

OcientAIQ for IoT and Edge Operations

Tens of millions of devices. No sampling. Deeper insight into usage and capacity.

The Problem

Connected vehicles, smart meters, industrial sensors, and consumer IoT devices are adding billions of endpoints to CSP networks—each with its own signaling behavior, billing relationship, SLA expectation, and security exposure. For CSPs, this creates a shared challenge for IoT business leaders and network-operations teams alike: how to manage massive, high-cardinality device telemetry without letting infrastructure cost scale linearly with traffic growth.

The usual answer is to aggregate or sample the data, but that is where the most valuable signals disappear. Device anomalies, connectivity faults, security risks, and predictive-maintenance indicators often live in the long tail of the event distribution. Once that detail is averaged away, CSPs can no longer answer the questions that matter most: Which devices are trending toward failure? What is the leading indicator? And how can teams act before fleet-wide issues become service-impacting events?

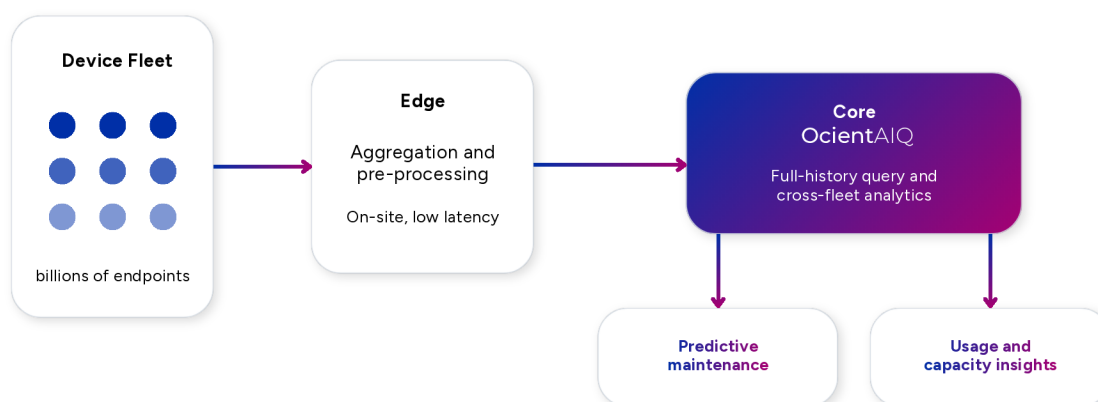
The Solution

OcientAIQ™ for IoT and Edge Operations turns full-fidelity telemetry into operational intelligence. Instead of sampling, aggregating, or overwriting device and connectivity data, OcientAIQ retains the complete event history — preserving the long-tail signals that matter.

Predictive-maintenance models learn from years of actual device behavior. Fault detection runs against the same unsampled record the device generated. Teams investigate anomalies, service issues, and emerging risks with the context needed to act.

OcientAIQ connects device identity, SIM relationships, billing accounts, network-element assignments, firmware versions, and other operational context across fragmented datasets. With lineage attached to every result, the output holds up in high-stakes workflows — from SLA reporting and regulatory audits to fraud investigations and customer escalations.

From device fleet to usage and capacity insights



Full-fidelity device telemetry retained without sampling

What Full Fidelity Unlocks

Device-fleet observability. A single view of device health, connectivity state, and usage history across the full fleet — no aggregation loss, no blind spots.

SIM and connectivity lifecycle analytics. SIM-swap and account-takeover patterns identified across device identity, signaling, and billing records — with full lifecycle lineage for every SIM.

Anomaly and fault detection. Sub-minute time-to-insight across the live edge and the full event history in the same query, so teams act on current state with long-horizon context.

Predictive maintenance. Models trained on years of actual device behavior surface failure candidates before they become service events, not after.

Edge-to-core correlation. Device, edge, and core telemetry on one governed store, so connectivity faults trace back to RAN and transport events without a separate engineering project.

IoT-segment SLA evidence and reporting. Continuous SLA measurement against committed service tiers, with dispute-ready reporting and lineage traceable to source records.

What Makes OcientAIQ Different

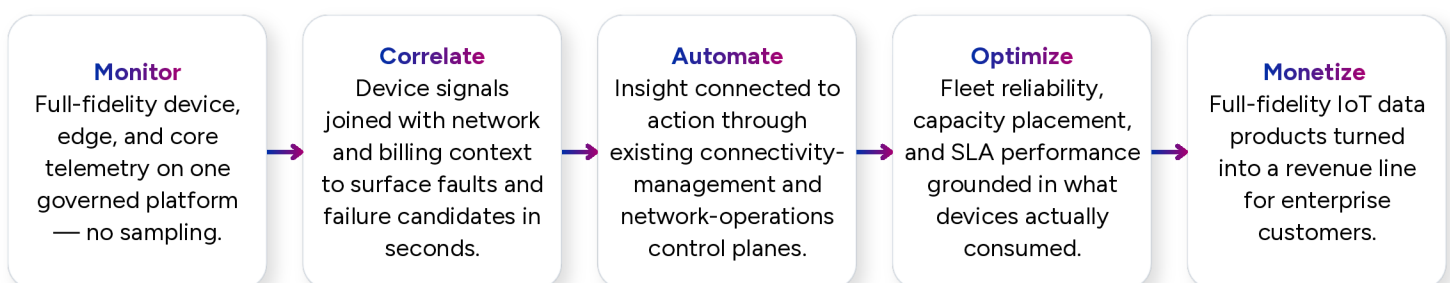
Per-domain tools stay in place. OcientAIQ is not a rip-and-replace. It sits underneath tools already running, preserving existing investments while delivering the joined view existing tools cannot achieve individually.

Connects to the AI ecosystems you already run. OcientAIQ builds and maintains the structured context your agents need. Bring Claude, GPT, Gemini, or Llama and put them to work on production analytics, not demos.

Predictable economics. No query tax. Infrastructure TCO reduction of 50-90% versus legacy stacks. Each additional solution area lands at a fraction of the marginal cost of the first.

Sovereign by design. Runs on prem, hybrid, or air-gapped. SAML/OIDC zero trust. No data movement.

From Device to Revenue



See what full fidelity changes for your fleet.