EVE Overview

A new paradigm to securely manage the industrial edge
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

IT/OT Admin & Operations Manager (Full-stack central mgmt)

DevOps & Data Scientists (Develop software and analytics models)

Field Technician (Deploys and services systems)

Azure APIs

EVE APIs

Legacy App eg. SCADA
Edge AI App

Azure IoT Edge Runtime

EVE-OS

intel
AMD
NVIDIA
XILINX
Commercial Ecosystem Opportunities

Project EVE is focused on managing app workloads at the industrial edge

See [https://www.lfedge.org/resources/publication-download/](https://www.lfedge.org/resources/publication-download/)
EVE Technology and Security Overview
EVE Architecture

EVE-OS
- EVE services
- containerd

RAM overhead: 500M
CPU overhead: 1 core
Disk overhead: 500M

Partition A
Partition B
EVE managed, workload-centric storage
User Edge Compute Hardware

Hypervisor (KVM [default] or Xen, ACRN)

Guest 1
K3OS

Guest 2
Windows 10
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

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

Node calls “home” for configuration and updates

No field expertise required

Any Silicon

Any User Edge Compute Node
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

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

---

**ZEDCloud API**
https://zedcontrol.zededa.net/api/v1/docs/
EVE API Security Works Through Firewalls, Proxies

In the field (edge locations):
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)

EVE Controller

The Edge Node is configured to trust a particular proxy certificate

EVE Sends data to ZedControl

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.
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

Edge Virtualization Engine

- EVE-EVC API - config, status, metrics, logs
- Remote instance local consoles
- Volume manager
- EVErouter: DHCP, DNS, ACLs, VPN
- local + NAT
- switch
- cloud
- I/O virtualization and assignment
- EVEmanager: instance orchestrator
- HW info, metrics
- Domain mgr
- dom0
- EVEagent: config, status, metrics
- log manager
- Eth, wlan, wwan
- Eth interface manager
- Network interface manager
- Grub gpt priority boot
- Disk encryption
- Downloader
- Device onboarding
- Crypto device identity
- TEE/TPM

Hardware Layer

- EVE-EVC API - config, status, metrics, logs
- Remote instance local consoles
- Volume manager
- EVErouter: DHCP, DNS, ACLs, VPN
- local + NAT
- switch
- cloud
- I/O virtualization and assignment
- EVEmanager: instance orchestrator
- HW info, metrics
- Domain mgr
- dom0
- EVEagent: config, status, metrics
- log manager
- Eth, wlan, wwan
- Eth interface manager
- Network interface manager
- Grub gpt priority boot
- Disk encryption
- Downloader
- Device onboarding
- Crypto device identity
- TEE/TPM

Support any app on any HW
Manage connectivity
Secure the data & device
Monitor & manage all edge resources and EVE image

Run “apps” at the edge

- EVErouter:
  - DHCP
  - DNS
  - ACLs
- EVEagent:
  - config,
  - status,
  - metrics
- Downloader
- EVEmanager:
  - instance orchestrator
- Verifier
  - sha, sigs
- HW info,
  - metrics
- Domain mgr
- dom0
- I/O virtualization
  - and assignment
- EVErouter:
  - DHCP
  - DNS
  - ACLs
  - VPN
- local + NAT
- switch
- cloud
- I/O virtualization
  - and assignment
- EVEmanager:
  - instance orchestrator
- HW info,
  - metrics
- Domain mgr
- dom0
- EVEagent:
  - config,
  - status,
  - metrics
- log manager
- Eth, wlan, wwan
- Eth interface manager
- Network interface manager
- Grub gpt priority boot
- Disk encryption
- Downloader
- Device onboarding
- Crypto device identity
- TEE/TPM

THE LINUX FOUNDATION
EVE-OS Architecture

Edge Virtualization Engine

- EVEagent: config, status, metrics
- EVEmanager: instance orchestrator
- DNS
- DHCP
- ACEs
- VPN
- Downloader
- Inetface manager
- HW info, metrics
- Domain mgr
- dom0

Remote instance local consoles
Volume manager
EVEmanager: instance orchestrator
I/O virtualization and assignment

Instance A
Instance B
Instance C
Instance D

Hardware Layer
- Eth, RS 485, BTLE etc

TEE/TPM

THE LINUX FOUNDATION
EVE Architecture

Hardware Layer

EVE-EVC API - config, status, metrics, logs

Edge Virtualization Engine

Self update
- Linux watchdog
- Baseos manager
- TEE/TPM

Device connectivity
- Network interface
- Ethernet
- WWAN

Device APIs
- EVEagent: config, status, metrics
- EVEmanager: instance orchestrator
- EVErouter: DHCP, DNS, ACLs, VPN

Device identity onboarding
- Device onboarding
- Crypto device identity
- Driver domain(s)

Secure boot and remote trust
- Measured boot and remote
- Verifier

Edge container runtime
- EVEmanager: instance orchestration
- EVEagent: HW info, Domain info, dom0

Edge container connectivity and storage
- I/O virtualization and assignment
- Volume manager

Deployed edge containers
- Instance A
- Instance B
- Instance C
- Instance D

Instance connectivity
- Remote instance local consoles
- Volume manager

Eth, RS 485, BTLE etc

Open EVC available

Commercial EVC: ZEDEDA
Embracing LF Edge Open Source Collaboration
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
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?