OnDefend

Cloud Penetration Testing

Expose Hidden Cloud Vulnerabilities and Attack Paths

Cloud environments introduce risks that configuration reviews alone can't validate - misconfigured permissions, exposed storage, and identity weaknesses that attackers exploit to escalate privileges and move laterally.

OnDefend cloud penetration testing uncovers vulnerabilities and attack paths across AWS, Azure, GCP, OCI, and hybrid environments, supporting SOC 2, ISO 27001, HIPAA, PCI DSS, and NIST compliance.

Testing Capabilities

Amazon Web Services (AWS)
Identifies misconfigurations, IAM weaknesses, and control gaps across AWS services and workloads.

Microsoft Azure
Assesses identity, networking, and application controls in Azure for exploitable weaknesses.

Google Cloud Platform (GCP)
Identifies exposure across GCP services, workloads, and GKE Kubernetes environments.

Other Cloud Platforms
Tests OCI, IBM Cloud, private, hybrid, and multi-cloud environments, including containers and IaC.

Outcomes

- Misconfigurations, IAM weaknesses, exposed APIs, and insecure workloads identified and prioritized
- Prioritized findings with severity ratings, affected cloud resources, and remediation steps
- Validated cloud security controls across AWS, Azure, GCP, and hybrid environments
- Compliance evidence for SOC 2, ISO 27001, HIPAA, PCI DSS, NIST, and related frameworks

By validating cloud security against real attacker techniques, organizations can reduce exposure, improve configuration hygiene, and operate in the cloud with confidence.

OnDefend.com