

# Assurance That Keeps Pace With Threats

Threats evolve almost daily, and annual, point-in-time evaluations no longer keep pace with expanding attack surfaces, AI-driven risks, and other evolving threats.

Extend the value of security investments by maintaining visibility and control between planned assessments. GuidePoint Security's Continuous Security Validation (CSV) service provides perpetual validation that security controls are working against the latest threats. Through a combination of regular, automated testing and expert analysis, GuidePoint helps organizations close security gaps before attackers find them and demonstrate measurable security effectiveness to leadership, auditors, and regulators without waiting for the next scheduled test.

## Demonstrate Sustained Cyber Readiness

Annual security testing establishes critical benchmarks, but threat actors do not pause between assessments. Security leaders may not fully know the risk that lives in the annual testing gap.

GuidePoint's Continuous Security Validation (CSV) service closes that gap and transforms cybersecurity from an annual exercise to always-on protection. CSV embeds automated and expert-led testing directly into security operations to test controls across network, cloud, endpoint, identity, and operational technology (OT) environments on an ongoing basis. This approach ensures continuous readiness and eliminates surprises when facing audits, scheduled tests, or actual attacks.

### This comprehensive security validation service delivers several critical advantages for security teams and leadership:

- ✓ **Real-time visibility** into security posture across the entire attack surface
- ✓ **Continuous vetting** of security tools and controls against current attacker tactics, techniques, and procedures
- ✓ **Earlier identification and remediation** of weaknesses before attackers exploit them
- ✓ **Ongoing compliance readiness** that eliminates end-of-year audit scrambles
- ✓ **Measurable evidence of security effectiveness** for boards, regulators, and stakeholders



## 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.



# Security Testing Reimagined for Continuous Posture Improvement

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. The team delivers Continuous Security Validation (CSV) through a flexible combination of managed security services, automated platforms, and expert-led engagements. GuidePoint meets organizations where they are and helps them build toward a mature, always-on security validation program aligned to their threat exposure, compliance requirements, and business objectives.

## CSV service components include:



**Penetration-Testing-as-a-Service (PTaaS):** Continuous automated and manual testing with real-time vulnerability discovery, prioritized findings, and remediation tracking through a unified portal.



**Breach-and-Attack-Simulation-as-a-Service (BASaaS):** Expert configuration, sensor deployment, platform optimization, and ongoing management of BAS platforms to continuously test security controls against known attack techniques and threat actor behaviors.



**Phishing-as-a-Service:** Year-round simulation campaigns managed by experienced offensive security professionals, aligned to industry-specific threats and coordinated with security awareness training.

## The Power of Automation + Human Analysis

Automated testing platforms identify security gaps, vulnerabilities, and potentially exploitable attack surfaces at scale. However, technology alone cannot replace the judgment, context, and creativity of an experienced security professional. GuidePoint’s CSV service combines the efficiency of automation with the critical thinking of certified offensive security experts who understand how attackers operate. GuidePoint analysts maintain continuity across engagements, developing deep familiarity with each organization’s environment, security stack, and risk tolerance over time. The result is validation that grows sharper and more precise with every engagement cycle.

### This model delivers three compounding advantages:

- ✓ **Deeper findings:** Analysts who know the environment ask better questions and pursue more meaningful attack paths
- ✓ **Faster remediation:** Contextual guidance reduces the time between finding and fix
- ✓ **Stronger programs:** Ongoing collaboration builds internal security team capabilities alongside external validation

## Why GuidePoint Security

When cyber threats hit, you want the best on your side. GuidePoint Security designs, deploys, and delivers Continuous Security Validation that drives real results. We simulate attacks and identify vulnerabilities across any environment – faster, smarter, and with less risk to strengthen your defenses. Accelerate your business with confidence – 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.

