

ARTIFICIAL INTELLIGENCE (AI) SECURITY SERVICES

Secure AI and Use AI to Secure What Matters

AI is increasing efficiency, innovation, and threat defense for operational resilience. It also introduces cybersecurity and compliance concerns with new attack surfaces and threat vectors that magnify and strengthen attacks.

AI adoption increases concerns around data privacy, unauthorized access, adversarial threats, and governance. Backed by experts at the forefront of AI advancement, GuidePoint AI Security services help improve security posture, detect AI-based threats, protect data and identities, and ensure regulatory compliance during AI adoption and beyond. Our team helps design, deploy, and deliver tailored AI security services and solutions that drive real results. Accelerate your business with AI – and protect what matters most.

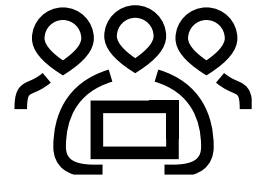
Secure AI Adoption

GuidePoint Security helps turn AI from a security risk into a strategic advantage. Our AI Security experts provide comprehensive technical and advisory cybersecurity support to help organizations securely and confidently incorporate AI technologies into their IT environment and use AI to strengthen defense against evolving threats.

GuidePoint Security's team of highly certified experts help organizations move faster, smarter, and safer. We build strategies and processes to govern and secure AI use within IT and OT environments and workflows, accelerating innovation, productivity, time to market, and cost savings while minimizing risk. We also help organizations harness AI to speed threat hunting, detection, and response, empowering organizations to identify unmonitored entry points, defend against AI-based threats, and make more informed decisions.

GuidePoint works closely with organizations to:

- ✓ Improve overall security posture
- ✓ Quickly detect and shut down AI-based security threats
- ✓ Fast-track AI adoption while ensuring regulatory compliance and architectural security
- ✓ Control shadow AI with visibility and governance
- ✓ Protect sensitive data and identities
- ✓ Improve visibility across users, data, and systems
- ✓ Ensure ethical, transparent AI behavior
- ✓ Align with compliance and business objectives



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.



Deploy AI with Confidence, Not Compromise

GuidePoint Security works closely with clients to understand their specific business needs and challenges, and tailors solutions that align with their goals and budget. We look across the cybersecurity ecosystem and recommend the best-fit solutions. Our technical and advisory services include:

Strategic and Advisory AI Services

Build a secure, business-aligned AI strategy and roadmap. We help assess AI readiness, streamline security controls, and optimize processes to reduce exposure and support scalable AI adoption.

AI and Agentic Platform Security

Make Agentic AI work smarter and more securely. We help organizations gain visibility into AI agents and tools so they can implement robust guardrails and prevent adversarial testing.

Data Security and AI Governance

Establish frameworks to safeguard sensitive data throughout the AI lifecycle and support responsible AI use at scale. We help define policies, ownership models, and controls that align with standards such as NIST AI RMF or ISO 42001.

Identity and Access Management

Incorporate AI into an “everything is identity” strategy. Our strategic and tactical services help secure AI agents/ NHIs, and support AI and Agentic AI program automation and governance.

AI Technical Services

Ensure right-fit technology selections from the start. Our experts conduct health checks, provide vendor-objective technology selection and deployment services, and align outcomes to unique business priorities and compliance objectives.

Cloud Security

Assess, design, and build security into cloud native AI/ML platforms. Our team helps connect agents through cloud-hosted gateways, define and enforce guardrails, secure pipelines, and govern AI agents.

AI Application Security

Identify potential flaws, threats, and vulnerabilities within applications that leverage AI technology, development practices, and deployment pipelines. We help architect, evaluate, and test secure-by-design applications of all types, including agentic and generative AI.

AI-driven Incident Response

Prepare for AI-fueled attacks. We help organizations develop incident response playbooks, tune AI-enabled detection tools, and apply behavioral analytics to keep data and systems secure.

Why GuidePoint Security

AI brings incredible potential to businesses – both to their success and threat defense. Realize the full power and potential of AI with GuidePoint Security. We help organizations of every size and industry design, deploy, deliver and govern AI solutions that safeguard data, identities, and assets, and accelerate business success. We help integrate solutions 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.



1900 Reston Metro Plaza, Suite 701 • Reston, VA 20190
[guidepointsecurity.com](https://www.guidepointsecurity.com) • info@guidepointsecurity.com • (877) 889-0132
DS.AI.2607