Trend Micro to Open-source AI Model and Agent to Drive the Future of Agentic Cybersecurity

Leveraging NVIDIA AI to deliver powerful proactive security and scalable threat prevention for GenAI applications

DALLAS, March 19, 2025 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cybersecurity leader, today announced the open-sourcing of Trend Cybertron[1], an AI model and agent framework designed to accelerate the development of autonomous cybersecurity agents. As one of the first specialized cybersecurity LLMs, it provides organizations and researchers worldwide access to advanced cybersecurity capabilities at no cost[2]. The specialized Trend Cybertron model is fine-tuned using Llama 3.1 and supports rapid, reliable deployment with NVIDIA NIM inference microservices on NVIDIA accelerated infrastructure.

Kevin Simzer, COO at Trend Micro:"The secret sauce of Trend Cybertron is the data it continuously learns from, fine-tuned for optimized threat detection and mitigation. By bringing to bear the very highest quality threat data and NVIDIA's industry-leading AI expertise, we've made proactive security a reality, enabling us to predict and prevent threats like never before. This innovation isn't just a win for our customers—it's about making the entire digital, connected world a safer place."

Global organizations are struggling to innovate and grow while being weighed down by security challenges, fragmented point solutions, and an overwhelming flood of threat alerts. The complexity demands a shift to a proactive approach. Powered by NVIDIA AI at the core, Trend Cybertron moves beyond chasing threats, applying intelligent, decision-making AI agents to predict and respond.

Pat Lee, Vice President of Strategic Enterprise Partnerships at NVIDIA "With the ability to understand, reason and take action, AI agents give organizations a powerful new cybersecurity tool. Agentic AI security agents built with the Trend Cybertron model and framework using NVIDIA AI can analyze massive amounts of data in real-time to detect potential threats, adapt dynamically, and respond autonomously. "

To operationalize this vision, Trend has built its agentic AI strategy with NVIDIA AI software to accelerate cybersecurity automation, helping organizations proactively manage risks, with resource scanning, risk assessment, priority-based reasoning, and actionable remediation suggestions.

Organizations can apply multiple blueprints and seamlessly integrate AI agents to automate security tasks with resource scanning, proactively mitigate threats, and scale their defenses to manage threats more effectively, all within the NVIDIA ecosystem. Specifically, this will help:

- **Enhance security posture:** enabling teams to precisely anticipate risk across the entire attack surface.
- **Reduce alert overload**: alleviate fatigue for SecOps teams through more accurate prioritization.
- **Save developers' time**: overcome security skills shortages by providing actionable insights to help them identify and remediate risks.
- **Unleash greater value:** deliver more powerful insights from existing risk sensors.

Trend Cybertron is designed to proactively manage risk, leveraging threat intelligence from over 250 million sensors worldwide—the broadest in the industry. It interprets user queries, generates actionable plans, and performs a holistic risk assessment by retrieving real-time cybersecurity intelligence from Trend Micro's cloud, ultimately providing tailored recommendations and best practices to secure an enterprise's AI systems.

NVIDIA provided support and AI microservices for developing and deploying the model. Trend Micro trained and optimized the Trend Cybertron model for inference using NVIDIA DGX supercomputing to reduce the time required to fine-tune the model.

Trend Cybertron currently consists of an 8-billion-parameter AI model and an initial specialized AI agent, with additional models and agents in development to expand its cybersecurity capabilities. A larger and more advanced version with 70 billion parameter of the model is planned for the near future to address the cybersecurity challenges of tomorrow.

To learn more about Trend Cybertron, please visit Trend Micro at NVIDIA GTC: https://resources.trendmicro.com/NVIDIA-GTC-event.html

1: Trend Cybertron is licensed under the Trend Micro Community License, which restricts its use in connection with any competing product or service. For full license details, visit ***Trend Micro Community License****.*
2: Access to Trend Cybertron is open-source, but the use of NVIDIA infrastructure, such as GPUs, may involve associated costs.

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.

1. *Access to Trend Cybertron is open-source, but use of NVIDIA infrastructure, such as GPUs, may involve associated costs.*
2. *Trend Cybertron is licensed under the Trend Micro Community License, which restricts its use in connection with any competing product or service. For full license details, visit* ***Trend Micro Community License****.*

SOURCE Trend Micro

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

---