GUIDEPOINT® SECURITY

VULNERABILITY AND EXPOSURE MANAGEMENT SERVICES

Outpace the Growing Wave of Zero-Day Vulnerabilities

AI has accelerated critical zero-day vulnerability discovery to the point where it's outpacing patch cycles. Exploits drop within hours, fixes lag or never come, and teams struggle to prioritize what matters most.

Turn zero-day chaos into a managed response that keeps pace with AI-driven vulnerability discovery. GuidePoint Security helps organizations modernize prioritization with asset criticality, business context, exploit validation, and real-time threat intelligence. Organizations can discover exposed assets, determine remediation priority, and shield what can't be patched. Backed by vulnerability and exposure management experts, GuidePoint helps organizations accelerate patch cycles so that they move at attacker speed.

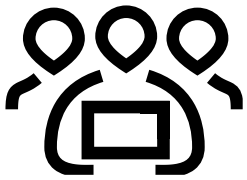
Make the Next Zero-Day a Managed Event

Recent vulnerabilities, including PHP2Shell and Java4Shell, went from disclosure to attack in hours. Meanwhile, a full 3% of all critical software defects tracked by MITRE ATT&CK were discovered in October 2026. Traditionally cadenced patching cycles can't keep pace in this AI-driven world.

GuidePoint Security helps organizations accelerate the scoping, discovery, prioritization, validation, and mobilization of threat exposures and mitigating patches. Through actionable diagnosis, we help customers prioritize and fix the vulnerabilities that put business operations at risk.

With GuidePoint, organizations can:

- **Prioritize by real exploitability** using EPSS, CISA KEV, and business context in addition to severity scores
- **Know which vulnerabilities attackers are exploiting now** with threat intelligence from GuidePoint Research & Intelligence (GRIT)
- **Find unknown and internet-facing assets before attackers do** with discovery, inventory, and EASM
- **Reduce risk before patches are available** with virtual patching, WAF, IPS, and other compensating controls



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 Community.

CISSP · CCSP · GPEN · GCIH · OSCP · CISA

Scope → Discover → Prioritize → Validate → Mobilize

Diagnose | Act

Accelerate Vulnerability Management to Stay Ahead of AI-Driven Attacks

Prioritize the exposures attackers are most likely to target and respond to critical zero-days without waiting for the next patch cycle. GuidePoint helps modernize vulnerability and exposure management through four flexible service options that fit each organization's maturity, goals, and budget. Each option below can stand on its own, or combine as the organization's program matures.

Exposure Management Program Assessment and Design

Start with a benchmark of the organization's current program, then design a target state and phased roadmap that fits operational realities. An Exposure Management Program Assessment and Design includes:

- Gap analysis across scoping, discovery, prioritization, validation, and mobilization
- A risk-based prioritization model that layers EPSS, CISA KEV, threat intelligence, exploit availability, asset criticality, and business context on top of CVSS
- Zero-day response playbooks for triage, emergency change, and compensating controls
- CMMI-based maturity benchmarking
- Governance, with clear ownership and accountability so the right people and processes are in place

Fractional and Full Staff Augmentation

Embed expert vulnerability management engineers and analysts alongside internal teams, from a fractional resource that fills specific skills gaps to full-time dedicated staff. GuidePoint can close skills gaps and accelerate programs by running triage, tuning EASM and WAF controls, reporting on risk reduction, and driving zero-day response while helping build internal competencies.

Vulnerability Management-as-a-Service (VMaaS)

Operationalize vulnerability and exposure management quickly with co-managed or fully managed VMaaS options. GuidePoint's experts can manage platforms, optimize scans, and prioritize findings against live GRIT intelligence. With VMaaS, GuidePoint can coordinate rapid response when the next zero-day hits, while customers keep full visibility and control over their environments.

Compensating Controls and Continuous Discovery

Protect assets, even for delayed patches, unpatchable devices, and end-of-life systems. GuidePoint deploys and tunes EASM, WAF virtual patching and WAF posture validation, restricts origin bypass paths, and integrate with ITSM, SOAR, and threat intelligence systems to turn exposure data into automated, risk-based action.

Why GuidePoint Security

When zero-days threaten your organization, you want the best on your side. GuidePoint Security designs, deploys and delivers tailored vulnerability and exposure management solutions that drive real results. We combine GuidePoint Research & Intelligence, vendor-objective engineering, and managed operations to shrink your window of exposure. 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.

GUIDEPOINT® SECURITY

1900 Reston Metro Plaza, Suite 701 • Reston, VA 20190
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132
rDS.ZDER.2611