

SecEdge Launches AI-PASSPORT™ to Combat the Growing Threat of Backdoored AI Models

New cryptographic “passport” gives AI models verifiable identity, provenance and integrity, demonstrated on NVIDIA Jetson Thor with NVIDIA Nemotron™ open models

ANAHEIM, CA, UNITED STATES,
September 23, 2026 /

EINPresswire.com/ -- SecEdge, Inc.
unveiled [AI-PASSPORT™](#), a

groundbreaking solution for AI model authenticity, provenance, and integrity verification. Introduced at Embedded World North America 2026, AI-PASSPORT™ is being demonstrated live at booth 6226 and in the NVIDIA Robotics Lab on NVIDIA Jetson Thor

using open models from the NVIDIA Nemotron family. Technical sessions will highlight the growing need for AI trust across enterprise, robotics and edge deployments.



SecEdge AI-PASSPORT™ delivers verifiable identity, provenance and integrity to help protect AI models from backdoor threats. See it, in action at SecEdge Booth 6226 and the NVIDIA Robotics Lab at Embedded World NA 2026 in Anaheim.

“

AI PASSPORT™ extends the same principle behind our work with NVIDIA Halos to every AI model: security and safety start with verifiable trust.”

Sami Nassar, CEO, SecEdge

Open-source AI is becoming the software supply chain challenge of the AI era. Without trusted provenance, malicious actors can modify, poison, or impersonate widely used models and redistribute them as authentic releases. The result is a growing risk of counterfeit AI entering enterprise, industrial, robotics, and edge deployments, often without detection.

AI-PASSPORT™ is a cryptographically verifiable trust credential that establishes an AI model’s identity, provenance, and integrity for both open-source and proprietary AI models. It travels with the model and can be

verified without ever exposing or inspecting the model’s contents. This gives developers, deployers, and auditors a fast way to confirm that a model is the approved version, came from the expected source, and has not been modified since it was signed, ensuring organizations

deploy only trusted original models.

SecEdge is part of the full-stack functional safety architecture designed specifically for Physical AI. At the center of this ecosystem is the [NVIDIA Halos AI Systems Inspection Lab](#), the world's first ANAB-accredited inspection program for AI and functional safety, helping partners validate system integration and accelerate third-party certification.

"AI-PASSPORT™ extends the same principle behind our work with [NVIDIA Halos](#) to every AI model: security and safety start with verifiable trust," said Sami Nassar, CEO of SecEdge. "As AI models move from the data center to edge compute and edge devices, knowing exactly which model you're running, where it came from, and whether it's been tampered with becomes a safety and compliance requirement, not a nice to have."

Join SecEdge in the NVIDIA Robotics Lab for "Whose AI Are You Running?," a 15-minute Tech Talk focused on medical AI applications, followed by an opportunity to speak with SecEdge leadership. A session is scheduled for Wednesday, Sept. 23, from 1 to 1:15 p.m.

ABOUT SecEdge

SecEdge™ provides industry-leading digital security for physical AI infrastructure and edge devices. The SecEdge AI-TRUST™ Platform—AI-PASSPORT™, SEC-AI™ and SEC-TPM™ PLUS—delivers chip-to-cloud management and protection with verifiable identity and provenance for AI models. Its award-winning technologies also enable trusted device identity, secure provisioning and trusted access—the foundation for secure AI deployment at the edge and compliance with industry standards and government regulations.

Learn more at www.secedge.com or send an email to info@secedge.com.

###

Jennifer Walken
SecEdge, Inc.
jennifer.walken@secedge.com
Visit us on social media:

[LinkedIn](#)
[Facebook](#)
[YouTube](#)
[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/944191472>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable

in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.