

UIS Cloud Product Brief

Multi-Cloud Application Platform

The Sovereign Multi-Cloud Operating System for Cloud-Native Enterprises



Powered by **DaoCloud**

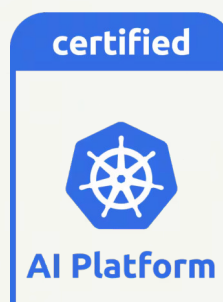
EU 8-Pillar Sovereign · AI Conformance · Gartner · Forrester

Executive Summary

Enterprise infrastructure is no longer a single cloud. It is a federation of competing clouds, private data centres, and edge clusters – each carrying its own compliance obligations, cost profile, and SLA commitment. Managing that complexity without sacrificing control is the defining infrastructure challenge of this decade. It is made exponentially harder when your sector – financial services, healthcare, critical infrastructure, public administration – demands that sovereignty is not a marketing claim but a legally defensible, independently verified posture.

UIS Cloud's Multi-Cloud Application Platform is built for exactly that world. Delivered as the multi-cloud management module of DCE 5.0, it integrates natively with the full UIS Cloud container platform – or deploys independently for organisations adopting a modular path to cloud-native infrastructure. Recognised by Gartner and Forrester, it is the enterprise-grade, Kubernetes-native multi-cloud operating system that combines true cross-cloud workload orchestration with EU Full 8-Pillar Sovereignty – independently certified, not self-declared. For regulated enterprises, this is the difference between a tool and a trust framework.

AI-Conformant Vendors Globally
Among the first 14 worldwide



Pain Points Solved

We hear the same questions from regulated enterprises across every sector. These are not theoretical concerns — they are live compliance and operational risks.



We operate across five clouds. We have no unified control plane.

Single-pane-of-glass management for all clusters — public, private, and edge — with Kubernetes-native APIs. No vendor lock-in.



Our regulator requires data sovereignty we cannot currently demonstrate.

Your regulator does not accept 'we use a European region' as a sovereignty answer. EU Full 8-Pillar Sovereignty certification covers data residency, access control, audit trail, portability, encryption, legal jurisdiction, operational independence, and supply chain sovereignty — every dimension independently verified, not self-declared. Present it to your auditor on day one.



We cannot afford application downtime. Our SLA is contractual.

A contractual SLA you cannot technically guarantee is a liability, not a commitment. Multi-region high availability with automatic cross-cluster failover means your SLA is backed by architecture, not by a recovery procedure someone runs manually at 2am. Grey release and canary deployment across all clouds reduce release risk — and the regulatory change-management documentation that comes with it — to near-zero.



Cloud costs are spiralling. We cannot see where the waste is.

Uncontrolled multi-cloud spend is a CFO problem and a FinOps gap. Real-time cost visibility by cluster, cloud, and workload — with cost-aware scheduling that automatically places workloads on the most economical compliant compute — converts cloud spend from a line item you cannot explain into one you can defend to your board. Validated deployments have achieved 45% cloud cost reduction through intelligent cross-cloud resource scheduling.



We are locked into our current cloud vendor. Migration is terrifying.

Vendor lock-in is not just an operational risk — it is a supply-chain sovereignty failure under Pillar 5 of the EU framework. Kubernetes-native API compatibility means zero-modification migration from single-cluster to multi-cloud. No proprietary format dependency. No re-architecture. If you need to move a workload away from a cloud provider — for cost, compliance, or geopolitical reasons — you can do it without rebuilding.



We rely on one cloud provider for 80% of our workloads. Our regulator is asking about concentration risk

DORA Article 26 requires financial institutions to manage ICT third-party concentration risk — over-reliance on a single cloud provider is a named regulatory obligation, not just an operational preference. Multi-Cloud Application Platform distributes workloads across providers with policy-governed placement, giving you a demonstrable, auditable answer to the concentration risk question before your supervisor asks it.

Sovereignty: The EU 8 Pillars

Most vendors offer 'data sovereignty.' In a multi-cloud estate, that is the easiest pillar to compromise and the hardest to prove. UIS Cloud delivers EU Full 8-Pillar Sovereignty across every cloud, every cluster, and every edge node in your estate — independently verified, not self-declared. In a federated environment, every pillar is harder to maintain: legal jurisdiction can fragment across providers, supply-chain sovereignty requires every vendor in the chain to be assessed, and operational independence must hold even when a provider goes down.

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.

Core Capabilities

Every capability is designed to be deployable in a regulated environment from day one — no sovereignty retrofitting required.

Unified Deployment

Deploy once across any cloud, any region, any cluster — public, private, or edge. Karmada-based federation provides Kubernetes-native API compatibility — zero modification to existing workloads. No dependency on cluster location. No commercial vendor lock-in.

Cross-Cloud Auto-Scaling

Burst elastically across clusters and cloud providers based on real-time demand. Cost-aware scheduling ensures you always use the most economical compute available.

Grey & Canary Releases

Multi-cloud canary and grey-release pipelines reduce release risk across all clusters simultaneously. Roll back in seconds without cross-cloud coordination overhead.

Multi-Region HA & Failover

Built-in dual-active city architecture, two-city three-centre DR, and cross-region disaster recovery — out of the box, not as an add-on. SLA contractual commitments become achievable.

Cost Intelligence

Multi-cloud spend without visibility is undefendable to a CFO and unexplainable to an auditor asked to review cloud concentration risk. Real-time spend visibility by cluster, cloud, and workload — with automated cost-aware scheduling — gives your FinOps team the data and your board the answer. Validated deployments have achieved 45% cloud cost reduction through intelligent cross-cloud resource scheduling.

Open & Neutral by Design

No proprietary lock-in. Jointly governed by contributors from internet, finance, manufacturing, telecommunications, and cloud industries. Freedom to migrate, extend, and audit every layer of the stack.

Hyperscale-Proven Reliability

Tested at extreme scale, it reliably supports large clusters, several hundred thousand nodes and 1M+ pods — enabling platform teams to run global multi-cloud workloads at hyperscale with full reliability and control.

Intelligent Scheduling Policies

Karmada-native PropagationPolicy and OverridePolicy APIs give platform teams precise control over where workloads run and how they are configured per cluster — automatically adapting image registries, storage classes, and resource constraints by region and cloud vendor. No manual per-cluster configuration required.

Why UIS Cloud— and Why Now

The regulated world is tightening. NIS2, DORA, GDPR enforcement, and sector-specific mandates from the EBA and ECB are converting sovereignty from a nice-to-have into a board-level risk item. The window to act proactively — before your regulator asks — is narrowing.

UIS Cloud has spent many years building infrastructure that regulated enterprises can actually use — not retrofitted for compliance, but designed from the first commit for sovereignty, portability, and verifiability. We are among the first 14 globally AI-conformant infrastructure vendors and we carry the credentials to prove it: Gartner recognition, Forrester validation, and 1000+ enterprise references across financial services, healthcare, telecommunications, energy/utilities, public administration, and high-growth internet and SaaS businesses operating at cloud-native scale.

You do not need to choose between cloud agility and regulatory compliance. With the UIS Cloud Multi-Cloud Application Platform, you get both — and you get them in a form your auditor will recognise, your regulator will accept, and your board will thank you for.

14

AI-Conformant Vendors Globally

Among the first 14 worldwide

1000+

Global Enterprise References

Finance, telco, healthcare, and public sector — at scale, in production.

8

EU Sovereignty Pillars

Every pillar. Ready for your next audit.



Contact [UIScloud.io](https://uiscloud.io) to schedule your Multi-Cloud platform consultation.