



OPC FOUNDATION + XQ: FROM INTEROPERABLE INDUSTRIAL DATA TO TRUSTED DATA

Zer Trust Data

Executive Summary

The OPC Foundation's mission is to deliver vendor-neutral, secure, and reliable interoperability. Through initiatives spanning edge-to-cloud communications, agentic AI integration, digital twins, and Digital Product Passports (DPPs), OPC UA has established itself as the global standard for making industrial data readable across disparate ecosystems.

As industrial data moves beyond the traditional operational technology (OT) network perimeter into multicloud environments and third-party AI systems, a critical gap emerges:

- **Network-level and session-based security models do not maintain persistent control over data once it leaves the transport layer.**

XQ complements OPC UA by providing a data-centric governance and cryptographic control layer.

While OPC UA ensures data is interoperable, XQ ensures that data remains persistently controllable, traceable, and policy-bound wherever it travels.

Strategic Fit & Positioning

"OPC UA makes industrial data interoperable. XQ makes that data persistently controllable."

Positioning XQ as a complementary governance extension—rather than an OT protocol security alternative—honors OPC UA's established security framework (authentication, encryption, and session integrity) while addressing the next lifecycle challenge: **data sovereignty post-delivery**.





Functional Mapping: OPC UA + XQ

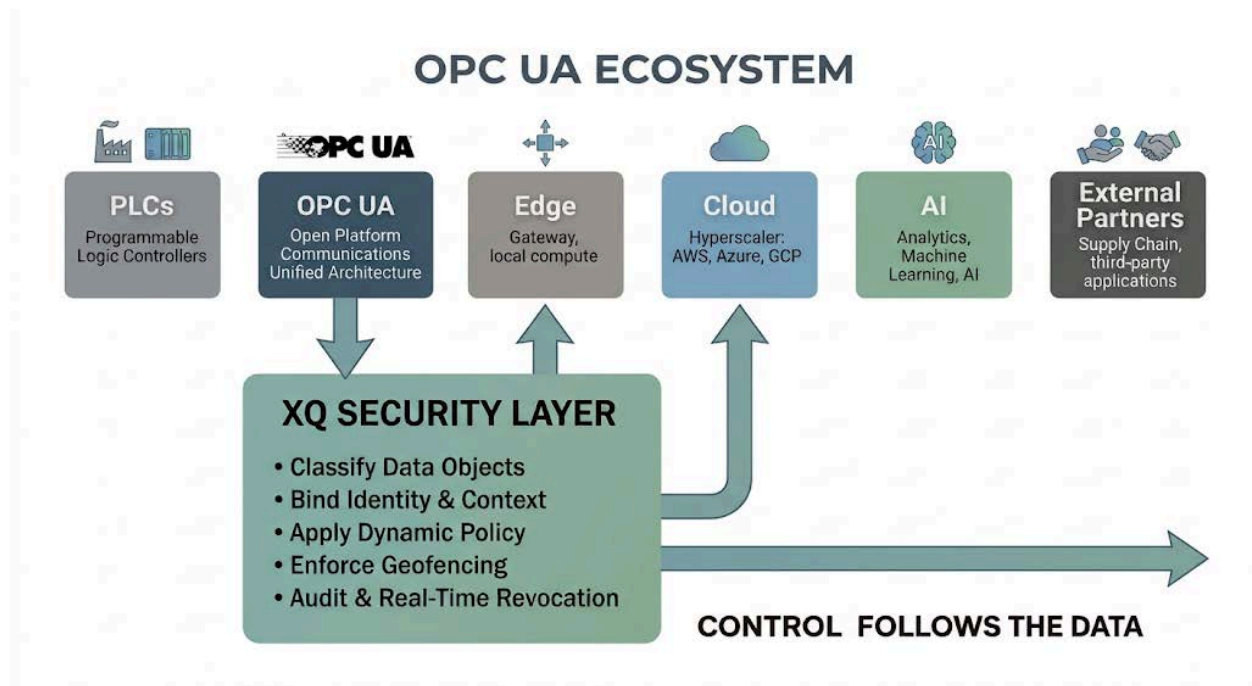
1. Providing Context to Fortinet

OPC Foundation Objective	OPC UA Delivers	XQ Adds
Interoperability	Standardized protocol & information models	Portable, data-centric security policies
Secure Communications	Transport encryption, mutual authentication	Persistent cryptographic control after session termination
Edge-to-Cloud	Standardized data movement across boundaries	Data-level sovereignty across multi-tenant clouds & jurisdictions
Industrial AI	Semantically structured, AI-ready assets	Policy-driven data authorization for autonomous AI agents
Digital Twins & DPPs	Standardized asset representations	Dynamic, selective attribute disclosure based on recipient identity
Cross-Company Exchange	Interoperable information exchange	Cryptographically enforced access rights without network access
OT/IT Convergence	Unified information layer	Zero Trust data governance spanning OT, IT, and external partners





Architectural Blueprint



Key Strategic Use Cases

1. Persistent Control Beyond Network Boundaries

When an OPC UA server publishes telemetry (e.g., `Turbine-17 / bearing_temp / 93°C`), transport security protects the data in transit. Once ingested into data lakes, edge caches, or third-party analytics platforms, XQ cryptographically binds access policies directly to the payload:

- **Asset:** Turbine-17
- **Classification:** Critical Infrastructure
- **Permitted Users:** Maintenance AI, Certified Engineers
- **Constraints:** US Jurisdiction Only | 30-Day Expiration | Non-Exportable





2. Multi-Cloud & Vendor-Neutral Sovereignty

XQ provides a unified policy and key management layer across heterogeneous cloud targets (AWS, Azure, private clouds) without forcing lock-in into cloud-native security silos. Data stored across disparate platforms remains encrypted under a single zero-trust policy model.

3. Granular Authorization for Agentic AI

As OPC UA standardizes Companion Specifications for AI agents, XQ provides object-level entitlement management. Autonomous agents receive access only to the precise data fields required for execution, preventing accidental exposure of IP, recipes, or regulatory-controlled attributes.

4. Differentiated Access for Digital Product Passports (DPPs)

A single OPC UA information model underlying a DPP can serve multiple stakeholders with tailored access views enforced via XQ encryption:

- **Consumers:** Sustainability & provenance metrics
- **Regulators:** Compliance and safety logs
- **Suppliers & OEMs:** Proprietary engineering and maintenance specifications

Proposed Initiative: OPC UA "Trusted Data" Extension

XQ can partner with the OPC Foundation to introduce a working group or joint initiative focused on **Data Sovereignty for Industrial AI & Cloud Infrastructure**.

- **Core Mission:** Define standardized mechanisms for binding persistent policy, cryptographic protection, and auditability to OPC UA information models as they cross organizational and jurisdictional boundaries.

