AI EDGE LABS

ZEDEDA

Secure and Manage Edge Distributed Environments at Scale

Edge distributed environments may have no physical perimeter, are heterogeneous, include devices that can be too constrained to run traditional security solutions, can be characterized by the network infrastructure ranging from complex to non-existent, with a lot of existing legacy protocols in place, little to no onsite IT staff, and run into the tens of thousands or more at a scale.

A comprehensive Edge security framework requires two capabilities:

Crypto-based device identification that eliminates local device login credentials combined with measured boot and remote attestation through the entire stack beginning at the firmware through to the OS, container and application

Runtime Edge-based security, that provides autonomous AI-powered multi-layered protection in real-time and can be easily scaled to any new deployments without any downtime or changes.

ZEDEDA and **AI EdgeLabs** have partnered to deliver a comprehensive and unique cyber security solution for distributed infrastructure that can be deployed in one-click within minutes to all your Edges across multiple locations.

ZEDEDA delivers an open, distributed, cloud-native Edge orchestration and management solution, simplifying the security and remote management of Edge infrastructure and applications at scale. ZEDEDA leverages an open architecture built on EVE, from the Linux Foundation. EVE delivers an industry leading identity and software attestation workflow that ensures the device can be trusted and that the entire software stack is exactly as expected.

AI EdgeLabs provides a distributed, multi-layered, Edge-native security to ensure runtime protection for Edge infrastructure at scale. AI EdgeLabs is a comprehensive AI-based solution that directly deploys to Edge or IOT gateway and secures both virtual and physical Edge environments in autonomous mode, ensuring continuous inline defense against any type of threats in real time, even for disconnected offline systems or those with intermittent connection.

Visualize. Orchestrate. Secure.

Our joint **ZEDEDA** & **AI EdgeLabs** platform solution addresses the unique security challenges of distributed Edge infrastructure and provides a multi-layered Edge-native security.

Zero trust — security model addressing the unique, perimeter-less security challenges of Edge infrastructure

Zero touch — instantly on-board Edge infrastructure and applications from the cloud — no on-site expertise required

TPM-based cryptographic identities

Network-based asset discovery and monitoring — comprehensive and accurate real-time view of the network assets and anomalies

Real-time threat detection and response at 2/3/4/ layers to protect any type of threats and attacks from the applications deployed across ZEDEDA environments:

- DDoS attacks
- MiTM detection
- Brute-Force
- Botnets
- LLMNR
- Reconnaissance
- Malware
- Ransomware

Distributed AI-Based Edge Firewall and ACL for network connectivity

Zero-hardware footprint offers software-defined, lightweight solution — no more than 4% CPU, reduced maintenance requirements and little human involvement

Simple integration via docker container technology

Unlimited scalability across all distributed infrastructure

Successful Outcomes

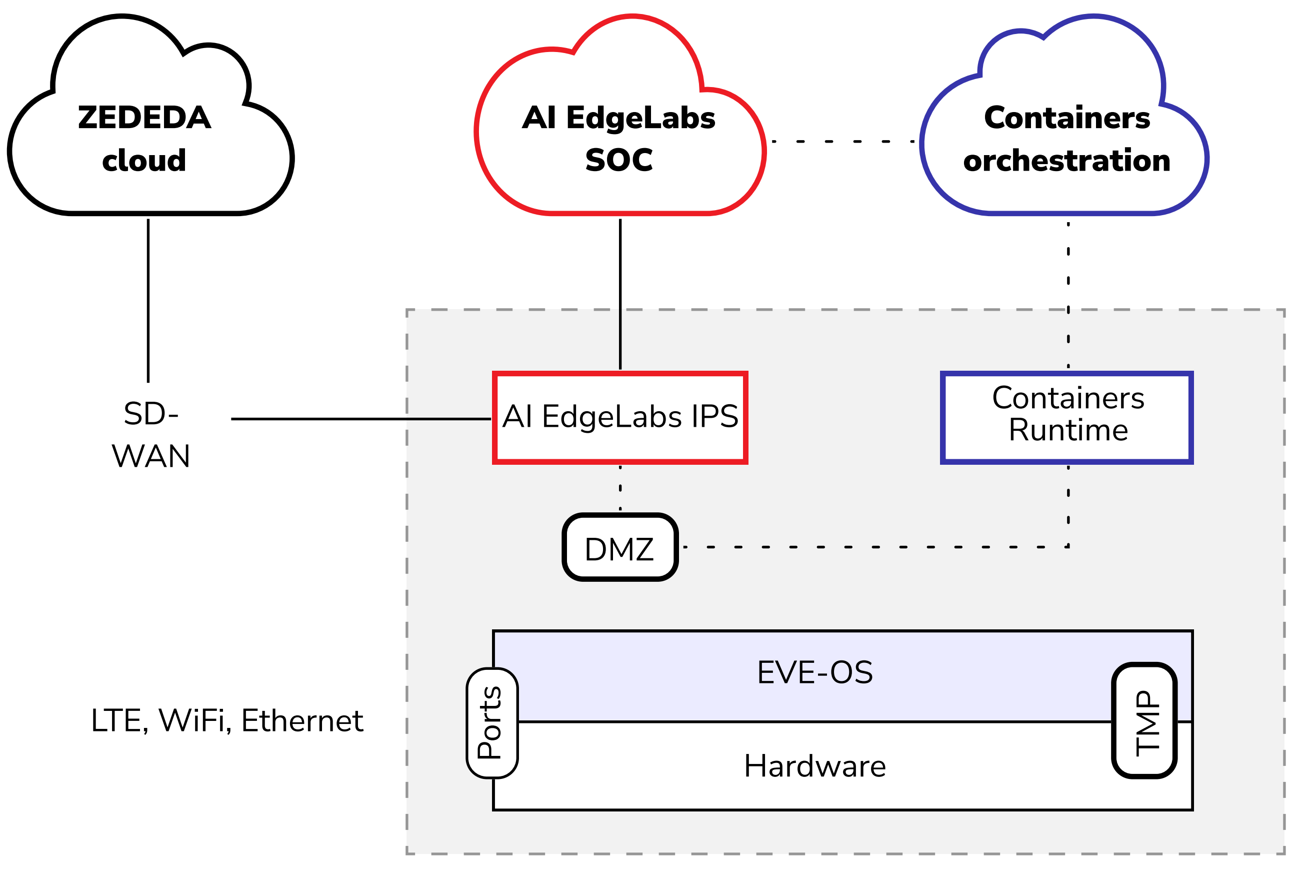
Real-time threat detection & response	**99,9%**	precision
Improved performance	**97%**	reduced downtime and outages
Cost efficiency	**<15%**	reduction of the total security costs
Enhanced compliance		no outside data transition

Integration and Deployment

AI EdgeLabs’ functionality is deployed on Edge devices with a single click through the **ZEDEDA** Marketplace.

ZEDEDA’s orchestration solution remotely manages the underlying infrastructure, including hardware, EVE, and application VMs and containers.

AI EdgeLabs deploys a lightweight container (agent) on each host, which acts as a gateway for the internal ecosystem of the deployed virtual machines and containers. On-host internal VLAN network provides NAT-based approach for the network communication between services and exposures outside, so that AI EdgeLabs guarantees advanced AI/ML-based firewalling capabilities for the threats and attempts to down or hack the system.



Zededa + AI EdgeLabs integration scheme

Industries We Serve

Retail

Telecom

Transportation & Logistics

Railway

Oil & Gas

Manufacturing

Healthcare

Energy & Utilities

Agriculture

Automotive

Smart Cities

Government & Military

Engage with AI EdgeLabs and ZEDEDA teams:

AI EdgeLabs | contact@edgelabs.ai

Zededa | sales@zededa.com