

Mature your security posture with penetration testing.

Penetration Testing and Security Assessments

Over the past five years, penetration testing has undergone a remarkable transformation, becoming an indispensable asset for organizations worldwide. With the escalating sophistication of cyber threats, more businesses are recognizing the critical importance of comprehensive security measures. Penetration testing has evolved from merely checking a box for compliance to building a proactive strategy for safeguarding sensitive data and maturing your security posture. As a result, businesses are not just investing in penetration testing; they're investing in peace of mind and stronger cyber resilience.

Penetration Testing and Security Assessments can help you achieve:



**Reduced
Risk**



**Increased
Performance**



**Cost
Reduction**

Finding the Right Solution

While penetration testing is critical to identifying and remediating vulnerabilities within your organization, it can also play a significant role in driving the maturity of your overall security program. CDW's approach to penetration testing is intended to not just identify risk but to frame it in the context of your broader security landscape.

- **Penetration Testing Services:** CDW offers Internal, External and Web Application Penetration tests that are designed to assess the security posture of an organization's digital infrastructure. By simulating real-world cyberattacks, we identify vulnerabilities in networks, applications and systems, allowing businesses to address weaknesses before malicious actors exploit them. These comprehensive evaluations provide invaluable insights into potential risks, through focused paths to compromise. This enables organizations to prioritize resources and implement targeted security measures to mitigate threats effectively.
- **Security Assessments:** CDW's Security Assessments are Pen Test engagements that have been enhanced to deliver purpose-driven engagements built to look deeper and go further. The CDW Offensive Security Assessments start with penetration testing followed by deep analysis to help enumerate potential paths to compromise that may not be discovered in a standard penetration test.

CDW + PEN TESTING

CDW's Penetration Testing methodology is constantly being updated to represent the current state of the discipline. The Offensive Security team treats security not as a static skill set but as a practice that requires study and constant innovation.

Key Features

- Testing is based on current, real-world attack methodologies.
- Attack chains are designed to lead from initial contact to exploitation.
- Areas of strength and control gaps are documented.
- Analysis of risk and impact is based on actual risks, vulnerabilities and exploits.
- Prioritized recommendations are specific to your enterprise environment.
- Deliverables and summaries are tailored to security and executive/board stakeholders.

Benefits

- Provides a deep understanding of the risk and vulnerability state of your enterprise environment.
- Analyzes not just the technical environment, but also the critical services that support the domain.
- Delivers real-world understanding of the capability of your controls to defend against a breach.
- Provides risk, impact and cost-based insights into practical remediations for discovered issues.
- Empowers business leaders to improve cyber outcomes through fiscal strategies.

CDW's full lifecycle of Services can support your organization no matter where you are on your journey



Design



Orchestrate



Manage



On-Premises



On-Journey



Cloud-Based



Services Overview

CDW's Offensive Security solutions are an evolution in cyber risk management, providing a comprehensive assessment that drives both tactical security remediation advice and business-level investment recommendations.

Penetration Testing		Security Assessments	
Outcomes			
Identifies a viable path to compromise through testing and technique.	✓	Provides all the benefits of penetration testing plus additional potential paths to compromise.	✓
Provides updates and insights from highly collaborative consultants.	✓	Delivers a deep analysis of the components that govern your enterprise environment.	✓
Delivers practical recommendations to identify where changes can be made to improve security posture.	✓	Provides a review of configuration management to identify vulnerabilities in your environment.	✓
Services			
Internal Penetration Testing: Increases the overall security posture by identifying internal vulnerabilities, opportunities for privilege escalation and lateral movement.	✓	Configuration Management Assessment: Uses Authenticated Vulnerability Scanning to determine the risk associated with vulnerabilities in operating systems and applications.	✓
External Penetration Testing: Designed to help organizations proactively identify and assess their full external attack surface exposed to the internet.	✓	Domain Security Assessment: Assesses the configuration of Active Directory to help determine which configurations, users, groups or other items contribute to potential risk.	✓
Wireless Penetration Testing: Assesses an organization's wireless attack surface by identifying wireless assets and evaluating their respective security policies and implementations.	✓	Account Audit: Audits the account passwords and associated policies putting your organization at risk for compromise by attackers.	✓

Proofpoints

20+

Years of Pen Testing

50+

Dedicated Pen Testing
team members

100+

Individual certifications

PMO

A team of project managers
specializing in Pen Testing

**To learn more about Penetration Testing and Security Assessments,
contact your account manager or call 800.800.4239.**

