DRAGOS

WHITEPAPER

Enhancing xOT Visibility: Achieving Full Situational Awareness Through Safe Active Discovery

Table of Contents

INTRODUCTION

Inherent Visibility Gaps in Extended OT (xOT) Environments

Operational technology environments have evolved significantly, becoming increasingly interconnected, digitalized, and complex. Today, those environments extend far beyond traditional PLCs and SCADA systems to include IoT sensors, IP cameras, HVAC controllers, badge readers, building management systems, and a growing class of edge and IT assets whose failure directly affects physical operations. Dragos refers to this expanded environment as extended operational technology, or xOT: any system that influences a physical process or drives a high-impact operational outcome.

With this expansion, the need for comprehensive visibility has never been more important. Effective management of cybersecurity risks, asset protection, regulatory compliance, and rapid incident response all depend on the ability to see across the entire xOT landscape.

Traditionally, passive monitoring has served as the foundation for visibility due to its inherent safety, minimal operational disruption, and continuous coverage. By passively capturing network data, organizations have established reliable baselines for asset behaviors, accurate inventories, threat detection, and compliance validation.

Despite these significant advantages, passive monitoring alone cannot always address every visibility requirement arising from unique operational challenges:

- **Assets that do not provide enough data:** Passive monitoring may yield basic information but will not always provide detailed information that we might be seeking down to the firmware or ladder logic.
- **Dormant or rarely communicating devices:** Many xOT assets such as environmental sensors, backup controllers, standby equipment, and recently installed devices not yet in active service are powered and network-connected but generate little or no traffic during normal operations. Passive monitoring has nothing to observe, so these devices never appear in the asset inventory. They remain invisible until an adversary finds them first.
- **Shadow devices:** These include both “forgotten” assets or devices that we may not have expected to be on a network. They may be both sanctioned and unsanctioned devices that “fly under the radar”. Assessment data shows that it is not uncommon for up to 30% of devices were previously unknown to security teams.

Industry cybersecurity frameworks, including the NIST Cybersecurity Framework, IEC 62443, and CIS Controls, acknowledge the essential role that carefully implemented active collection can play in closing these visibility gaps. Today, driven by more complex threats, an expanding xOT environment, the strategic use of active collection is gaining widespread acceptance as a multi-detection engine for safely discovering all assets, enriching asset data, uncovering previously unknown risks, and strengthening the overall cybersecurity posture.

This paper provides guidance on when, why, and how organizations can strategically deploy safe active discovery to complement passive monitoring, aligning closely with established cybersecurity best practices while also ensuring operational resilience.

When and Why to Consider Active Collection

Active collection involves the controlled, intentional, and safe querying of assets to gather comprehensive and precise asset information. It should always be deployed strategically, within controlled scenarios, and aligned with an organization's specific risk tolerance. Organizations require active capabilities for:

01

Asset Discovery

Many xOT environments contain assets that are previously unaccounted for, particularly in low-traffic, remote, or air-gapped environments. This includes dormant devices that are network-connected but rarely or never Active collection addresses this by querying the assets with the same protocol and methodologies it expects rather than waiting for them to generate traffic.

02

Detailed Asset Attributes

Key attributes such as OS versions, firmware details, patch levels, and module or chassis relationships are crucial for accurate cybersecurity management but often cannot be reliably captured passively.

03

Validation & Enhancing of Passive Discovery Data

Confirm and validate details of assets initially identified through passive monitoring, ensuring accuracy, and also by filling in the gaps to reduce blindspots.

04

Enhanced Operational Workflows

Integrating the aforementioned enriched asset data into security and operational workflows improves vulnerability tracking, informs patching decisions, and strengthens broader xOT risk strategies.

05

Vulnerability Management

Detailed asset data is necessary for accurately matching vulnerabilities to assets, enabling organizations to quickly identify and remediate critical risks using the “Now, Next, Never” prioritization framework.

06

xOT Device Hardening

Identifying and remediating factory-default credentials, expired certificates, vulnerable firmware, and insecure configurations across device estates.

Extend Visibility with the Dragos Active Collector

The Dragos Platform is specifically designed to extend visibility through controlled, active discovery. Centrally managed through the Dragos Platform interface, the Active Collector is strategically deployed and fully customizable by the administration to minimize operational risk and disruption by deploying safe active querying where it is warranted, thus aligning closely with operational considerations and organizational risk tolerance.

Extend xOT Coverage

Dragos’s extends safe active discovery capabilities to the full xOT environment, including other non-traditional OT assets that may be part of the OT control loop such as IP cameras, HVAC controllers, badge readers, building management systems, PDUs, IIoT sensors, and other proprietary-firmware devices that represent the fastest-growing segment of the operational attack surface.

- IP cameras
- HVAC controllers
- BMS
- Badge readers
- PDUs
- IIoT sensors
- Proprietary-firmware devices

FOUR STAGE METHODOLOGY

Intelligent Active Discovery: A Four-Stage Methodology

The Dragos platform leverages Intelligent Active Discovery, a structured four-stage methodology designed from the ground up for safety in operational environments. It safely and actively queries for devices. Every stage is rate-limited, administrator-controlled, and non-disruptive.

Stage 1

Discovery Agendas and Probes

The engine begins with self-calibrating "Agendas" that tune probe sequencing, packet rate, and port scope on a per-device basis — a fragile PLC is handled differently than a printer. The approach is deliberately tiered, starting with the absolute minimum interaction required to confirm a device exists and escalating only as far as needed:

Tier 0

ARP and ICMP only — minimal, non-disruptive traffic, just enough to confirm something is on the network. This is where dormant devices that never generate traffic are first surfaced. A device that has been powered on and connected for months but never communicated will appear here for the first time.

Tiers 1-4

Protocol-native communication per device type — BACnet, EtherNet/IP, SNMP, S7, HART-IP, Modbus, and others, using the native management protocol each device speaks.

Tiers 5-10

Deeper protocol interrogation for fully classified devices — DHIP, Redfish, Profinet, FINS, OPC-UA, and more — only invoked when needed and only after the device is already identified.

This tiered approach is what distinguishes Intelligent Active Discovery from traditional scanning. A conventional scanner hammers ports in rapid succession across a broad range. Dragos communicates with each device in its own language, starting with a whisper and going no louder than necessary.

Stage 2

Profiling Model

Based on what each device returns, the profiling model makes a deterministic identification that is named from evidence the device itself provided, not inferred from MAC address ranges or traffic patterns. Examples of what this looks like in practice:

Over BACnet	A Distech Controls ECY-VAV controller identifies itself by Vendor Identifier 364 and its own model name.
Over EtherNet/IP	An Allen-Bradley 1756-L83E/B PLC returns Vendor ID 1 (Rockwell) and Device Type 14 (PLC).
Over SNMP and TLS	An HP LaserJet provides its sysDescr string and TLS subject CN.
Over DHIP and WSD	A Honeywell-branded camera answers on TCP port 37777 with an ONVIF name.

Every identification is evidence-based. This is why classification is first-time accurate and defensible and why it cannot be replicated by watching traffic on a SPAN port.

Stage 3

Targeted Interrogation

Once a device is precisely identified, Dragos knows exactly which deeper queries it supports and returns with targeted questions to extract the attributes that drive real security decisions: firmware revision, serial number, application software version, certificate status, keyswitch position, and 15 or more verified attributes per device. This depth of ground truth is not achievable through passive observation alone.

Stage 4

Extraction and Enrichment

All verified attributes are fed directly into the Dragos Platform asset inventory, replacing estimated or inferred records with deep situational data. The enriched inventory immediately improves downstream security workflows: vulnerability prioritization becomes more accurate because the asset data driving “Now, Next, Never” scoring is verified, hardening workflows operate on confirmed device states, and threat detection context is tied to real asset attributes rather than educated guesses.

The critical safety principle across all four stages: the moment a device is fully classified, the safe active discovery operation stops communicating with it entirely. Every probe is rate-limited, scoped to approved targets, and fully administrator-controlled. This is a structured protocol conversation, not a port scan.

What Dragos Delivers

Dragos provides three core value pillars.

Expanded xOT Coverage

Discovers cameras, printers, HVAC controllers, building management systems, IIoT sensors, and other devices that passive sensors miss entirely, including dormant devices that have never generated observable network traffic.

Enriched Asset and Vulnerability Inventory

Administrators and operators will gain deeper intelligence including the actual firmware version, model number, and down to the ladder logic, thereby replacing gray areas or blind spots with verified ground truth. Merged asset and vulnerability catalogs across both platforms give security teams complete situational awareness, directly improving "Now, Next, Never" vulnerability prioritization.

Additive Hardening Capabilities

Seven capabilities now available on the xOT device layer: password management (rotating factory-default credentials automatically), certificate management (renewing expired certificates at scale), firmware management (safe upgrades prioritized by CISA KEV and EPSS scoring), configuration management (enforcing secure baselines and monitoring for drift), device state monitoring, and device log retrieval.

Discovery vs. Scanning: Understanding the Difference

The Dragos platform employs safe active collection techniques designed to carefully manage and reduce operational risk, ensuring greater safety, precision, and continuity within xOT environments. Crucially, Dragos provides customers with full control over all active collection processes, enabling them to align operations precisely with their unique risk tolerances. Safe Active Discovery is optional and always administrator-controlled.

	DRAGOS SAFE ACTIVE DISCOVERY	ACTIVE SCANNING
Collection Method	Controlled, precise queries using native OT protocols	Broad, automated queries across numerous protocols
Target Scope	Targets specific devices or assets with specific protocols	Targets wider network segments
Operational Risk	Lower operational risk, though caution is still required	Higher operational risk and greater unpredictability
User Control	User-managed to align with operational needs and risk tolerance	Limited customer control over query parameters
Dormant Device Discovery	Safely queries for devices & finds assets passive monitoring never sees	Relies on device responses; cannot find devices that generate no network traffic
xOT Device Coverage	All assets that may not be considered OT but are part of the control loop in the OT environment	Network-layer only; cannot interrogate proprietary xOT firmware

REAL-WORLD EXAMPLES

Active Technology in Practice

Strategic deployment of active collection significantly improves visibility and cybersecurity management across various industries. The following examples illustrate practical scenarios and benefits.

Oil & Gas

Validating Critical Asset Firmware

In the oil and gas industry, passive monitoring alone proved insufficient for maintaining full situational awareness, especially regarding critical remote PLCs that communicated infrequently. Standby and backup controllers in these environments are particularly problematic — powered and connected, but dormant enough that they never register in a passive inventory. These sporadic communications provided limited diagnostic information and incomplete firmware data, complicating vulnerability assessments and patch prioritization.

By implementing Dragos, operators can precisely capture firmware versions and patch statuses across both active and dormant assets across the breadth of the xOT environment. This enables confident identification and targeted remediation of vulnerabilities, significantly enhancing cybersecurity without disrupting ongoing operations.

Manufacturing

Enhancing Visibility for Chassis-Based Devices

In the manufacturing sector, traditional passive monitoring struggles to capture the complex hierarchical relationships inherent in chassis-based devices, such as PLCs, modules, and input/output (I/O) cards. Passive methods typically represent these assets as flat, unstructured lists, lacking the context needed to effectively understand their interdependencies and associated potential vulnerabilities.

By deploying the Dragos platform, organizations can safely and directly query these devices, accurately mapping hierarchical relationships among PLCs and the entire control loop. This enables security teams to gain immediate contextual visibility, clearly identify vulnerabilities, assess operational impacts, and make informed decisions without only partial visibility.

Electric Utilities

Overcoming Visibility Gaps in Isolated Substations

Blind spot challenges are particularly pronounced in electric utilities. Environmental limitations, such as lack of port mirroring capabilities or difficulties installing TAPs, often create substantial visibility blind spots; compounded by the fact that many substation devices operate in standby states and generate no observable traffic.

To address these challenges, utilities can deploy the Dragos Platform to safely and actively discover previously undetected or inadequately documented devices. Safe Active Discovery extends that reach to substation-connected IP devices including RTU-adjacent sensors, environmental monitors, and network-attached equipment, using the four-stage methodology to ensure every collection is safe, non-disruptive, and scoped to approved maintenance windows. This targeted approach delivers comprehensive asset visibility, full situational awareness, without compromising operational resilience.

Data Centers

Closing the xOT Device Gap

Data centers operate with extreme device density, and physical and cyber systems are converging rapidly. IP cameras, BMS devices, IoT sensors, PDUs, and UPS systems are all on the network and all reachable by adversaries. These devices ship from the factory with default credentials that are almost never changed, and traditional vulnerability management tools cannot reach them. Many are also effectively dormant from a network traffic perspective such as a UPS on standby or a camera covering a low-activity area generates almost nothing for passive tools to observe.

Dragos discovers the full device population using Safe Active Discovery, identifies default credentials and vulnerable firmware, and enables remediation at scale without manual per-device effort. The password management and firmware management capabilities address the highest-volume security gaps with the least operational disruption.

4 Steps To Implement Active Collection Safely

Recognizing the risks of active monitoring, organizations must thoughtfully balance the benefits with operational safety. To reduce these risks, organizations should:

01

Test Collection Methods in Non-Production Environments

Validate active collection workflows, document expected outcomes, and confirm tool behavior before deploying into live environments.

02

Clearly Define Collection Scope and Objectives

Restrict collection activities to explicitly defined critical goals and essential asset groups.

03

Assess Environmental Status Prior to Collection

Verify the current operational status and sensitivity of xOT systems before initiating collection to proactively avoid unintended disruptions.

04

Retain Full Administrator Control at Every Step

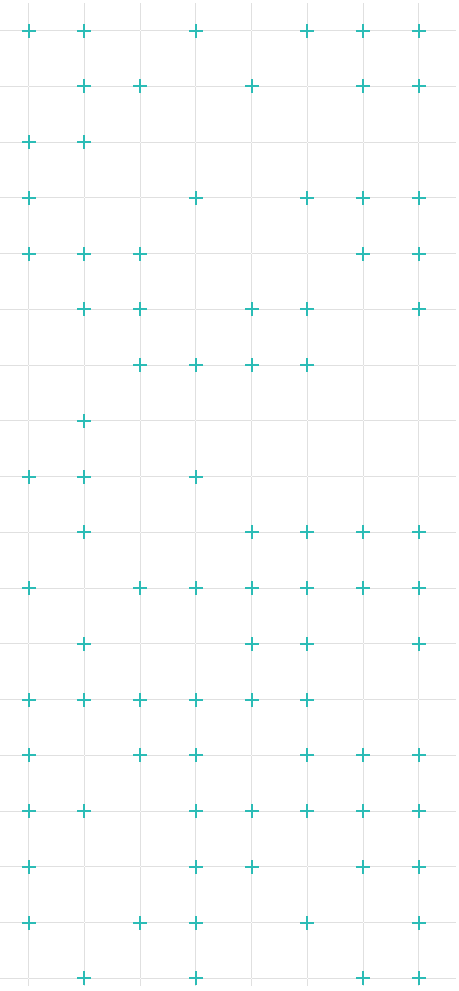
The Dragos operated within user-defined authorization for every action. No changes are made autonomously. Administrators define what is collected, which devices are in scope, and when activities occur.

Comprehensive xOT Visibility with the Dragos Platform

Achieving comprehensive visibility into xOT environments requires thoughtful integration of active and passive monitoring methods. Active discovery excels at identifying hidden assets, including dormant devices that passive monitoring will never see, and providing precise and enhanced asset information. Continuous passive monitoring captures real-time asset behaviors, network changes, and threats without operational disruptions.

The Dragos Platform delivers this balanced approach, offering robust, integrated visibility tailored specifically for xOT environments.

The Complete Visibility Suite Includes:



- ✓ **Passive Network Detection:** Continuously monitor OT network traffic across 600+ industrial protocols, providing foundational, non-disruptive visibility into asset behaviors, network activities, and potential threats.
- ✓ **Active Discovery:** Strategically leveraged for devices and scenarios where passive collection does not provide the detail required. This extends active collection to the proprietary-firmware xOT device layer using the four-stage methodology of Discovery Agendas, Profiling, Targeted Interrogation, and Enrichment. Finds dormant devices passive sensors miss entirely. Feeds firmware and make/model data directly into the Dragos Platform asset inventory. Includes additive hardening capabilities for password, firmware, certificate, and configuration management.
- ✓ **Lightweight Collectors:** Software-based collectors deployed onto OT systems to gather asset data safely without requiring direct network scanning.
- ✓ **Data and Project File Imports:** Allow ingestion of asset data, logs, and configuration information from both xOT & OT devices and existing asset databases without the need for network deployment or direct queries.
- ✓ **Third-Party Integrations:** Integration capability for ingesting existing asset and security data from third-party tools, enhancing visibility and fully leveraging existing information sources.

Together, these capabilities deliver what no single collection method can achieve: a continuously updated, verified inventory of every asset in the xOT environment, from the core SCADA systems to the dormant IoT asset in the corner of the substation.

Conclusion

The combination of a multi-detection engine of both passive and active montoring, when strategically deployed and carefully managed significantly enhances visibility, security and control across the full range of xOT environments. The Dragos Platform enables precise identification of visibility gaps, validation of asset information, and proactive vulnerability management for OT workstations, engineering systems and the larger control loop that makes up the xOT environment. This extension that reaches to the xOT device layer using a four-stage methodology is safe, protocol-native, and fully administrator-controlled. It fully represents the fastest-growing and most frequently overlooked segment of the operational attack surface.

By aligning deployment with operational constraints and risk tolerance, teams can effectively enhance visibility, improve cybersecurity posture, and safeguard operational resilience across their entire digital estate.

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com