

UIS Cloud Product Brief

IoT / Edge Platform



Powered by **DaoCloud**

EU 8-Pillar Sovereign · AI Conformance · Gartner · Forrester

Executive Summary

Regulated industries are deploying tens of thousands of edge nodes — at factory floors, hospital sites, energy substations, and retail branches — and they face an immovable constraint: data cannot leave a controlled, sovereign boundary. While global hyperscalers offer 'sovereign regions,' they remain subject to extraterritorial data access mandates (such as the U.S. CLOUD Act) that create an inherent conflict with local residency laws. We eliminate this jurisdictional risk entirely.

Our IoT / Edge Platform is a cloud-edge integrated distributed application platform built on KubeEdge — a Kubernetes-native architecture that delivers decentralized control-plane autonomy to the edge. This ensures your critical infrastructure—whether in a remote oil field or a secure hospital wing—remains fully operational and locally manageable during total backhaul disconnection or network isolation.

Engineered for Jurisdictional Immunity, our architecture adheres to the EU 8-Pillar Sovereignty Framework by design. We provide native 'Audit-by-Default' capabilities, ensuring that data provenance and processing never exit your defined regulatory boundary.

For organizations where the Edge is the Compliance Frontier, our platform transforms regulatory burden into a competitive advantage.

It is equally well suited for industry solution providers building sovereign edge applications for regulated markets.

The Challenges You Are Facing

Sound familiar?

Your edge estate is growing. Your regulatory obligations are intensifying. Your current infrastructure was not designed for both at once.

Data Sovereignty Exposure

Cloud-connected edge nodes push telemetry, logs, and inference data to hyperscaler regions outside your regulatory jurisdiction. Every audit cycle, this is a finding.

Offline Node Failures

When WAN connectivity drops, your edge applications stop. Downtime at a substation, a clinic, or a production line is not theoretical — it is measured in euros and regulatory notices.

Heterogeneous Device Sprawl

You manage edge nodes from five vendors, on three operating systems, with four management consoles. Onboarding a new site takes weeks — which means every planned expansion carries a field-ops cost your budget did not anticipate, and every new node added to a fragmented estate is another endpoint your security team cannot uniformly audit.

Cloud-Heavy AI Inference

Model inference routed back to centralised cloud adds measurable latency, consumes bandwidth, and creates data-egress risk for sensitive operational data.

Operational Cost Creep

Per-device licensing from hyperscalers scales linearly with your estate. At 10,000 nodes, the economics collapse.

What Our Platform Delivers

A single, Kubernetes-native control plane that runs from your cloud — or your on-premises management cluster — down to every edge node, every device, and every AI inference workload you operate. Designed for the edge conditions that your production environments actually face.

Edge Node Onboarding & Lifecycle Management

Weeks-long site onboarding is a field-ops budget problem and a security audit gap.

Zero-touch provisioning brings a new edge node from registration to managed, policy-enforced, auditable state in minutes — from a single console, regardless of vendor or OS. Every node in your estate is uniformly managed from Day 1.

Device Connectivity & Protocol Normalisation

Connect OT and IT devices using standard industrial protocols without complex protocol gateways. Eliminate integration overhead across heterogeneous environments.

Offline Autonomy & Local Execution

Edge nodes continue executing applications, enforcing policies, and persisting data when cloud connectivity is unavailable. Your operations do not stop because your WAN does.

Cloud-Edge & Edge-Edge Messaging

Reliable, encrypted, ordered message delivery between cloud and edge — and between edge nodes themselves. Data synchronises automatically on reconnect.

Edge Application Deployment & Scheduling

Deploy containerised applications to any edge node or fleet using Kubernetes-native scheduling. Manage application versions and updates centrally across your entire edge estate.

Built-in Edge AI Inference

Run validated AI/ML models at the edge — computer vision, anomaly detection, predictive maintenance — without routing sensitive data to a cloud inference endpoint.

Sovereignty: The EU 8 Pillars

❗ At the edge, sovereignty is harder to maintain and easier to violate. A cloud-connected edge node that pushes telemetry to a non-sovereign region is a sovereignty breach at every polling interval. A management console hosted outside your jurisdiction means your operational decisions can be subject to foreign law. UIS Cloud's IoT / Edge Platform extends all 8 pillars of EU sovereignty to every node in your estate – from the management cluster to the last-mile device.

1

Strategic Sovereignty (15%)

Definition: Retaining unimpeded, autonomous decision-making authority over the digital future.

UIS: Enables sovereign control over strategic direction and risk acceptance.

2

Legal & Jurisdictional Sovereignty (10%)

Definition: Exclusive governance of systems and data by European law.

UIS : Enables full legal non-extraterritorial enforcement.

3

Data and AI Sovereignty (10%)

Definition: Complete ownership and control over data, models, and insights.

UIS: Enables customer-managed encryption keys, audit of software stack, and ownership of data/models.

4

Operational Sovereignty (15%)

Definition: Autonomous capability to operate, manage, and maintain digital infrastructure.

UIS: Allows transfer and retention of essential technical know-how.

5

Supply-Chain Sovereignty (20%)

Definition: Resilient, diversified, and vendor-neutral technology sourcing.

UIS: Enables vendor-agnostic design and reduced dependency on single sources.

6

Technology Sovereignty (15%)

Definition: Mastery and control over critical technology stacks and platforms.

UIS: Enables adoption of open, auditable, and verifiable technologies.

7

Security & Compliance Sovereignty (10%)

Definition: Independent cybersecurity capabilities under domestic regulations.

UIS Enables robust defense mechanisms and sovereign compliance audits.

8

Environmental Sustainability (5%)

Definition: Sustainable and efficient digital operations aligned with climate goals.

UIS: Enables eco-friendly and optimized infrastructure.

Built for Regulated Industries

Sector	Deployment Pattern	Sovereignty Requirement
Utilities / Energy	Substation edge nodes with offline autonomy; SCADA data never leaves site boundary	NIS2 operational continuity + data residency ✓
Healthcare	Clinical edge AI inference for imaging analysis without PHI leaving hospital network	GDPR Article 9 sensitive data + EU AI Act compliance ✓
Financial Services	ATM / branch edge with local transaction processing and fraud detection at node	DORA resilience + PCI-DSS data control ✓
Smart Manufacturing	OT/IT convergence on factory floor; predictive maintenance AI at machine level	Industrial IP protection + NIS2 OT segmentation ✓
Smart City	Distributed edge nodes across transport, lighting, and public safety infrastructure; real-time event processing at city scale	Low-latency operational data + data residency ✓
Retail	In-store edge nodes for inventory management, customer analytics, and POS resilience with offline autonomy	PCI-DSS data control + offline continuity ✓

Outcomes You Can Take to Your Board



Reduce Operational Cost

Meaningful reduction in edge infrastructure OpEx through unified management and zero-touch provisioning.



Pass Your Next Audit

8-Pillar Sovereignty certification means your edge estate is compliant by architecture, not by exception.



Respond in Milliseconds

Edge-local AI inference and application execution significantly reduces cloud round-trip latency for time-critical operations.



Zero Data Egress Risk

Operational data, telemetry, and AI outputs never leave your defined boundary. Provable. Auditable.



Stay Up When WAN Goes Down

Offline-first architecture means your nodes execute autonomously. Reconnect when ready — no data loss.



No Vendor Lock-In

Open CNCF KubeEdge core. Portable workloads. Walk away without re-engineering if you ever need to. The Next Step

Ready to Operate at the Edge — Without Compromising Sovereignty? You have built your compliance frameworks with precision. Your edge infrastructure should match that standard. Our team works exclusively with regulated industries — banking, healthcare, utilities, and critical national infrastructure — and we bring 1000+ reference implementations and recognition from Gartner and Forrester to every engagement.

Some of our Clients

STATE GRID



CSCN



Book a Sovereign Edge Architecture Review

01

Sovereign Edge Architecture Review

A 60-minute session dedicated to mapping your current infrastructure against stringent sovereignty requirements. We'll identify critical gaps and opportunities for immediate improvement.

02

Reference Proof of Concept

Deploy our platform on your existing infrastructure with a proven use case. We'll match you with a relevant reference customer from your sector to demonstrate real-world impact and compliance.

03

Production Deployment

Achieve a full sovereign edge estate that is compliant, auditable, and operationally independent. Our solutions ensure seamless integration and long-term security, giving you peace of mind.