GUIDEPOINT® SECURITY

GENERATIVE AI SERVICES

GuidePoint Security's expertise extends to Generative AI, which is incorporated into many cybersecurity disciplines

While the pace of Generative AI development is rapid, your implementation should strive to adapt with an evolving regulatory landscape.

Generative AI brings many potential business productivity gains, but also inherently introduces risks to your critical information assets and operational environments. GuidePoint Security has extensive experience with Generative AI across all security domains, from design and discovery to cataloging, data mapping, risk assessment, risk mitigation, and leveraging Generative AI to enhance security use cases.

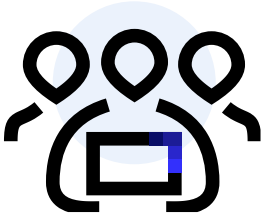
GuidePoint Security experts can help your organization navigate the full spectrum of Generative AI opportunities and challenges, ensuring that your critical information assets are protected and your data privacy and security needs are met.

Our comprehensive services are designed to enable the benefits of Generative AI while proactively identifying and mitigating associated risks.

Benefits of Our Generative AI Consulting Services:

- Mitigate risks associated with deploying Generative AI models
- Evaluate and select the right Generative AI models and solutions that align with your strategic goals and technical requirements
- Ensure safeguards are in place for protecting the security and privacy of sensitive data when using Generative AI systems
- Incorporate best practices for integrating Generative AI into your existing IT infrastructure and ensure secure interoperability
- Adhere to industry and regulatory compliance standards
- Implement threat modeling and architecture reviews to adopt a shift-left approach in securing your Generative AI systems from the outset
- Ensure your incident response plans can address potential security breaches or failures in your Generative AI systems

Our team can also help you by providing training and development programs to upskill your workforce in Generative AI technologies, and ultimately foster a culture of continuous learning and innovation.



Put a Highly-Trained, ELITE Team on Your Side

More than 50% of our workforce consists of tenured cybersecurity engineers, architects and consultants.

Hundreds of Industry and Product Certifications

CISSP® OSCP OSCE GSE GWAPT GPEN

GuidePoint Security's Generative AI Expertise

Our experts make sure your security program accounts for Generative AI technology across the following areas:

Governance:

We help ensure your security policies and standards consider Generative AI technology and solutions, by providing:

- AI model and agent discovery scanning
- AI data mapping, risk assessment, readiness, and maturity assessments
- TPRM considerations for third-party vendors
- Data Firewalls and Generative AI guardrails

Design:

Our team provides Generative AI architecture design considerations for your environment, as well as:

- Threat modeling of Generative AI solution designs and MLSecOps pipelines
- Generative AI model selection guidance
- Model training guidance and analysis
- Generative AI use case analysis

Implementation:

We help fortify your Generative AI development efforts through:

- Targeted secure code reviews of the implemented design
- Generative AI/LLM secure development training
- Guidance on code-level security testing tools during implementation (SAST, SCA, SBOM, ML-BOM, etc.)

Verification:

We ensure the security of your Generative AI solutions through rigorous runtime testing. Our services include:

- Generative AI-focused application security assessments based on the OWASP Top 10 for LLMs and the MITRE ATLAS framework
- Internal, External, and Cloud penetration testing focused on infrastructure and pipelines that support Generative AI systems

Operations:

We help maintain the security and visibility of your Generative AI systems during runtime to ensure ongoing protection and compliance, including effective incident management. Our services include:

- Guidance on selecting and implementing technologies for the protection and visibility of Generative AI systems, such WAF, RASP, API security, CSPM, ASPM, etc.
- Incident Management considerations regarding Generative AI systems

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.

GUIDEPOINT® SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132