Trend Micro Enhances AI Safety and Security in NVIDIA Enterprise AI Factories

Trend Secure AI Factory supports NVIDIA NeMo continuous model safety evaluation and improvement lifecycle

DALLAS, June 11, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced its adoption of the NVIDIA Agentic AI Safety blueprint, enhancing foundational security to help ensure customers' AI systems are protected across their full development and deployment lifecycle.

To read more about how Trend enhances security across NVIDIA Enterprise AI factory deployments, please visit: https://www.trendmicro.com/en_us/research/25/f/cybertron-nvidia-universal-llm-nim-microservices.html

Kevin Simzer, COO at Trend: "Global organizations are racing to innovate with agentic AI systems, and there's a critical need to ensure the safety and security of these systems. The NVIDIA Agentic AI Safety blueprint provides an important enabling technology that works in conjunction with Trend's threat intelligence to support safety across all phases of the AI lifecycle – from model adoption, deployment, and runtime protection — allowing customers to innovate with AI faster."

The "Trend Secure AI Factory" is built around unified cybersecurity platformsTrend Vision One™ and Trend Vision One Sovereign Private Cloud. It's designed to help customers mitigate risk at every layer of the AI factory, encompassing data, models, microservices, infrastructure, networks, and users.

Pat Lee, VP of Strategic Enterprise Partnerships at NVIDIA: "Embedding real-time, autonomous threat detection into enterprise AI factories empowers organizations to confidently scale innovation without compromising on protection. By integrating advanced cybersecurity directly into AI factories with Trend and NVIDIA Agentic AI blueprints, enterprise data, models, and workloads can remain resilient and trusted —unlocking the full potential of AI in a secure, accelerated environment."

To achieve this goal, Trend is deepening its AI-driven capabilities through the integration ofTrend Cybertron, its cybersecurity-specific large language model. Built to detect and respond to evolving threats in real-time, Trend Cybertron is now deployable via NVIDIA universal LLM NIM microservices, enabling scalable, secure inference across cloud, hybrid, and on-premise environments. This addition supports the alliance's shared goal of delivering intelligent, production-ready infrastructure for the AI era.

Thanks to capabilities including data security, infrastructure posture management, API guardrails, and CI/CD validation, the Trend Secure AI Factory directly supports and reinforces NVIDIA Agentic AI Safety blueprint by:

- Integrating with the NVIDIA NeMo model assessment, training, and customization framework to ensure model safety mechanisms scale reliably and securely across enterprise environments.
- Safeguarding model integrity against poisoning and misuse during the training and evaluation phases
- Securing the deployment environment, including microservices and infrastructure (e.g., NVIDIA NIM and AI agents), with Trend Container Security. This helps to prevent adversarial manipulation or resource-based attacks.
- Protect sensitive datasets with Data Risk Posture Management (DSPM), leveragingNVIDIA AI Enterprise, which includes NVIDIA Morpheus, NVIDIA RAPIDS, and the NVIDIA AI Safety Recipe for evaluations and post-training, to adhere to privacy and compliance standards.
- Providing guardrails, network protection, and secure AI agent interactions with application users, via Trend Zero Trust Secure Access (ZTSA) AI Service Access
- Strengthening sovereign AI with trusted security controls, viaTrend Vision One Sovereign Private Cloud

Justin Vaïsse, Director General at the Paris Peace Forum: "As AI becomes increasingly embedded in critical systems, its safety and security must be treated as global priorities. We welcome the role of companies like Trend in advancing responsible AI by contributing tangible, scalable solutions to multi-actor partnerships. This kind of cross-sector collaboration is essential to fostering trust and resilience in the technologies shaping our shared future."

About Trend Micro
Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's AI-powered cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, Trend's platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 70 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

SOURCE Trend Micro Incorporated

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---