Catalyst

Orchestrate the Mission.

Power the Network.

Product White Paper

O R B I S

impact@orbisops.com

Executive Summary

Modern security and defense operations depend on data flowing between systems, organizations, and partners — reliably, securely, and at mission speed. But the architectures connecting those systems were not designed for the operational tempo or the trust complexity that today's environments demand.

Most organizations have capable systems. What they lack is a secure, governed way to connect them — one that doesn't require surrendering data ownership, consolidating into a single platform, or building fragile point-to-point integrations that break every time a new partner, sensor, or mission requirement is introduced.

Orbis Catalyst is a secure data mesh platform that unifies fragmented data across systems, sensors, and decision-makers — without relocating it. Built on Zero Trust Architecture with post-quantum encryption, Catalyst delivers real-time data access and partner-specific visibility across federated environments, making security a feature of the architecture rather than a barrier to operations.

Catalyst is the implementation framework that makes the Common Operational Data Layer (CODL) operational. Where CODL defines the standard, Catalyst delivers the running system.

The organization that can connect its data securely and share it selectively — without rebuilding its infrastructure each time — holds a structural advantage over one that cannot.

1. The Integration Problem at Scale

Security organizations have spent decades building capable systems: surveillance platforms, biometric repositories, intelligence analysis tools, border monitoring networks, command-and-control environments. The investment is real. The problem is that each system was procured independently — different directorate, different contract, different vendor — and connects to others through custom interfaces built one at a time.

This point-to-point integration model does not scale. An enterprise with twenty systems and forty custom links does not become more capable when it adds a twenty-first system. It becomes harder to maintain. Every modernization effort risks breaking existing connections. Every new acquisition creates more technical debt.

The problem intensifies when data must cross organizational boundaries. Coalition operations, intelligence-sharing agreements, interagency task forces, and multinational partnerships all require controlled data exchange between entities that maintain separate systems, separate classification authorities, and separate governance frameworks. Without a structured mechanism for managing these exchanges, data moves informally — manually downgraded, duplicated across channels, or simply withheld because the sharing infrastructure doesn't exist.

AI has been deployed as a partial solution, and many implementations are capable within their own data silos. But a model trained on one agency's data cannot correlate across another's. An inference service operating on inconsistent, ungoverned inputs produces unreliable outputs. AI does not fix an architecture problem — it inherits one.

2. What Catalyst Is

Catalyst is a secure, virtual data mesh that connects systems, sensors, and decision-makers through a unified fabric — without requiring data to be relocated, consolidated, or duplicated. It gives organizations precise control over who can see and use what data, when, and how.

It is not a database. It is not a centralized repository. It is not a platform that requires agencies to surrender ownership of their data or migrate off existing systems. Catalyst imposes a common integration standard — not a common system — and provides the security, governance, and connectivity infrastructure that makes that standard operational.

Federated Security and Access Control

Catalyst is built on the Zanzibar authentication model, delivering fine-grained, role-based access control at global scale. Data owners define access policies at the most granular level required — by classification, by partner, by mission, by time window — and those policies are enforced automatically, at machine speed, across every interaction. Security decisions are not made informally or after the fact. They are architectural properties of the system.

Unified Data Fabric

Data silos exist because integration is expensive, fragile, and slow. Catalyst eliminates them by standardizing data access through a GraphQL federation gateway. Systems that previously required custom bilateral integrations — each with its own adapter, its own format mapping, its own maintenance cycle — connect through a single governed interface. The result is seamless integration without duplication, without delay, and without the compounding technical debt of point-to-point connections.

Post-Quantum Encryption

Catalyst employs Kyber PQ-TLS to ensure resilient, future-proof data transport — even in contested environments where adversaries may be harvesting encrypted traffic for future decryption. Security is not an afterthought applied at the perimeter. It is embedded at the data level, ensuring that information remains protected in transit, at rest, and across every trust boundary it crosses.

Configurable Data Catalog

Mission data within the Catalyst fabric is indexed, discoverable, and secured through a dynamic catalog designed to scale with operations — regardless of data format or location. Analysts and systems can discover what data is available, understand its provenance and classification, and access it through governed channels without knowing or caring where the underlying source system resides.

Tool-Neutral Integration

Catalyst fits into the customer's existing technology stack rather than replacing it. Partners use their preferred tools — analytic platforms, visualization environments, reporting systems — while participating fully in a shared mission ecosystem through the Catalyst fabric. Adoption does not require wholesale tool replacement. It requires connecting what already exists.

3. Deployable at Any Scale

Catalyst is designed to operate at the scale the mission requires — from a single organization to a multinational coalition.

Single Agency

An individual organization — a military service, intelligence directorate, border authority, or law enforcement agency — can deploy Catalyst internally to unify its own fragmented systems. At this level, Catalyst standardizes internal data access, enforces consistent security policies across systems, and creates the governed data foundation on which agency-wide AI and analytics can operate reliably.

Federated Multi-Agency

Where two or more organizations choose to exchange data, their Catalyst instances federate through shared identity trust, cross-domain filtering, and policy-controlled release. Each agency retains full ownership of its data and defines what it makes available to others. Interoperability comes from shared standards and explicit policy — not from transferring data ownership or ceding operational control.

Coalition and Multinational

For allied or partner nations operating in coalition environments, bilateral intelligence-sharing arrangements, or regional security frameworks, Catalyst brings attribute-based access controls and cryptographic identity models that allow data to flow across national boundaries without surrendering sovereignty over release decisions. Each nation maintains its own Catalyst instance, its own classification authority, and its own policy enforcement. Federation between partners is governed by explicit trust agreements mapped to technical controls — a nation sharing with a Five Eyes ally operates under one release policy while the same nation sharing with a newer bilateral partner operates under another, and both coexist within the same architecture.

4. Built for Innovation

Catalyst is not a static platform. It is designed to accommodate the operational changes that security environments demand.

Whether onboarding a new sensor, linking a foreign partner, or deploying a tactical edge node in a disconnected environment, Catalyst makes the process fast, secure, and repeatable. New data sources connect through standardized adapters. New partners are onboarded through policy configuration rather than custom engineering. Edge nodes operate autonomously under degraded connectivity, synchronize securely when connectivity is restored, and maintain compartment isolation throughout.

This matters because the organizations that adopt Catalyst are not operating in stable, predictable environments. They are operating in environments where the mission, the coalition, and the threat change — and the data architecture must change with them without a redesign cycle each time.

5. How Catalyst Fits the Operational Stack

Catalyst is the secure infrastructure and governance layer within the Orbis product family.

Orbis Pulse, the Data-as-a-Service platform, acquires and curates DIGINT data from across the vendor landscape — ingesting, normalizing, and enriching it into unified, schema-enforced datasets. Catalyst provides the secure delivery mechanism, ensuring that Pulse-curated data reaches authorized consumers through governed channels with full access control and audit traceability.

Orbis Discovery, the analyst intelligence workbench, is the operational surface where analysts search, synthesize, and produce intelligence. Discovery operates on data that Pulse has curated and Catalyst has secured — giving analysts confidence that what they are working with is current, complete, and appropriately governed.

The three products form a complete operational stack. Pulse handles data supply. Catalyst handles data governance and secure connectivity. Discovery handles intelligence production. Each can be adopted independently, but together they deliver an end-to-end capability from raw data to finished intelligence — secured and governed at every layer.

6. The Strategic Case

The argument for Catalyst is not primarily about technology. It is about decision speed.

Organizations that can connect their data across systems, share selectively with partners, and maintain security without creating operational bottlenecks will consistently outperform those that cannot. Every day spent building a custom integration, negotiating a manual data-sharing workaround, or waiting for a cross-domain solution to be provisioned is a day that the adversary is not waiting.

Catalyst reduces integration cost by replacing dozens of bilateral connections with a single governed fabric. It reduces vendor dependency by providing a tool-neutral architecture that works with any system the customer already operates. It enables structured collaboration between organizations that currently share data informally or not at all. And it creates the conditions under which AI can be deployed at scale — with consistent inputs, auditable lineage, and controlled access.

These outcomes follow directly from replacing architectural fragmentation with architectural discipline. Catalyst does not ask organizations to abandon their existing systems. It asks them to connect those systems through a standard that is secure by design, governed by policy, and built to adapt as the mission evolves.

Conclusion

Orbis Catalyst is not a technology acquisition. It is a decision about how a security enterprise governs its most operationally critical function: the movement of information between the people and systems that depend on it.

It can start within a single agency, federate across partner organizations, and scale to multinational coalition operations — each step building on the last, each step delivering measurable value before the next begins. It does not require a large-scale migration, a forced consolidation, or the displacement of existing systems. It requires connecting them through a secure, governed fabric and holding to that standard.

Catalyst makes it deployable. CODL makes it durable. Together, they give organizations the architectural foundation to act on what they know — when it matters.

The organization that governs how its data moves governs how fast it can act. In security environments, speed of action is the advantage.