



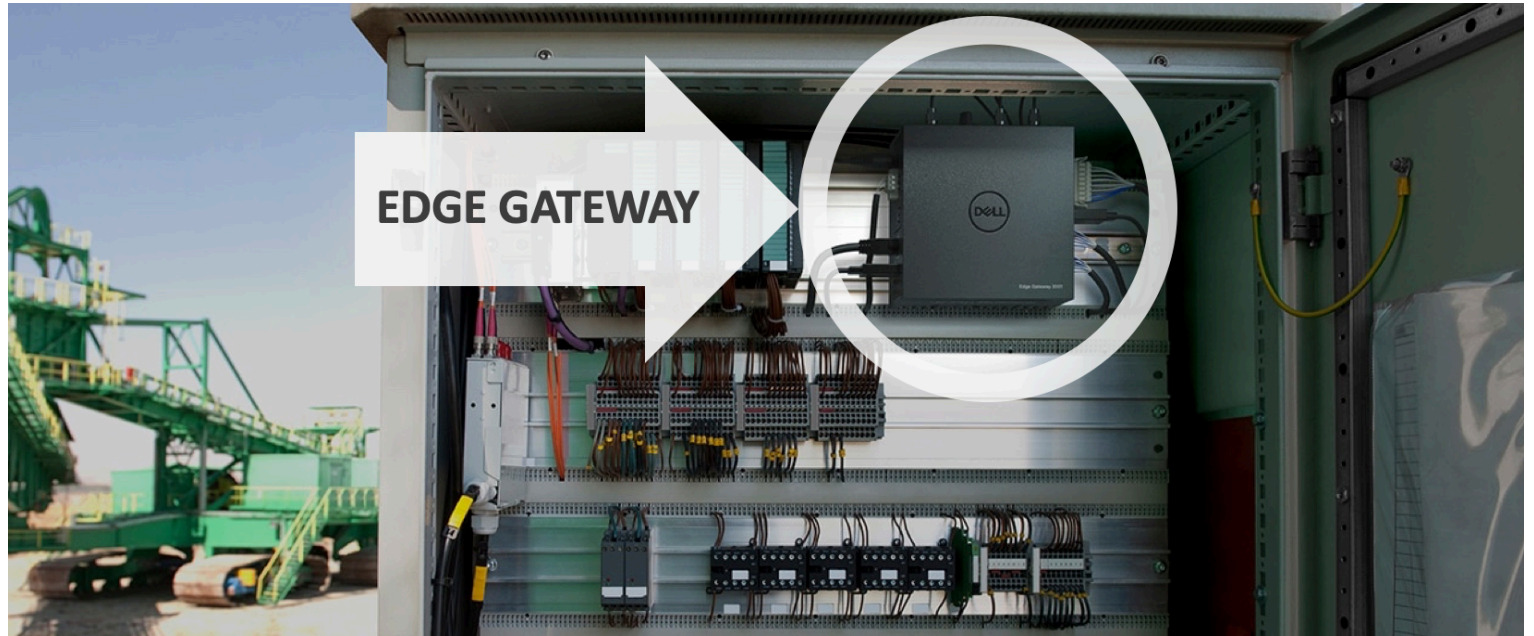
Linux Foundation's Project EVE: A Cloud-Native Edge Computing Platform

Roman Shaposhnik AKA @rhatr
Founder, VP of Product & Strategy @ZEDEDA Inc.
Board member @Apache Software Foundation & Linux Foundation



Edge Computing is... “cloud-native” IoT

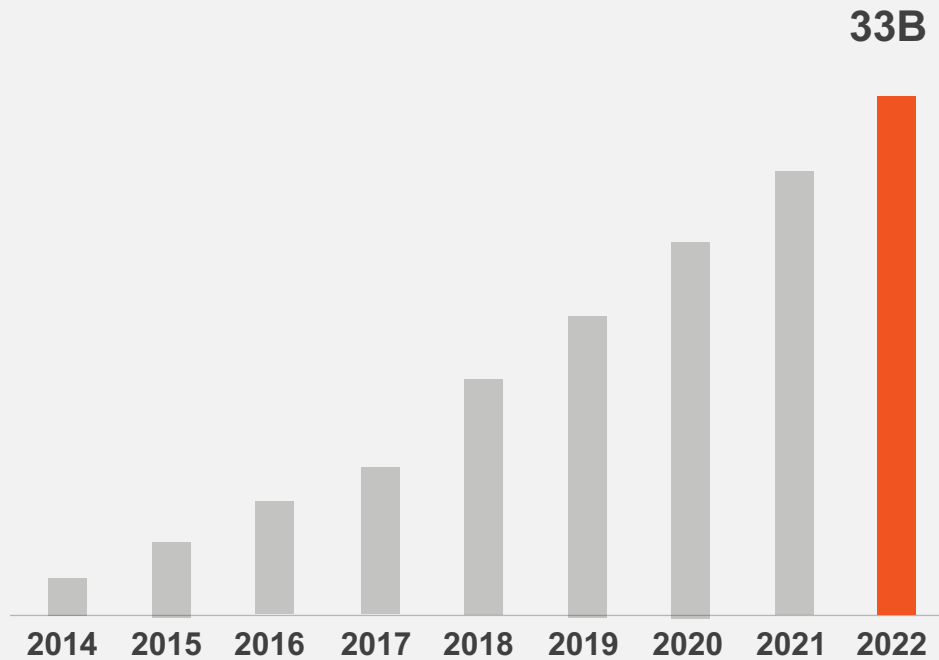




Edge ain't your gramp's
Embedded and/or IoT

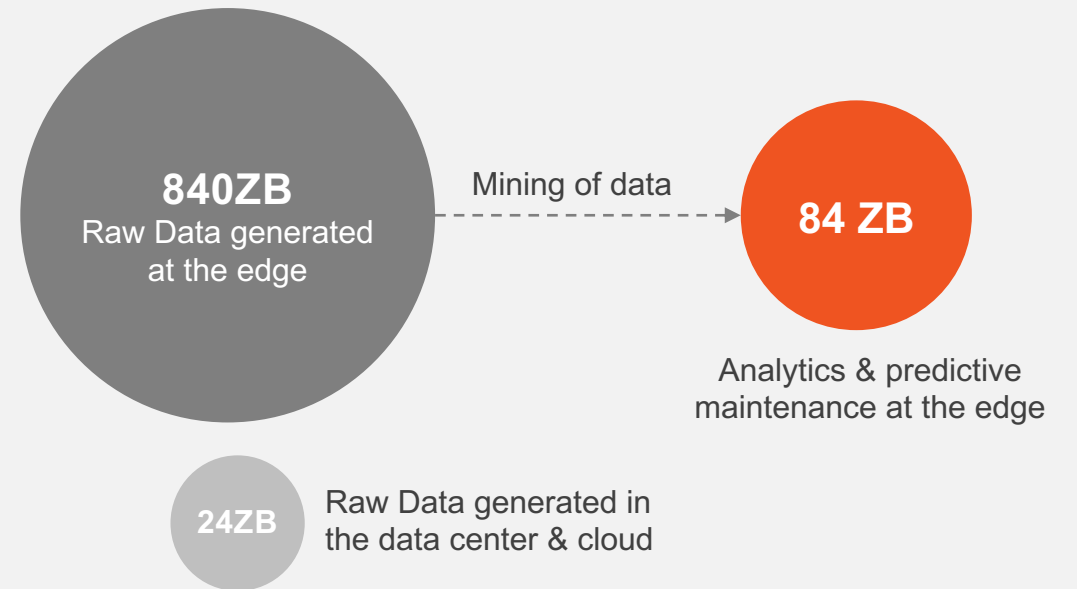
CONNECTED DEVICE

2022 (33 Billion)



DATA AT THE EDGE

2022 (840 ZB)



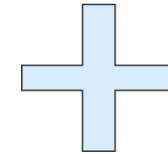
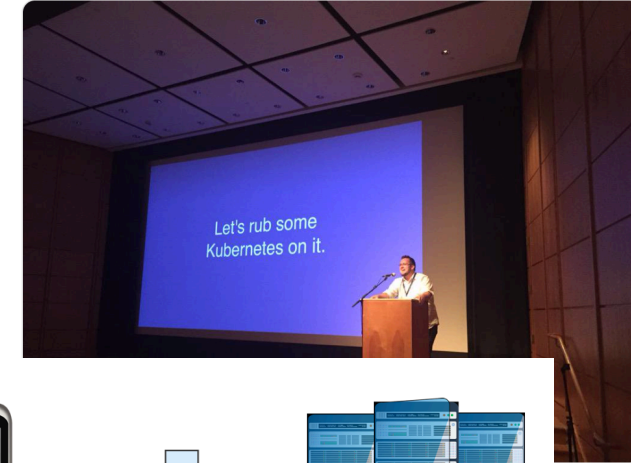
**Data must be pre-processed at the edge
due to bandwidth, latency and cost**

Are you ready to live on the Edge?

- **Edge is one final “Cloud” we’re building**
 - Remember: everything has to be “Cloud Native”
 - Edge DevOps anyone?
- **So... Edge is just another cloud?**
 - Yes and no. It is more like mobile + DC
- **Can we rub some Kubernetes on it?**
 - APIs – most likely
 - Implementations -- absolutely not!
- **Economics of the Edge**
 - Super-heterogeneous ownership
 - Huge business opportunity seen by VCs
 - AI (especially autonomous) is a “killer app”



After watching Kelsey Hightower videos on YouTube all you want to do is go rub some Kubernetes on it. [#AutomaCon](#)



RANCHER LABS See what else Rancher is up to

K8S Docs GitHub

★ Star 7,498 ▼ Fork 442

Lightweight Kubernetes

Easy to install. A binary of less than **40 MB**. Only **512 MB of RAM** required to run.

Watch our recorded k3s demo on-demand, and get a copy of our slides here

[Watch Demo](#)

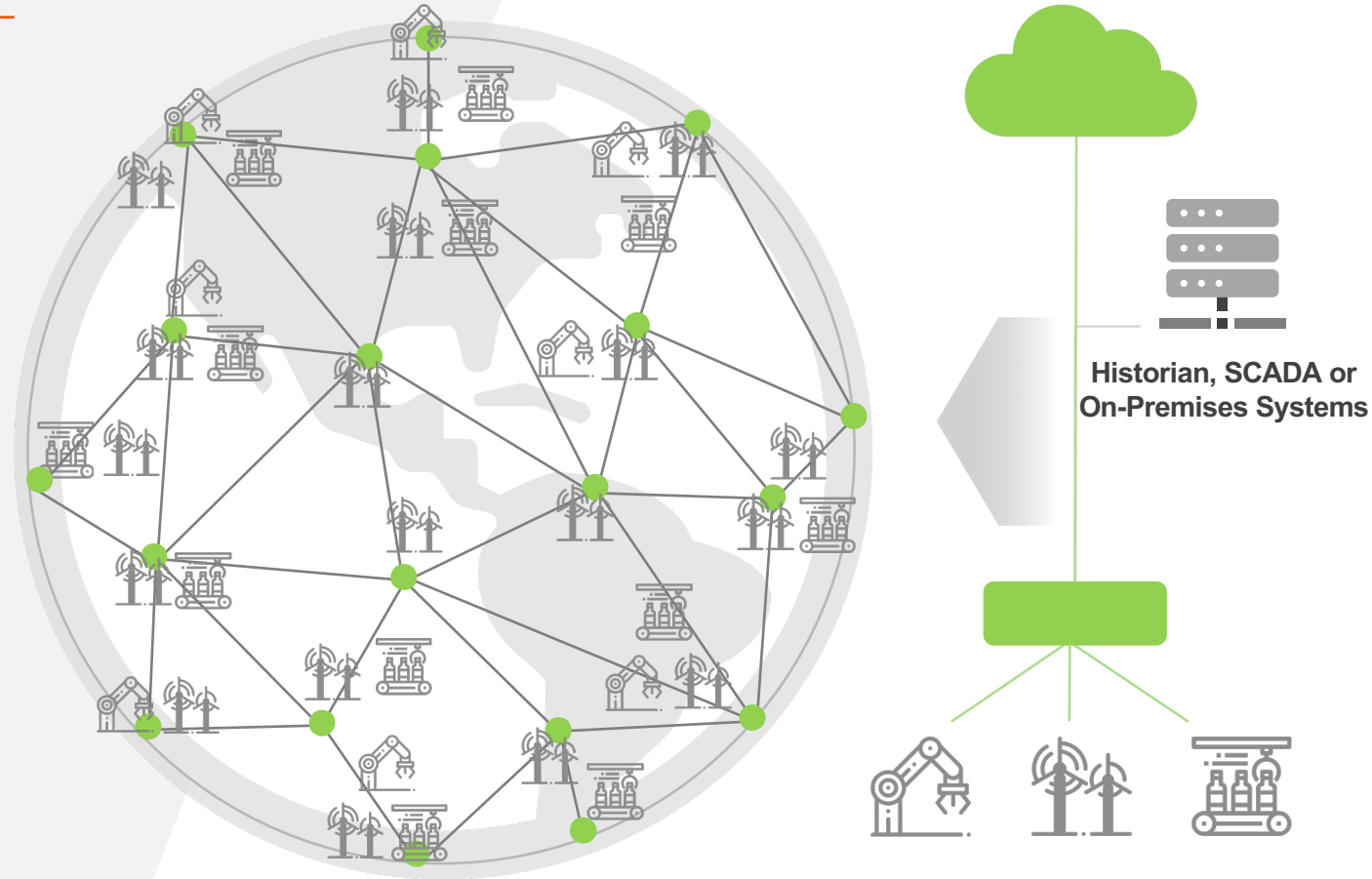
This shouldn't take long...

```
curl -sL https://get.k3s.io | sh -
# Check for Ready node, takes maybe 30 seconds
k3s kubectl get node
```

For detailed installation, [refer to the docs](#)

Challenges at the Edge

- **Diversity of hardware and apps**
 - Infrastructure management
 - Orchestration of apps
- **Scale and automation**
 - Geographically disperse
 - Deployment and maintenance
- **Security – increased threat vector**
 - No perimeter network security
 - No perimeter physical security
- **Vendor lock-in is impossible**
 - Distributed Ownership...
 - ...hence it *has* to be open





Guarding Against Physical Attacks: The Xbox One Story — Tony Chen, Microsoft



Watch later



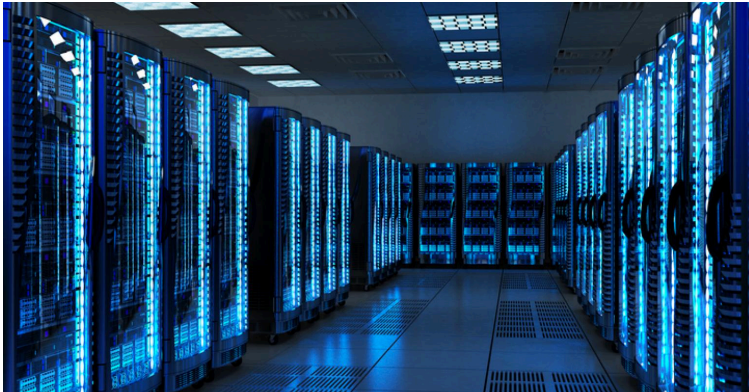
Share



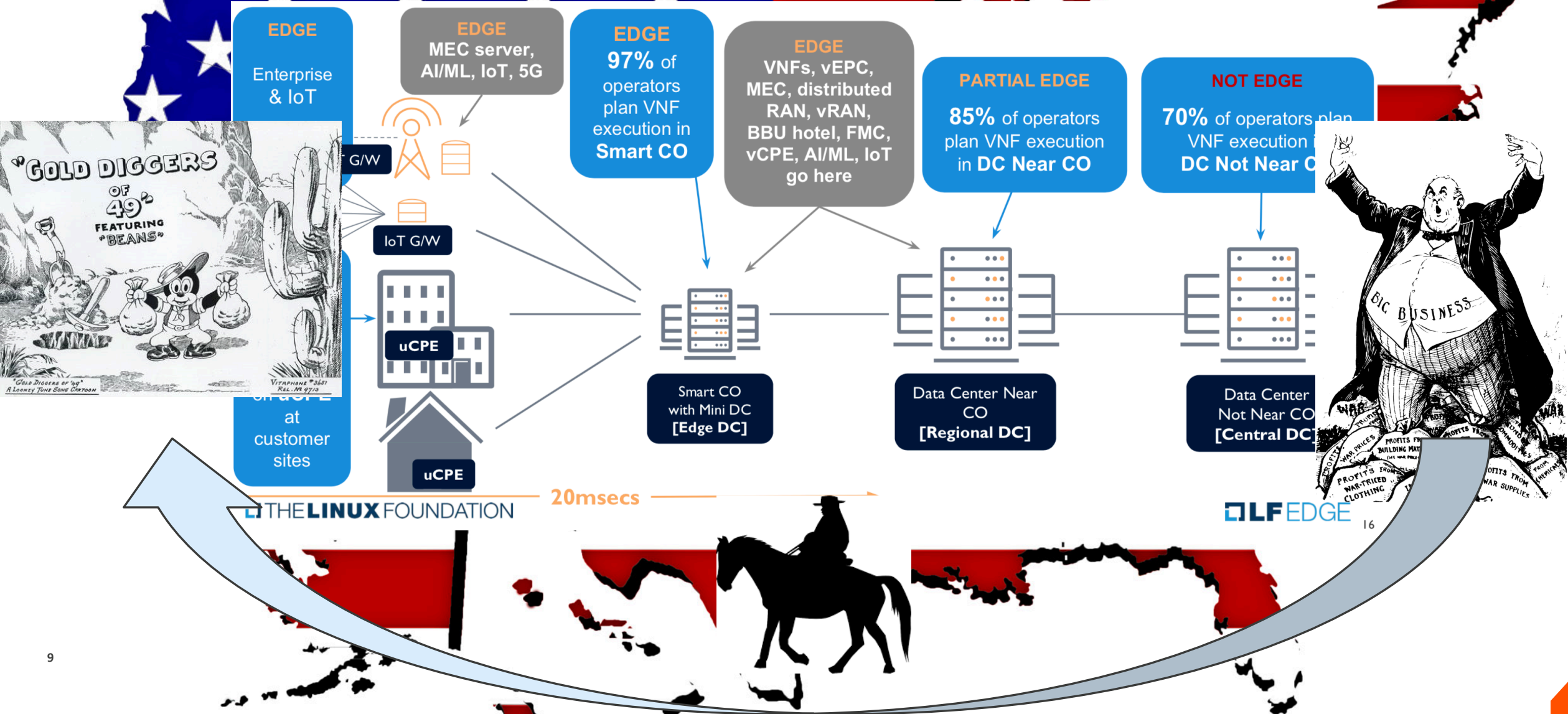
Guarding Against Physical Attacks: The Xbox One Story

Tony Chen
Microsoft
Platform Security Summit 2019
10/1/2019

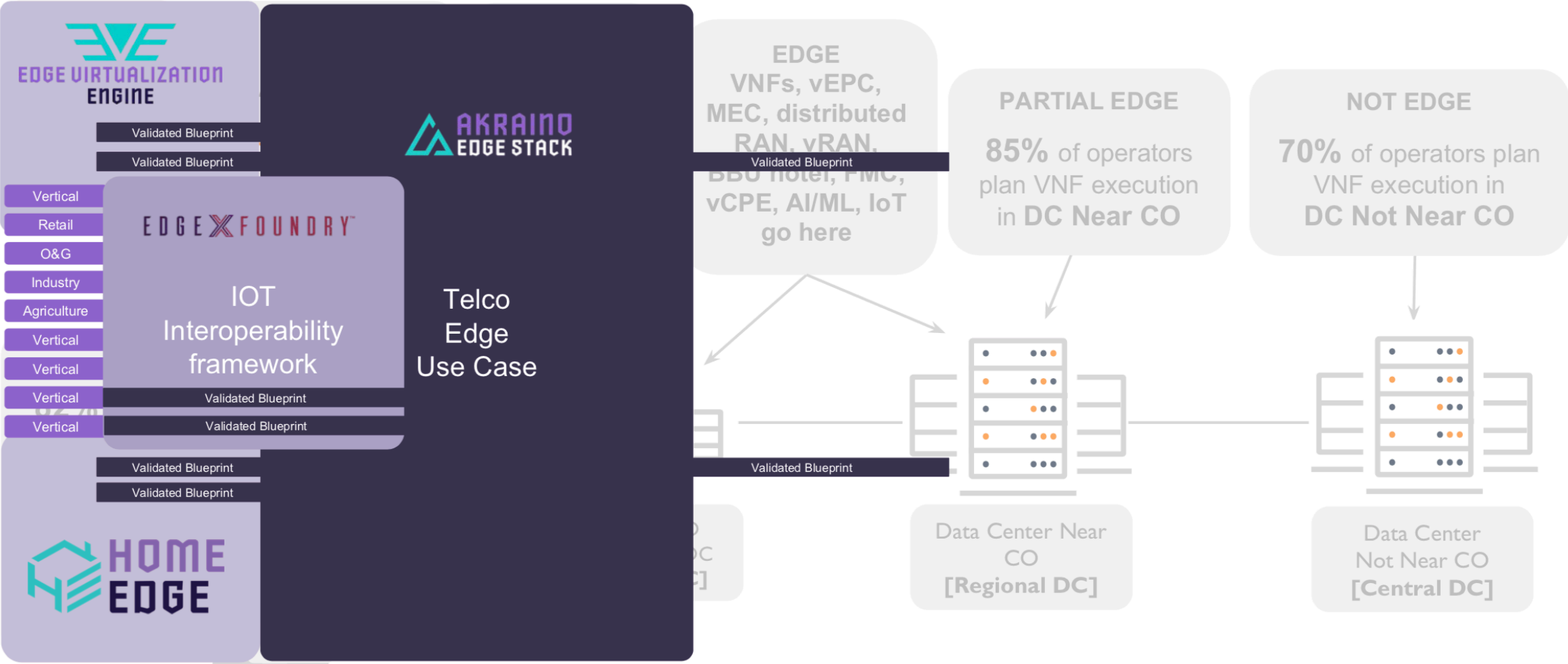
From the people who brought you CNCF



Go West, young man, go Edge!



LF Edge Projects



LF Edge Projects

Drivers

- › Complementary and aligned vision on multiple LF projects
- › Fuels faster adoption and deployment
- › Edge market is fragmented and creating a larger entity provides leadership

Projects





EDGE VIRTUALIZATION
ENGINE

Edge Requirements



ZERO TOUCH



FREEDOM OF ANY
APP | HARDWARE | CLOUD



IoT SCALE

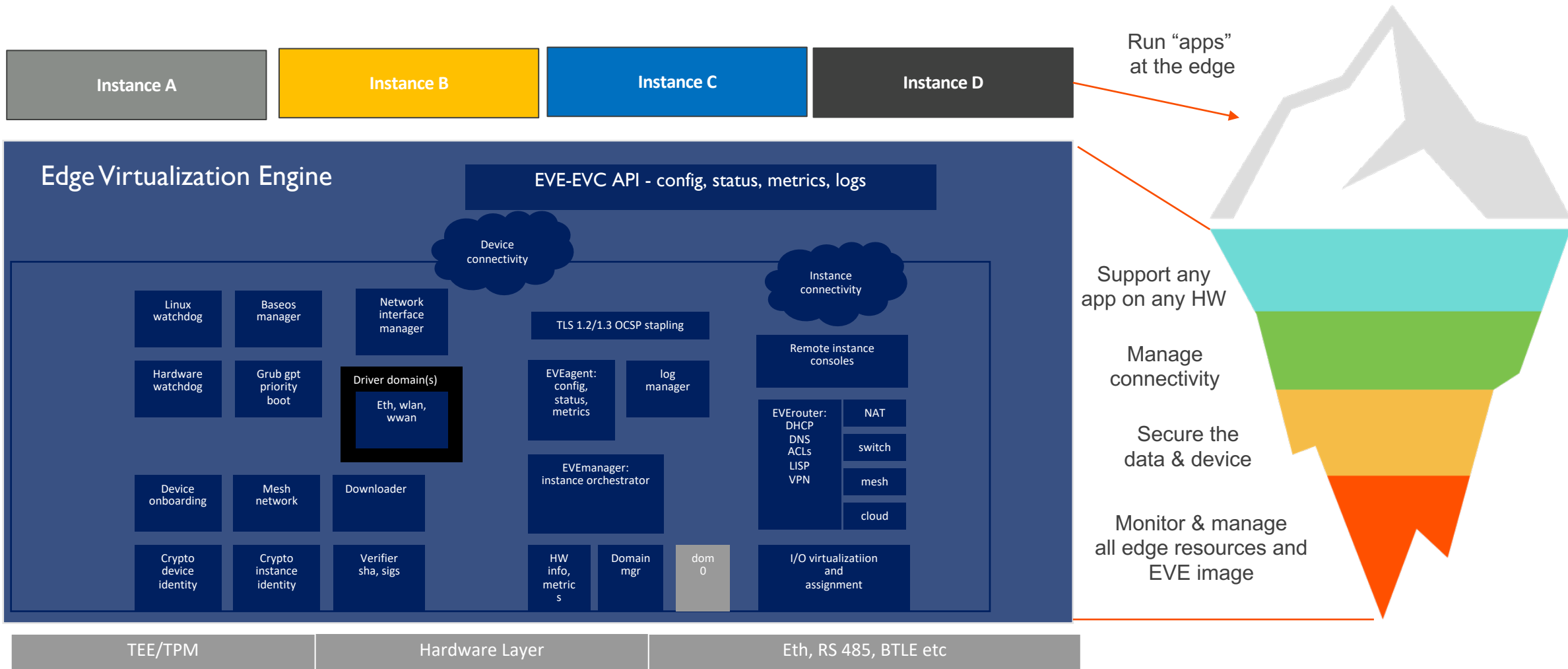


CLOUD NATIVE

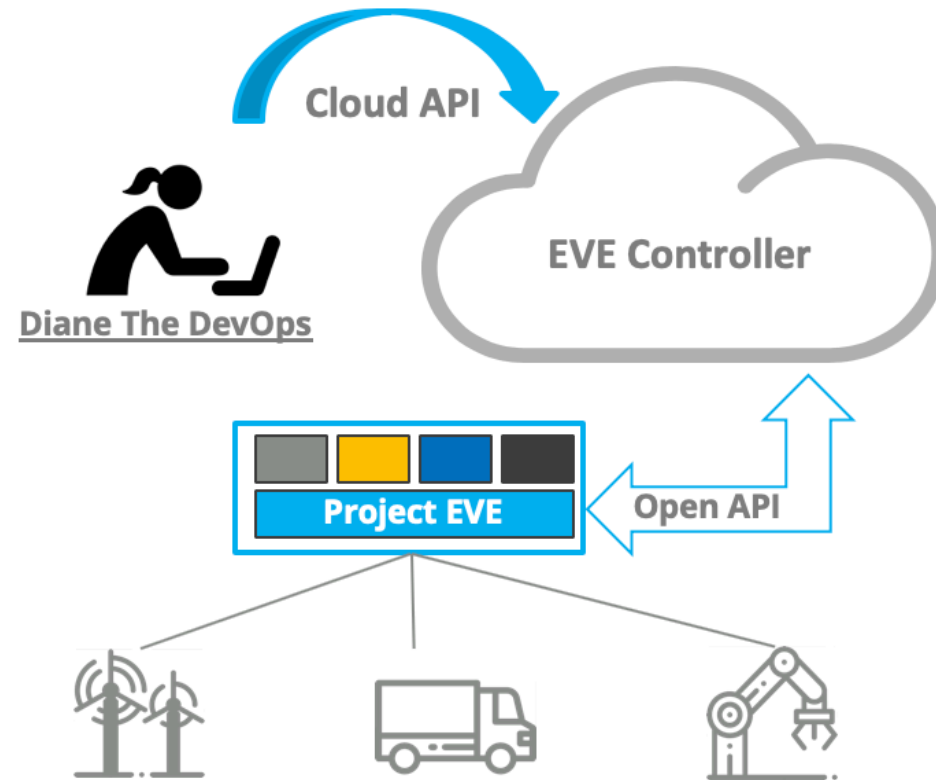


ZERO TRUST

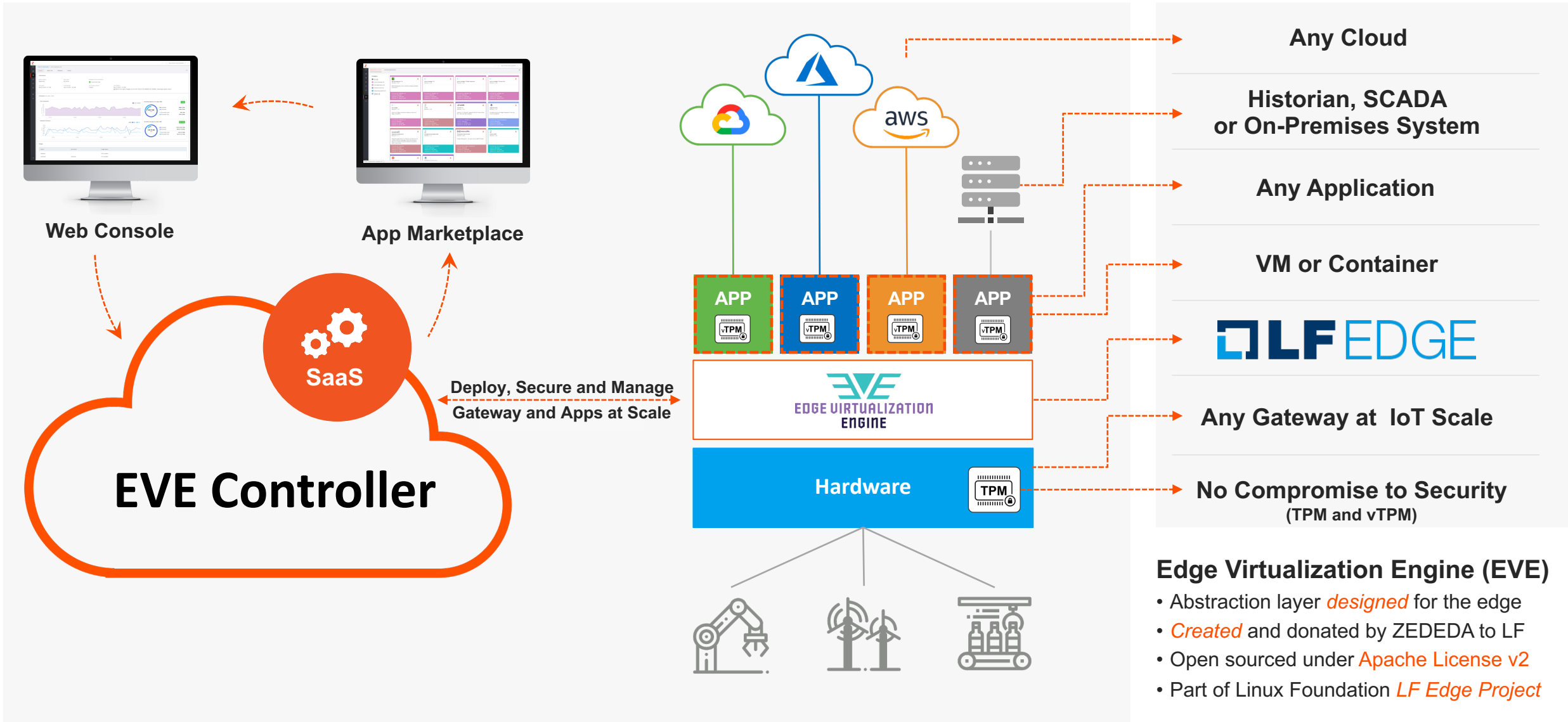
App deployment is but the tip of the iceberg



A complete Edge "Cloudification" proposal

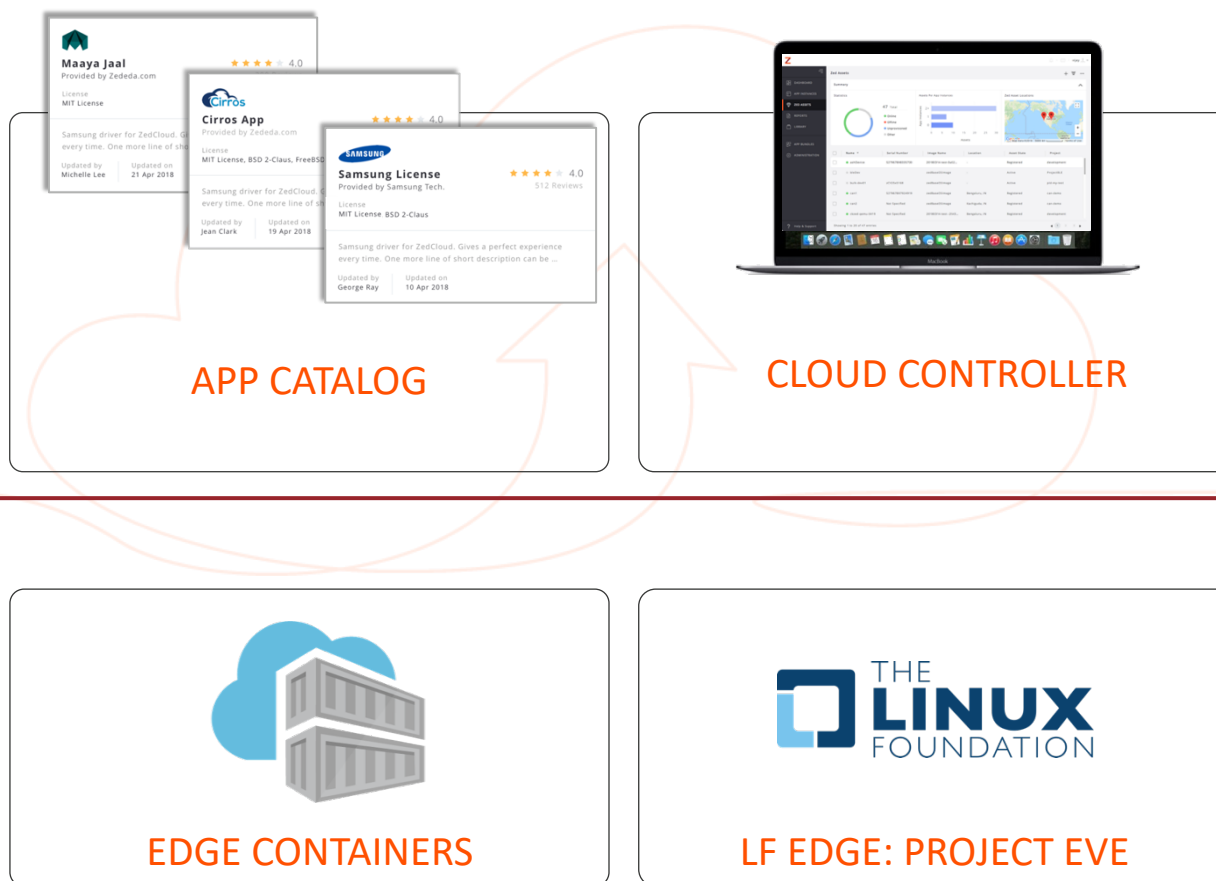


Edge Infrastructure Challenges Solved with **Edge Virtualization**

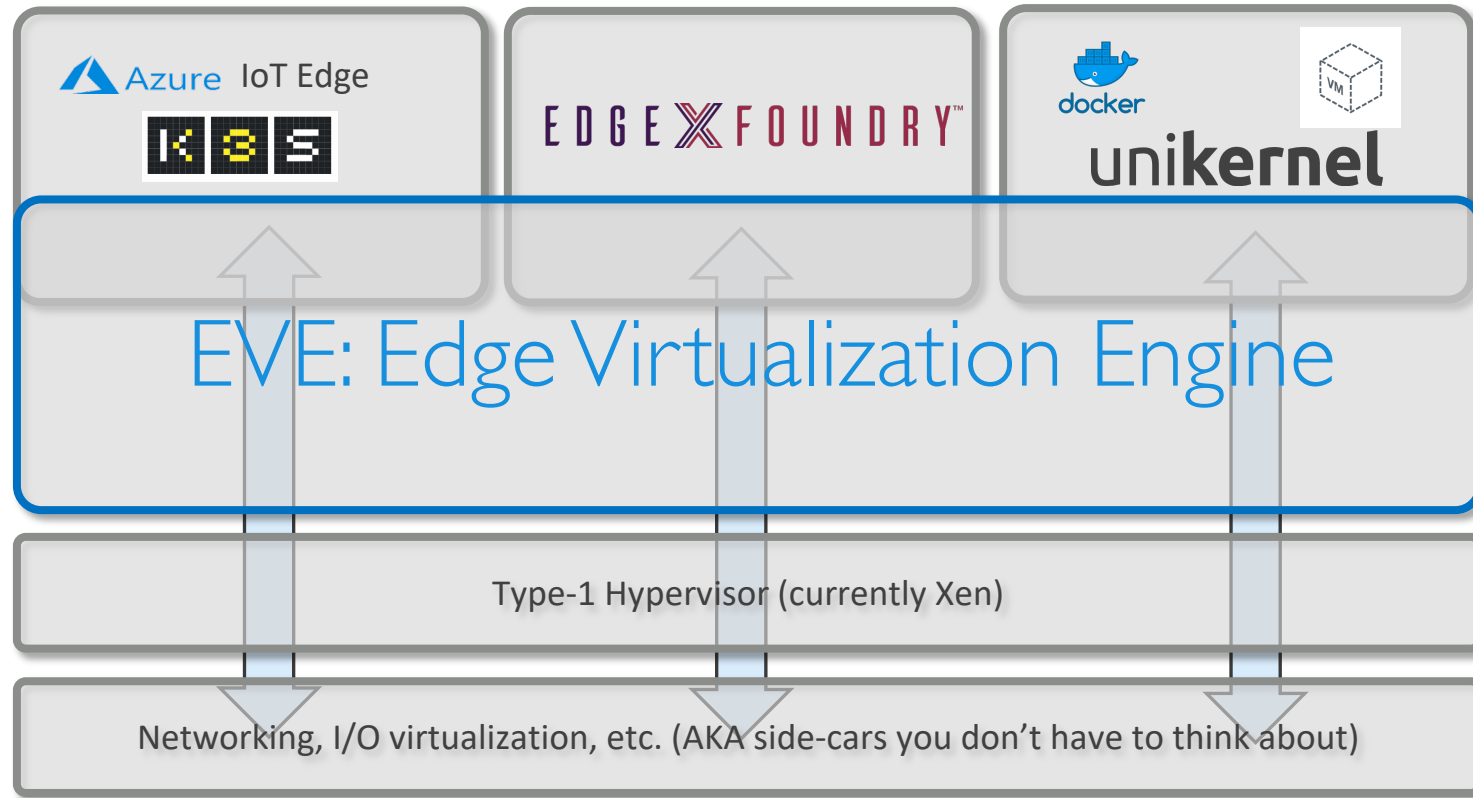


4 pillars of complete Edge “Cloudification”

ZEDEDA
Edge Virtualization
Software





EVE's architecture



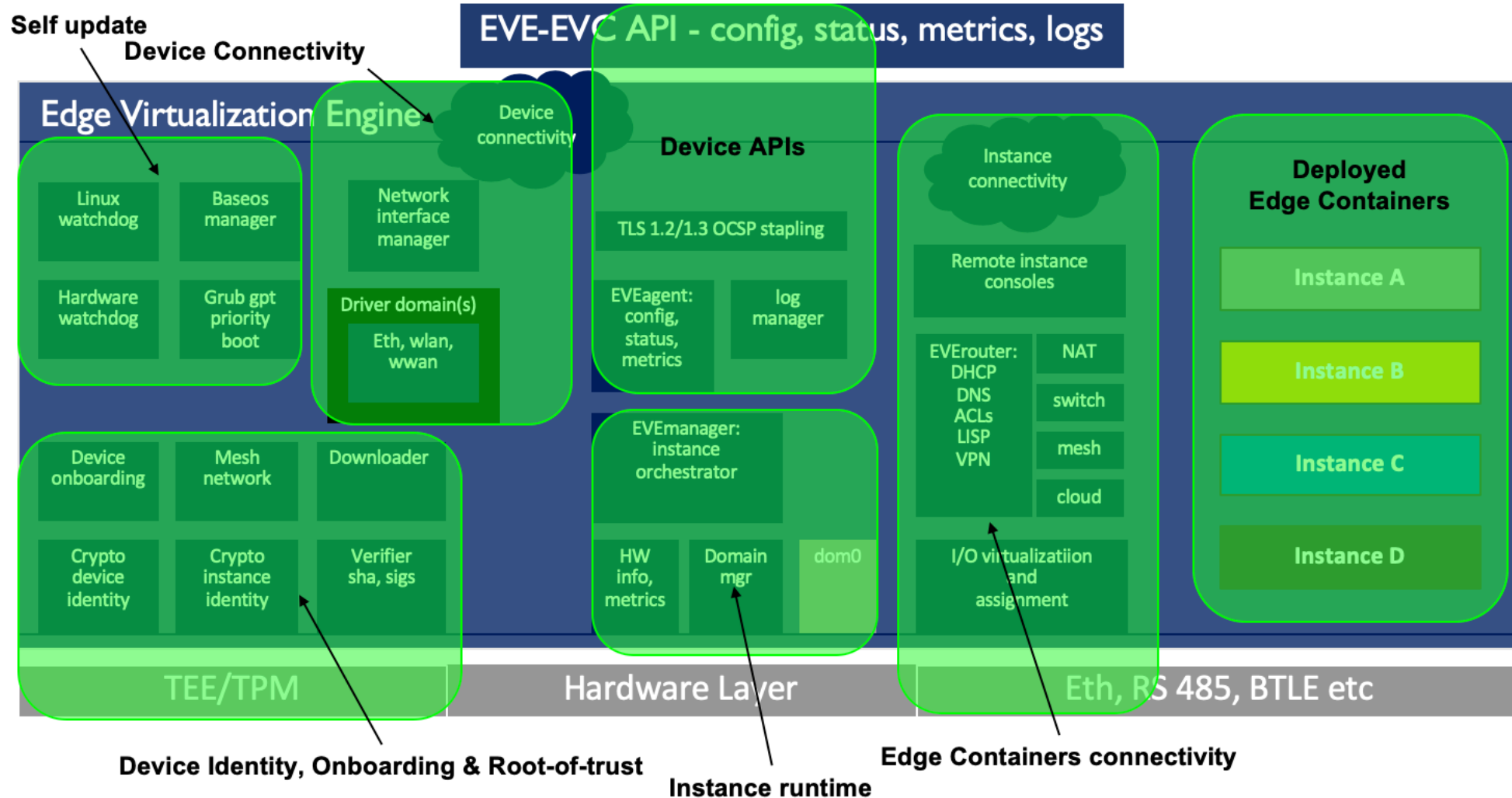
EVE is going to be for the Edge...

....what Android is for Mobile

		
App and OS Sandboxing	Hardware Assisted Virtualization	JVM
App Bundling	Edge Container (ECOs)	APK
App Deployment	Cloud Orchestrated & Pre-loaded	
H/W support	Intel, ARM (+RISC V)	Intel, ARM, MIPS

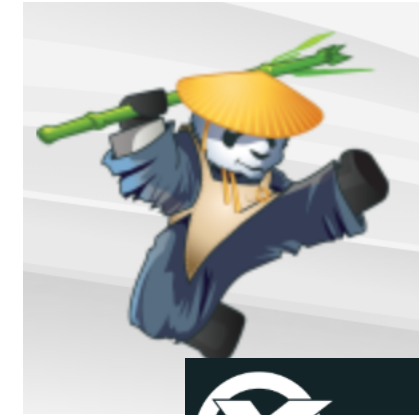
EVE: a post-, post-modern OS

EVE deep dive... could be pretty deep



LF Edge's EVE deep dive

- Inspired by QubesOS, ChromeOS, SmartOS
- Based on Type-1 Hypervisors (Xen or ACRN)
 - No KVM allowed!
 - Containers are fine, but everyone gets a lightweight VM
- DomU is...
 - linuxkit
 - Alpine Linux
- But wait, there's more:
 - We are driving towards unikernel architecture
 - Everything is Golang based
 - Moving to AtmanOS (GOOS=xen go build ...)
- Introducing: Edge Containers



ĀtmanOS



Edge Containers

- **A true extension to the OCI specification**
 - Image specification (not much of a change)
 - ~~Runtime specification~~
 - Registry Support (via OCI Artifacts Initiative)
- **Related initiatives**
 - Kata Containers, Singularity Containers, etc.
 - Weave.works's Project Ignite (Firecracker MicroVMs)
 - Rancher's K3S + K3OS
- **Top 3 goals:**
 - Filesystem-level composition (aka OCI layers)
 - Block-level composition (VMs and Unikernels)
 - Hardware mapping
- **Registry as a "nexus of Liquid Software"**



K3S



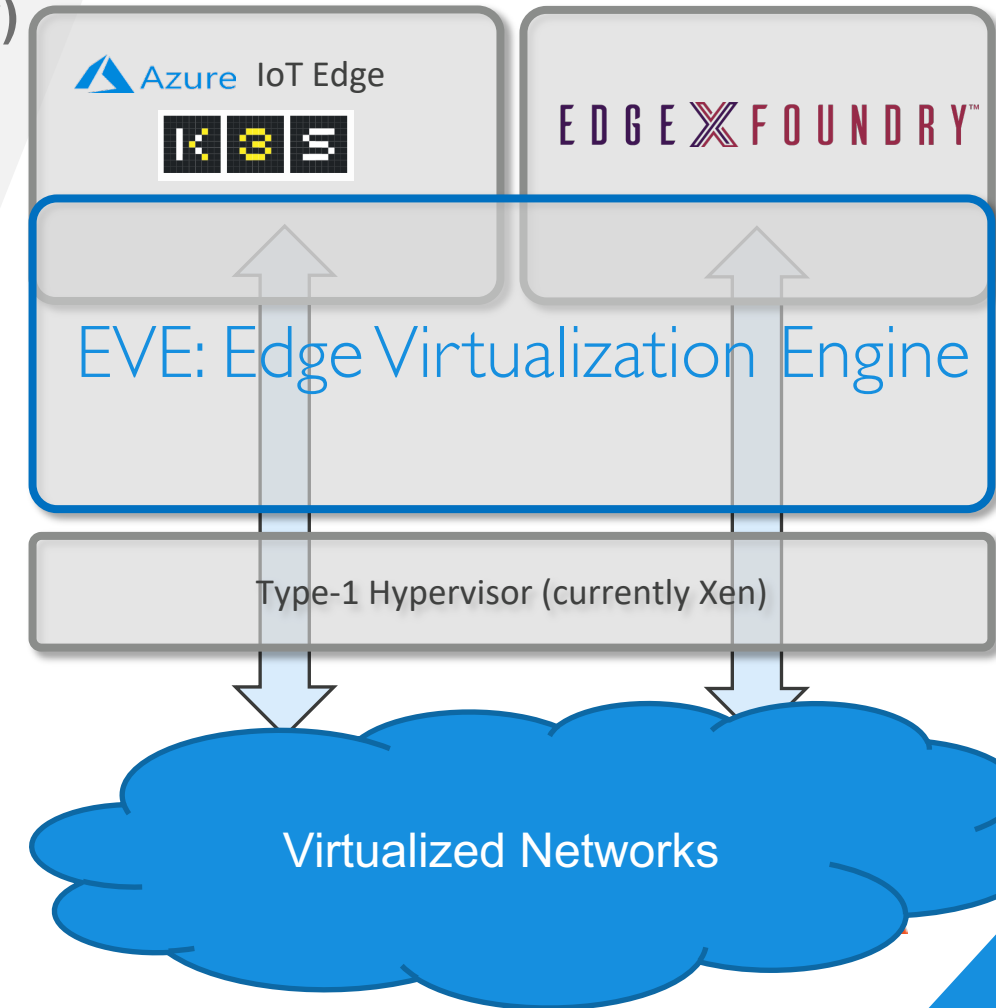
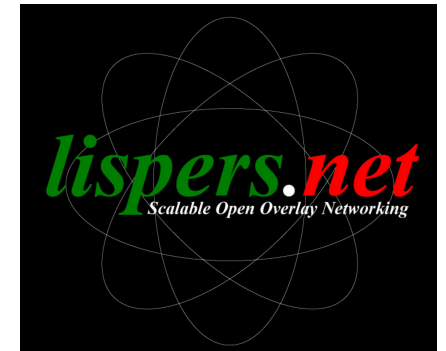
K3OS



Firecracker

EVE's networking is intent based

- Directly assigned hardware (Edge Container capability)
- Switch Network
 - A simple, virtualized L2 network (Ethernet++)
- Local Network
 - A traditional, L3 (IP++), NATed network
- Cloud Network
 - "Please connect me to this AWS VPC"
- Mesh Network
 - Based on LISP RFC 6830
 - Gives you a flat IP6 overlay with...
 - ...crypto-identity based routing
 - ...service mesh (regardless of NATs, etc.)

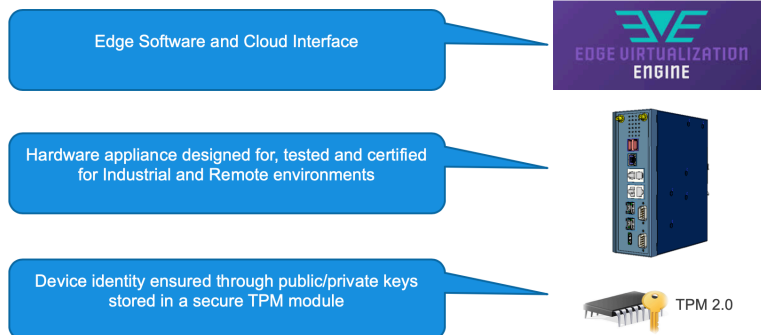


EVE's trust model – Zero Trust

- Trusted systems don't exist, trustworthy ones may
- Root-of-trust
 - Always derived from a hardware element (TPM, TEE, etc.)
 - Hardwired root CA cert for Controller Trust
- Measured boot with EVE Controller fencing
- Crypto identity for all elements in the system
- No ssh access, no usernames/passwords
- Defense-in-depth (kudos to Qubes OS)
 - Hypervisor-enforced isolation
 - Stub domains for drivers
 - Microservices running as Unikernels

LEC-6041B-ZE1 (Lanner Security Engine)

Lanner

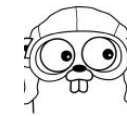
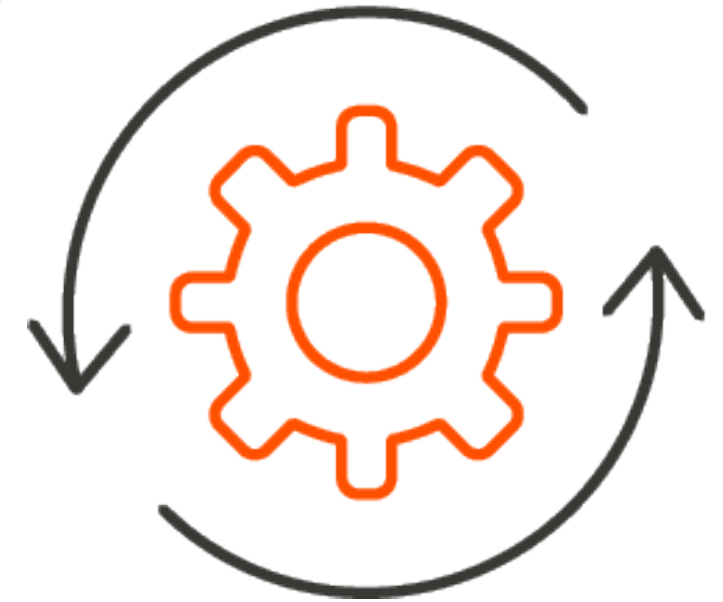


The operating systems

Code you know about	Ring 3 (User)	X86 CPU you know about
	Ring 0 (Linux)	
Code you don't know about	Ring -1 (Xen etc.)	
	Ring -2 kernel and ½ kernel Control all CPU resources. Invisible to Ring -1, 0, 3	
Code you don't know about	SMM ½ kernel. Traps to 8086 16-bit mode.	X86 CPU(s) you don't know about
	UEFI kernel running in 64-bit paged mode.	
Code you don't know about	Ring -3 kernels	
	Management Engine, ISH, IE. Higher privilege than Ring -2. Can turn on node and reimage disks invisibly. Minix 3.	

EVE's software update model

- **Prevent bricking by**
 - Applications are easy: just redeploy
 - EVE itself: dual partitioning + multiple levels of failover
- **Avoid the need for physical contact with Edge Nodes**
- **Manage everything starting from Firmware**
 - Good news: we are based on UEFI...
 - ...which also happens to be bad news
 - Coreboot is really exciting
 - Don't deploy things you don't need (ILOs, BMCs)



u-root/u-root

oreboot README



Hardware-protected vTPM 2.0

Current Landscape

Multiple vTPMs published or under development, but few vTPMs are protected with hardware mechanisms

No public vTPM addresses the TPM 2.0 requirements of shielded functions:

- vTPM contents can easily be influenced

QEMU Virtual TPM:

- Instances run as user space processes
- Separation provided by OS kernel

Proposed Approach

Based on TPM 2.0 spec and reference code (Microsoft)

Provide a BSD-licensed vTPM implementation that isolates each vTPM instance on a platform, provides the complete TPM 2.0 interface, and can be used by standard OS drivers for TPM 2.0

Strong Isolation Properties:

- Isolate runtime for the Protected Capabilities and the Shielded Location for the Protected Objects
- Platform Security: leverage SGX, memory encryption and other hardware-based separation technologies

Hardware-protected vTPM 2.0

Use Cases:

- Cryptographic key generation and protection, e.g. Windows Bitlocker or other disk encryption keys
- Measured Launch (SRTM/DRTM)
- Integrity Measurement & Attestation
- Local Hardware Security Module (HSM)

Initial Participants:

- TrenchBoot, OpenXT, QubesOS / Invisible Things Lab, LF Edge Project EVE / Zededa

Target for open-source implementation delivery:

- Q3 2020

Collaborators Welcome:

- Requirements & Design
- Implementation & Validation
- Crowdfunding & OSS/commercial adoption

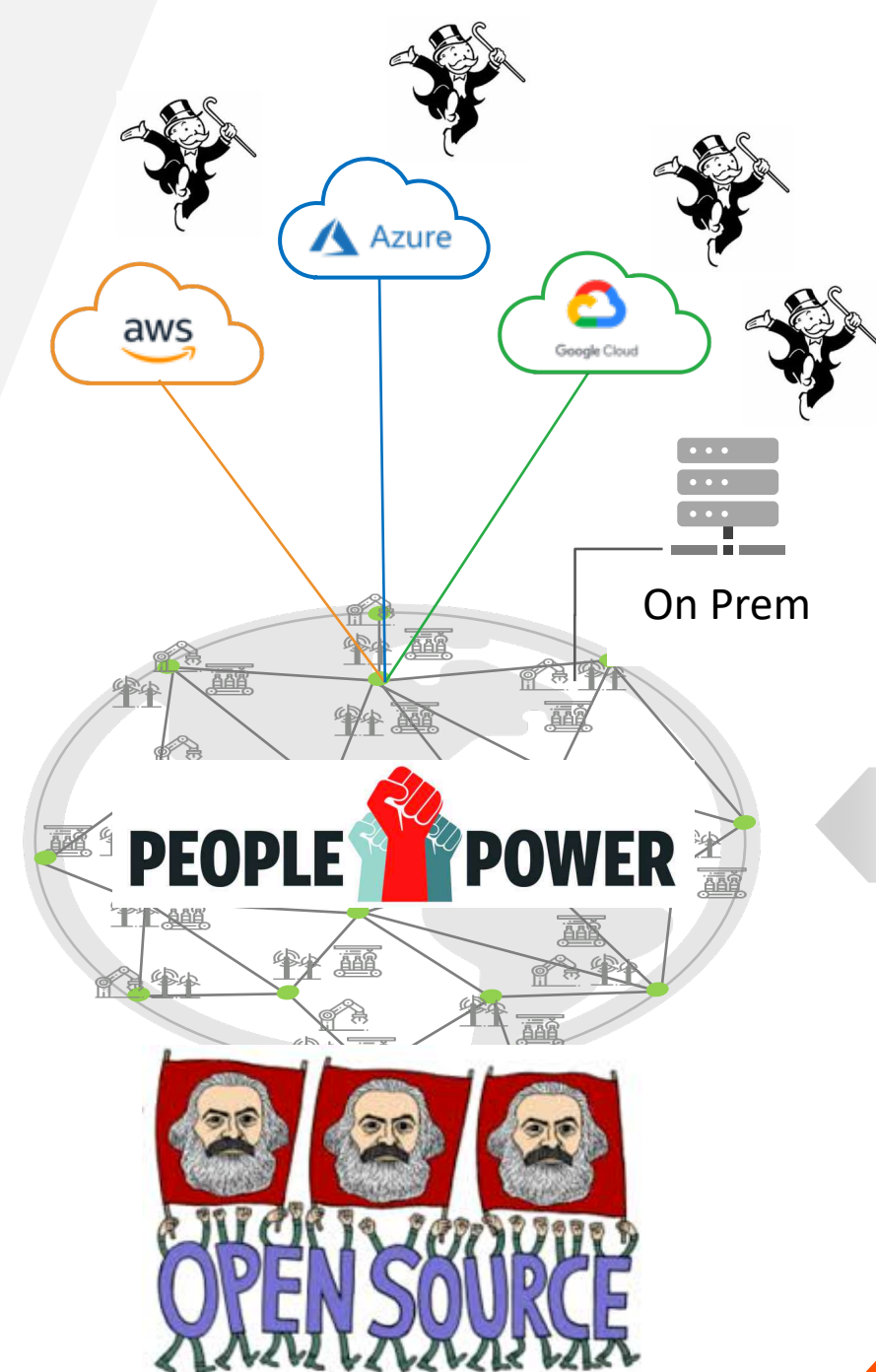
CONTACT

- DPSmith@ApertusSolutions.com
- trenchboot.github.io
- [LF Edge](https://lfedge.org)

Demo time!

Key takeaways

- Edge Computing today is where Public Cloud was in '06
 - It is a pioneer's land - sorry "settlers" and "town planners"
- Edge Computing is the one final Cloud left and it is the only one that can **NEVER** be taken away from us
- Edge Computing represents a **HUGE TAM**
 - VC activity is really picking up
- Kubernetes (implementation) is dead – long live Kubernetes (APIs)
- Edge Computing is a lot of fun, so...
 - Help us build LF Edge EVE...
 - ...or pick any other LF Edge Project



An aerial night photograph of a city, likely San Francisco, showing a dense grid of streets and buildings illuminated by city lights. A prominent bridge, possibly the Golden Gate Bridge, is visible in the lower-left corner, crossing a body of water. The overall scene is dark, with the city lights providing the primary illumination.

THANK YOU!

Follow EVE and LF Edge:

@eve_edge



@LF_Edge