EVE Overview

A new paradigm to securely manage the industrial edge

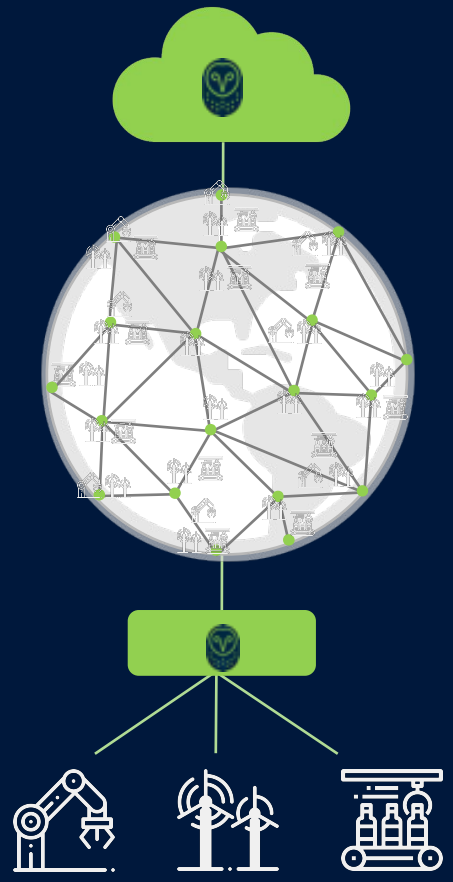
THE LINUX FOUNDATION

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

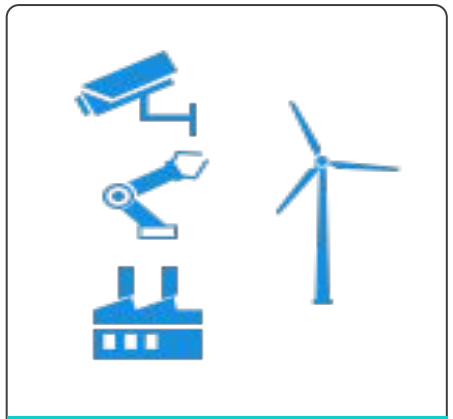
Challenges at the Edge

- **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



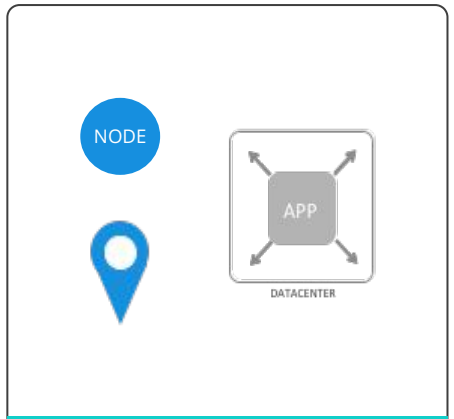
How EVE Modernizes the Industrial Edge

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



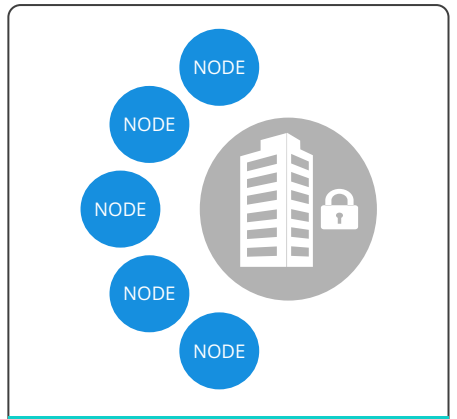
Diversity

Inherent diversity of technology and domain expertise required



Scale

Unprecedented scale and geographic distribution of deployed nodes

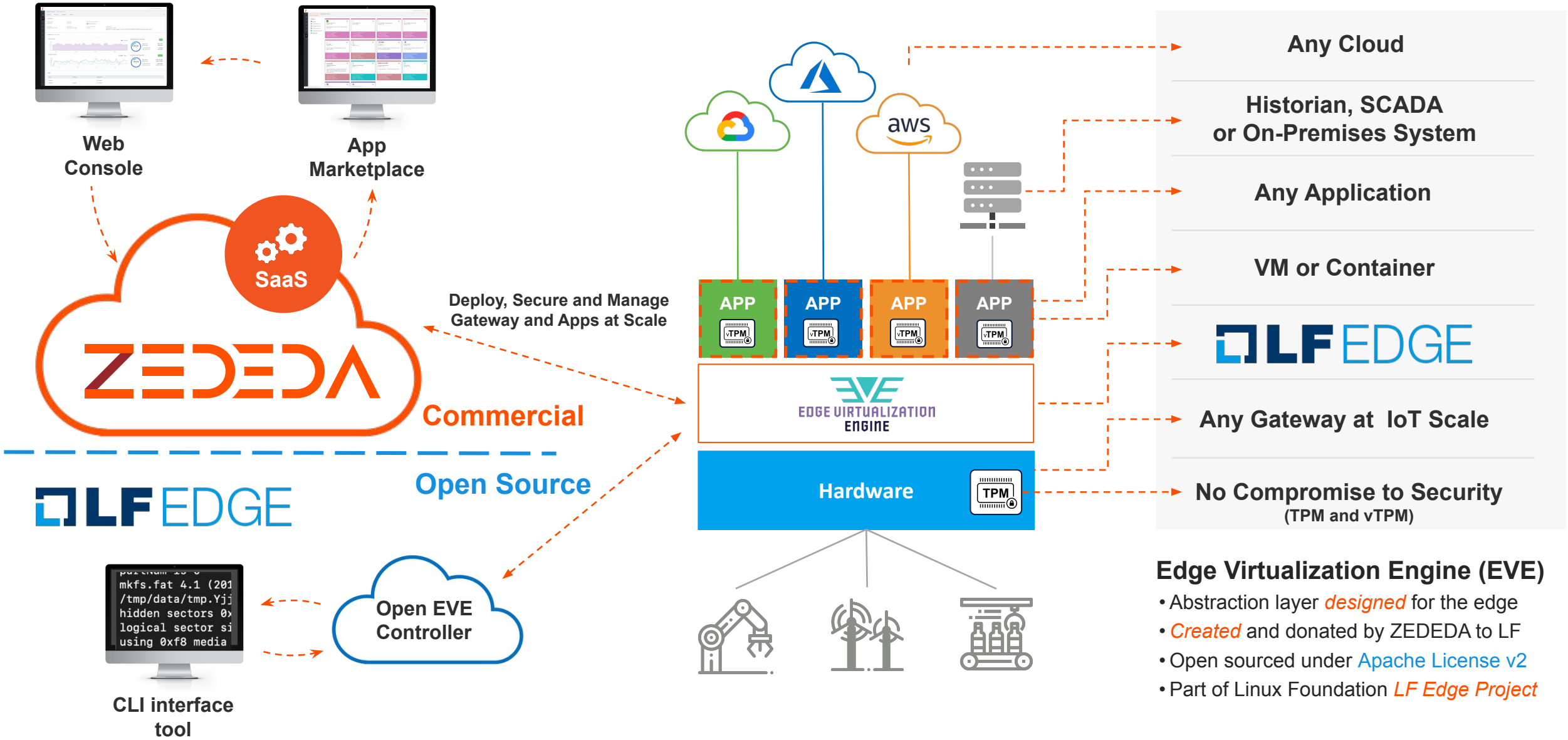


No Perimeter

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

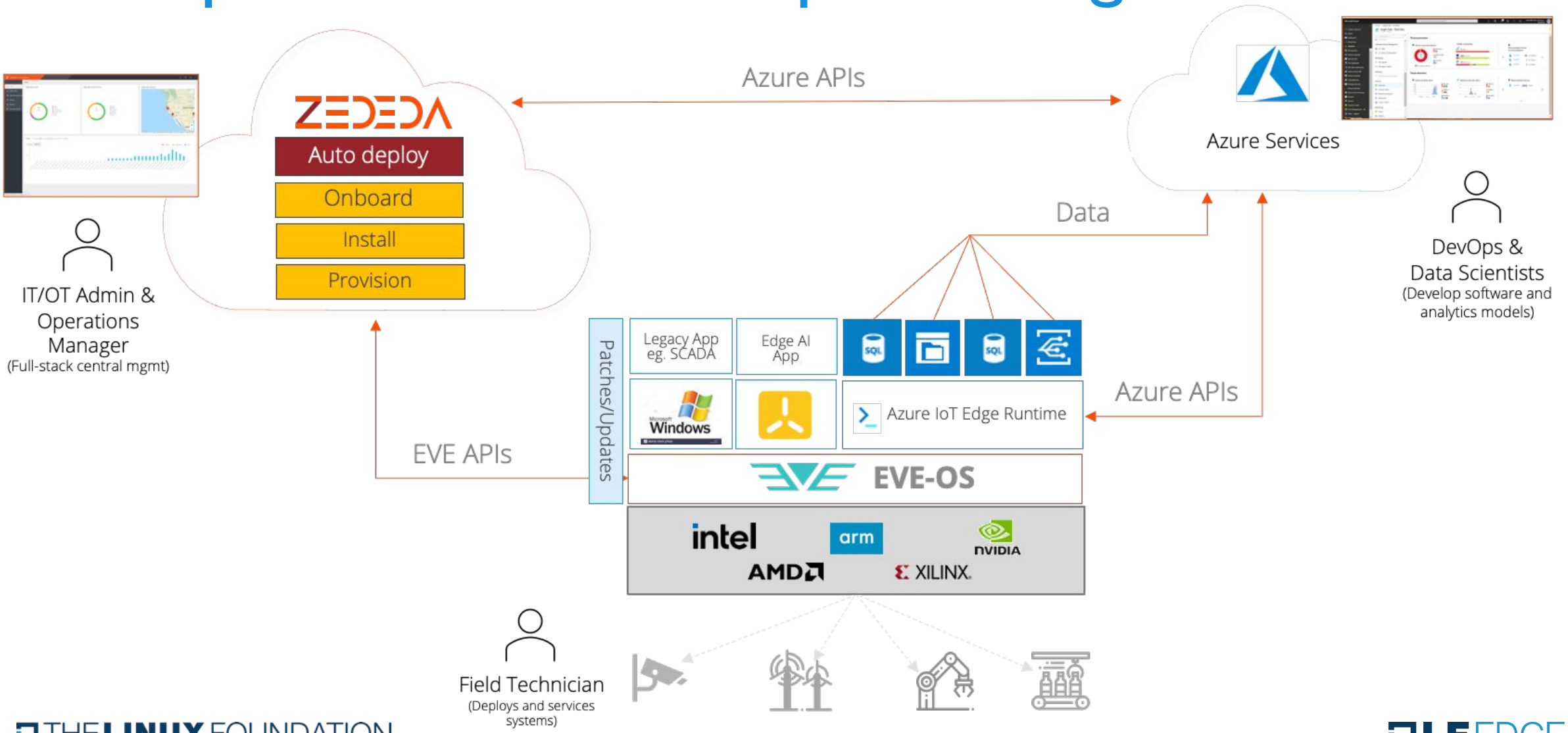
Challenges Solved with Edge Virtualization



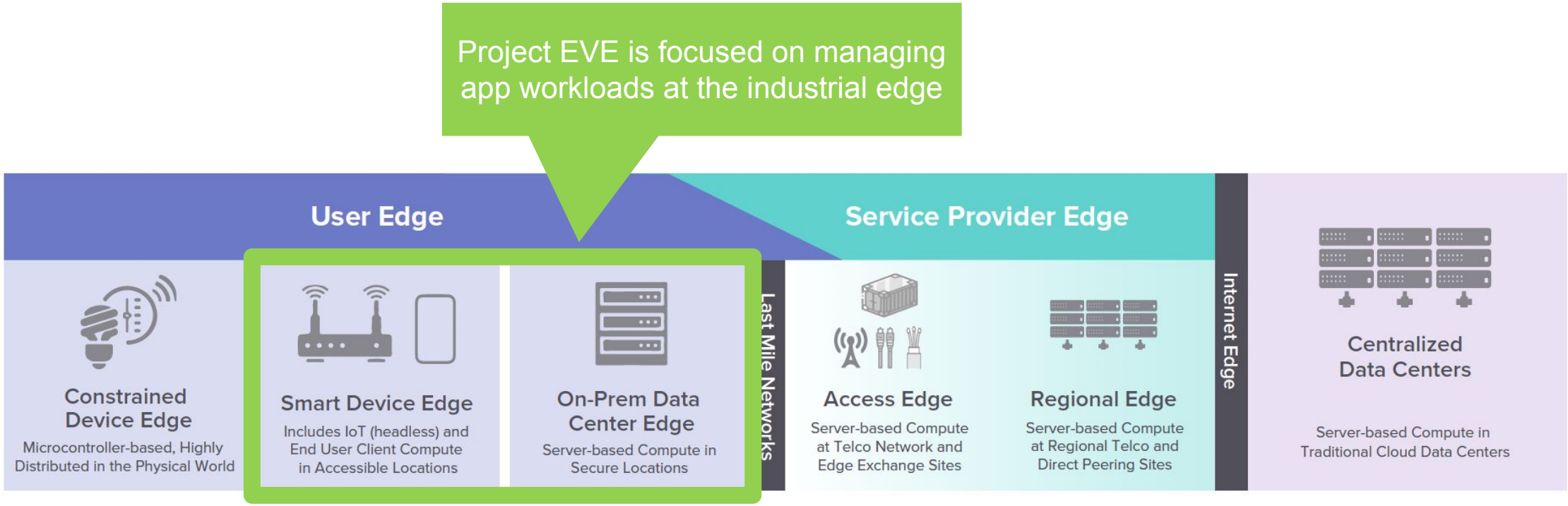
Edge Virtualization Engine (EVE)

- 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



Commercial Ecosystem Opportunities

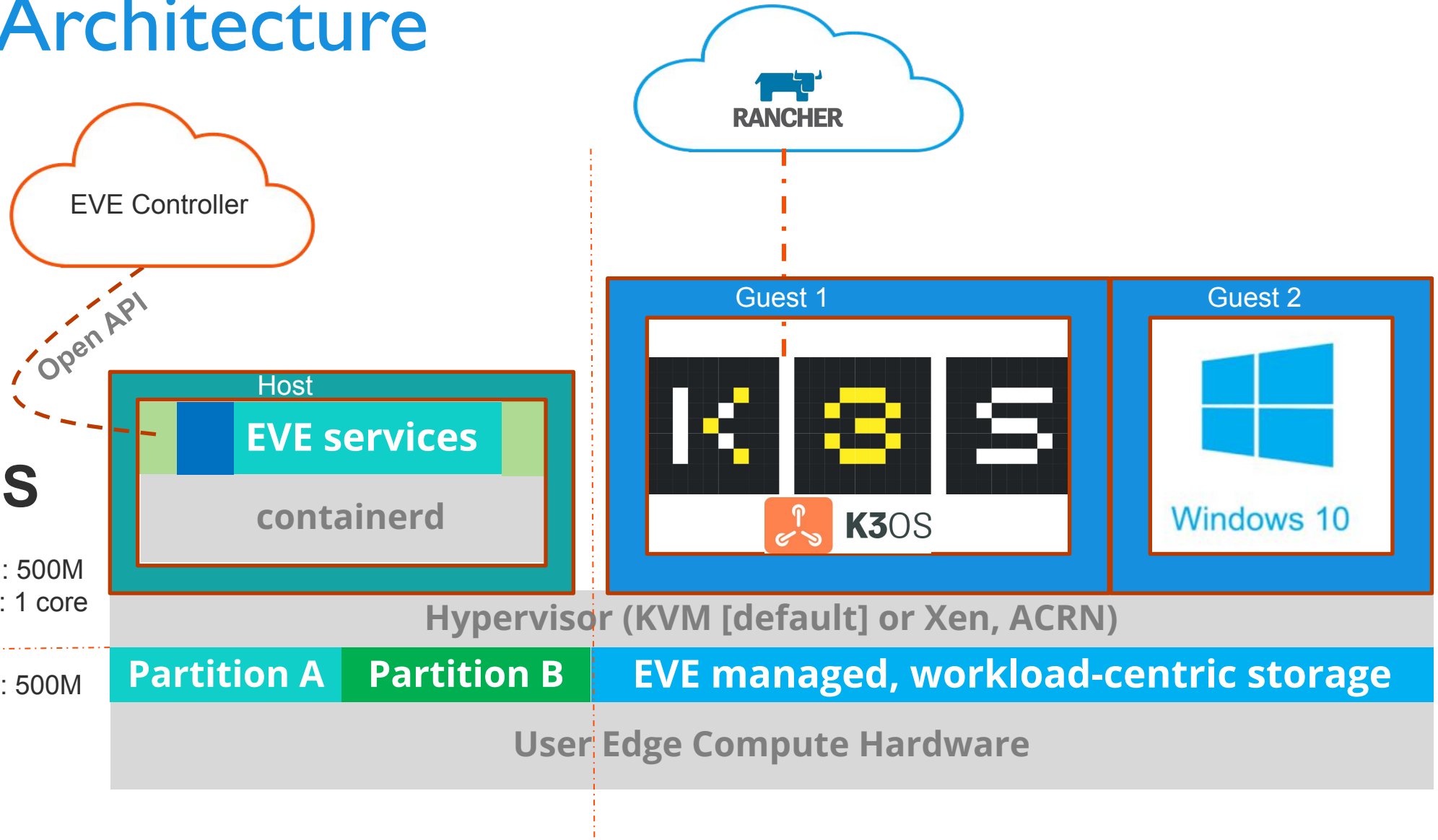


See https://www.lfedge.org/resources/publication-download/

EVE Technology and Security Overview

THE LINUX FOUNDATION

EVE Architecture

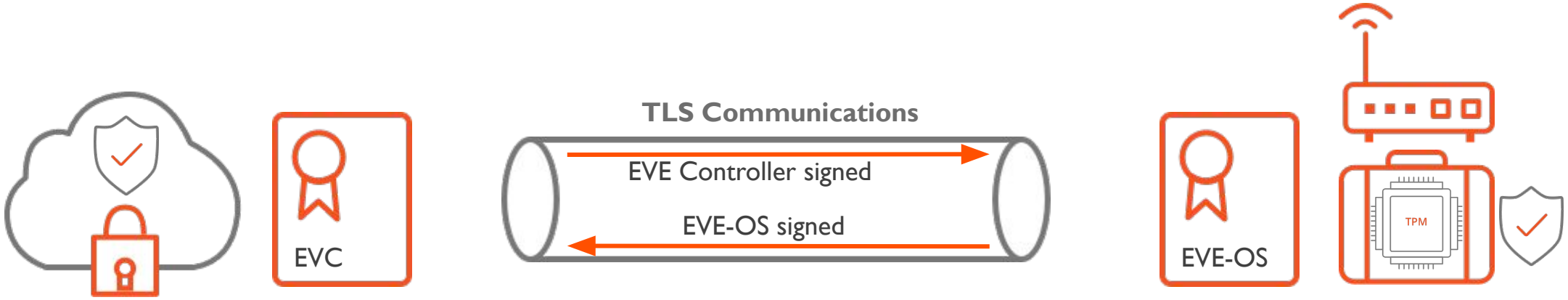


EVE-OS

RAM overhead: 500M
CPU overhead: 1 core

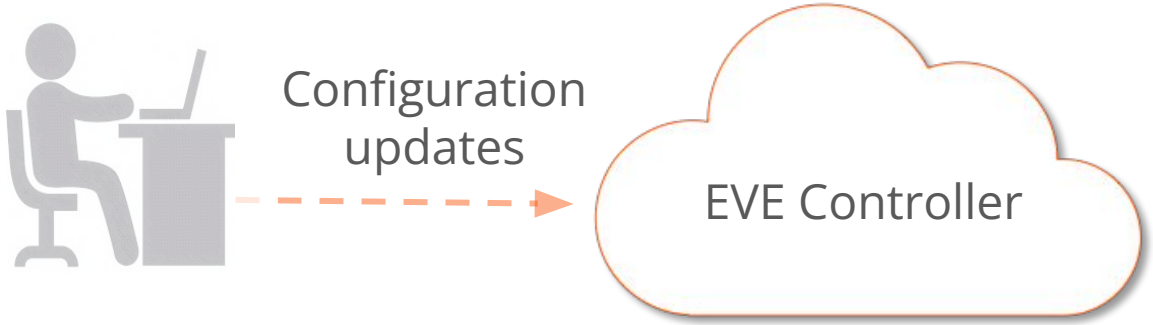
Disk overhead: 500M

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

Remotely Manage Any Edge Node



No field expertise required

Node calls "home" for configuration and updates

- Any type of silicon and device
- Automated on-boarding
- Autonomous operations

Any Silicon

intel NVIDIA ARM

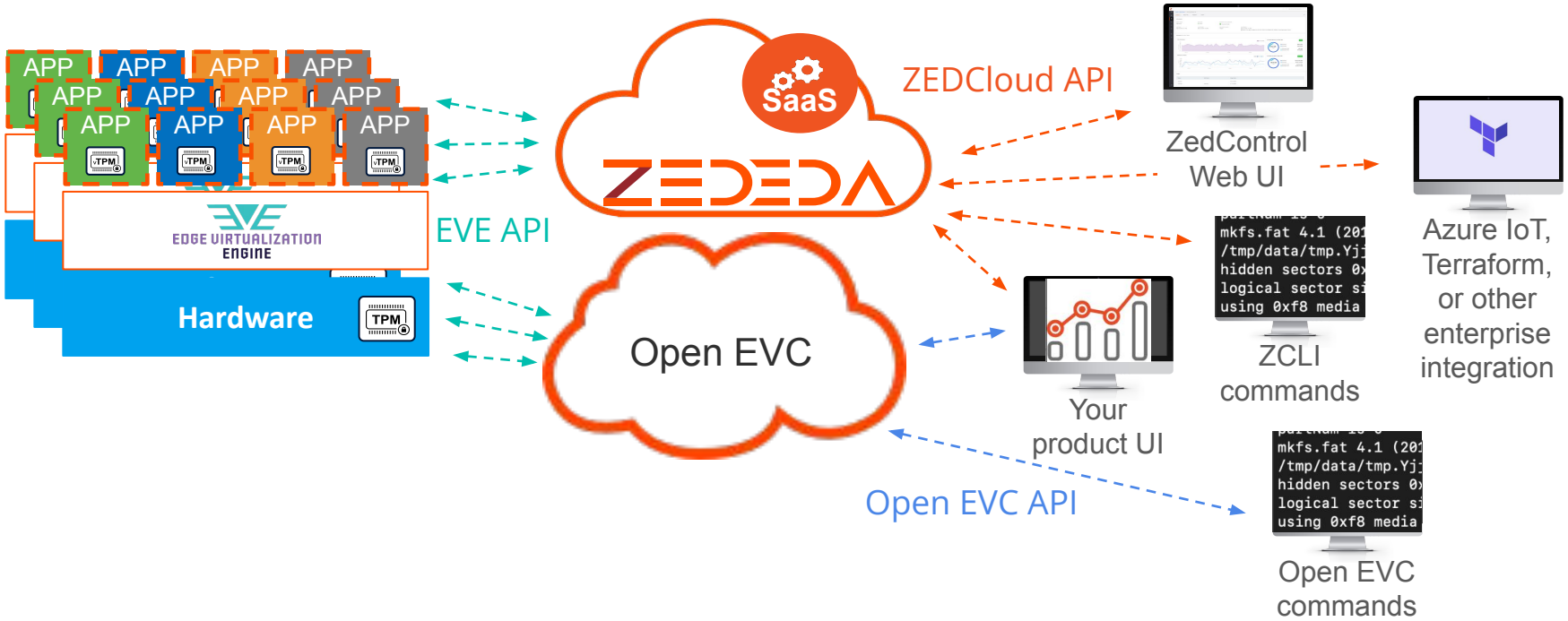
Any User Edge Compute Node

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

Publicly Documented APIs

EVE-OS
Secure API over TLS

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

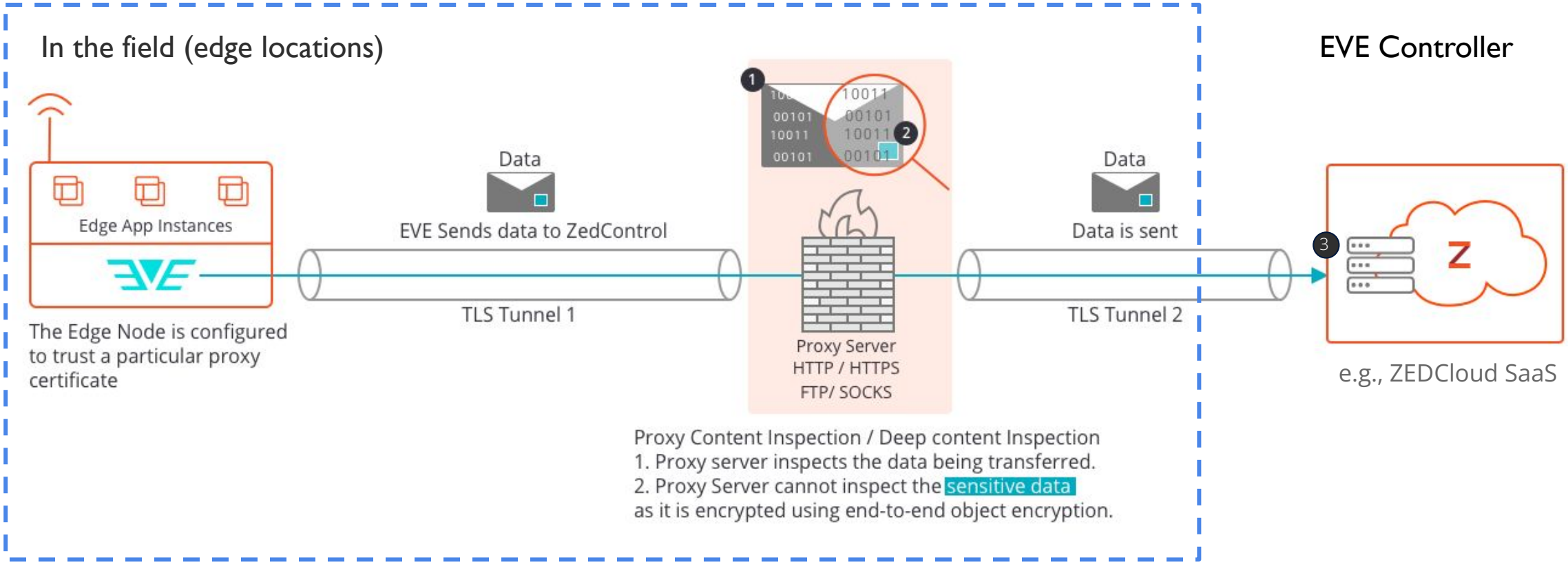


EVE-OS API
https://github.com/lf-edge/eve/tree/master/api

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

EVE API Security Works Through Firewalls, Proxies



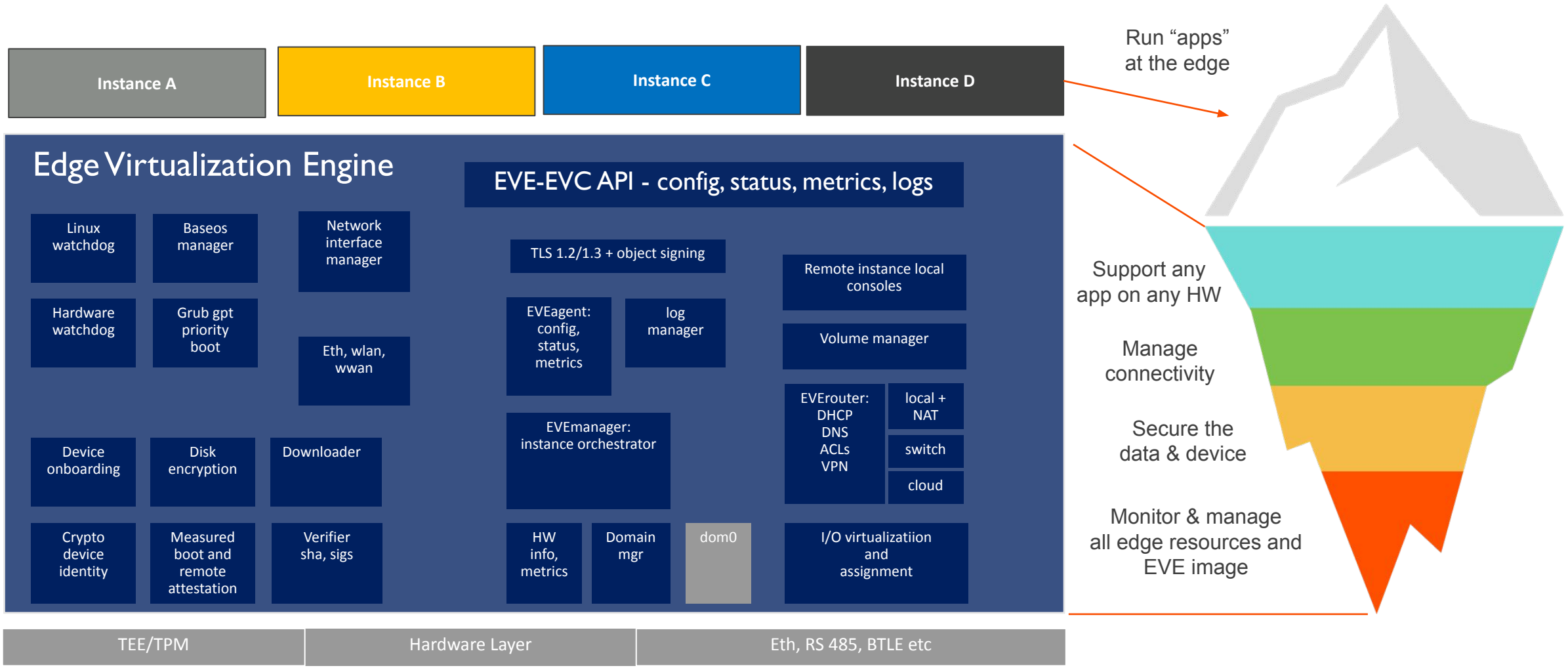
1. TLS to trusted parties (direct to controller and/or via proxy)
2. End-to-end signature over payload (proxy can not view nor modify)
3. Sensitive data encrypted end-to-end (also at rest)

Zero Trust

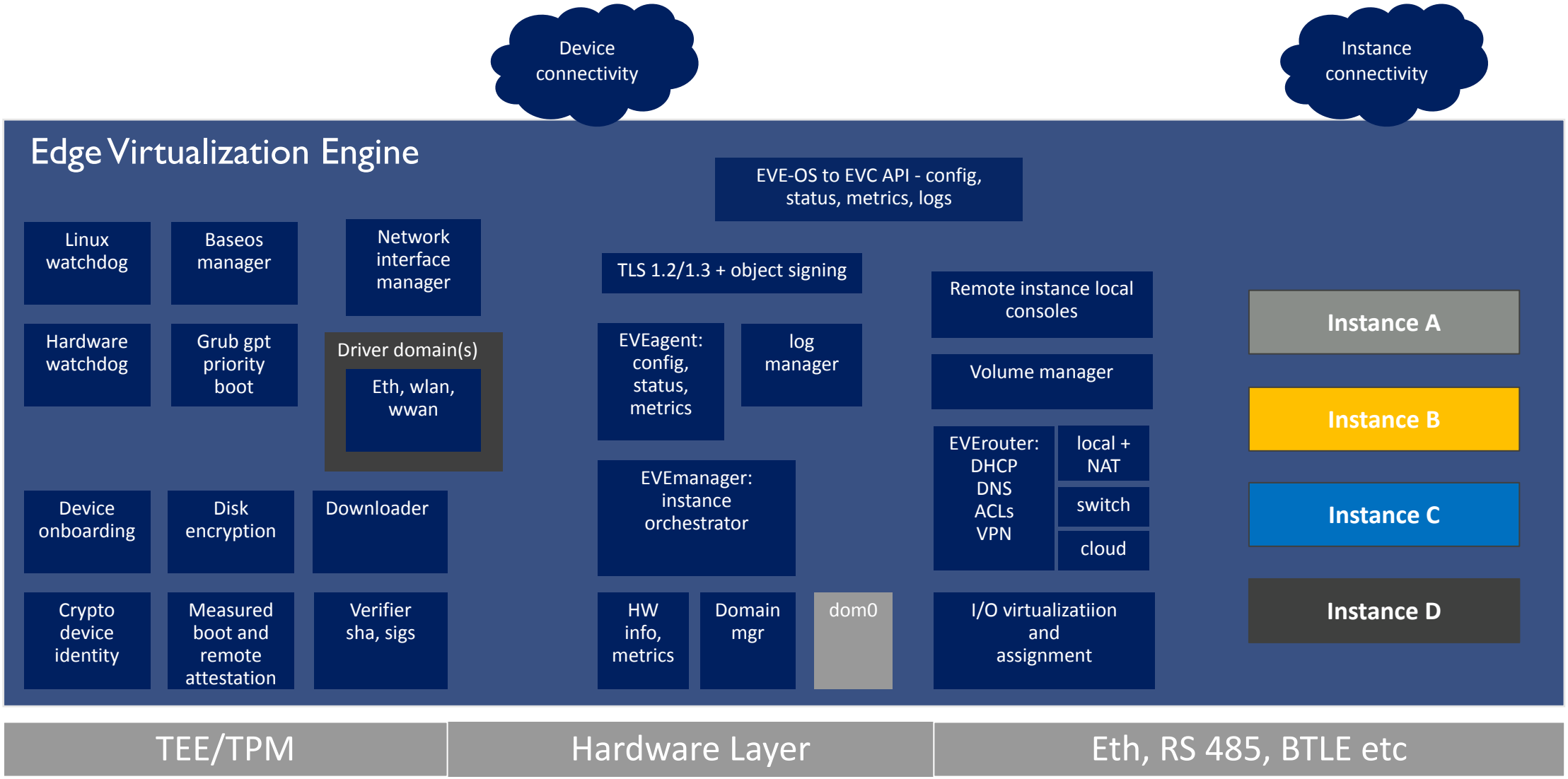
People, Process, and Technology

- 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

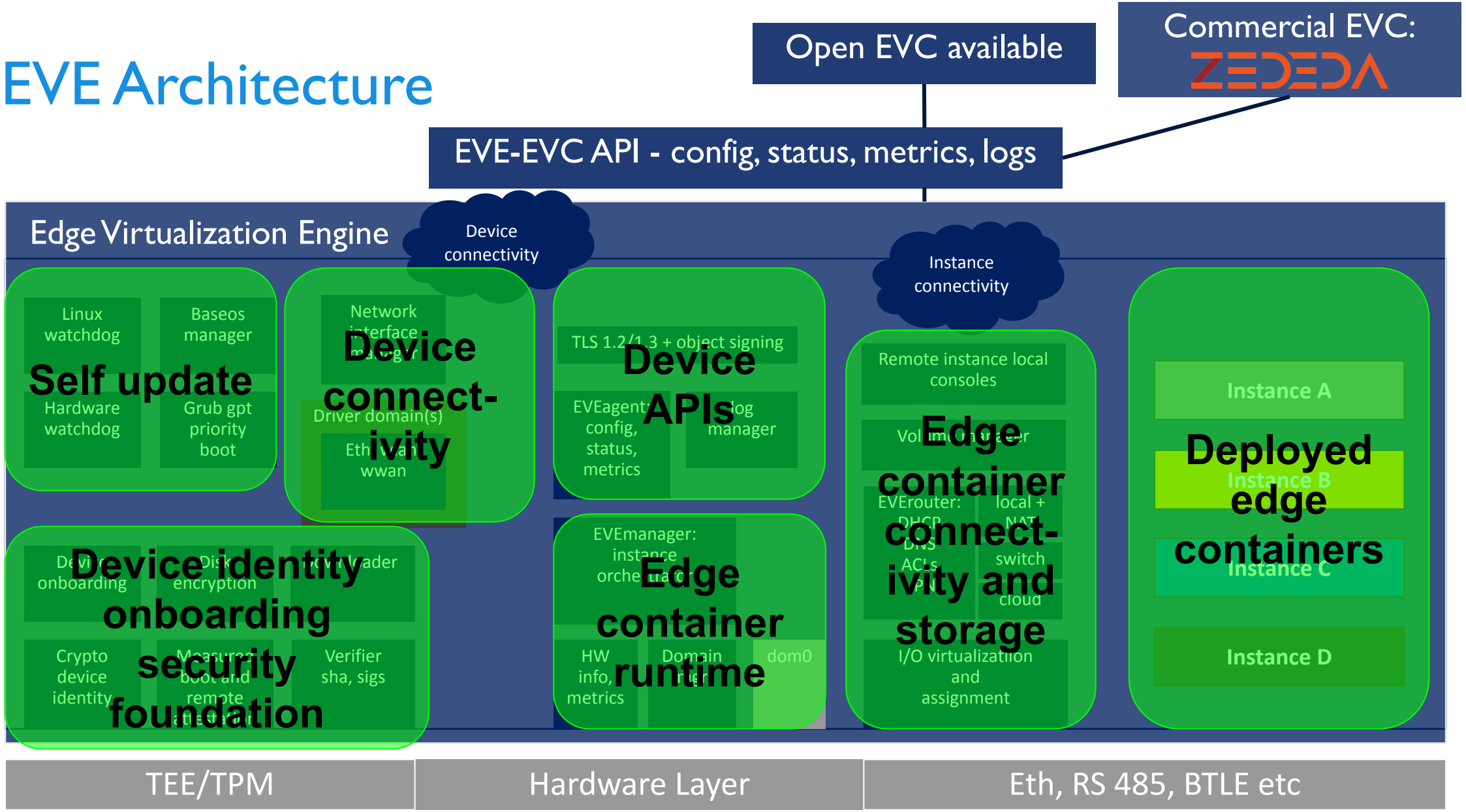
App Deployment: Tip of the Iceberg



EVE-OS Architecture



EVE Architecture



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

Key Takeaways

THE LINUX FOUNDATION

EVE Value: Key Takeaways

- Digital transformation at the edge brings unique requirements
  - Remote cloud-based administration for massive scale
    - Device security and full control over app orchestration
  - Support for disparate embedded hardware (any hardware)
  - Enablement of both legacy and cloud-native applications
  - Critical IT need: "lock down and own the bare metal"
- Evolution means handling old (VMs) and new (containers and clusters)
- Networking is harder than you think, especially with security
- Stay ahead of the competition by leveraging and engaging in the power of open source, open community, and open ecosystems

Ready to Transform Your Edge?

THE LINUX FOUNDATION