AI-built tools, are prime targets. We don't just run automated scans, we see how resistant they are to true exploit attempts.

APIs & Integrations



Internal and external APIs quietly expand your attack surface. We probe for broken authentication, excessive data exposure, and business logic flaws that scanners can miss.

Compute, Containers & Pipelines



Virtual machines, Kubernetes clusters, serverless functions, and CI/CD pipelines each carry their own risks. We test the workloads and the automation that deploys them.

Lateral Movement & Impact



A single foothold is rarely the whole story. We chain attacks across your tenant to prove what an attacker could actually reach, control, and exfiltrate.

WHY SEVN-X

Cloud providers set strict rules of engagement, and testing safely inside them takes experience many companies don't have. We have built and broken cloud environments ourselves. We lead with testing by hand, we chase real-world impact instead of framework checkboxes, and **we stick around to help you remediate, with a report that speaks to engineers and executives alike.**

● Real exploitation, not scans

● Cloud-native and app-layer

● We help you remediate

