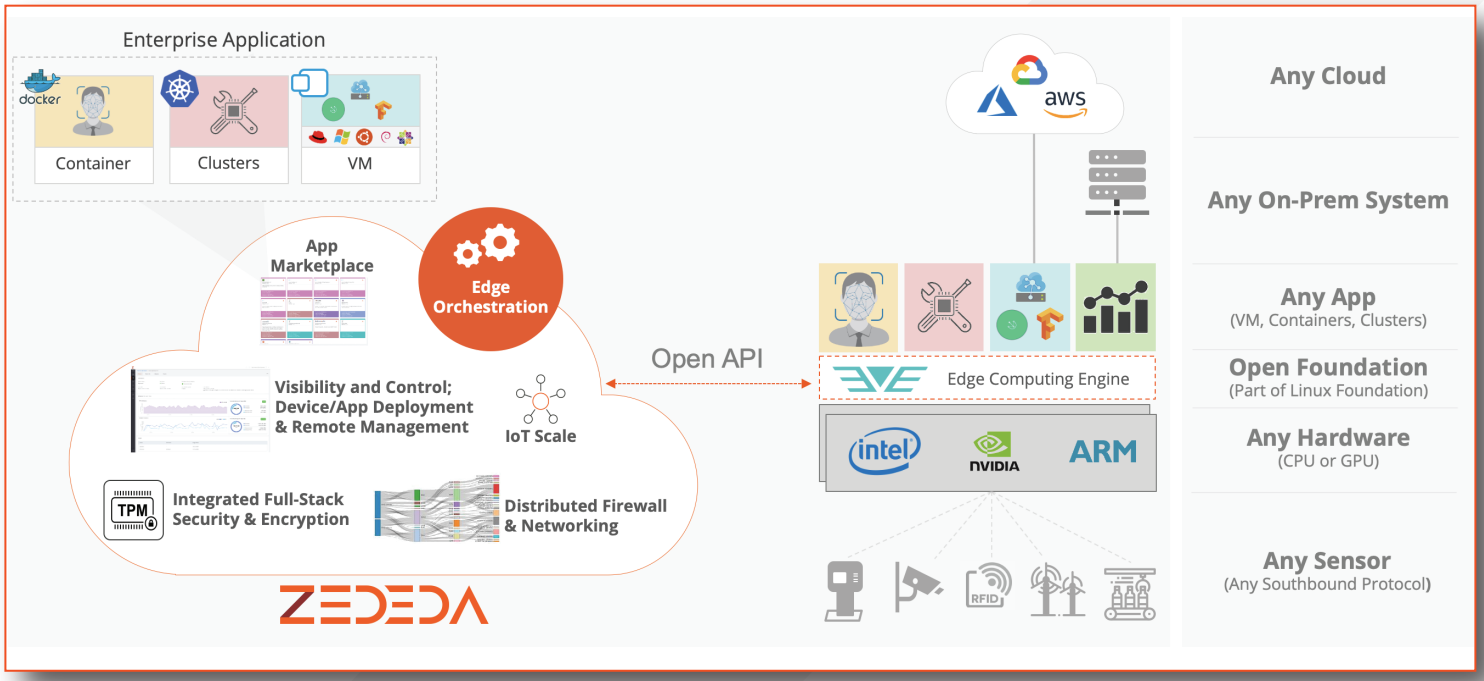
ZEDEDA

Cloud Agility at the Distributed Edge

The explosion of edge data requires more processing at the network edge for reasons of bandwidth costs, latency, autonomy, security, and privacy. Existing solutions do not meet the unique needs for orchestrating apps and hardware deployed at the edge due to the diverse mix of technologies, required domain expertise and lack of standardized infrastructure outside of physically-secure data centers.

ZEDEDA is a simple and scalable cloud-based orchestration solution for the distributed edge that delivers visibility, control and security for edge computing deployments in the field. Customers can now have full-stack remote management and observability for any distributed edge computing hardware and application while connecting to any cloud or on-premises system. With ZEDEDA, customers can now easily dropship hardware without onsite expertise and add intelligence on-demand to any edge compute node at scale to make real-time decisions, maximize operational efficiency and drive new business outcomes.

Visibility, Control and Security for the Distributed Edge



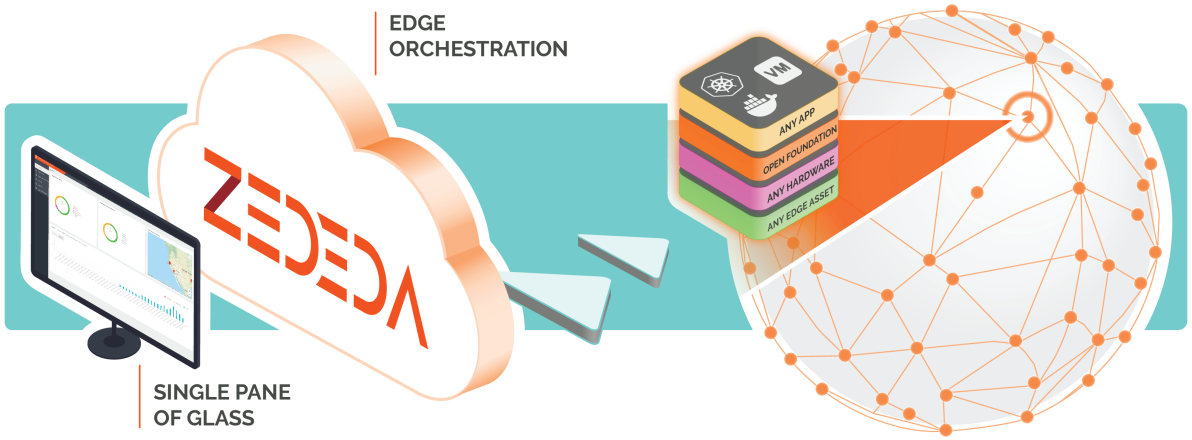
ZEDEDA leverages EVE-OS, a secure, open universal operating system, developed with vendor-neutral and open source governance as part of the Linux Foundation's LF Edge organization. EVE-OS simplifies the deployment, orchestration and security of cloud-native and legacy applications on distributed edge compute nodes. EVE-OS encrypts data, maintains device and software integrity and supports VMs, containers and clusters (Docker and Kubernetes). With an open and flexible foundation, customers can now easily future-proof their edge deployments.

ZEDEDA Advantage

Zero Limits: Use any hardware, deploy any app and connect to any cloud—no vendor lock-in! Onboard and manage any number of nodes , consolidate workloads (run legacy and cloud-native apps simultaneously) and bulk deploy (or update) apps remotely with a single click of a button.

Zero Touch: Get compute nodes up and running quickly. Dropship and instantly provision hardware remotely at scale, with all OS and system software automatically downloaded from the cloud. Upgrades are risk free (no bricking) with automatic roll-forward or roll-back and failover mechanisms (configuration, images, network and ports).

Zero Trust Security: Eliminate hardware spoofing, detect anomalies in your software stack, and ensure device integrity with hardware root of trust (e.g., TPM) while governing data flow across apps and nodes with distributed firewall capabilities. Easily meet compliance and regulatory requirements, reduce data breaches and stop leakage with Role-based Access Controls (RBAC), cloud security and centralized management.



Key Features

Remote & Centralized Deployment and Management at Scale

- Deploy or upgrade apps and base OS of hardware
- Visibility, reports and status of all hardware and apps
- Alerting, events, resource utilization, and analytics

Security and Privacy

- Hardware root of trust (e.g., TPM)
- Measured boot and remote attestation
- Crypto-based identification (no username/passwords)
- Data encryption at rest and in-flight
- Distributed firewall for every app
- Physical security - port isolation
- Role-based access control (RBAC)

Open Edge Ecosystem of Apps and Solutions

- Marketplace for ZEDEDA and partner-certified apps
- BYO-Apps in branded/private store
- Single-click bulk deployment (or updates) of apps

Freedom of Choice

- Any ARM, x86, or GPU-based hardware
- Support VMs, containers & clusters (Docker & Kubernetes)
- Any cloud (AWS, Microsoft Azure & Google Cloud Platform)
- One-click VPN connectivity to any cloud
- Overlay network for intra-edge compute node connectivity
- Policy-based network failover; ethernet, LTE, satellite & Wifi