GUIDEPOINT® SECURITY

AGENTIC AI SECURITY SERVICES

Lifecycle Management for an Autonomous Workforce

AI agents are becoming autonomous actors in the enterprise, accessing systems, using data, and executing actions often without human oversight. Yet most organizations have not included them in their identity lifecycle, or set trust boundaries or governance controls to manage those agents.

Enable autonomous AI to move faster without sacrificing visibility, security, or control. GuidePoint helps organizations build the security, governance, and operational foundation needed to securely scale AI agents across the business. Our Agentic AI Security Services provide a practical, prioritized approach to discovering,assessing, governing, securing, and managing agents across your environment. From visibility and risk assessment to access governance, policy enforcement, lifecycle management, monitoring, and continuous oversight, GuidePoint AI Security Services help teams extend cybersecurity disciplines to a new class of enterprise actors.

Better Manage AI Agents at Scale

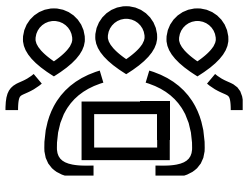
As organizations deploy AI agents alongside service accounts, APIs, cloud workloads, CI/CD pipelines, and other non-human identities (NHIs), existing security models and processes built primarily around human users can't keep up. AI agents need credentials, permissions and access like human users, but they operate at machine speed. Agents are emerging as a new class of enterprise identity, and their adoption velocity demands dedicated governance and controls.

Agentic AI security spans three control planes: identity (who or what may act), data (what an agent may access), and runtime (what an agent may do in the moment). Identity is the foundational control plane upon which both data and runtime controls depend.

GuidePoint helps you modernize your cybersecurity, identity, and governance strategies to secure, manage, and scale autonomous AI across your environment.

Our approach helps organizations:

- Discover and inventory AI agents across the environment
- Establish trust boundaries and kill-switch controls for autonomous operations
- Strengthen governance and accountability as agent adoption scales
- Reduce risk exposure without adding operational friction
- Extend existing security programs to address agentic AI



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.



Comprehensive Security Services for Agentic AI

GuidePoint helps organizations build the security, governance, and operational foundation needed to confidently adopt and scale autonomous AI agents, from strategy and assessment through implementation and ongoing management. Whether you're just getting started or looking to mature an existing program, our tailored services meet you where you are:

Strategic and Advisory Services – Broad review of technology stack, people and processes to assess AI readiness, plan, build and optimize AI-ready cybersecurity roadmap and programs to support agentic AI initiatives.

AI Architecture Advisory – Architectural guidance on how to implement the architecture roadmap using secure design principles to enable safe and secure agentic AI adoption and deployment.

Risk Management and Third-Party Risk Management (TPRM) – Risk management & mitigation from AI adoption and assess risk introduced by third-party agents, plugins, tools, and model providers across your environment.

Security Tooling and Evaluation – Vendor-objective support to find, deploy and optimize right-fit agentic AI solutions and align outcomes to your unique business priorities and risk tolerances to achieve better outcomes.

Compliance and Regulatory Alignment – Ensure compliance with evolving regulatory frameworks (e.g., EU AI Act, NIST AI RMF, ISO 42001), and sector-specific requirements.

Secure Agent Development Lifecycle – Embed security into the full agent development lifecycle with secure-by-design guidance for engineering teams building agentic systems.

Managed Services and Operations – Ongoing monitoring, policy tuning, and platform operations that evolve alongside your agent population, business needs, and regulatory landscape, from lifecycle management through continuous governance enforcement.

Incident Response and Forensics – Development and operationalization of AI-specific incident response capabilities and playbooks. Services close the gap between traditional IR playbooks and the novel failure modes introduced by autonomous systems.

AI Technical Services (Security Engineering) – Forward deployed engineering to help build and deploy AI agents with appropriate identity lifecycle controls and AI security tooling across your environment.

Data Protection and Privacy – Design and implement data loss prevention controls purpose-built for agent interactions. Addresses the novel data flow paths created by autonomous agents that traditional DLP architectures were not designed to govern.

Why GuidePoint Security

When cyber threats evolve, organizations need confidence that every identity, human and non-human, is secure. GuidePoint Security combines cybersecurity expertise, AI, identity strategy, and technology guidance to help organizations build resilient AI Security programs. Our vendor-objective approach enables clients to assess AI risks, strengthen governance and lifecycle controls, and implement scalable strategies that reduce identity risk and secure the automation, applications, and AI capabilities that power the business.

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
DS.AAI.2610