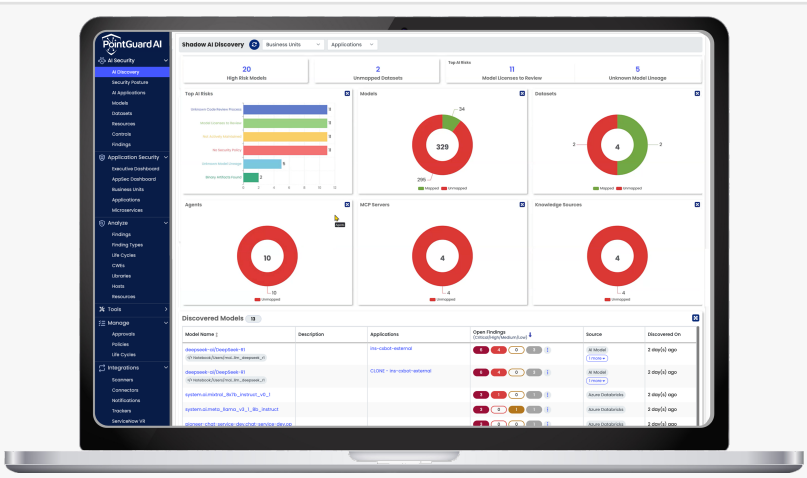
PointGuard AI Extends AI Discovery to Secure AI Agents, Moltbots, and MCP Servers

Platform brings full visibility and control to the expanding agentic AI attack surface



Comprehensive Discovery of AI Models, Agents, & MCP Servers

SAN JOSE, CA, UNITED STATES, February 24, 2026 /EINPresswire.com/ -- PointGuard AI today announced expanded AI Discovery capabilities that now secure AI agents, Moltbots (OpenClaw), and Model Context Protocol (MCP) servers in addition to large language models and AI platforms. As enterprises rapidly deploy agentic AI systems that autonomously retrieve data, invoke tools, and execute workflows, PointGuard AI delivers comprehensive visibility across the full AI ecosystem.

AI risk is no longer limited to model outputs. Agents can independently access enterprise systems, connect to sensitive data, and execute actions through MCP servers. Moltbots introduce further ecosystem-level complexity by enabling distributed, coordinated AI activity across environments. This evolution dramatically expands the attack surface and increases the potential blast radius of a single misconfigured or ungoverned AI component. Security teams must now manage interconnected AI supply chains, not just standalone models.

> “Agents, Moltbots, and MCP integrations are expanding AI risk quickly. We have extended AI Discovery to give organizations complete visibility across their entire AI ecosystem.”
>
> *Warlu Kothapalli, CTO*

Complete AI Discovery and AI-BOM Visibility
PointGuard AI Discovery continuously identifies and inventories models, agents, Moltbots, MCP servers, datasets, notebooks, endpoints, and external AI services across code repositories, cloud environments, and runtime infrastructure. The platform scans source code to detect AI components early in development, identifies calls to external AI services and agent frameworks, and flags hard-coded secrets or exposed credentials tied to AI systems.

Through integrations with leading AI platforms and agentic frameworks including Copilot, AWS, Google, OpenAI, Claude, CrewAI, and LangGraph, PointGuard provides continuous visibility across both development and production environments. Discovered AI assets are mapped to business applications and owners, delivering clear, application-level AI risk posture.

PointGuard also delivers SBOM-style lineage tracking across models, agents, Moltbots, datasets, and MCP servers, creating a comprehensive AI Bill of Materials. This AI-BOM enables organizations to understand dependencies, external integrations, and supply chain relationships before those connections create security or compliance exposure.

A key differentiator is the Trusted MCP Directory, which evaluates MCP servers for vulnerabilities, malicious prompts, secrets exposure, licensing posture, publisher trust, and adoption maturity. Organizations can assess the security and operational integrity of MCP services before integrating them into agent workflows. This level of intelligence is critical as agents increasingly rely on external tools and protocols to execute business-critical tasks.

“AI architectures are changing faster than traditional security programs can adapt,” said Warlu Kothapalli, Chief Technology Officer at PointGuard AI. “Our customers are deploying agents, Moltbots, and MCP integrations at scale. We expanded AI Discovery to give them complete visibility across the entire AI ecosystem before risk turns into impact.”

With unified discovery, comprehensive AI-BOM intelligence, and deep MCP ecosystem insight in a single platform, PointGuard AI enables enterprises to adopt agentic AI with greater speed, control, and confidence.

For more information, visit www.pointguardai.com.

Willy Leichter
PointGuard AI
email us here
Visit us on social media:
LinkedIn
YouTube