GUIDEPOINT
SECURITY

PENETRATION TESTING AS A SERVICE

Wash → Rinse → Repeat. Penetration Testing as a Service improves your cybersecurity hygiene by understanding your attack surface and performing continuous validation of your security controls.

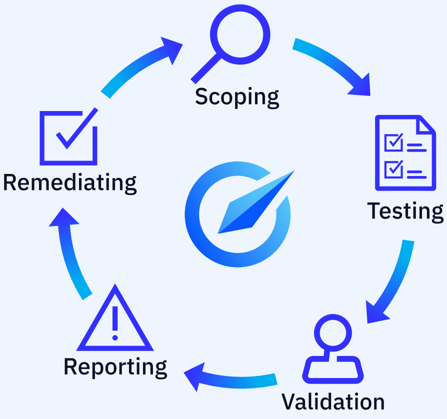
Resource shortages delay security testing and leave fixable problems open to exploitation. Hackers are always on–shouldn't your testing be, too?

The expertise of our certified penetration testers combined with the power of automated attack platforms builds the foundation of our Penetration Test as a Service (PTaaS) platform. Automation paired with manual validation–delivered in an ongoing cycle–creates a powerful complement to your Vulnerability Management Program.

In today's global economy, all hours are "business hours", and your security should follow suit. An insufficient penetration test will oftentimes leave a company with a false sense of security.

Traditional, point-in-time penetration testing tends to focus on high-risk vulnerabilities, which can leave lower-risk vulnerabilities open to exploitation. This is a natural result of the limited scope traditional testing needs to adopt due to time and resource constraints. But in today's attack landscape, attackers will take any opportunity given to them.

GuidePoint's Penetration Testing as a Service goes beyond a typical point-in-time pentest by combining traditional testing and reporting with recurring, automated testing and continuous reporting. With this service you gain real-time, actionable results based on rapid identification, exploitation, reporting, and remediation of vulnerabilities as they arise instead of only once or twice a year.



Put a Highly-Trained, ELITE Team on Your Side

GuidePoint's Threat & Attack Simulation team is staffed by professionals who are technically adept and possess a diverse set of collective skills, enabling them to be extraordinarily adaptable to all security assessments.

Hundreds of Industry and Product Certifications

OSCP OSCE GPEN C|EH
GSE GWAPT CISSP CREST

Enhance Your Security Program with Robust and Continuous Penetration Testing

Both traditional penetration testing and automated penetration testing have a complementary place in your security program.

While traditional penetration tests will always deliver deeper results, they are limited by the industry personnel shortage. Traditional testing is usually constrained to a narrow, defined scope in order to ensure you receive the most value for the time the team is engaged, and the test may need to wait until a team has the bandwidth.

Conversely, automated penetration testing takes a broader approach without diving as deeply into every vulnerability discovered. Because it isn't limited by personnel constraints, automated testing can be conducted year-round and can begin as soon as the scope is defined.

Together, automated and traditional penetration testing deliver the best results possible. As automated results are delivered throughout the year, your team can patch critical vulnerabilities in real time. And when the time comes to engage with a traditional penetration testing team, you will already have an idea of the areas that may need to be retested or probed deeper.

Traditional Penetration Testing

- Pentesting teams provide dedicated, hands-on attention to conduct in-depth tests focused on narrow areas of scope.
- Human knowledge and expertise deliver realistic testing, leveraging tried and true methods exploited by real attackers.
- Results are delivered as a report at the conclusion of testing. Customers are encouraged not to remediate discovered vulnerabilities during testing, as it may interrupt the penetration team's work and stop them from finding deeper issues after initial exploitation.

Automated Penetration Testing

- Automated tooling enables rapid penetration testing to find and exploit vulnerabilities, paired with expert penetration testers to auditing and validate results.
- The testing platform ingests and leverages newly discovered exploits to rapidly test across the environment to identify new vulnerabilities as quickly as possible.
- Results are delivered throughout testing via a unified portal. Because automated testing focuses on rapid vulnerability discovery instead of deep testing, customers are able to remediate vulnerabilities as they are discovered, spreading the work over time.

About Us

GuidePoint Security provides trusted cybersecurity expertise, solutions and services to help organizations make better decisions that minimize risk. GuidePoint's unmatched expertise has enabled a third of Fortune 500 companies and more than half of the U.S. government cabinet level agencies to improve their security posture and reduce risk.