OnDefend

Network Penetration Testing

Uncover Hidden Attack Paths Across Your Networks

Standard scans identify potential weaknesses but can't show how attackers move through your environment, escalate privileges, or bypass controls. Uncovering real network risk requires simulating a real adversary.

OnDefend network penetration testing validates attacker behavior across your network layers, delivering prioritized findings and compliance support for SOC 2, ISO 27001, HIPAA, PCI DSS, and NIST.

Testing Capabilities

External Network Testing

Tests internet-facing systems for vulnerabilities, exposed services, and perimeter control gaps.

Internal Network Testing

Evaluates internal vulnerabilities and excessive privileges to assess lateral movement risk.

Active Directory Testing

Tests domain configurations and trust relationships to identify privilege escalation paths.

Wireless, VPN & Remote Access

Tests Wi-Fi, VPN, and remote access for authentication weaknesses and segmentation gaps.

Outcomes

- Vulnerabilities, misconfigurations, and weak authentication identified and prioritized
- Prioritized findings with severity ratings, affected systems, and remediation steps
- Reduced attack surface across internal, external, wireless, VPN, and AD environments
- Compliance evidence for SOC 2, ISO 27001, HIPAA, PCI DSS, NIST, and related frameworks

By validating how attackers move and persist within your network, organizations can reduce exposure, accelerate remediation, and build confidence in their security posture.

OnDefend.com