Secure Zero Touch Kubernetes Orchestration for the Distributed Edge

Effortlessly Scale Kubernetes at the Edge

TECHNOLOGY BRIEF

The Challenge

The edge is emerging as the next frontier of computing and organizations are looking to replicate the benefits of cloud-native principles in the field for IoT, AI, 5G, network virtualisation and security use cases. As the number of edge devices grow at a rapid pace, along with the capacity to produce immense volumes of business-critical data, the need to analyze data closer to the source has become ever more important due to bandwidth, storage, security and latency reasons.

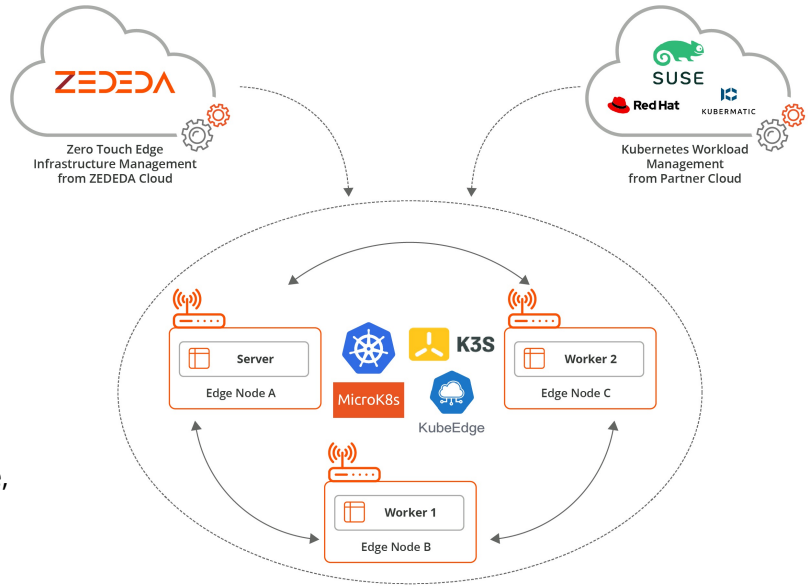
Despite the rapid growth and popularity of containerized applications, deploying Kubernetes at the distributed edge—compared to centralized data centers—is a challenge due to infrastructure and software heterogeneity. Kubernetes has been used in data center deployments for several years, and extending Kubernetes to distributed edge locations requires the right security model and an orchestration backend that can scale to large fleets of clusters, including managing a diverse landscape of hardware. Furthermore, cloud and data center Kubernetes solutions lack an adequate Zero Trust security model, are resource intensive for smaller footprint edge nodes, are expensive, and require specialized skill sets that are not commonly found in the field.

The Solution: Zero Touch Kubernetes Orchestration

ZEDEDA's orchestration solution greatly simplifies Kubernetes infrastructure management, security and visibility as customers look to deploy Kubernetes clusters outside of centralized data centers. The ZEDEDA cloud has a simple and intuitive UI along with comprehensive APIs that abstract all the complexities of provisioning Kubernetes clusters at the distributed edge while automating cluster bring-up on target edge nodes in minutes. The ZEDEDA solution can support any Kubernetes distribution, including K3s, K8S, KubeEdge, and MicroK8s by simply adding them to the ZEDEDA app marketplace.

ZEDEDA enables simple field deployment of edge computing nodes with any combination of Kubernetes clusters, native Docker containers and VMs. The solution supports remote management and risk-free updates from the cloud, without requiring specialized IT skills. It supports autonomous field operation through an eventual consistency model in which edge nodes continue to run in the current state if they lose connection to the centralized orchestration service.

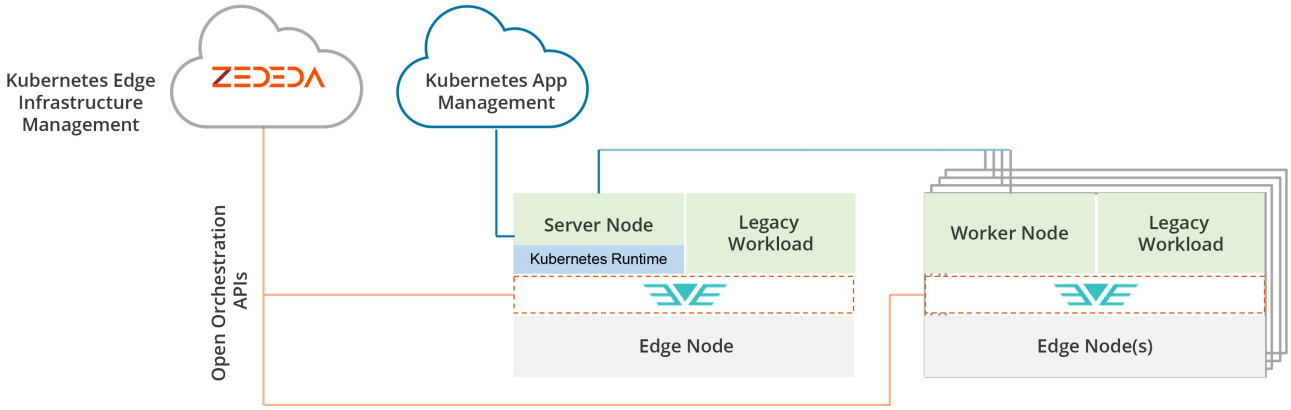
To further simplify Zero Touch deployment, ZEDEDA has partnered with leading OEMs of edge computing hardware to preload EVE-OS from the factory. Once power and network are connected, all it takes are a few clicks to securely onboard a device, install a Kubernetes distribution and deploy apps.



Kubernetes at the Distributed Edge

Security First

ZEDEDA's state-of-the-art and market leading Zero Trust security architecture assumes that edge nodes distributed in the field are physically-accessible, in addition to not having a defined network perimeter. Features include support for silicon-based root of trust, measured boot, remote attestation, crypto-based ID (eliminating local device login), full disk encryption, remote port blocking, distributed firewall, and more. The distributed firewall capability enables secure routing of data between edge applications and both on-prem and cloud resources based on network-wide policies.

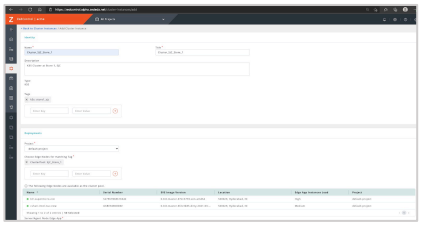


ZEDEDA Orchestration for the Distributed Edge

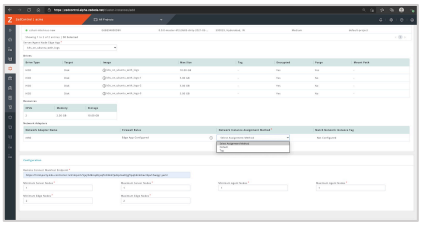
How it Works

ZEDEDA's cloud orchestration solution leverages the bare metal EVE-OS deployed on edge nodes. EVE-OS is an open, secure and universal operating system for distributed-edge computing with vendor-neutral APIs, hosted within Project EVE in the Linux Foundation's LF Edge organization. In addition to preventing vendor lock-in, EVE-OS provides an anchor point to unify an ecosystem of edge computing hardware and software while integrating with customers' existing CI/CD workflow to support any combination of virtual machines (VMs) and native Docker containers for the deployment of any combination of legacy Windows-based applications (e.g., SCADA, HMI, Historian, VMS, POS), monolithic Linux-based images, and other popular container runtimes such as Docker/Moby, Azure IoT Edge and AWS Greengrass.

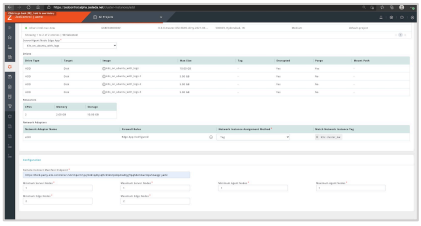
Setting up a cluster within the ZEDEDA cloud simply requires selecting the target edge hardware, configuring the cluster and setting up the networking parameters and the entire process of deploying and bringing up the cluster is automated in the background.



Edge Node Selection



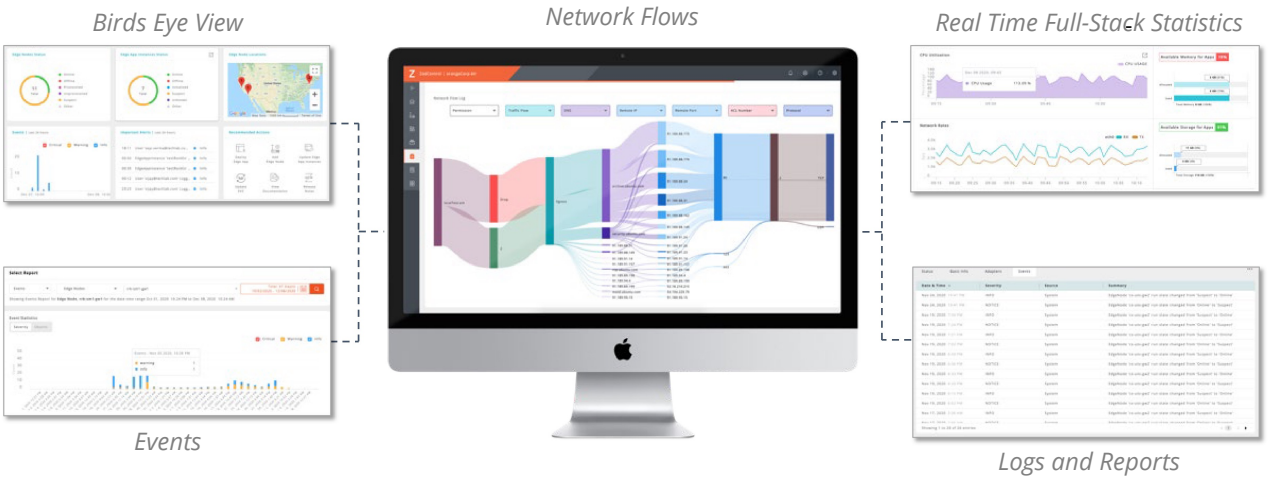
Cluster Configuration



Cluster Networking

Full Visibility into Kubernetes Infrastructure

ZEDEDA provides a rich set of visibility for both day one and day two management of edge nodes (e.g., CPU, memory, disk, and network usage, network flow visualization), clusters and applications. This is both by single edge node or application and across a fleet deployment.



Visibility, Control and Security for the Distributed Edge

Benefits

Flexible	Support for any Kubernetes distribution, including K3s, K8S, KubeEdge and MicroK8s. All users have access to the public marketplace and have the option to create private marketplaces with curated content, in addition to white-labeling the overall orchestration solution.
Simple	Deployment of Kubernetes clusters without requiring IT skills in the field and support for autonomous operation with risk-free updates from the cloud.
Comprehensive	Remote management of the entire lifecycle of both the Kubernetes runtime and the underlying hardware at scale.
Extendable	Optimized for remote deployment and management of distributed edge computing hardware and applications, spanning a single edge gateway in the field to a small server cluster at the fringes of an on-prem data center.
Secure	Zero Trust security architecture built on hardware root of trust (e.g., TPM) ensures Kubernetes clusters, application and data are protected to eliminate any vulnerabilities at the distributed edge, where physical security countermeasures are of paramount importance outside secure data centers.
Open	EVE-OS unifies the edge ecosystem and enables customers and OEMs with choice of hardware, applications, cloud, and services to future-proof edge deployments with no vendor lock-in.

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 futureproofing 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 teams based in Bangalore and Pune, India and Berlin, Germany.

Contact us at sales@zededa.com to learn more about this solution brief and how we can help you with your digital transformation.

www.ZEDEDA.com