# Lenovo Protects AI Models

## AT THE EDGE WITH THE EMSPARK™ SECURITY SUITE

## INTRODUCTION

The Lenovo ThinkEdge SE70 is a powerful and flexible AI edge platform for the enterprise designed to meet the expanding intelligent transformation needs from logistics, transportation and smart cities to retail, healthcare and manufacturing. Powered by the NVIDIA® Jetson™ Xavier™ NX platform, the solution allows customers to transform every-day IP cameras into 'smart' cameras that run computer vision apps at the edge.

## THE PROBLEM: PROTECTING AI MODELS AT THE EDGE

Lenovo's ThinkEdge SE70 houses an end-user's AI model of choice, supporting 3rd party services delivering AI Models. In order to support 3rd party AI models and delivery mechanisms, and ensure end users that their models are safe, it was critical for Lenovo to deliver a solution that would protect AI at the edge. Without assurance that models are safe, the interests of AI model developers, Lenovo, and end users of the solution are all at risk.

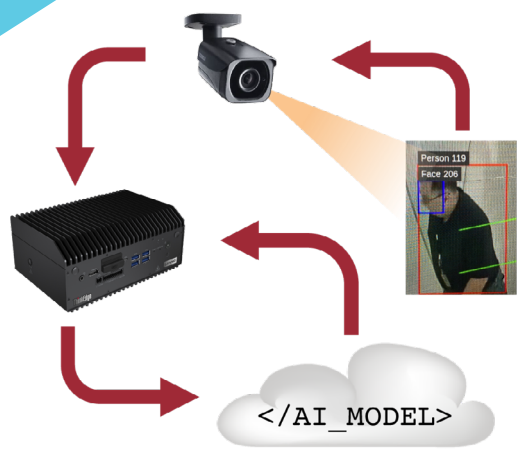
## THE EMSPARK™ SOLUTION

Lenovo collaborated with SecEdge to integrate the EmSPARK™ Security Suite and provide AI model protection on the SE70.

In this approach, the following steps are taken:

- The application is encrypted, and locked to the device, in storage (e.g. flash memory).
- EmSPARK™ initiates the sequence of loading and running the model.
- A Trusted Application, housed in a secure enclave created by EmSPARK™, verifies, decrypts, and loads the application.
- Interfacing with the Rich Environment's operating system (e.g. Linux), the Trusted Application loads the application directly into Random Access Memory (RAM) and runs it.

This approach is an efficient way to greatly reduce the attack surface and overall risk profile applied to running an AI model on the Lenovo SE70.




*Deploying AI models at the Edge for Intelligent Video Analytics with the Lenovo ThinkEdge SE70.*

## SOLUTION BENEFITS

With a solution providing reliable protection of AI models on the ThinkEdge SE70:

- Lenovo's ThinkEdge SE70 can be deployed in a variety of applications involving intelligent video analytics, supporting best-in-class AI models.
- Lenovo's technology partners, producing industry-changing models for edge analytics, can be assured that their intellectual property is safe.
- Lenovo's customers can deploy the ThinkEdge SE70 safely and securely in their application of choice, while implementing optimized AI models at the network edge.

## LEARN MORE

**Press Release:**
Sequitur Labs Collaborates with Lenovo to Protect AI Models at the Edge

**Learn More:**
EmSPARK™ for NVIDIA

**Whitepaper:**
Protecting AI at the Edge

Lenovo

Lenovo (HKSE: 992) (ADR: LNVGY) is dedicated to building exceptionally engineered personal computers. Lenovo's business model is built on innovation, operational efficiency and customer satisfaction as well as a focus on investment in emerging markets. Formed by Lenovo Group's acquisition of the former IBM Personal Computing Division, the company develops, manufactures and markets reliable, high-quality, secure and easy-to-use technology products and services worldwide. Lenovo has major research centers in Yamato, Japan; Beijing, Shanghai and Shenzhen, China; and Raleigh, North Carolina. For more information see www.lenovo.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 1127
Issaquah, WA 98027

+1 425 654 2048

info@secedge.com
www.secedge.com