OnDefend

Application Penetration Testing

Uncover Application Vulnerabilities Before Attackers Do

Automated scanners find surface-level issues but miss business logic flaws, access control weaknesses, and chained attack paths. Real application risk requires hands-on validation by operators who think like adversaries.

OnDefend application penetration testing maps real-world attack paths and validates security controls across web, mobile, desktop, and API applications, supporting requirements for SOC 2, ISO 27001, HIPAA, NIST, and PCI DSS.

Testing Capabilities

Web Application Testing

Tests web applications for exploitable vulnerabilities, logic flaws, and access control weaknesses.

Mobile Application Testing

Evaluates iOS and Android apps for authentication weaknesses, insecure storage, and backend risks.

Desktop Application Testing

Assesses execution permissions, update mechanisms, and backend communication in desktop apps.

API Security Testing

Tests APIs for weak authentication, authorization failures, input handling flaws, and data exposure.

Dynamic Application Testing

Evaluates live applications for injection flaws, authentication weaknesses, and access control issues.

Source CodeAnalysis

Analyzes source code to detect insecure coding patterns, logic errors, and vulnerabilities before deployment.

Outcomes

- Exploitable vulnerabilities, logic flaws, and access control weaknesses identified and prioritized
- Prioritized findings with severity ratings, affected components, and remediation steps
- Validated security controls across web, mobile, desktop, and API environments
- Compliance evidence for SOC 2, ISO 27001, HIPAA, PCI DSS, NIST, and related frameworks

By validating application security before release, organizations can prevent exploitation, reduce remediation costs, and deliver software customers can trust.

OnDefend.com