PREPARED BY
Technology By Design

Penetration Testing

Penetration testing, or "pen testing," is a proactive cybersecurity practice that simulates real-world attacks against your systems, networks, or applications to uncover weaknesses before adversaries do. Unlike automated scans, penetration testing involves ethical hackers who think and operate like real attackers. This process helps organizations understand their true risk exposure and provides a roadmap for strengthening defenses.

How Can We Help?

Our penetration testing engagements follow a methodical approach that maximizes security insight and minimizes disruption:

Penetration testing is a critical reality check for your cybersecurity strategy. By safely exposing weaknesses, you gain insight, control, and confidence in your environment's ability to withstand real threats.

- **Scoping & Planning**
- **Reconnaissance & Enumeration**
- **Exploitation**
- **Post-Exploitation & Impact Analysis**
- **Assess Business Impact of Successful Exploitation**
- **Reporting & Remediation**
- **Optional Retesting**

Why It Matters?

Cyber threats are increasingly sophisticated and opportunistic. Many security gaps-such as misconfigured systems, insecure code, or flawed access controls-go undetected until it's too late. A penetration test exposes these vulnerabilities under controlled conditions, helping organizations close gaps before they're exploited. For regulated industries or those handling sensitive data, pen testing also supports compliance and customer trust.