



Penetration Testing Assess Services

Validating real-world risk through expert-led penetration testing

Service Overview

Penetration testing provides a clear, evidence-based view of how a capable attacker could exploit your organisation today, helping move from assumed risk to validated, real-world exposure.

The service delivers targeted testing across external infrastructure, web applications, and APIs, enabling organisations to assess individual attack surfaces or gain a complete view of their external security posture.

Delivered by CloudGuard's expert security consultants, the engagement produces validated, prioritised findings with clear remediation guidance enabling organisations by supporting faster risk reduction, audit readiness.

Penetration testing remains a critical control as external attack surfaces continue to expand across cloud, applications, and APIs, increasing the number of exploitable entry points.

- **Readiness** – Identify exploitable exposure before attackers do
- **Responsiveness** – Rapidly detecting and validating exploitable risk
- **Resilience** – Strengthening defences through evidenced, actionable insight

Service Value

The Value the Entra Assess Service Delivers:

- Clear visibility of exploitable vulnerabilities across external infrastructure, Web applications, and APIs
- Evidence-based understanding of real-world risk, validated by expert consultants
- Prioritised, actionable recommendations to support targeted security hardening
- Audit-ready reporting aligned to ISO 27001, PCI DSS, SOC 2 and customer due diligence requirements
- Reduced false positives through consultant-led validation and contextual risk analysis
- Improved confidence in security posture for technical teams, leadership, and external stakeholders

Why this matters now

As organisations expand across cloud, web applications, and APIs, their external attack surface grows, introducing more exploitable entry points for attackers. Traditional scanning and compliance assessments do not reveal how vulnerabilities can be exploited in practice, making penetration testing critical for understanding real-world risk and prioritising remediation effectively.

Penetration Testing Service Scope

Our Penetration Testing service aligns to the five service components:

External Infrastructure

Assessment of internet-facing IP ranges, endpoints, and cloud-hosted services to identify exploitable vulnerabilities across the external perimeter.

Web Applications

Testing of in-scope web applications (authenticated and unauthenticated) to identify weaknesses in application logic, authentication, and user flows.

API Security

Evaluation of API endpoints (REST, GraphQL, SOAP) to uncover vulnerabilities in data handling, authentication, and schema implementation.

Attack Surface Discovery

OSINT driven reconnaissance to identify exposed assets, map the true external attack surface, and highlight previously unknown risks.

Reporting & Recommendations

Delivery of technical and executive reports with validated, prioritised findings and actionable remediation guidance.

Our Approach

Delivered through a collaborative and supportive engagement:

Engagement Initiation – Confirm scope, asset inventory, testing objectives, and targeted asset information

Reconnaissance & Discovery – Identify and validate the true external attack surface using OSINT techniques

Active Testing – Perform automated and expert-led testing to identify exploitable vulnerabilities across the agreed scope

Expert Validation – Review, validate, and contextualise findings to eliminate false positives and prioritise real risk.

Report & Present – Deliver clear technical reporting with prioritised, actionable remediation guidance.

Why CloudGuard

CloudGuard delivers enterprise-grade cybersecurity for growing businesses. Combining automation-led technology with UK-based experts, we provide 24/7 protection, without the complexity or cost of traditional platforms. Our fully managed approach simplifies detection, protection and improvement, so you can focus on growing with confidence.

[Get in touch](#)

