ZEDEDA

SIMPLE, SECURE ORCHESTRATION FOR THE DISTRIBUTED EDGE

ZEDEDA Architecture White Paper

Executive Summary

As organizations execute on their digital transformation strategies, they are incorporating more edge computing technology into their operations to help improve business outcomes, lower costs and ensure security and data privacy.

Edge computing workloads are being driven by IoT, AI, networking and security use cases across all industry verticals to deliver outcomes such as remote condition monitoring, predictive maintenance, and improved logistics, safety and security and customer experience. The edge is a continuum and traditional data center solutions are not suitable for managing and securing computing nodes at the distributed edge-deployed both on-prem and in the field, outside of physically-secure data centers.

ZEDEDA offers the industry's most advanced orchestration solution for distributed edge computing to help customers accelerate their journey to the edge. Built on an open source foundation and optimized for the unique requirements of the distributed edge, the cloud-based ZEDEDA solution eliminates lock-in and drastically simplifies the deployment and full lifecycle management of both hardware and applications in the field at scale. Featuring support for diverse hardware, a zero trust security model, and flexible application deployment models, the solution enables users to leverage existing infrastructure investments alongside modern, cloud-native innovations.

Contents

Introduction

Edge data is exploding due to increasing capability and falling cost of computer hardware and network connectivity, in addition to technology trends such as IoT and AI. This is driving a need for distributing computing at the edge to supplement cloud resources. Edge computing moves data processing and analysis closer to endpoints where data is generated in order to enable rapid decision-making, reduce the cost associated with transferring large amounts of data to the cloud, and improved resiliency, security, privacy and user experience. In order to support this distribution of compute resources, organizations need an orchestration solution that enables scalable management and security.

Orchestration solutions that provide management and security for distributed edge computing need to scale massively in terms of hardware and application instances, nodes and locations. They need to be flexible to enable a diverse mix of deployment architectures, business models and skill sets spanning Operations Technology (OT) to IT organizations. They need to be fully automated, centrally managed, and enable autonomous operation in the field to maximize uptime for critical operations. Finally, distributed edge orchestration solutions need to be built from the ground up to address the unique security requirements of compute nodes that are located outside of physically secure data centers and may not have a defined network perimeter. Traditional data center orchestration and security solutions are not suitable for the distributed edge because they are not built with these unique requirements in mind.

This white paper explores how ZEDEDA's orchestration solution for distributed edge computing enables customer success through its simple, subscription-based service together with value-add from ecosystem partners. It highlights key considerations for distributed edge computing and provides an overview of the core solution components.

Key Challenges at the Distributed Edge

The edge is a continuum, and both hardware and software become increasingly heterogeneous the closer deployments get to the physical world - in locations such as the factory floor, inside wind turbines, on oil rigs, on trucks, and within retail stores, to name a few. There are diverse hardware architectures (e.g., x86, Arm, GPU) and form factors and many of these devices are resource constrained.

The distributed edge also has a large footprint of legacy infrastructure and applications that are business-critical but not compatible with containerization. Orchestration solutions for distributed edge computing need to support both legacy and modern cloud-native applications to ensure that enterprises have a transition path and aren't forced to "rip and replace" existing investments.

Unlike deployments of computing resources in the data center, distributed edge computing nodes often have no physical or network perimeter. As such, orchestration solutions should leverage a zero trust security model and not rely on having an owned network or firewall to protect them. In the OT world, a security compromise can lead to immediate loss of production and risk to safety, making it especially important that any issues are addressed promptly and gracefully.

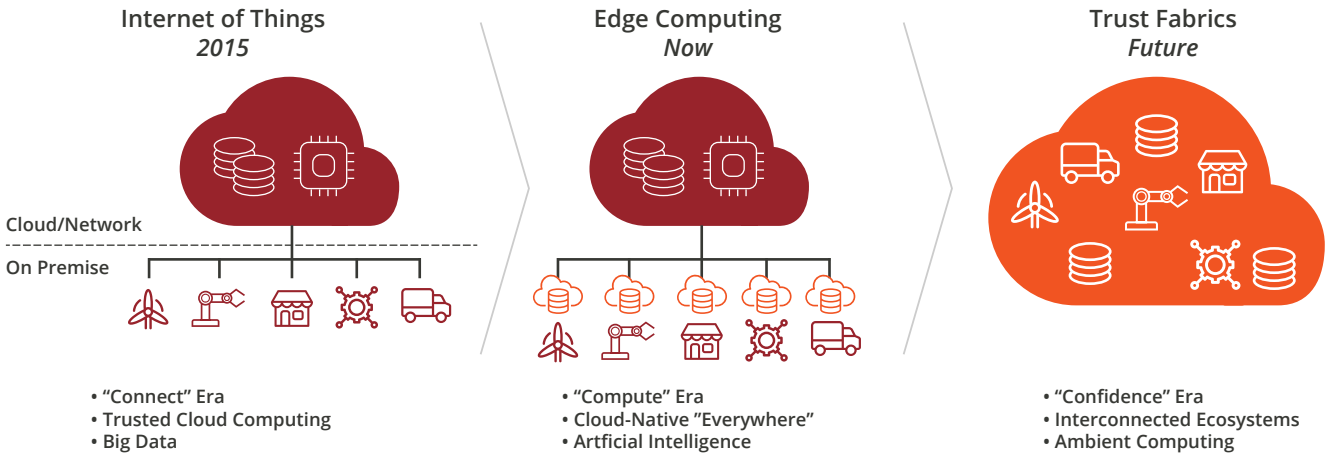
Further, as the Internet of Things (IoT) drives device deployment scale into the billions this will necessitate millions of distributed edge computing nodes that an organization must secure and manage in order to pre-process data and ensure network security. Solutions oriented towards securing and managing centralized data center infrastructure aren't designed to address this scale factor.

Finally, diverse skill sets spanning IT and OT (e.g., network and security admins, DevOps, production, quality and maintenance engineers, data scientists) are necessary to deliver distributed edge solutions that bridge the physical and digital worlds. These organizations often have differing priorities, for example IT typically prioritizes security, privacy and governance, whereas OT prioritizes uptime, quality and safety.

Solutions for distributed edge orchestration and security need to address these challenges, balance the needs of all stakeholders, and be priced appropriately to support business models.

The Importance of an Open Edge Architecture

The market has attempted to address the inherently diverse nature of the edge with a dizzying landscape of proprietary platforms. However, the ultimate value of digital is interconnecting ecosystems to foster new experiences and revenue streams. Key to realizing this goal over time is to invest today in open, trusted infrastructure that is aligned to several core principles.



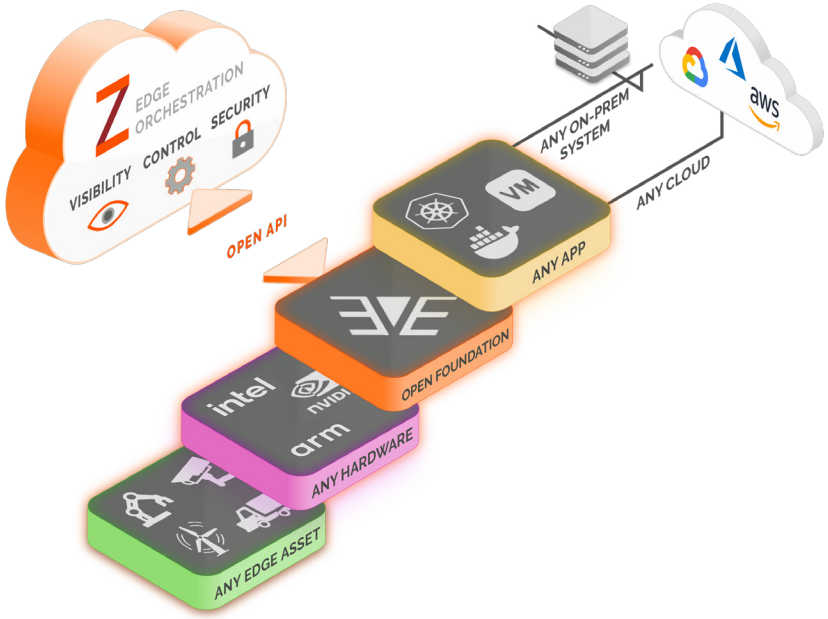
Evolution in a Connected World Requires an Open Edge

First, it is critical to abstract data, applications and domain knowledge from underlying infrastructure so tools for data ingestion, security and management are consistent regardless of use case. Second, it is important to untether data from backend services as close as possible to the edge source so all permutations of edge to cloud data flow are supported without risk of lock-in. Finally, it is important to extend cloud-native principles wherever possible while also recognizing technical tradeoffs, for example latency and safety-critical applications at the edge that require embedded software.

In summary, it is critical to establish a multi-cloud strategy rooted in an open edge, prioritizing domain knowledge and/or offering necessarily unique hardware, software and services on top of open, consistent infrastructure. Architecting infrastructure with these principles in mind enable users to smart small but scale into creating new business models and experiences for both internal stakeholders and end customers.

The ZEDEDA Solution

ZEDEDA is the leader in orchestration for the distributed edge, enabling customers with a cloud-native solution that delivers visibility, control and security for edge computing deployments in the field. Companies can now have full-stack remote management and observability for any distributed edge computing hardware, edge application and with any on-prem system or cloud.



The ZEDEDA Solution Stack

The ZEDEDA solution is built on three core principles:

Zero Limits

Supporting orchestration of diverse edge hardware and applications at scale, including both legacy and cloud-native software investments without any vendor lock-in. ZEDEDA is not in the data path so customers are free to develop edge solutions with any combination of applications and on-prem and cloud backends.

Zero Touch

Enabling simple field deployment of edge computing nodes without requiring IT skills and supporting autonomous operation and remote management with risk free updates from the cloud. This requires an eventual consistency model in which edge nodes continue to run in the current state if they lose connection to the centralized orchestration service.

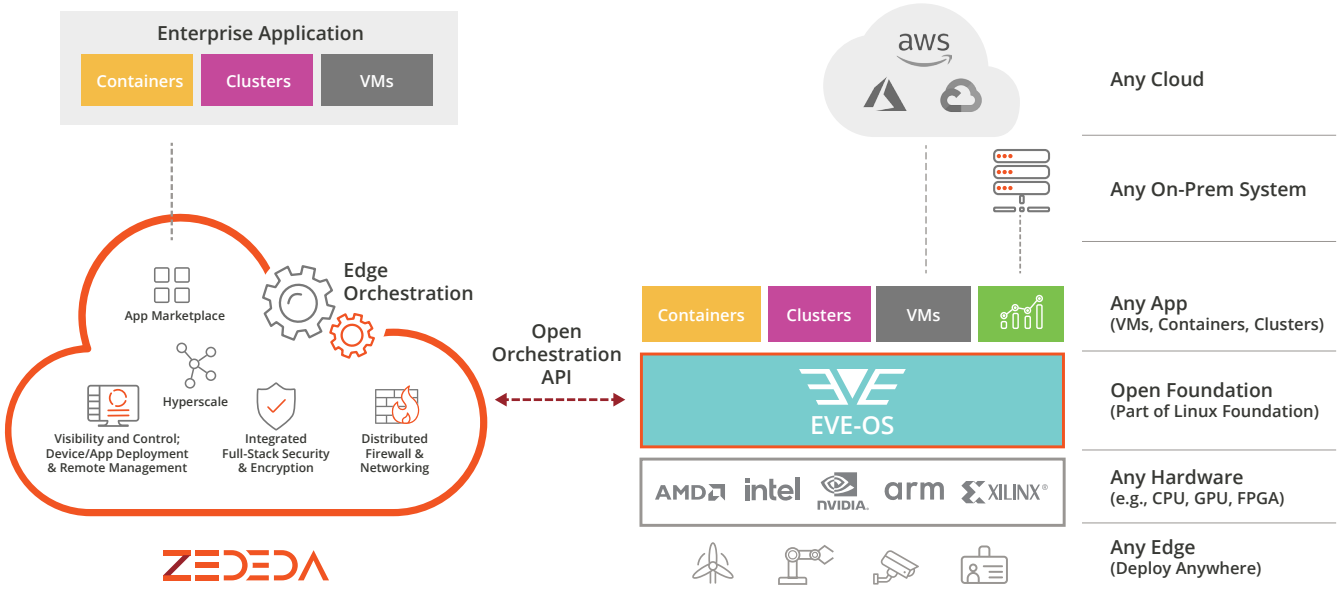
Zero Trust

Implementing a zero trust model for physical and cyber security to address the unique, perimeter-less security requirements of the edge.

The solution is composed of two key components: the cloud-based ZEDCloud orchestration service and the open-source EVE-OS from the Linux Foundation.

ZEDEDA Cloud Orchestration Service

The ZEDEDA cloud service provides a centralized console with easy-to-navigate UI that enables both IT and OT admins and DevOps resources to remotely orchestrate distributed edge computing hardware and applications at scale. It enables full visibility into the health of deployed edge infrastructure and the ability to bulk deploy choice of applications, and subsequently remotely update these applications, guest operating systems (if utilized) and EVE-OS itself. Role-based Access Control (RBAC) enables admins to provide different levels of system access based on policy.



ZEDEDA Cloud Orchestration Service (left) and EVE-OS (right)

The cloud service is based on a multi-tenant architecture with the baseline option being an instance hosted on a shared cloud cluster for the lowest startup cost. Customers also have the option for their own dedicated instance on a private cluster to maximize customization options.

The ZEDEDA cloud communicates with deployed edge nodes through the open EVE-OS orchestration API. This ensures that users are not locked into any particular orchestration service, including ZEDEDA. The commercial cloud component also provides a comprehensive set of APIs for orchestration, with key API functionality being exposed in the ZEDEDA GUI. Developers can leverage the broader set of APIs for their own custom solutions and integration with preferred systems.

The solution is sold and consumed as a service with a subscription-based enterprise license and "pay-as-you-go" model that includes 24/7 support for both the ZEDEDA cloud orchestration service and EVE-OS. White-label models are also available for OEM's and SI's. The "pay-as-you-go" model offers customers the flexibility to start small and scale as their business needs evolve.

EVE-OS

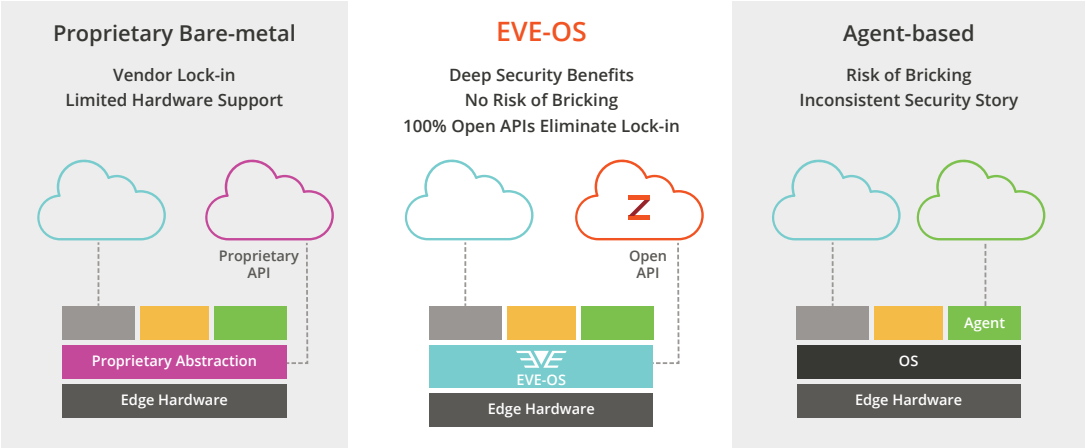
Developed within Project EVE in the Linux Foundation's LF Edge organization, EVE-OS is an open, Linux-based operating system designed to meet the unique requirements of the distributed edge. This includes abstracting data and applications from infrastructure, supporting flexible application deployment models (e.g., VMs, Docker containers, Kubernetes clusters) and implementing a zero-trust security model.

The hosting of Project EVE within LF Edge ensures vendor-neutral governance of the code base and related specifications. All technical meetings are open to the public to ensure transparency. The ultimate goal for EVE-OS is to do for the distributed edge computing landscape what Android did for the mobile industry—create a universal abstraction layer that enables scale and supports an open application ecosystem.

Comparison of Architectural Approaches for Edge Nodes

As a bare-metal solution, EVE-OS provides a deep security story with hardware root of trust and policy-based management of both applications and hardware. With direct access to hardware there's no risk of bricking a device in the field during an update of EVE-OS, guest operating systems or applications. Being completely open source prevents lock-in to any particular backend.

In comparison, orchestration solutions built on a proprietary bare metal foundation may offer similar benefits for security and application support, but with the significant drawback of locking users into the provider's full stack. Meanwhile, agent-based orchestration solutions have the advantage of supporting choice of host operating system but have security vulnerabilities without significant investment in OS hardening and present the potential to brick a device during an update, requiring a truck roll to address.



Comparison of Architectural Approaches for Edge Node Orchestration

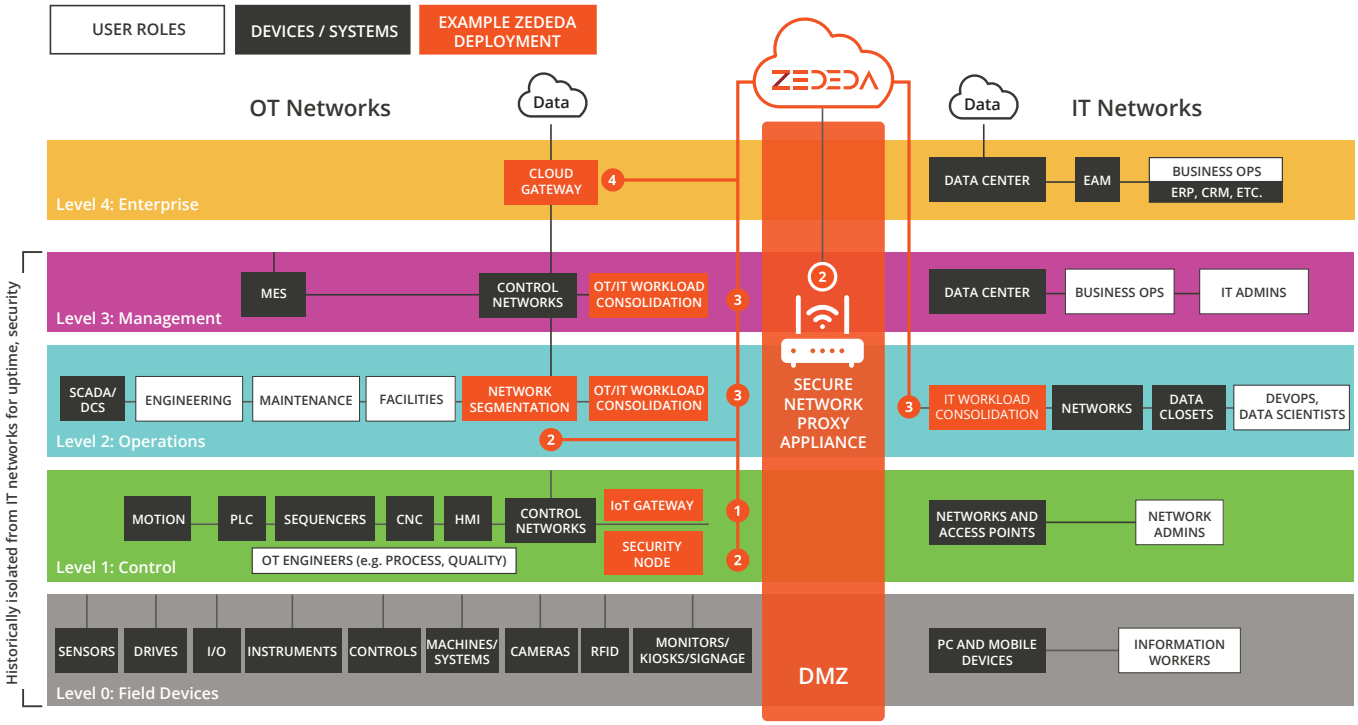
EVE-OS is architected to provide a balance between both approaches, resulting in a universal, open foundation for distributed edge computing deployments. Further simplifying deployment scale is a growing ecosystem of hardware providers supporting EVE-OS and preloading it in their factories.

Example Deployment Patterns

The ZEDEDA solution can support any use case and in any vertical with choice of hardware and applications. The figure below highlights several example deployment models in a typical OT/IT environment that have segmented networks to protect critical operations.

Examples shown in the figure below include:

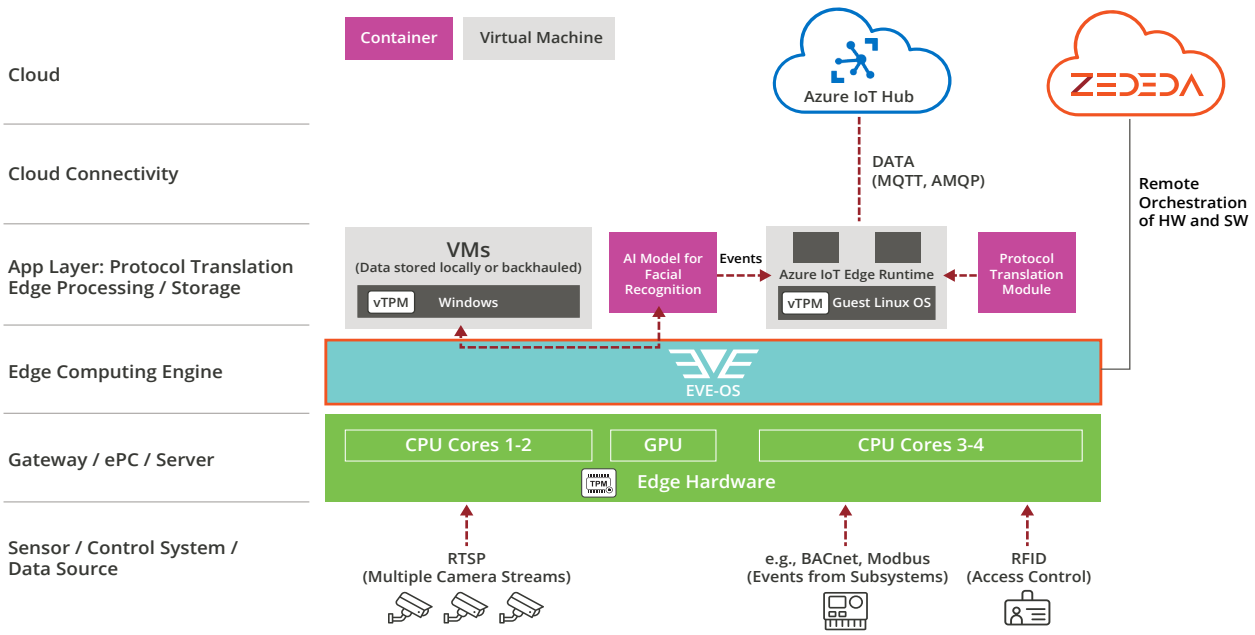
1. IoT gateways
2. Dedicated edge security nodes performing functions like network segmentation, protocol inspection and firewall
3. Single node and clustered computing to consolidate applications
4. Cloud edge gateways that extend network functions from service providers to on-prem end user environments



Typical Deployments in Layered Enterprise Networks

In terms of software deployment patterns on a given edge computing node, the following example reflects a solution for video surveillance in which Windows-based Video Management Solution (VMS) deployed in a VM passes data to a containerized AI model performing facial recognition, which in turn outputs event data to Azure IoT Edge for future pre-processing and transmission to Azure.

Additional examples include consolidating existing historians, SCADA and HMI applications alongside new containerized functions for manufacturing use cases and deploying Windows-based Point of Sale (PoS) software alongside a containerized IoT stack in a retail application.



Example Deployment in Safety and Security with Applications in Both VMs and Containers

Key EVE-OS Features

Developed within LF Edge's Project EVE, the modular, Linux-based EVE-OS enables organizations to extend their cloud-like experience to edge deployments distributed outside of the data center and perform full lifecycle management and remote orchestration of choice of hardware and applications deployed in virtual machines, Docker containers and/or Kubernetes clusters. Support for virtual machines enables customers to lift and shift legacy software investments, in addition to deploying container runtimes such as Kubernetes, Azure IoT Edge, and AWS Greengrass.

The scope for Project EVE includes:

- Delivering the flexible and modular EVE-OS with built-in security
- Providing a reference controller implementation (Adam and Eden)
- Specifications and definition of open orchestration APIs

EVE-OS is a curated architecture compared to typical Linux distributions that require integration of all necessary components to deliver a ready-to-use deployment foundation. The result is a stack that can be loaded on choice of edge hardware to immediately scale deployments.

Key EVE-OS features include:

- **Support for any distributed edge computer hardware** – CPU (e.g., x86, Arm) and accelerators (e.g., GPU, FPGA)
- **Optimization for single edge compute nodes** with as low as 512MB of memory to multi-node clusters
- **Choice of embedded hypervisor** (e.g., Xen, KVM, ACRN)
- **Support for legacy apps** in VMs alongside modern containerized workloads
- **Zero-trust model** that utilizes hardware-based root of trust, measured boot, encryption and distributed firewall for the secure, frictionless data flow from edge to cloud
- **Fail proof rollback/forward updates** for both EVE-OS and apps to maximize uptime
- **Support for autonomous operation** with an eventual consistency model
- **Open, vendor-neutral APIs** that eliminate lock-in

EVE-OS Resources

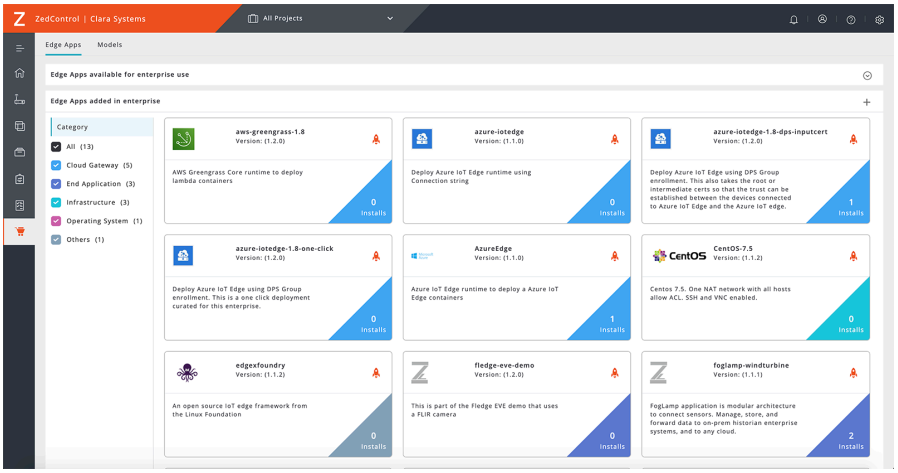
For more information visit:
https://www.lfedge.org/projects/eve/

Download EVE-OS
https://github.com/lf-edge/eve

Application Orchestration

The ZEDEDA cloud supports bulk orchestration of any combination of VMs, Docker containers and Kubernetes clusters on EVE-OS in the field. Applications are defined through deployment manifests that are similar in principle to Kubernetes Helm charts. These manifests indicate the on-prem or cloud repository where the application runtime is located, along with policy-based settings for CPU, memory and disk allocation, networking settings and more.

While Docker containers have been widely used in edge data center deployments for several years, extending Kubernetes-based cloud-native development to distributed edge locations requires the right security model and an orchestration backend that can scale to large fleets of nodes. EVE-OS supports choice of Kubernetes runtime deployed in a virtual machine and ZEDEDA's zero trust security model and optimizations for deployment at hyperscale provides users with the ideal solution for extending Kubernetes to edge computing applications distributed outside of the traditional data center.



ZEDEDA App Marketplace

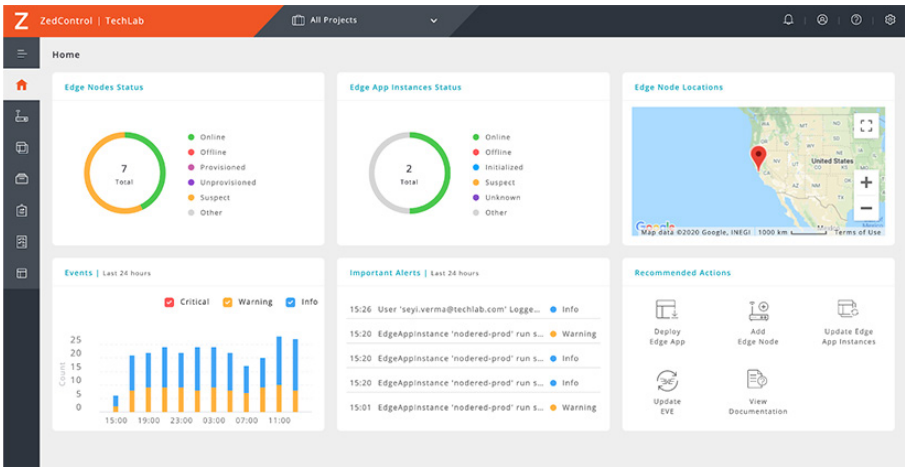
Developers can easily integrate the ZEDEDA solution with their existing CI/CD pipeline and different user roles can be granted various levels of permissions to perform certain tasks. The in-built marketplace enables end users to bulk-deploy their choice of edge application with a single click. The public app store is accessible to all users and features leading edge computing applications from ZEDEDA's open ecosystem. Enterprises, OEMs and SIs also have the option of curating their own preferred applications—both internal and 3rd-party—in their own private stores.

Manageability and Visibility

Successful deployment and operation of edge computing requires handling both day one issues such as deployment and onboarding of edge nodes and the applications which will run on them, and day two issues such as ongoing monitoring of the correct and secure operation of the devices and applications, plus the ability to update the configuration and software to respond to new needs and/or deploy security-relevant patches. This requires a management system which is built with the complete hardware and software lifecycle in mind, and which addresses the unique needs of the distributed edge.

ZEDEDA's management solution starts at the factory or in the supply-chain when EVE-OS is installed on the edge node. This enables secure, zero-touch on-boarding with simple LED feedback to the installer to indicate that the edge node has connected to the ZEDEDA orchestration cloud.

Lifecycle management capabilities for edge nodes include specifying and changing how the various network ports and I/O adapters are used and configured; either to be used by EVE-OS to connect to the ZEDEDA cloud, leveraged by applications, or shared for both. It also includes being able to perform secure, fail-safe updates of EVE-OS itself with automatic fallback should anything go wrong.



ZEDEDA Dashboard

Application lifecycle management includes being able to specify the origins of content, volumes, application network connectivity, and the applications themselves together with their parameters. The ZEDEDA cloud supports a number of different workflows for bulk deployment of applications to enable scalable operations from day one.

As part of the lifecycle management of both edge nodes and applications there is a rich set of visibility both by single edge node or application (e.g., CPU, memory, disk, and network usage, visualizing network flows) and across a larger deployment. For instance, showing the distribution of application versions across a fleet to facilitate bulk update of the applications.

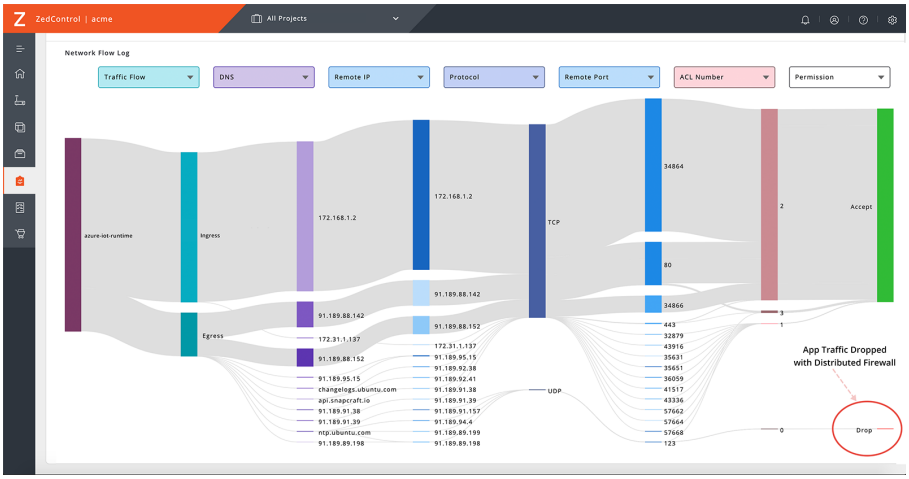
Edge Networking

The networking needs at the distributed edge are much richer than in the cloud, both in terms of downstream and upstream connectivity. Downstream of a distributed edge device there is often one or more local networks connected to sensors, actuators and industrial systems. In many cases this is in the form of Ethernet networks, but also common are wireless radio technologies and non-IP wired transports such as serial (e.g., RS485 for Modbus RTU) in legacy environments. Different edge computing hardware will offer different connectivity capabilities, which needs to be matched with the needs of the application(s) and the deployment environment.

Upstream connectivity is often in the form of Ethernet via some enterprise network to reach the Internet, but can also be cellular radio (3G, LTE, 5G) and even satellite communications for highly remote locations. Due to different bandwidth and cost tradeoffs, there might be combinations e.g., using LTE but with a satellite link as a backup.

Further complicating upstream connectivity, an OT organization or third-party service provider deploying an edge computing solution might not have full insight or control of the enterprise network used. We often see complications due to various proxy and firewall configurations in the IT network which have an impact on both the configuration and security of the deployed solution.

Last but not least, an application which is migrated from the cloud to the edge might make assumptions that it is running in a well-defined Virtual Private Cloud (VPC) which provides network isolation. ZEDEDA enables successful deployment at the edge by ensuring that the VPC can easily and securely be extended to the edge without requiring deep networking expertise.



Network Flow Visualization from Edge to Cloud

The ZEDEDA solution includes support for configuring a rich set of uplink connectivity, including fail-safe configuration updates with automatic fallback should the configuration be incorrect, which is key to ensure that the edge node never loses connectivity with the ZEDEDA cloud. The system is built with the distributed edge in mind and handles failover between different network uplinks and disconnected operation using an eventual consistency model for configuration management and state reporting.

The solution also provides different types of network and I/O connectivity for applications including isolated connectivity e.g., to shop-floor networks, air-gap networks which are entirely local to the edge node for defense-in-depth, and secure inclusion of applications in a VPC in a public cloud.

All of this is possible without requiring any more networking expertise than deploying the same application in the cloud, and while supporting lifecycle management for VMs, Docker containers, and Kubernetes clusters in a uniform way.

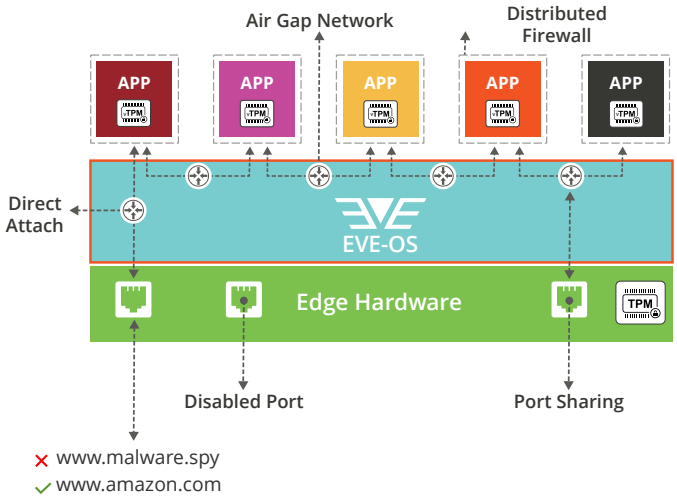
ZEDEDA's edge networking and I/O connectivity supports different hardware options through the use of model descriptions for the edge nodes which the customer chooses to deploy.

Edge Security

Distributed edge computing requires addressing the typical IT security concerns when it comes to network and application security, including configuring credentials and keys. But it also requires addressing unique threats introduced when deploying diverse physical infrastructure in the field. Examples include threats due to physical access, such as stealing devices, cloning disks and loading malware or replacing firmware through local USB ports. Additional threats are introduced due to the common lack of a network perimeter in the form of firewalls and intrusion detection systems. Exacerbating all of the above is a mix of skill sets in the field, with more limited availability of IT security support compared to in the cloud.

ZEDEDA's goal is to ensure that the deployment of hardware and applications at the distributed edge is not hindered by such security concerns by providing a holistic approach built from the ground up.

The ZEDEDA solution addresses security starting at the hardware and firmware level by leveraging standard Trusted Platform Modules (TPM) to prevent cloning of edge devices or their disks, using cryptographic identities for the edge devices and the application instances, and standard encryption on the network (TLS) plus disk encryption. The deployed applications are protected by connecting them to the networks and I/O which match their needs, in combination with using the distributed firewall built into EVE-OS. The solution also supports deploying third-party security applications on EVE-OS, for instance for intrusion detection and prevention, as well as anomaly detection across deployments in the ZEDEDA cloud.



Secure Application Connectivity

However, security is not accomplished solely by a collection of state-of-the-art **technologies**. Just as important are:

- Providing and supporting security **processes**, such being able to observe applications and EVE-OS to look for anomalies and enabling secure and robust patching of both applications and EVE-OS.
- Considering the role of **people**, as exemplified by simple, secure on-boarding of edge nodes without requiring security expertise by the installer and leveraging crypto-based ID to eliminate username and associated password management for EVE-OS, which can lead to local tampering.

Our approach to security is that it should not make the system harder to use, and it should not require any more security expertise than deploying the same application in the cloud.

Further details on security can be found in ZEDEDA Edge Security white paper.

Conclusion

The world is continuing to become more connected and increasingly upload-centric with more and more data being generated by billions of devices being pushed to the cloud, enabling new intelligent, responsive applications. These applications increasingly depend on edge computing to supplement the cloud for lowering the cost of bandwidth consumption, reduced latency, and improved security and privacy.

ZEDEDA delivers visibility, control and security for the distributed edge, with the freedom of deploying and managing any app on any hardware at scale and connecting to any cloud or on-premises systems.

Distributed edge solutions require a diverse mix of technologies and domain expertise and ZEDEDA enables customers with an open, vendor-agnostic orchestration framework that breaks down silos and provides the needed agility and future-proofing as they evolve their connected operations. Customers can now seamlessly orchestrate intelligent applications at the distributed edge to gain access to critical insights, make real-time decisions and maximize operational efficiency.

Summary of ZEDEDA Differentiation

- Supports VMs, containers and clusters for workload consolidation and future-proofing edge deployments
- Enables zero trust security model with hardware-root-of-trust, remote attestation, data encryption, anomaly detection and distributed per-app firewall capabilities
- Full-stack remote orchestration and observability for edge hardware and software at cloud-scale with APIs
- Truly open foundation eliminates lock-in and facilitates hardware, app and cloud interoperability
- Maximum uptime through fail-safe updates with an eventual consistency model
- Unparalleled out-of-the-box experience that fast tracks edge deployments with no IT experience required in the field
- App marketplace backed by an open edge ecosystem with an option of curating private stores

About ZEDEDA

ZEDEDA, the leader in orchestration for the distributed edge, delivers visibility, control and security for edge computing deployments. ZEDEDA enables customers the freedom of deploying and managing any app on any hardware at scale and connecting to any cloud or on-premises systems. Distributed edge solutions require a diverse mix of technologies and domain expertise, and ZEDEDA provides customers with an open, vendor-agnostic orchestration framework that breaks down silos and provides the needed agility and future-proofing as they evolve their connected operations.

Customers can now seamlessly orchestrate intelligent applications at the distributed edge to gain access to critical insights, make real-time decisions and maximize operational efficiency. ZEDEDA is a venture-backed Silicon Valley company, headquartered in San Jose, CA, with offices in Bangalore and Pune, India. For more information, contact info@zededa.com.

Authors

Erik Nordmark
Chief Architect, ZEDEDA

Roman Shaposhnik
VP Product and Strategy, ZEDEDA

Jason Shepherd
VP Ecosystem, ZEDEDA

Morris Novello
Product Marketing Consultant, ZEDEDA

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current ZEDEDA product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from ZEDEDA and its affiliates, suppliers or licensors. ZEDEDA products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of ZEDEDA to its customers are controlled by ZEDEDA agreements, and this document is not part of, nor does it modify, any agreement between ZEDEDA and its customers.