TrendAI™ Delivers Security-by-Design for AI Factories Powered by NVIDIA

New integration helps customers accelerate secure deployment of AI-centric datacentersthrough pre-validated design in NVIDIA DSX Air

DALLAS, March 16, 2026 /PRNewswire/ -- TrendAI™, the enterprise AI security leader, today announced a new integration with the NVIDIA DSX Air platform, which will empower customers to design, test, and prove AI factory security before deployment, rather than after.

To learn more about the TrendAI™ and NVIDIA DSX Air collaboration, please visit: https://resources.trendmicro.com/2026-nvidia-gtc.html

Rachel Jin, Chief Platform and Business Officer, Head of TrendAI™:"True innovation requires the best of both worlds: AI plus cybersecurity. Securing AI at scale isn't something you can bolt on later. It requires a purpose-built foundation. By empowering customers to check the impact of security on digital twin simulations, we're pioneering a new Secure AI Factory approach."

The NVIDIA DSX Air Platform provides the underlying environment where this design-first approach comes together.

Amit Katz, VP of Networking at NVIDIA:"NVIDIA is focused on simplifying and accelerating the design and validation of next-generation AI factories. Working with partners like TrendAI™ provides organizations with the visibility to detect threats across the entire stack, from cloud to endpoint, so they can focus on scaling AI without compromising security."

The NVIDIA DSX Air platform is a cloud-hosted network simulation platform that helps reduce the costs and accelerate the rollout of AI factories by enabling customers to create, validate, and test digital twins of data center infrastructure before physical installation. It offers faster integration, larger CapEx savings, and far greater scale than traditional lab environments.

However, security remains a critical consideration for any new AI factory project.

According to IBM, more than one in 10 global organizations reported data breaches involving their AI models or applications last year. This impact is significantly higher for organizations without AI or automation, which faced average breach costs $1.9 million more than those that did. A lack of proper access controls and supply chain issues, such as compromised apps, APIs, and plug-ins, were frequently cited, resulting in compromised data and disrupted operations. These risks are reshaping how organizations approach safe AI deployment.

AI factories built with security in mind from the start can help to reduce enterprise risk and breach impact by addressing these issues earlier in the lifecycle.

This is where TrendAI™ comes in. This new integration with the NVIDIA DSX Air platform helps teams understand the impact of security controls on AI factories without needing to deploy physical infrastructure upfront, lowering the barrier for PoCs and early evaluations.

There are two elements:

- **TrendAI Vision One™ AI Factory EDR**

A lightweight security agent deployed on NVIDIA BlueField data processing units (DPUs) with NVIDIA DOCA Argus software framework integration. It provides host visibility (file activity, network interfaces, and active processes), captures and analyzes network traffic, and leverages TrendAI™ threat intelligence to identify suspicious behavior. With TrendAI Vision One™ in place, customers can run red-team exercises that simulate MITRE threats in order to test their infrastructure and security posture.

- **High-performance network defense with TrendAI™ TippingPoint™**

Customers can test the efficacy and performance of virtual patching technology, which leverages theTrendAI™ Zero Day Initiative (ZDI) and industry-proven network detection and prevention capabilities (IDS/IPS) to protect AI factories from known and unknown threats, as well as exploitable vulnerabilities. Using the digital twin simulation, they can ensure patches will deploy safely and efficiently, in order to minimize disruption to live operations.

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, Microsoft, and NVIDIA. 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-Delivers-Security-by-Design-for-AI-Factories-Powered-by-NVIDIA