

## TrendAI™ Brings AI-Driven Security That Runs Entirely Under Customer Control to Sovereign and Private Clouds with NVIDIA Nemotron™ Open Models

*TrendAI™ runs NVIDIA Nemotron open models entirely inside customer-controlled infrastructure, delivering AI-driven threat detection and policy-based response without security data ever leaving the sovereign boundary.*

DALLAS, Oct. 21, 2026 /PRNewswire/ -- TrendAI™, the global AI security leader and enterprise business unit of [Trend Micro Incorporated](#) (TYO: 4704; TSE: 4704), today announced it is bringing NVIDIA Nemotron™ open models into [TrendAI Vision One™ for Sovereign and Private Cloud \(SPC\)](#), building on its collaboration with NVIDIA. The integration brings AI-assisted security operations into customer-controlled environments, extending capabilities such as guided investigation, security reasoning, and agentic SIEM to organizations with sovereignty, data residency and operational control.

TrendAI Vision One™ for Sovereign and Private Cloud (SPC) is available today, enabling organizations to deploy TrendAI Vision One™ in customer-controlled private cloud, sovereign cloud and on-premises environments. The Nemotron integration extends AI-assisted security operations into these environments while maintaining customer control over security data and deployment.

### Why Open Models Matter for Sovereignty

Highly regulated organizations need AI-driven security that fits their data-control requirements. Nemotron open models can support these requirements by bringing the model to the data rather than the data to the model. Customers decide where the model runs, which version is deployed, and who can access it, running AI-powered security operations on NVIDIA accelerated computing in their own data centers, sovereign clouds, and restricted-connectivity environments. TrendAI™ collaboration with NVIDIA on OpenShell provides an additional level of security for agents, ensuring organizations have control and visibility of agentic activities.

### Who Controls the Intelligence Acting on Your Data?

"Sovereignty extends beyond where data resides. Enterprises also need control over where the intelligence acting on that data operates, and how it is governed," says Rachel Jin, CEO, TrendAI™. "Organizations shouldn't have to give up the operational benefits of AI because their security data and operations need to remain within a customer-controlled environment. Our work is about bringing AI-powered security operations to the environments our customers choose to control."

"Open models give organizations the transparency and control to run on their own terms, which is critical for sovereign environments," said John Fanelli, Vice President, Enterprise Software at NVIDIA. "TrendAI's integration of NVIDIA Nemotron models enables enterprises to put their most sensitive data to work, without it ever leaving their control."

### Customer Perspective: Sovereignty Without Compromise

TITECH, which delivers sovereign security operations to customers in Oman, is working with TrendAI™ as a design partner on the Nemotron integration ahead of general availability.

"TrendAI Vision One for Sovereign and Private Cloud has provided our local customers in Oman with a trusted foundation for keeping security operations under customer control while complying with country data residency regulations," says TITECH CEO, Mohammed Hassan. "Nemotron-powered capabilities will let us offer advanced threat analysis and AI-assisted security operations to our customers while maintaining data sovereignty and operational control."

The integration supports AI-assisted threat analysis, policy-based response, and guided security operations within customer-controlled environments. These capabilities help organizations improve security operations with AI while maintaining control over where security data and AI processing reside.

### Customer Outcome: Security and control from the start

"As enterprises apply AI to real-world deployment, security and control must be embedded into the infrastructure from day one," says Business Manager of Security at Bechtle AG, Mathias Schick. "Our customers want to harness the full potential of AI without compromising data sovereignty, security, or operational control. Integrating AI-powered security into sovereign and private-cloud environments is an important step toward enabling secure AI adoption at scale, particularly for organizations with stringent security and compliance requirements."

### TrendAI Vision One™ for Sovereign and Private Cloud (SPC) with NVIDIA Nemotron integration supports:

- **Customer-controlled AI:** NVIDIA Nemotron open models deployed and run on customer-controlled infrastructure, with no dependency on external inference services
- **AI-assisted threat analysis:** Reasoning across security signals to identify complex threat patterns, attack chains, and AI-native attack paths
- **Policy-based threat response:** Supporting protective actions through organization-defined policies and security-team controls

- **Guided security operations:** Helping security teams investigate threats and prioritize response activities
- **Agentic SIEM capabilities:** Correlating telemetry and assisting with security reasoning while maintaining team oversight

TrendAI Vision One™ for Sovereign and Private Cloud (SPC) is available today. Visit [trendaisecurity.com/platform/sovereign-private-cloud](https://trendaisecurity.com/platform/sovereign-private-cloud) or visit TrendAI™ at NVIDIA GTC Berlin's expo (October 21-22, 2026) to preview these planned capabilities.

#### **About TrendAI™**

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility, governance, and consolidated security that inspires confidence, drive innovation, and eliminate 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 stop threats up to 115 days earlier, powered by world-leading threat and attack intelligence. Through deep ecosystem partnerships with market leaders like NVIDIA, Anthropic, AWS, Google, and Microsoft, TrendAI™ enables teams to securely move at the speed of AI. AI Fearlessly. Learn more at [trendaisecurity.com](https://trendaisecurity.com).

SOURCE TrendAI

For further information: [media\\_relations@trendmicro.com](mailto:media_relations@trendmicro.com)

---

<https://newsroom.trendmicro.com/2026-10-21-TrendAI-TM-Brings-AI-Driven-Security-That-Runs-Entirely-Under-Customer-Control-to-Sovereign-and-Private-Clouds-with-NVIDIA-Nemotron-TM-Open-Models>