

PENETRATION TESTING SERVICES

Turn Hypothetical Questions Into Measurable Security Improvements

Organizations invest heavily in security tools and controls, but often lack full confidence those defenses will withstand evolving, real-world attacks when it matters most.

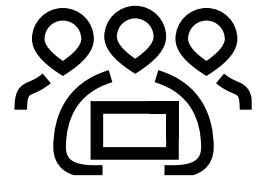
Organizations need to trust that their defenses will hold when an attack hits. GuidePoint Security's penetration testing service delivers evidence-based insight to confirm what is working, uncover what is not, and prioritize remediation based on real-world risk rather than theoretical vulnerability scores. Every tailored engagement translates complex technical findings into clear, actionable guidance that security teams and leadership can act on and close gaps with confidence.

Validate Defenses. Reduce Real Risk.

Traditional security testing cadences and approaches no longer reflect how modern attackers operate. Today's threat actors move fast, chain vulnerabilities together, and exploit misconfigurations across complex hybrid environments.

GuidePoint Security's Penetration Testing service delivers point-in-time and continuous expert-led assessments that reveal realistic attack paths to critical assets. GuidePoint Threat and Attack Simulation (TAS) team is composed of highly specialized and certified cybersecurity professionals who act as "ethical hackers" to test and improve an organization's security defenses. Their efforts give security teams a clear picture of actual risk exposure and a prioritized roadmap to strengthen defenses before attackers find the gaps to:

- ✓ **Understand real-world attack paths**, not just theoretical vulnerability lists
- ✓ **Validate existing security tools** to better detect and prevent actual threats
- ✓ **Receive prioritized remediation guidance** based on business risk and exploitability
- ✓ **Satisfy compliance requirements** for PCI DSS, HIPAA, SOC 2, and more
- ✓ **Communicate risk clearly** to leadership and the board with executive-ready reporting
- ✓ **Establish a security baseline** and measure program improvement over time



Stronger Together. Protecting What's Next.

Working with GuidePoint, your organization will be backed by our elite team of highly-trained cybersecurity engineers, architects and consultants who come from organizations of all sizes, including Fortune 100 companies, the Department of War, and U.S. intelligence agencies.



Expert-led Testing to Validate Defenses Against Real-world Attack Scenarios

GuidePoint's TAS team delivers penetration testing engagements tailored to each organization's specific environment, threat exposure, and security maturity. Certified offensive security professionals combine manual exploitation techniques with targeted tooling to uncover vulnerabilities that automated scanners routinely miss, including complex, multi-step attack chains and logic-based weaknesses unique to the organization's architecture.

GuidePoint's penetration testing services span the engagement lifecycle, including:

Internal Penetration Testing

Understand exactly how far an attacker could go if they gained a foothold inside the network. GuidePoint simulates insider threats and compromised endpoints to reveal the realistic business impact of an internal breach, test whether security monitoring would catch it, and identify the highest-priority gaps before a real attacker finds them first.

External Penetration Testing

Discover what attackers see before they ever touch the network. GuidePoint uncovers exploitable perimeter vulnerabilities and maps the Open Source Intelligence (OSINT) available to a determined threat actor, giving organizations a clear picture of external exposure and the insight needed to close critical gaps at the edge.

Scenario-based and Cloud Penetration Testing

Validate defenses against the specific threats that matter most to the organization. Whether the concern is ransomware, supply chain compromise, identity-based attacks, or misconfigured cloud infrastructure across AWS, Azure, or GCP, GuidePoint tailors engagements to answer the questions that keep security leaders up at night and confirm whether critical assets are truly protected.

Penetration-Testing-as-a-Service (PTaaS)

Move beyond periodic or annual assessments and maintain continuous confidence in security posture. GuidePoint's PTaaS model combines automated testing with ongoing expert-led assessments to surface vulnerabilities in real time as environments grow and threats evolve, so organizations are never more than one assessment cycle away from knowing where they stand.

Why GuidePoint Security

When sophisticated threats target the organization, knowing whether defenses will hold is not a question that can wait for the next scheduled assessment. GuidePoint Security designs and delivers tailored penetration testing engagements that put security controls, processes, and people to the test across any environment. With a team of experts and a proven methodology built around real-world attack techniques, GuidePoint helps organizations find exploitable gaps, prioritize what matters most, and build measurable confidence in their security posture. Accelerate the security program with certainty and protect what matters most.

About Us

GuidePoint Security brings together proven expertise, great relationships, and leading technologies to solve our client's most complex cybersecurity challenges. As a trusted cybersecurity advisor and partner, GuidePoint keeps people, data, and operations safe. We deliver tailored cybersecurity services that adapt to safeguard the nation's leading organizations today and provide complete confidence in their cybersecurity tomorrow. Stronger Together. Protecting What's Next.