EVE-OS Overview

How to Modernize the Edge and Stay Secure

THE LINUX FOUNDATION

Learning Content

› Edge Computing Challenges

› How EVE Modernizes the Industrial Edge

› Commercial Ecosystem Opportunities

› EVE Technology and Security Overview

› Embracing LF Edge Open Source Community Collaboration

□ THE LINUX FOUNDATION

Challenges at the Edge

- **Security**
  - No guarantee of network security
  - No guarantee of physical security
  - Onerous security overlays at the edge

- **Diversity of deployed infrastructure**
  - Mixture of remote devices
  - Plethora of apps to orchestrate
  - App integration with several Clouds

- **Scale and automation**
  - Huge # of edge devices, geographically disperse
  - Long maintenance lifecycle (7+ years)

- **Unreliable connectivity**
  - Network outages, latency, expensive bandwidth
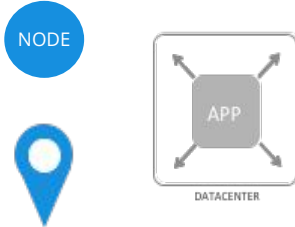 - Might not even control edge network

THE LINUX FOUNDATION
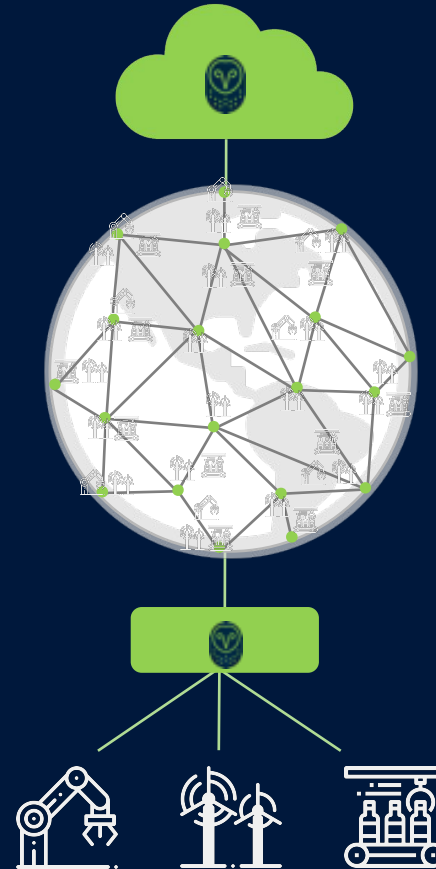
How EVE Modernizes the Industrial Edge

EVE addresses the unique properties of distributed edge computing nodes deployed outside of the traditional datacenter
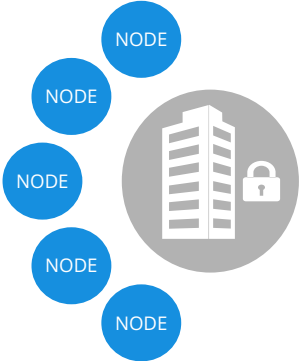
Diversity

Inherent diversity of technology and domain expertise required

Scale

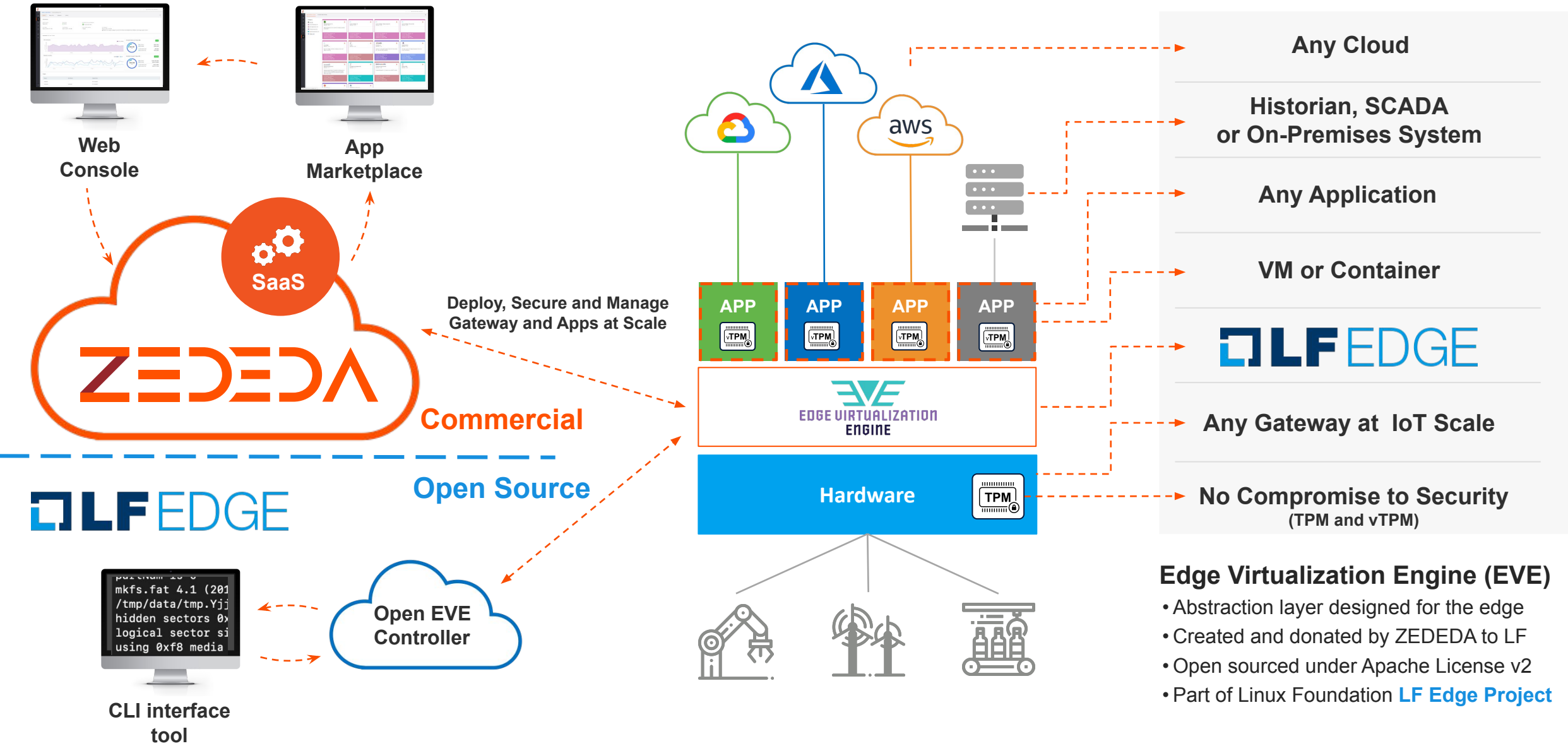Unprecedented scale and geographic distribution of deployed nodes

No Perimeter

No physical or network perimeter dictates a zero trust security model

The distributed edge needs a standard foundation for orchestration and virtualization that is flexible, open and agnostic

THE LINUX FOUNDATION

Challenges Solved with Edge Virtualization

Web Console

App Marketplace

SaaS

ZEDEDA

Commercial

Open Source

LF EDGE

CLI interface tool

Open EVE Controller

Deploy, Secure and Manage Gateway and Apps at Scale

APP vTPM

APP vTPM

APP vTPM

APP vTPM

EDGE VIRTUALIZATION ENGINE

Hardware TPM

aws
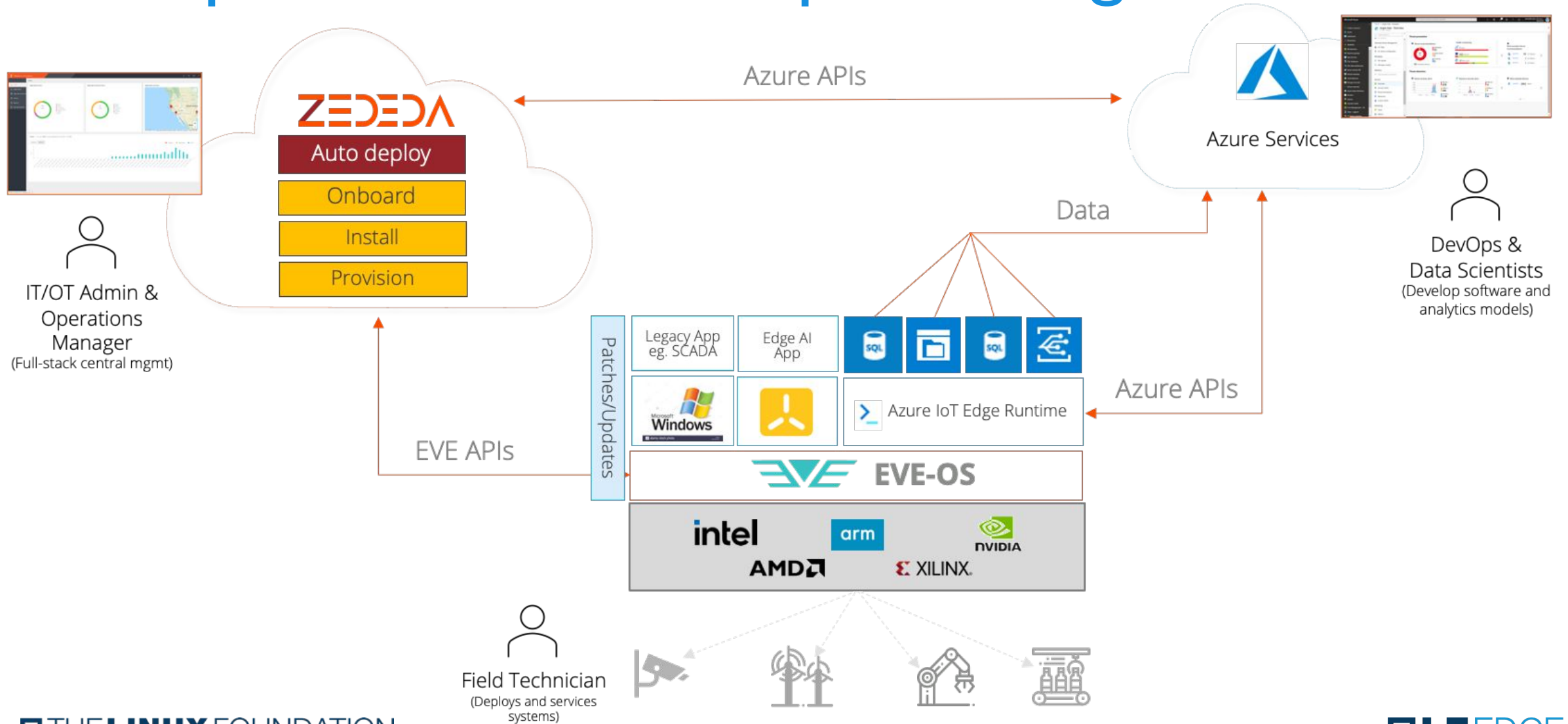
Any Cloud

Historian, SCADA or On-Premises System

Any Application

VM or Container

LF EDGE

Any Gateway at IoT Scale

No Compromise to Security (TPM and vTPM)

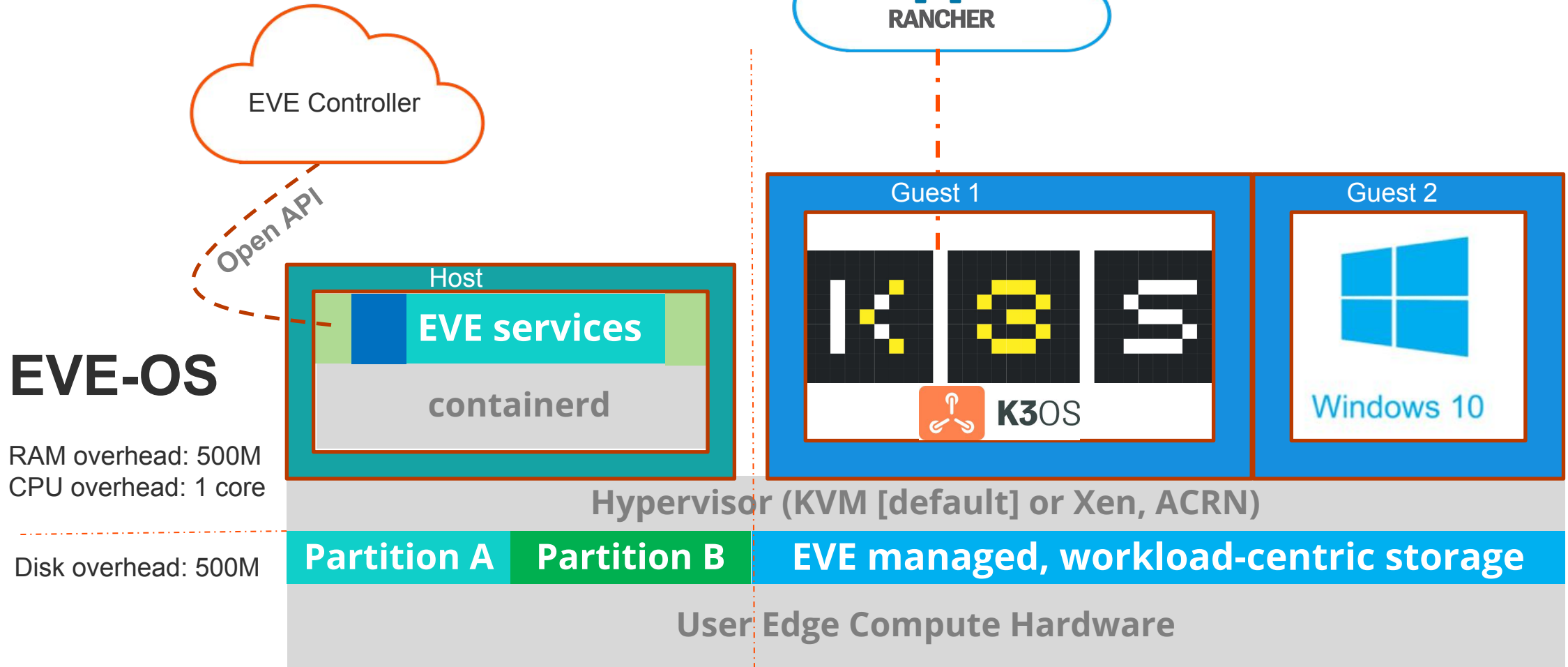**Edge Virtualization Engine (EVE)**
- Abstraction layer designed for the edge
- Created and donated by ZEDEDA to LF
- Open sourced under Apache License v2
- Part of Linux Foundation **LF Edge Project**

Example ZEDEDA Enterprise Integration

EVE Technology and Security Overview

THE **LINUX** FOUNDATION

EVE Architecture

RANCHER

EVE Controller

Open API

EVE-OS

RAM overhead: 500M
CPU overhead: 1 core

Disk overhead: 500M

Host

EVE services

containerd

Guest 1

K3OS

Guest 2

Windows 10

Hypervisor (KVM [default] or Xen, ACRN)

Partition A | **Partition B** | **EVE managed, workload-centric storage**

User Edge Compute Hardware

EVE-OS to EVE Controller "Onboarding"
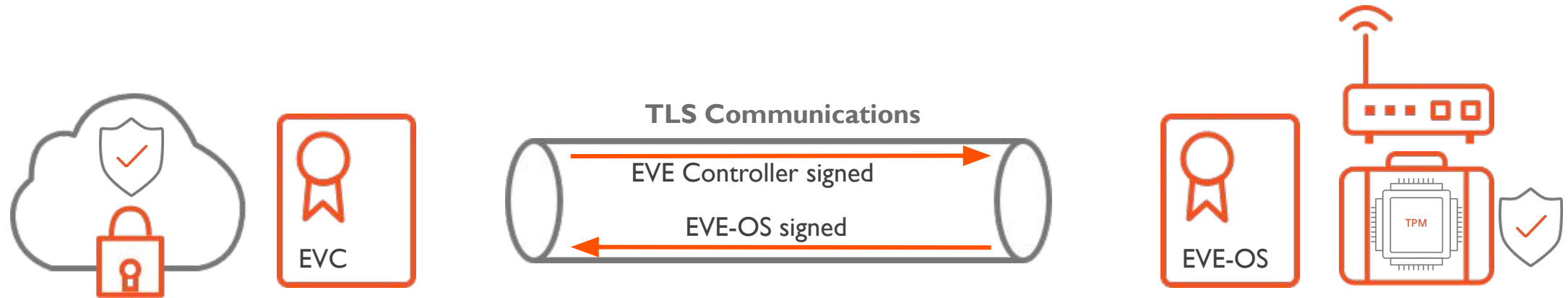
- › Cryptographic device identity created when EVE-OS installed (factory)
  - › Key pair generated in TPM; private key never leaves TPM
  - › Device is imprinted with the controller to trust (a root CA certificate)
- › Device can be pre-onboarded in factory, optionally with applications too
- › User registers their hardware using device certificate or serial number
- › See https://github.com/lf-edge/eve/blob/master/docs/REGISTRATION.md

THE **LINUX** FOUNDATION

Remotely Manage Any Edge Node

No field expertise required

Configuration updates

EVE Controller

Node calls "home" for configuration and updates
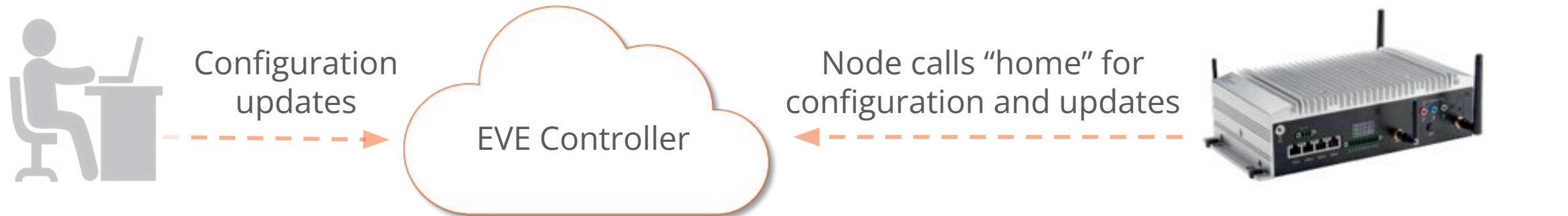
- Any type of silicon and device
- Automated on-boarding
- Autonomous operations

Any Silicon

intel   NVIDIA   ARM

Any User Edge Compute Node

ADVANTECH   DELL   Hewlett Packard   Lanner   SUPERMICRO
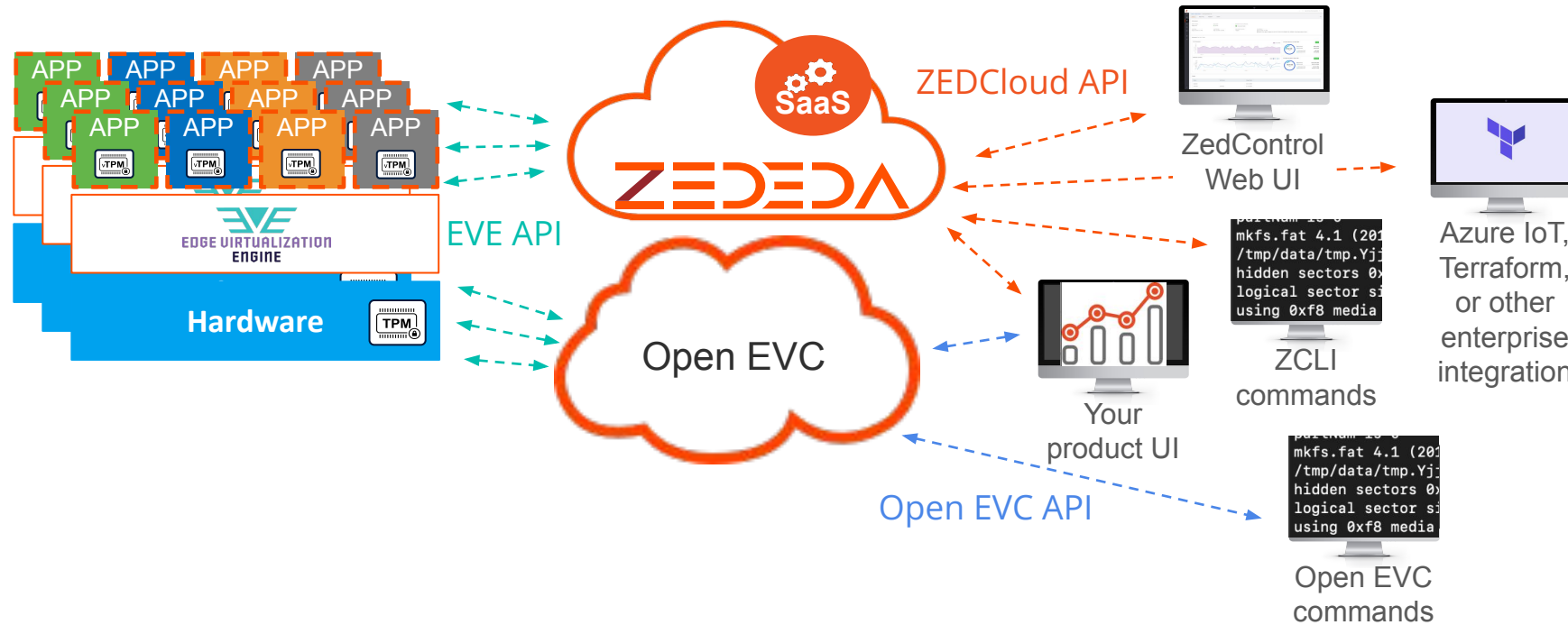*Enabling an Intelligent Planet*   Enterprise

THE **LINUX** FOUNDATION

Publicly Documented APIs

EVE-OS
Secure API over TLS

EVE Controller (ZEDCloud or Open EVC)
Secure API over HTTPS

ZEDCloud API

EVE API

Open EVC API

ZedControl
Web UI

Azure IoT,
Terraform,
or other
enterprise
integration

ZCLI
commands

Your
product UI

Open EVC
commands

EVE-OS API
https://github.com/lf-edge/eve/tree/master/api

ZEDCloud API
https://zedcontrol.zededa.net/api/v1/docs/

Open EVC Interface (API)
https://github.com/lf-edge/eden/blob/master/docs/data-from-eve.md

THE **LINUX** FOUNDATION

EVE API Security Works Through Firewalls, Proxies

In the field (edge locations)

Edge App Instances

EVE

The Edge Node is configured to trust a particular proxy certificate

Data

EVE Sends data to ZedControl

TLS Tunnel 1

Proxy Server
HTTP / HTTPS
FTP/ SOCKS

Data

Data is sent

TLS Tunnel 2

EVE Controller

e.g., ZEDCloud SaaS

Proxy Content Inspection / Deep content Inspection
1. Proxy server inspects the data being transferred.
2. Proxy Server cannot inspect the sensitive data as it is encrypted using end-to-end object encryption.

1. TLS to trusted parties (direct to controller and/or via proxy)
2. End-to-end signature over payload (proxy can not view nor modify)
3. Sensitive data encrypted end-to-end (also at rest)

THE **LINUX** FOUNDATION

Zero Trust
People, Process, and Technology

Hardware Root of Trust	No Usernames & Passwords	Distributed Firewall	Layered Security Model	API to Centralized Management
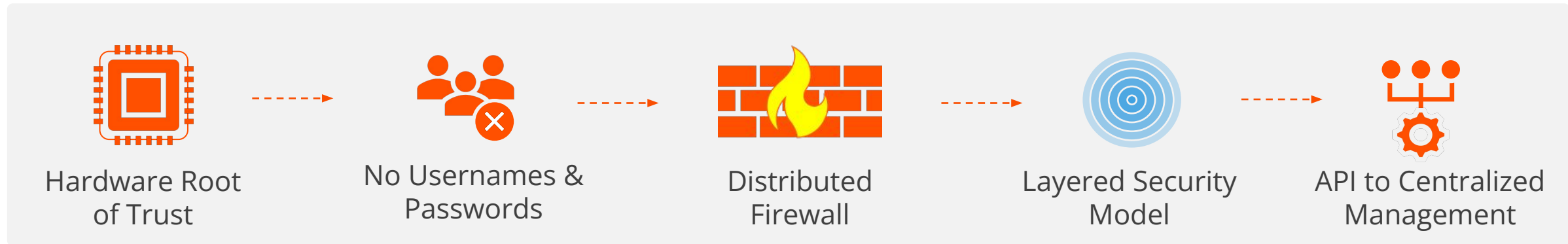
- **People**
  - Remove need for device usernames/passwords
  - Role-based access control (RBAC) and multi-tenancy in controller

- **Process**
  - "Zero Touch" hardware deployment to field
  - Design for 7+ year lifetime at the edge
  - Secure, scalable distribution of updates
  - API reports (resource usage, firewall violations) enable analytics in controller

- **Standard security technologies for the user edge**
  - Hardware root of trust (e.g., TPM)
  - Crypto-based identification
  - Measured boot and remote attestation
  - Encryption at rest and in-flight (TLS); keys sealed by TPM
  - Signed images for EVE-OS and applications
  - Use hypervisors for strong isolation and defense in depth
  - Distributed firewall for every app
  - Physical security – port isolation
  - Support deployment of virtual security appliances

THE **LINUX** FOUNDATION

Embracing LF Edge Open Source Collaboration

THE **LINUX** FOUNDATION

Community Collaboration Resources

Project page https://www.lfedge.org/projects/eve/
Wiki https://wiki.lfedge.org/display/EVE/EVE
  › Mailing list https://lists.lfedge.org/g/eve
  › Zoom calls (calendar subscription on wiki)
GitHub https://github.com/lf-edge/eve
Slack https://lfedge.slack.com

Roadmap
https://wiki.lfedge.org/display/EVE/Feature+Roadmap

![The Linux Foundation]

Ready to Transform Your Edge?

THE **LINUX** FOUNDATION