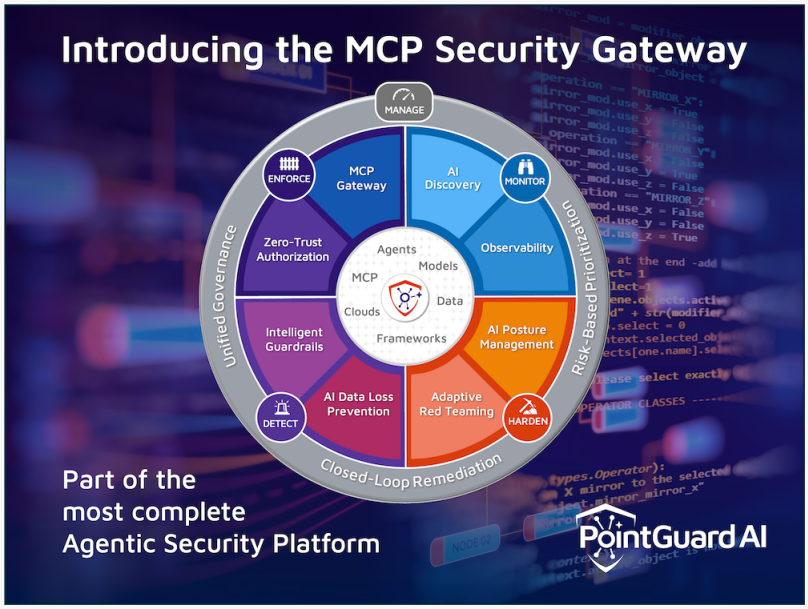
PointGuard AI Unveils MCP Security Gateway to Secure Autonomous AI Agents

Zero-trust authorization, contextual security, and built-in guardrails bring governance to agentic AI



PointGuard AI MCP Security Gateway

SAN JOSE, CA, UNITED STATES, March 18, 2026 /EINPresswire.com/ -- PointGuard AI today announced the MCP Security Gateway, a security control point designed to protect enterprises as autonomous AI agents expand across business systems. The gateway provides zero-trust authorization, tool-level controls, and runtime guardrails to ensure agents interact safely with enterprise tools, APIs, and data.

The gateway is part of the PointGuard AI Agentic Security Platform, which secures autonomous agents, MCP infrastructure, models, and data across the full AI lifecycle while giving organizations visibility and governance across complex AI ecosystems.

> The MCP Security Gateway provides the control point enterprises need to ensure agents operate safely and in alignment with business policies."
>
> *Pravin Kothari, CEO of PointGuard AI*

AI agents are rapidly transforming enterprise operations by autonomously interacting with systems and services. But as MCP servers proliferate, agents can gain uncontrolled access to tools and sensitive data. Without strong guardrails, mistakes or malicious inputs can trigger unintended actions across enterprise environments.

Industry analysts have highlighted the need for security control points in agentic architectures. Gartner® recently recommended organizations "Deploy AI/API gateways or MCP proxies to mediate traffic, enforce policies and monitor agent behavior continuously." 1

The PointGuard AI MCP Security Gateway acts as a centralized policy enforcement layer for agent ecosystems. It authenticates agents and MCP servers through enterprise identity systems, enforces granular tool permissions, and inspects agent interactions in real time to prevent unsafe behavior.

“Autonomous AI agents introduce new risks because they can interact with multiple systems without direct oversight,” said said Chad Quayle, Sr. Director, Chief Data & AI Security Architect at Finastra, one of the world's largest financial services technology companies. “Security teams need clear controls over what agents can access and what actions they can take.. “Security teams need clear controls over what agents can access and what actions they can take. The PointGuard AI MCP Security Gateway helps provide that level of visibility and policy enforcement.”

PointGuard differentiates with contextual security, which evaluates risk across multiple dimensions including the agent’s role, real-time situational context, behavioral history, and the trust relationship between agents, MCP servers, and downstream data sources. This enables adaptive policies aligned with enterprise workflows.

The platform is also built secure-by-design, embedding security directly into the agent development lifecycle. Governed prompt management, enterprise secrets vault integration, and human-in-the-loop approvals help ensure agents are deployed safely from the start.

“Agentic AI is moving from experimentation to production faster than most organizations expected,” said Pravin Kothari, CEO of PointGuard AI. “The MCP Security Gateway provides the control point enterprises need to ensure agents operate safely and in alignment with business policies.”

About PointGuard AI
PointGuard AI delivers an enterprise security platform for generative and agentic AI, securing models, agents, MCP ecosystems, and applications. The platform combines discovery, AI red teaming, guardrails, data protection, and a fully integrated MCP Security Gateway for zero-trust control of agent interactions.

1. Gartner, Manage the Cybersecurity Risks of the Model Context Protocol, by Craig Lawson, 14 November 2025
Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner’s business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose.

Willy Leichter
PointGuard AI

+1 6504640683
email us here
Visit us on social media:
LinkedIn
YouTube
