# TrendAI™ to Secure Enterprise Adoption of Agentic AI with NVIDIA

*TrendAI™ to support NVIDIA OpenShell open source runtime to add security for autonomous AI agents*

DALLAS, March 16, 2026 /PRNewswire/ -- TrendAI™, the enterprise AI security leader, today announced expanded collaboration with NVIDIA to support NVIDIA OpenShell, a new open source runtime for agentic AI introduced at NVIDIA GTC. The solution enables organizations to deploy autonomous AI agents with built-in governance, continuous risk visibility, and runtime enforcement, addressing key barriers to production adoption of agentic AI.

***TrendAI™ is teaming with NVIDIA to add security for the open source NVIDIA OpenShell runtime as the ecosystem evolves. Learn more: https://resources.trendmicro.com/2026-nvidia-gtc.html***

**Rachel Jin, Chief Platform and Business Officer, Head of TrendAI™:**"Agentic AI changes the security equation. When AI systems can plan, take action, and interact with other tools on their own, the risk profile looks very different from traditional AI. Our collaboration with NVIDIA allows us to bring security directly into the architecture so organizations can adopt agentic AI with the visibility and control they expect."

Traditional AI security models were built for short-lived interactions between users and models. Agentic AI changes that dynamic by operating continuously and taking action across environments.

NVIDIA OpenShell is an open source runtime for long-lived, self-evolving agents capable of planning, memory, and tool execution. While these capabilities unlock significant productivity gains, they also introduce risks related to unauthorized skills, hidden behaviors, prompt injection, and unintended system access.

**Pat Lee, vice president, Strategic Enterprise Partnerships at NVIDIA:**"Agentic AI opens the door for a new class of applications that can plan, reason, and take action. By working with TrendAI™, we're helping developers add visibility and controls to make it safer to run autonomous AI."

TrendAI™ can transform agentic AI from a high-risk experiment into an**e**nterprise-ready architecture. Organizations gain the ability to define trust boundaries, enforce policy at runtime, and maintain continuous visibility into autonomous AI behavior, all while preserving the flexibility and power that make agentic systems valuable.

TrendAI™ adds an enterprise-grade security layer that governs how agents behave, what tools they can access, and how risk is detected and enforced, before, during, and after execution.

The collaboration extends across the NVIDIA AI-Q blueprint and the NVIDIA NeMo Agent Toolkit, enabling consistent security, governance, and observability as agentic systems scale across enterprise environments.

TrendAI Vision One™'s layered security architecture for OpenShell provides:

- Centralized AI governance and compliance enforced directly in the agent runtime
- Skill and tool risk visibility, including continuous scanning of agent skills and MCP integrations
- Dynamic behavioral analysis to detect hidden or malicious actions
- Inline policy enforcement that blocks untrusted skills and actions at runtime
- AI specific threat protection, including prompt injection and sensitive data exposure detection
- Continuous monitoring and auditability through agentic telemetry and SIEM integration. These capabilities allow organizations to define trust boundaries, enforce policy, and maintain visibility across autonomous AI agents without limiting innovation.

**About TrendAI™**
TrendAI™, a global leader in AI security, empowers enterprises to innovate fearlessly by securing AI, cloud, networks, endpoints, and data across the modern attack surface. At the core is TrendAI Vision One™, a unified cybersecurity platform that centralizes cyber risk exposure management and security operations to protect the entire AI lifecycle from infrastructure to models to users. The platform is fueled by world-class threat intelligence and insights that protect organizations from hundreds of millions of threats every day. With 6,000 TrendAI™ experts across 75 countries,TrendAI™ empowers security leaders to stay ahead of threats, driving proactive security outcomes across the entire attack surface. This includes critical environments like AWS, Google, and Microsoft. AI Fearlessly.

SOURCE TrendAI

For further information: Trend Micro Communications: 817-522-7911, media_relations@trendmicro.com https://newsroom.trendmicro.ca/2026-03-16-TrendAI-TM-to-Secure-Enterprise-Adoption-of-Agentic-AI-with-NVIDIA