Securing AI Models at the Edge
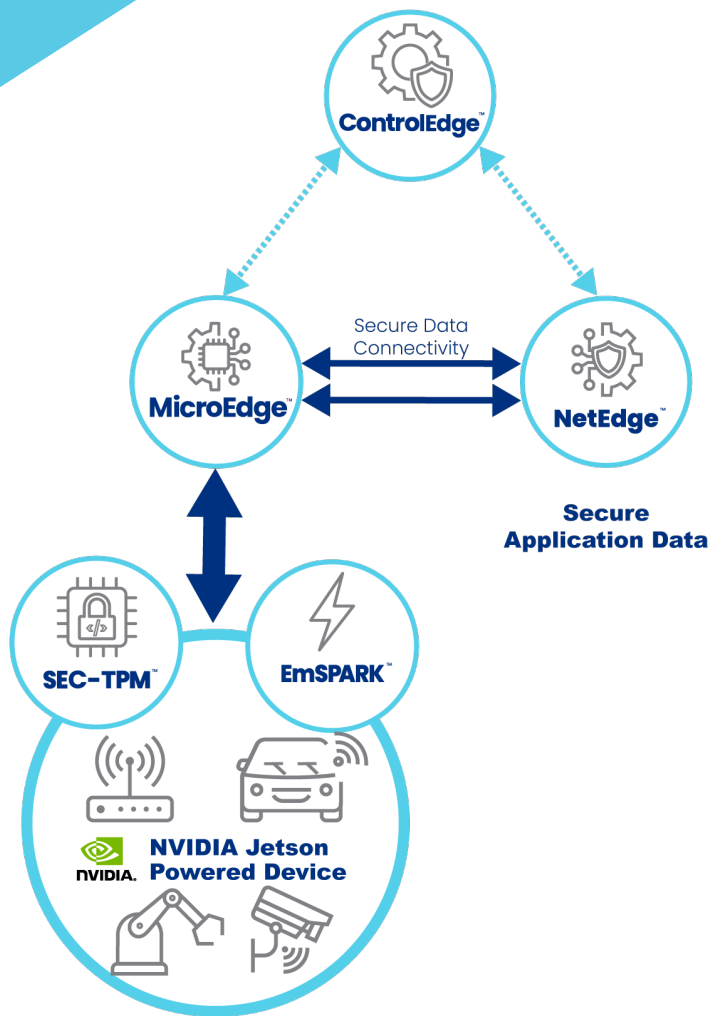
ON THE NVIDIA JETSON WITH SECeDGE™

INTRODUCTION

The explosion of Edge AI creates opportunities in dozens of industries. Deploying AI to the Edge improves performance, increases availability and lowers over cost of your solution. This new architecture, however, introduces security challenges. AI models are valuable intellectual property, and must be protected at the device with secure connections to their associated applications.

HOW CAN YOU AND YOUR PARTNERS ENSURE THAT YOUR AI MODELS ARE SAFE?

SecEdge delivers a complete chip-to-cloud solution for securing and managing AI at the Edge, fully integrated with the NVIDIA Jetson. The solution delivers:

+ **Device Security.** Secure boot, updates and failure recovery, as well as secure applications for cryptography, credentials management and cloud integration.

+ **Secure Provisioning.** TCG compliant firmware TPM support with an in-field provisioning and management service.

+ **AI Model Protection.** Proven methods to verify a model's authenticty and hide it from threats.

+ **Secure Data Connectivity.** Secure VPN tunnels to separately management AI model, application, and control data.

+ **Test and Development Tools.** Stage, test and deploy your solution in a matter of weeks with SecEdge Studio™.

Jetson Orin AGX, NX, and Nano
Jetson Xavier AGX and NX
Jetson TX2 and Nano

CASE STUDY

Lenovo Protects AI Models at the Edge

GET STARTED

Register to try SecEdge Studio™

ControlEdge™

Secure Data Connectivity

MicroEdge™

NetEdge™

Secure Application Data

SEC-TPM™

EmSPARK™

NVIDIA Jetson Powered Device

SecEdge Secure Edge AI Solution for NVIDIA.

NVIDIA.®

NVIDIA Corporation is a market leader in visual computing technology dedicated to creating products that enhance the interactive experience on consumer and professional computing platforms. Its graphics and communications processors have broad market reach and are incorporated into a wide variety of computing platforms, including consumer PCs, enterprise PCs, notebook PCs, professional workstations, handhelds, and video game consoles. NVIDIA is headquartered in Santa Clara, California and employs more than 1,900 people worldwide. For more information, visit the Company's Web site at www.nvidia.com.

SEC eDGE™
Digital Security to the Edge

SecEdge is a digital security SaaS Platform leader for IoT and Edge devices, providing advanced security solutions for Edge AI, Compute, Control and on-demand cellular IoT data connectivity. The SecEdge software-as-a-service platform provides a complete solution including device-level security, zero-trust networking, and secure data control and management, with connectivity via broadband internet or on-demand cellular data available anywhere. To learn more about SecEdge's security platform, visit us at www.secedge.com.

PO Box 201
Fall City, WA 98024

+1 425 654 2048

info@secedge.com
www.secedge.com