TARA
INNOVA

Oasis

From Unmanaged Streams to Governed Workflows — Secure Integration Streaming

The Challenge

IoT sensors push telemetry. Industrial controllers exchange commands. Services call APIs. Most of this traffic runs unmanaged — no visibility into what's flowing, no control over how it behaves, no integration with business processes. Firewalls see ports, not protocols. API gateways expect REST, not industrial controllers. Integration middleware connects systems but ignores security.

The Solution

Oasis is an integration streaming platform that connects IoT devices, machines, and services into managed, observable, workflow-integrated data streams. It sits at the boundary between unmanaged and managed — applying enterprise-grade security governance to every integration route.

Key Capabilities

- **Connect** — 300+ protocol connectors covering IoT, industrial, enterprise, and cloud protocols
- **Govern** — Channel and endpoint security on every route: device identity, rate control, payload validation, access policies
- **Transform** — Schema mapping, format conversion, enrichment, and filtering. Raw telemetry becomes structured business data
- **Route** — Delivery guarantees to data warehouses, SIEMs, dashboards, workflow engines with independent policies per destination
- **Observe** — Every message tracked, every decision logged. Real-time metrics on throughput, rejection rates, and latency with anomaly alerting

Deployment Modes

Mode	Description
Gateway	Inline integration and enforcement at network boundaries
Sidecar	Per-service deployment in containerized environments
Agent	Lightweight agent on constrained devices or edge nodes
Cloud Proxy	Managed endpoint for external integrations and SaaS platforms

Use Cases

- **IoT Fleet Management** — Normalize telemetry from heterogeneous devices, enforce identity, route to analytics platforms
- **Industrial Data Integration** — Bridge IT/OT with protocol mediation and OT-grade security governance
- **Service Orchestration** — Rate limits, API contract validation, circuit breaking across microservices

- **Compliance Pipelines** — Generate audit-grade evidence from operational streams mapped to NIS2, DORA, IEC 62443

Why Oasis

- **Security Built In** — Governance built into the integration layer, not bolted on afterward.
- **Universal Connectivity** — 300+ connectors. If your device or system can send data, Oasis can ingest it.
- **Full Audit Trail** — Every message from ingest to delivery traced for compliance evidence.
- **IT/OT Bridge** — Bridges the IT/OT divide without exposing either side.