PARTNER SOLUTION BRIEF

Industrial Defender + Waterfall Security Solutions

Hardware-Enforced OT Security Data Transmission — Now Officially Supported in v8.2

Certified Integration | Critical Infrastructure | NERC CIP | TSA | NIS2

THE CHALLENGE

The OT Visibility Dilemma

Critical infrastructure organizations face a fundamental tension:

Security and compliance teams need continuous visibility into OT assets, configurations, and vulnerabilities – but operational and regulatory requirements prohibit any bidirectional network connectivity into control systems.

Firewalls, jump servers, and software-enforced controls attempt to bridge this gap, but each introduces its own attack surface.

Misconfigured rules, compromised credentials, and vulnerable remote access tools have all contributed to real-world OT incidents. For organizations under *NERC CIP, TSA Security Directives, NIS2, and similar frameworks*, this gap between security necessity and architectural constraint is increasingly urgent. And increasingly audited.

THE JOINT SOLUTION

Where Waterfall Fits in the Architecture

Understanding this integration starts with knowing precisely where Waterfall sits in the Industrial Defender architecture.

JOINT SOLUTION BENEFITS

The Industrial Defender Collector (IDC) operates inside the OT network perimeter. It uses native OT protocols (Modbus, DNP3, S7, and others), SSH, and agentless methods to collect configuration data, security events, firmware versions, user accounts, and asset state from PLCs, RTUs, IEDs, HMIs, and other OT endpoints. The IDC has full, deep access to the OT environment by design.

The problem is the handoff: getting data from the IDC – inside the control network – out to the Industrial Defender Central Manager (IDCM) on the corporate network, without creating an inbound attack surface back into OT.

Waterfall's Unidirectional Security Gateway sits at exactly this boundary: between the IDC and the IDCM. It enforces hardware-level, one-way data transmission from OT to IT.

No return path exists. It is physically impossible for attack information to enter a protected network through a gateway.

This is what makes it stronger than any firewall or any software based defense.

As of Industrial Defender version 8.2, this integration is officially supported and validated, giving organizations a tested, auditable architecture they can specify in compliance documentation and procurement.

- ✓ **Official v8.2 Support**
- ✓ **Hardware-Enforced Boundary**
- ✓ **No Inbound Attack Surface**
- ✓ **IDC→IDCM Secure Handoff**
- ✓ **Full ID Active Collection Preserved**
- ✓ **Asset Inventory & Visibility**
- ✓ **Configuration Change Detection**
- ✓ **Vulnerability Monitoring**
- ✓ **Security Event Correlation**
- ✓ **NERC CIP Compliance Support**
- ✓ **TSA Directive Readiness**

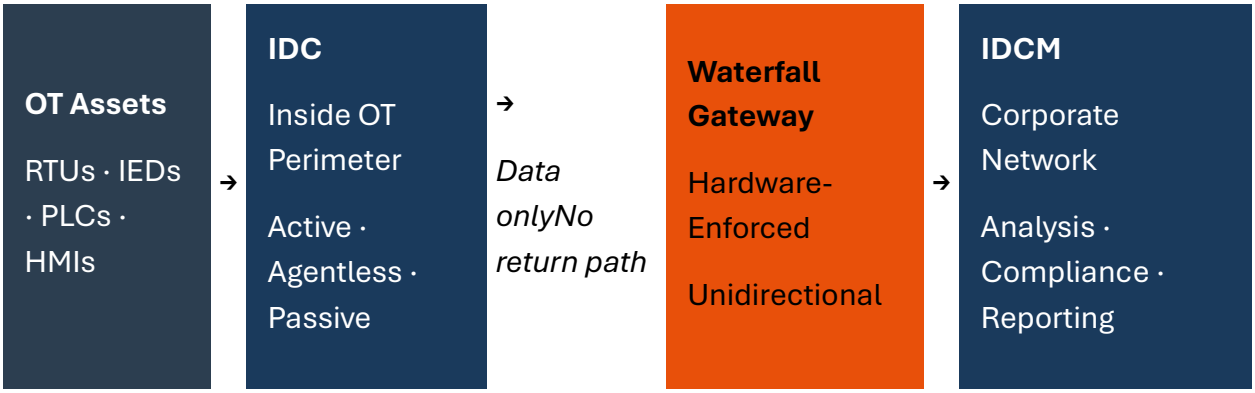
✓ **NIS2 / NIST Alignment**

✓ **Power Substation Protection**

✓ **Remote Site Architecture**

REFERENCE ARCHITECTURE

How the Integration Works



IDC — Inside OT Perimeter	Waterfall Gateway — The Boundary	IDCM — Corporate Network
Collects via active, agentless, and passive methods using native OT protocols. Operates within the control network security boundary.	Hardware-enforced one-way transmission from IDC to IDCM. No inbound communication possible. Physically cannot be misconfigured to allow return traffic.	Aggregates, correlates, and presents OT security data to enterprise teams. Full asset, compliance, and vulnerability picture — no OT access required.

SECURITY & COMPLIANCE OUTCOMES

What the IDCM Surfaces to Enterprise Teams

Once data crosses the Waterfall gateway, the IDCM delivers a unified OT security picture to security, compliance, and operations teams – without those teams ever needing access to the OT network:

- **Complete Asset Inventory** — Continuously updated registry of OT devices — firmware, hardware, vendor, model, and communication paths. A living record, not a one-time discovery snapshot.
- **Configuration Baselines & Change Detection** — Every change to ports, services, firewall rules, software, and user accounts is logged. Who changed it, when, and whether it deviated from the approved baseline.
- **Vulnerability Mapping** — Known CVEs and advisories correlated against your actual OT asset inventory. Exposure mapped to specific devices in your environment –= not generic advisories.
- **Security Event Correlation** — Events from the OT network correlated with configuration context. Analysts understand the why behind an alert, not just the what.
- **Compliance Evidence** — Structured reporting for NERC CIP (CIP-007, CIP-010, CIP-013), NIST CSF, NIS2, TSA Security Directives, and other frameworks. Audit-ready evidence, not just dashboards.

IDEAL USE CASES

Electric Utilities & Transmission Operators — NERC CIP

High-impact BES Cyber Systems require strict Electronic Security Perimeter controls under CIP-005. Power substations – often remotely located and architecturally isolated — are a primary deployment target for this integration. The Waterfall gateway satisfies unidirectional ESP requirements while enabling the continuous monitoring CIP-007, CIP-010, and CIP-013 demand. The v8.2 integration is tested and auditable.

Oil, Gas & Pipeline — TSA Security Directive Compliance

TSA Security Directives require continuous OT monitoring and anomaly detection capabilities. This architecture delivers both without introducing the remote-access risk profiles regulators are specifically targeting. Hardware-enforced boundaries satisfy the intent of the directives, not just the letter.

Centralized SOC with OT Visibility Requirements

Enterprise SOC teams need OT asset and security data without OT network access. Industrial Defender delivers a complete OT picture to the IDCM on the corporate network — analysts get what they need, and the OT network stays protected.

High-Consequence Environments Requiring Hardware Enforcement

For nuclear facilities, national infrastructure, and environments where software-based controls are architecturally unacceptable, hardware enforcement is the only valid answer. Waterfall's physical unidirectionality — not a software policy — makes this the right architecture for the highest-consequence deployments.

ABOUT THE PARTNERS

INDUSTRIAL DEFENDER

Since 2006, Industrial Defender has solved the challenge of safely collecting, monitoring, and managing OT asset data at scale. The platform covers OT asset management, vulnerability management, configuration and change management, policy compliance, and threat detection — purpose-built for complex industrial

WATERFALL SECURITY'S HARDWARE ENFORCED

Waterfall Security's hardware-enforced OT security solutions physically prevent all remote cyberattacks from reaching mission-critical networks, while simultaneously delivering real-time visibility and safe remote access. The

environments by engineers with decades of hands-on OT experience.

industrialdefender.com

result is fewer operational shutdowns, easier compliance, and confident digital transformation for the world's most important industries. Trusted at thousands of industrial sites worldwide since 2007.

waterfall-security.com

Schedule a Demo of the Joint Solution

1 (877) 943-3363 | info@industrialdefender.com | industrialdefender.com

Waterfall Security's hardware-enforced OT security solutions physically prevent all remote cyberattacks from reaching mission-critical networks, while simultaneously delivering real-time visibility and safe remote access. The result is fewer operational