



by pocteo

KEOS

Kubernetes Edge OS

An autonomous, immutable Kubernetes runtime for every site engineered to operate at the edge, even without WAN.

WHITEPAPER 2026

Pocteo Platform

<https://pocteo.tn>

OVERVIEW

Executive Summary

Modern enterprises run workloads in places where the cloud cannot reach reliably: factories, vessels, retail stores, vehicles, wind farms, hospitals, and defense sites. These environments demand a runtime that is autonomous, resilient, secure, and uniform across thousands of locations with intermittent or no connectivity.

KEOS (Kubernetes Edge OS) is the on-site runtime of the Pocteo Platform. It is an immutable, self-healing Kubernetes node that boots from bare metal, survives weeks without WAN, and keeps your workloads running where the data is produced. Combined with Pocteo Platform's fleet management, it lets one team operate ten thousand sites with the same ease as one.

CONTEXT

The Edge Problem

Edge sites break the assumptions of traditional Kubernetes: links are unreliable, hardware is constrained, sites are unattended, and security boundaries are physical. General-purpose distros require constant operator attention and degrade silently when isolated.

Unreliable connectivity operations must continue offline for days or weeks.

Constrained hardware gateways and industrial PCs with 2 vCPU / 4 GB RAM.

No on-site operators every action must be declarative and self-recovering.

Physical attack surface disks can be removed; secrets must be sealed.

Fleet scale hundreds to tens of thousands of sites with identical behavior.

POSITIONING

Why KEOS

KEOS is not a Kubernetes distribution to be installed and maintained. It is a self-contained operating system whose only job is to run a Kubernetes cluster, reconcile its declared state, and survive everything else.

Three Core Pillars

Autonomous	Each KEOS node reconciles its own state, even fully offline. No human action required on site, ever.
Immutable	Signed, read-only OS image. A/B partitions, atomic upgrades, automatic rollback. No drift, no SSH, no surprise changes.
Sovereign	Workloads, secrets, and identity remain on-site. The control plane never leaves your perimeter.

RUNTIME

Capabilities

Immutable, network-bootable OS

KEOS nodes PXE/iPXE-boot a signed, immutable image. No SSH, no drift, no hand-edits. A/B partitions deliver atomic upgrades with automatic rollback.

Disconnected by design

Operates for days or weeks without WAN. Local Git mirror, local container registry, local control loops. When the link returns, state reconciles in the background.

P2P mesh between sites

Neighboring edge clusters sync over an encrypted WireGuard mesh with Cilium Cluster Mesh workloads keep moving even when the cloud is unreachable.

Ruggedized, low-footprint

Runs on 2-core gateways, industrial PCs, vessels and vehicles. Tolerates power cuts, brown-outs and reboots with deterministic recovery.

Air-gap ready

Signed artifacts, sealed secrets, local Vault-backed identity. Edge API servers are never internet-exposed; control flows over egress-only mTLS tunnels.

GitOps to the node

Embedded FluxCD reconciles OS, Kubernetes, CNI, storage and workloads from one declarative manifest. Same blueprint on every site.

HOW IT WORKS

Architecture

KEOS clusters are governed by the Pocteo Platform control plane. A single declarative manifest describes the fleet operating system, Kubernetes version, CNI, storage, workloads, policies and every KEOS node drives itself to that state.

Cloud Edge Flow

1. DECLARE	In Pocteo Platform, define fleet, modes, OS, CNI, workloads in one manifest.
2. DISTRIBUTE	Signed artifacts replicate to every site over mTLS or a local Git mirror.
3. RECONCILE	Each KEOS cluster drives its own state autonomously, forever.

WHAT RUNS ON A KEOS NODE

Specifications

Form factors	Bare metal Industrial PC Vehicle gateway VM (Proxmox / vSphere / KVM)
Minimum footprint	2 vCPU 4 GB RAM 32 GB storage
Operating system	Immutable, signed, A/B partitioned (Talos-inspired)
Kubernetes	Upstream Kubernetes 1.31, single-node or HA
Networking	Cilium eBPF L2/BGP load balancing WireGuard mesh
Storage	Local-path Longhorn OpenEBS
Security	mTLS Vault Cert-Manager Kyverno Falco Tetragon
Connectivity	Online Intermittent Air-gapped

WHERE KEOS RUNS TODAY

Industries

Manufacturing

Run MES, SCADA bridges, OPC UA gateways and vision AI inside the plant. Production keeps running when the corporate network drops.

Automobile

On-vehicle and on-line workloads with deterministic boot, OTA updates and rollback. Fleet-wide governance from one manifest.

Agrotech

Farm gateways operate independently over LoRa/4G, syncing telemetry and models when bandwidth allows.

Defense

Air-gapped clusters with sealed secrets, signed supply chain, and disconnected lifecycle. No phone-home.

Healthcare

On-premise clinical workloads with isolation between patient data and shared services. HIPAA-compatible posture.

ASRS / Logistics

Real-time control loops co-located with robots and conveyors. Sub-millisecond local decisions, eventual cloud sync.

Hospitality

Per-property runtime for POS, IoT, and guest services. Each hotel keeps operating during ISP outages.

POSTURE

Security & Compliance

- Immutable base image** signed, read-only, verified at boot.
- Zero standing SSH** no shell on the node; all changes via signed manifests.
- Sealed secrets** Vault-backed identity, sealed at rest, never leaving the site.
- Supply chain** SBOM, cosign signatures, Kyverno admission policies.
- Runtime detection** Falco and Tetragon eBPF sensors on every node.
- mTLS everywhere** control and data plane authenticated end to end.

HOW A FLEET IS RUN

Operating Model

One platform team operates the entire estate from Pocteo Platform. There is no per-site tooling, no SSH bastion, no manual patching. New sites are provisioned by powering on hardware that PXE-boots the signed KEOS image and registers itself to the manifest.

- Day 0** bare metal boots KEOS, joins the fleet, applies the manifest.
- Day 1** workloads, networking, storage, observability arrive declaratively.
- Day N** OS and workload upgrades roll wave by wave with automatic rollback.

WHAT KEOS DELIVERS

The Promise

Operate ten thousand sites with the same ease and simplicity as managing one while guaranteeing they never stop running.

Contact

Pocteo Platform <https://pocteo.tn> hello@pocteo.tn