

TrendAI™ Extends the NVIDIA Agent Safety Platform with Threat Intelligence and Full AI Factory Security

TrendAI Vision One™ pairs hardware-level detection on NVIDIA BlueField DPUs and network security with Zero Day Initiative™ threat intelligence, helping enterprises safely move agent fleets from pilot to production

DALLAS, Sept. 28, 2026 /PRNewswire/ -- TrendAI™, the global leader in AI security and business unit from Trend Micro Incorporated ([TYO: 4704](#); [TSE: 4704](#)), today announced its support for the NVIDIA Agent Safety Platform, NVIDIA's full-stack infrastructure for running autonomous AI agents safely at enterprise scale. As organizations move autonomous, self-evolving agents into production, TrendAI™ and NVIDIA are aligned on a clear principle: no single control makes an agent secure. Security must be built into every layer the agent depends on.

AI agents are made up of three core components: the model that reasons, the harness that orchestrates the agent and its sub-agents, and the tools and data the agent can reach. Together, they let an agent hold credentials, remember context across sessions and act on production systems without a human approving each step. As enterprises scale from a handful of pilots to fleets of agents spanning teams and business units, security is now a critical control and often becomes the deciding factor in whether agentic AI reaches production.

The NVIDIA Agent Safety Platform places authority in the infrastructure beneath the agent. According to NVIDIA, OpenShell enforces policy outside the agent's execution environment, where it cannot be prompted away or bypassed, while NVIDIA BlueField-4 DPUs and NVIDIA DOCA add a host-independent security layer in silicon. TrendAI™ complements that enforcement layer with the intelligence that informs what the policy should be, the visibility to see what agents are doing, and the threat detection and response to act on it.

"Agentic AI is the most significant shift in enterprise technology in a generation, and security needs and guardrails are in place to keep the agents aligned with the intentions of the organization," said Rachel Jin, Chief Platform and Business Officer, Head of TrendAI™. "Security can't sit in one place. It has to cover the model, the harness, and every tool and data source an agent touches. NVIDIA is building the boundary that determines what an agent can do. TrendAI™ brings the threat intelligence and oversight that tell security teams what that boundary should be, and what is happening inside it. Together, we give organizations a practical path to scale agentic AI securely."

How TrendAI™ supports the NVIDIA Agent Safety Platform

TrendAI Vision One™ extends NVIDIA's agent safeguards across the whole AI factory, covering agents, models, containers, storage and networks on one platform:

- **Model protection.** Inline inspection of prompts and responses blocks prompt injection and jailbreaks and redacts sensitive data before it leaks.
- **Harness and tool governance.** Security teams control which tools and MCP servers agents can reach, inspect every tool call, and analyze how skills and AI artifacts behave at runtime.
- **Data and identity controls.** TrendAI Vision One™ finds and classifies the sensitive data that feeds AI, stops agents from reaching data they shouldn't, extends file security and data loss prevention to the files agents read and write, and strips excess privilege from agents and other non-human identities.
- **Hardware-rooted detection and response.** Using NVIDIA BlueField DPU and DOCA telemetry, TrendAI Vision One™ detection stays trustworthy even if the host OS is compromised, and correlates AI signals with endpoint, network, and identity telemetry so a hijacked agent cannot move laterally unseen.

Together, TrendAI™ and NVIDIA are leading the future of AI with proactive security designed to inspire innovation and eliminate risk.

Learn more

For more on why agent security has to extend beyond the model, read Rachel Jin's blog [Beyond Model Alignment: Securing Every Layer of the AI Agent](#). Learn how TrendAI Vision One™ secures enterprise AI [here](#).

About TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk. Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data. Global Fortune 500 companies rely on TrendAI™ to cut risk and stop threats up to 3 months earlier, powered by world-leading threat and attack intelligence.

Through deep ecosystem partnerships with market leaders like NVIDIA, Anthropic, AWS, Google, and Microsoft, TrendAI™ empowers your organization to securely drive forward at the speed of AI. AI Fearlessly. Learn more at trendaisecurity.com.

SOURCE TrendAI

For further information: media_relations@trendmicro.com

<https://newsroom.trendmicro.ca/2026-09-28-TrendAI-TM-Extends-the-NVIDIA-Agent-Safety-Platform-with-Threat-Intelligence-and-Full-AI-Factory-Security>