SecEdge SEC-TPM™ Advances Trusted Physical AI Systems with NVIDIA Halos AI Systems Inspection Lab

SecEdge SEC-TPM™ onboards to the NVIDIA Halos AI Systems Inspection Lab, enabling hardware-anchored AI model protection for trusted Physical AI systems.

SecEdge SEC-TPM enables hardware-anchored protection for AI models and Physical AI systems running on NVIDIA platforms. [Image courtesy of NVIDIA.]

SANTA CLARA, CA, UNITED STATES, March 16, 2026 /EINPresswire.com/ -- SecEdge, a provider of digital security solutions for Physical AI infrastructure, today announced that its SEC-TPM™ platform is onboarding into NVIDIA Halos AI System Inspection Lab, the first ANSI National Accreditation Board (ANAB) accredited inspection lab for AI-driven physical systems. The onboarding introduces device-level trust and AI model protection capabilities for NVIDIA-based Physical AI platforms supporting robotics, industrial automation, automotive, and medical systems.

> Securing the integrity of Physical AI is no longer optional—it is essential for trusted deployment.”
> *Sami Nassar, CEO of SecEdge*

NVIDIA Halos is a comprehensive full‑stack safety system for physical AI that unifies safety elements across vehicle and robotics architectures and their underlying AI models. It combines hardware and software components, tools, models, and design principles to safeguard AI‑based, end‑to‑end AV and robotics stacks.

SecEdge has been the security partner for NVIDIA Jetson since its inception, collaborating with NVIDIA to deliver SEC-TPM™, a TCG 2.0-compliant firmware Trusted Platform Module (fTPM) designed specifically for Jetson platforms. Integrated with NVIDIA JetPack, SEC-TPM operates within NVIDIA’s hardware-based secure execution environment to establish device identity and a hardware-anchored root of trust.

As AI models increasingly represent the core intellectual property of modern Physical AI systems,

protecting them from unauthorized copying, tampering, or reverse engineering has become essential. SEC-TPM introduces a hardware-rooted security layer that helps ensure AI models remain encrypted and authenticated from cloud delivery to deployment on edge devices.

Security enablement plays a critical role in the safe operation of autonomous systems. Hardware-anchored device trust and system integrity verification help ensure that AI systems operate with authenticated software and protected models. In Physical AI deployments, strong cybersecurity foundations are increasingly recognized as a prerequisite for safety assurance. “We believe security is foundational to system safety. Securing the integrity of Physical AI is no longer optional—it is essential for trusted deployment,” said Sami Nassar, CEO of SecEdge. “Through NVIDIA Halos AI Systems Inspection Lab, we are helping OEMs, ODMs, and AI developers deploy Physical AI systems with hardware-anchored trust while supporting alignment with evolving industry security requirements.”

BENEFITS OF SEC-TPM ONBOARDING TO NVIDIA HALOS AI SYSTEM INSPECTION LAB
AI MODEL PROTECTION
Helps prevent unauthorized access, alteration, or extraction of proprietary AI models deployed on edge devices.

HARDWARE ROOT OF TRUST
SEC-TPM provides a silicon-anchored trust foundation supporting measured boot, device identity, and secure cryptographic key management.

SEAMLESS DEPLOYMENT
Integrated with NVIDIA JetPack, enabling OEMs and system builders to deploy hardware-anchored security without complex custom integration.

SUPPORT FOR SECURITY AND SAFETY REQUIREMENTS
Supports alignment with frameworks referenced within the Halos inspection scope, including IEC 62443 and the EU Cyber Resilience Act (CRA).

ABOUT SecEdge
SecEdge™ provides industry-leading digital security for physical AI infrastructure and edge devices. Renowned for its award-winning AI model protection, the SecEdge SEC-TPM™ solution is a TCG 2.0-compliant firmware TPM seamlessly hardware-anchored with leading semiconductor platforms. From chip to cloud, SecEdge secures Physical AI and edge devices infrastructure, and enables frictionless compliance with industry and government regulations.

Learn more: visit www.secedge.com or contact info@secedge.com.

Jennifer Walken
SecEdge, Inc.

+1 408-462-1376
jennifer.walken@secedge.com
Visit us on social media:
LinkedIn
Facebook
YouTube
X
