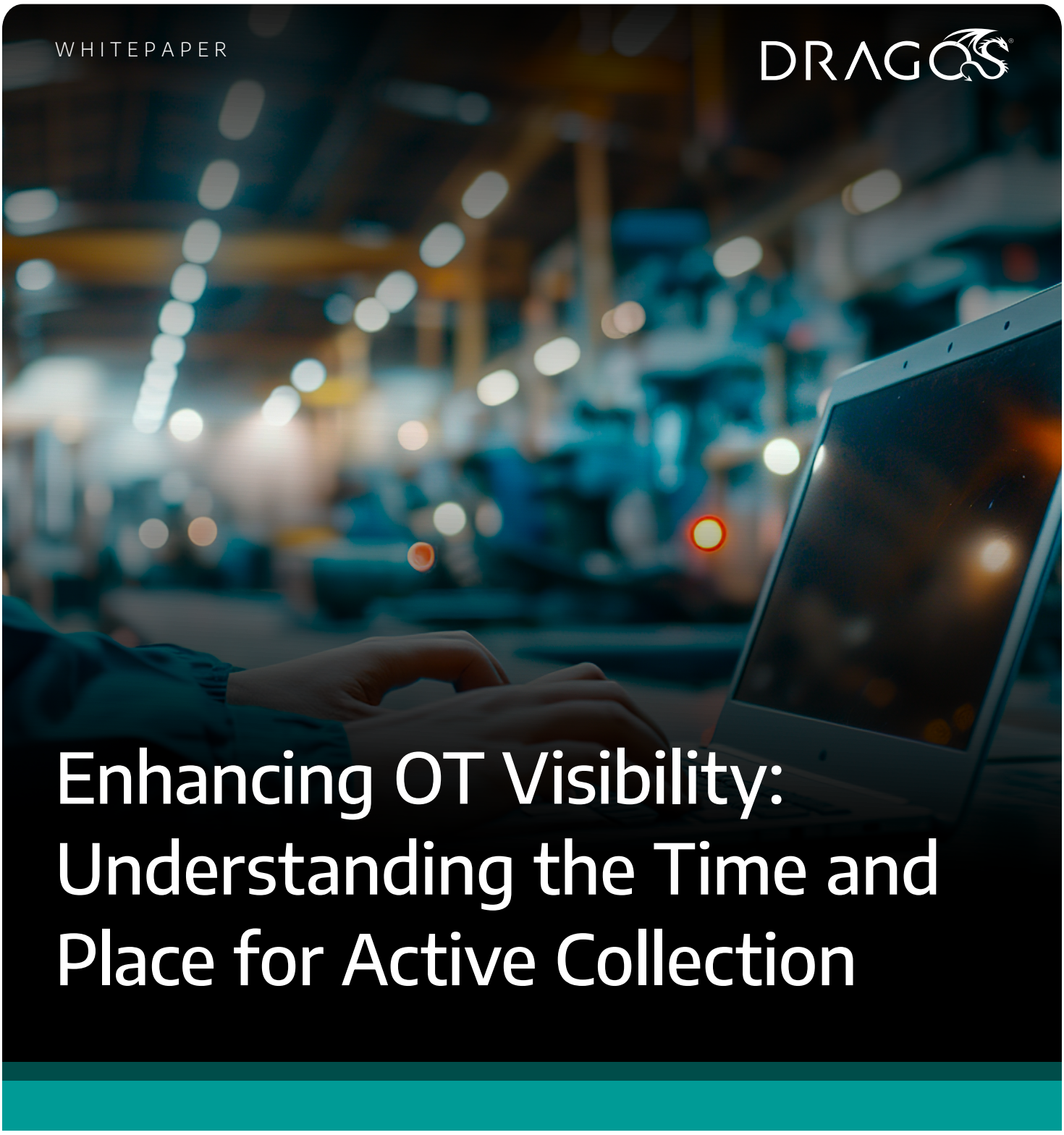
WHITEPAPER



Enhancing OT Visibility: Understanding the Time and Place for Active Collection

DRAGOS, INC

MAY 2025

TABLE OF CONTENTS

Introduction: Closing Visibility Gaps in Operational Technology (OT) Environments 3
When and Why to Consider Active Collection 3
Extend Visibility with The Dragos Agent – Active Collection 4
Real-World Examples: Active Collection in Practices 6
- Oil & Gas: Validating Critical Asset Firmware 6
- Manufacturing: Enhancing Visibility for Chassis-Based Devices 6
- Electric Utilities: Overcoming Visibility Gaps in Isolated Substations 7

Potential Risks of Improper Active Scanning 7
Implementing Active Collection with Operational Caution 7
Comprehensive Visibility with the Dragos Platform Visibility Suite 8
Conclusion 9

Introduction: Closing Visibility Gaps in Operational Technology (OT) Environments

Operational Technology (OT) environments have evolved significantly, becoming increasingly interconnected, digitalized, and complex. With these advancements, the critical need for comprehensive visibility has never been more urgent. Effective management of cybersecurity risks, asset protection, regulatory compliance, and rapid incident response depends heavily on the ability to achieve and sustain visibility across the entire OT 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, such as:

- **Assets communicating infrequently or only during specific operational events:** Passive monitoring relies on regular network communications; infrequent or event-driven communications reduce detection opportunities.
- **Devices located in isolated, air-gapped, or segmented networks:** Limited connectivity restricts opportunities for passive data collection.
- **Legacy network equipment or infrastructure constraints:** Networks lacking port mirroring capabilities or where installing TAPs is impractical or disruptive.
- **Limited capture of essential asset details:** Passive techniques can miss details like OS versions, firmware levels, patch statuses, and module relationships.

Increasingly, industry cybersecurity frameworks—like the NIST Cybersecurity Framework, IEC 62443, and CIS Controls—are acknowledging the essential role that carefully implemented active collection can play to close these critical visibility gaps. Historically, Dragos has prioritized passive monitoring due to operational safety concerns. Today, driven by more complex threats and expanding visibility requirements, the strategic use of active collection is gaining widespread acceptance as a complementary tool for enriching asset data, uncovering previously unknown risks, and strengthening cybersecurity posture.

This paper provides overview guidance on when, why, and how organizations can strategically deploy active collection to complement primary passive monitoring, aligning closely with established cybersecurity best practices, while thoughtfully navigating inherent operational risks.

When and Why to Consider Active Collection

Active collection involves the controlled, intentional 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:

- **Asset Discovery:** Many OT environments have assets that are previously unaccounted for, particularly in low-traffic, remote, or air-gapped environments.
- **Detailed Asset Attributes:** Key asset attributes such as OS versions, firmware details, patch levels, and module or chassis relationships are crucial for accurate and effective cybersecurity management but often cannot be reliably captured passively.
- **Validation of Passive Discoveries:** Confirm and validate details of assets initially identified through passive monitoring, ensuring accuracy of asset inventories and reducing uncertainty.
- **Vulnerability Management:** Detailed asset data is necessary for accurately matching vulnerabilities to assets, allowing organizations to quickly identify and remediate critical risks.
- **Enhanced Security and Operational Workflows**: Integrating enriched asset data into security and operational workflows improves vulnerability tracking, informs patching decisions, and strengthens broader OT risk strategies.

Extend Visibility with Dragos Active Collection (the Dragos Agent)

The Dragos Agent is a purpose-built software executable deployed directly onto Windows-based OT devices, specifically designed to extend visibility through controlled, active querying. It addresses scenarios where deploying passive sensors isn't feasible or effective. Centrally managed through the Dragos Platform interface, the Dragos Agent is strategically deployed to minimize operational risk and disruption, aligning closely with operational considerations and organizational risk tolerance.

The Dragos Agent specifically enables organizations to:

- **Discover Low-Traffic and Isolated Assets:** Identify previously undetected assets, particularly those that rarely communicate or reside in isolated segments.
- **Enrich Asset Inventories:** Collect detailed asset attributes including OS information, firmware versions, patch levels, and module or chassis relationships, greatly enhancing inventory accuracy and operational insight.
- **Enhance Vulnerability Management:** Capture comprehensive asset details necessary for precise vulnerability assessment and effective prioritization of remediation efforts.

Collection vs. Scanning – Understanding the Difference

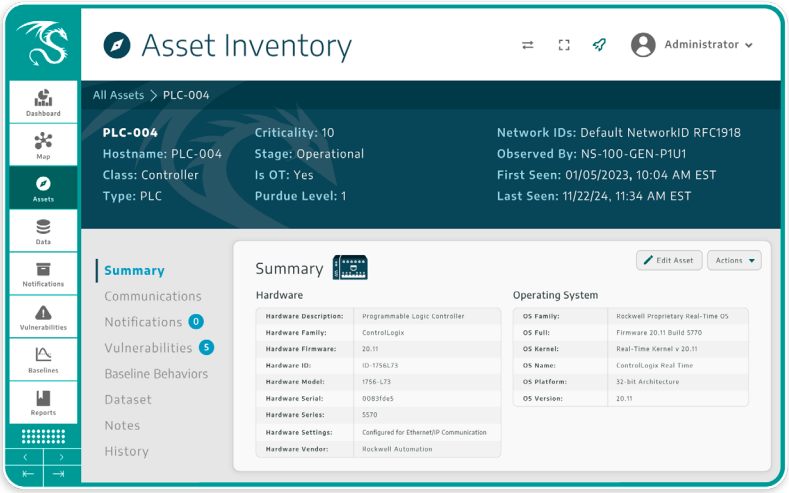
The Dragos Agent specifically employs active collection techniques to carefully manage and reduce operational risks, ensuring greater safety, precision, and continuity within OT environments. Crucially, Dragos provides customers with full control over their active collection processes, empowering them to align operations precisely with their unique risk tolerances and operational requirements. It should be noted that active collection is optional.

	Active Collection	Active Scanning
Collection Method	Controlled, precise queries	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
Real-World Example	A targeted active collection conducted during planned downtime enabled precise firmware validation of critical PLCs, allowing vulnerabilities to be effectively identified and patched without operational disruptions.	A seemingly controlled HTTP scan—even when carefully throttled—unexpectedly caused operational downtime due to unforeseen network negotiation issues.

Real-World Examples: Active Collection in Practices

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

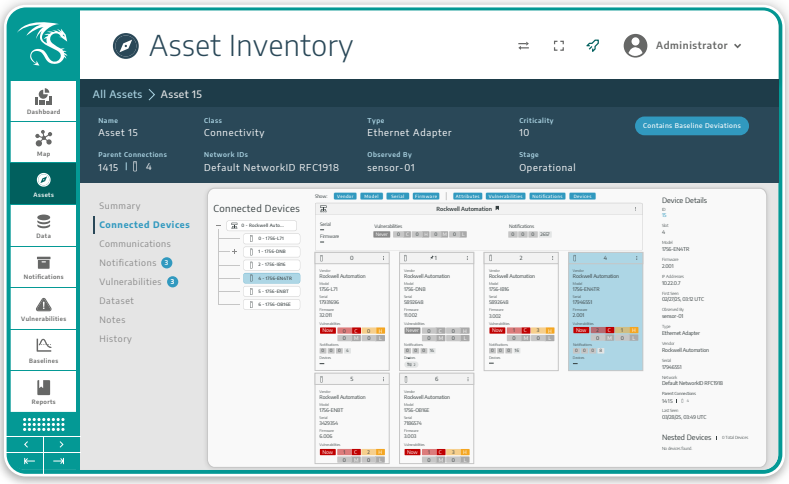
Oil & Gas: Validating Critical Asset Firmware



For example, in the oil and gas industry, passive monitoring alone proved insufficient for maintaining robust visibility, especially regarding critical remote PLCs that communicated infrequently. These sporadic communications provided limited diagnostic information and incomplete firmware data, complicating vulnerability assessments and patch prioritization.

By strategically implementing active collection through the Dragos Agent during scheduled downtimes, operators can precisely capture firmware versions and patch statuses. This enables confident identification and targeted remediation of vulnerabilities, significantly enhancing cybersecurity without disrupting ongoing operations.

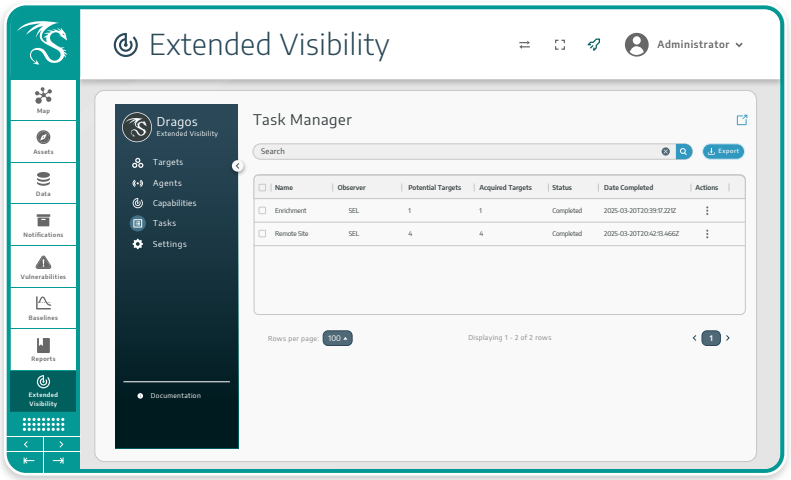
Manufacturing: Enhancing Visibility for Chassis-Based Devices



In the manufacturing sector, traditional passive monitoring struggles to capture the complex hierarchical relationships inherent in chassis-based devices, such as Programmable Logic Controllers (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 vulnerabilities.

By deploying the Dragos Agent, organizations can directly query these devices, accurately mapping hierarchical relationships among PLCs and their modules. This approach enables security teams to gain immediate contextual visibility, clearly identify vulnerabilities, assess operational impacts, and make informed decisions without labor-intensive manual correlation.

Electric Utilities: Overcoming Visibility Gaps in Isolated Substations



Visibility challenges are particularly pronounced in electric utilities, especially within isolated or air-gapped substation networks where passive monitoring is impractical or severely constrained. Environmental limitations, such as lack of port mirroring capabilities or difficulties installing TAPs, often create substantial visibility blind spots.

To mitigate these challenges, utilities can deploy the Dragos Agent during controlled maintenance windows, actively collecting previously undetected or inadequately documented devices. This targeted approach delivers comprehensive asset visibility, improved asset inventory accuracy, and enables proactive vulnerability management without compromising operational stability.

Potential Risks of Improper Active Scanning

While active collection brings considerable benefits, careless implementation can introduce operational and security risks, such as safety shutdowns, device unresponsiveness, and missed threats.

- **Safety Shutdowns:** Unexpected or improperly timed scans might trigger built-in safety mechanisms in critical control systems, causing costly and disruptive operational shutdowns.
- **Device Disruption:** Older legacy OT devices, not designed to handle network scanning queries, may freeze, crash, or become unresponsive, interrupting critical processes.
- **Missed Emerging Threats:** Active scanning provides only periodic snapshots, potentially overlooking real-time threats emerging between scheduled scans.

Implementing Active Collection with Operational Caution

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

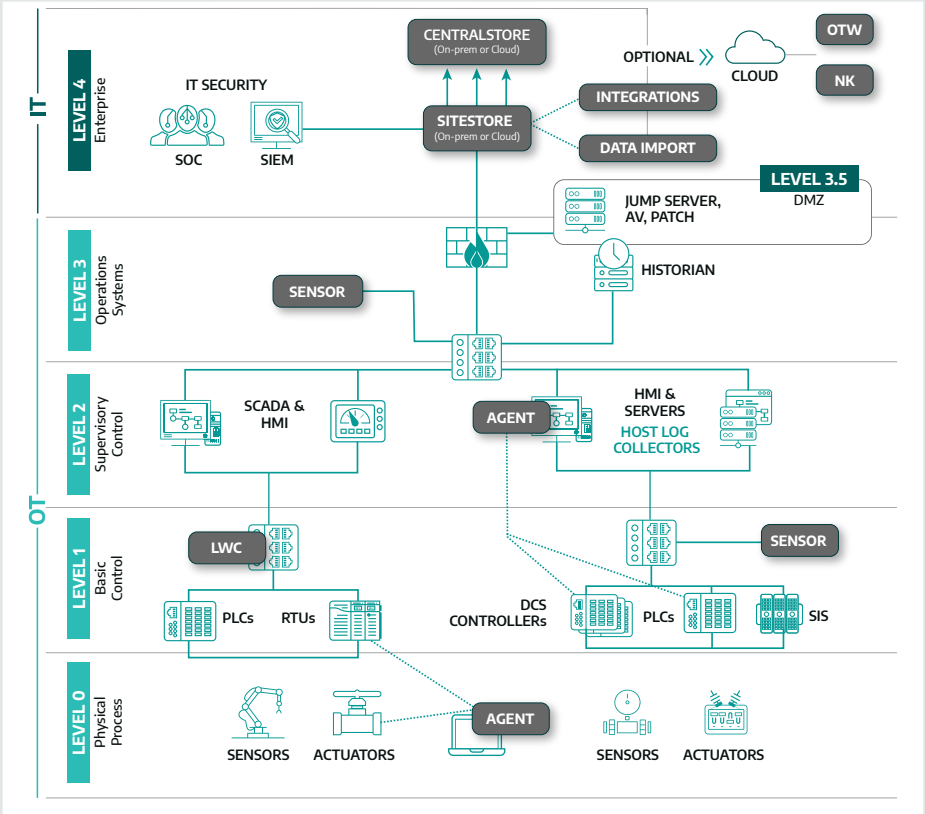
- **Test Collection Methods in Non-Production Environments:** Validate active collection workflows, document expected outcomes and confirm tool behavior before deploying into live environments.
- **Schedule Collection Activities During Planned Downtime, in Coordination with Operations:** Execute active collection after coordinating with operations and when possible, during low-risk times such as maintenance and assessment periods.

- **Clearly Define Collection Scope and Objectives:** Restrict collection activities to explicitly defined critical goals and essential asset groups.
- **Assess Environmental Status Prior to Collection:** Verify the current operational status and sensitivity of OT systems before initiating collection to proactively avoid unintended disruptions.

Comprehensive Visibility with the Dragos Platform Visibility Suite

Achieving comprehensive visibility into OT environments can be achieved with thoughtful integration of both active and passive monitoring methods.Active collection excels at identifying hidden assets and providing precise asset information, while continuous passive monitoring captures real-time asset behaviors, network changes, and threats without operational disruptions.

The Dragos Platform visibility suite delivers this balanced approach, offering robust, integrated visibility solutions tailored specifically for OT environments. The suite includes:



- **Passive Network Sensors (Cloud and On-Prem):** Continuously monitor OT network traffic, providing foundational, non-disruptive visibility into asset behaviors, network activities, and potential threats.
- **Active Collection with the Dragos Agent:** Strategically deployed for scenarios where passive sensors or other methods cannot practically be deployed, enabling controlled querying to obtain precise, detailed asset information.
- **Lightweight Collectors:** Software-based collectors deployed onto OT systems to gather asset data safely without requiring direct network scanning.
- **Data/Project File Imports:** Allow ingestion of asset data, logs, and configuration information from 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 by leveraging existing information sources.

Conclusion

Active collection, when strategically deployed and carefully managed, provides an effective complement to passive monitoring and significantly enhances visibility and cybersecurity management across a wide range of operational technology environments. Leveraging the Dragos Agent enables precise identification of visibility gaps, validation of asset information, and proactive vulnerability management. By aligning deployment with operational constraints and risk tolerance, teams can effectively enhance visibility, improve cybersecurity posture, and safeguard operational stability.

Those considering active collection should:

- Collaborate closely with operational teams to align on timing and objectives.
- Start with pilot deployments during planned maintenance.
- Continuously refine processes based on findings and operational feedback.

Taking these practical steps helps teams to quickly leverage active collection insights to improve asset visibility, manage vulnerabilities, and strengthen operational resilience.