Operational Visibility With The Dragos Platform

The Dragos Platform is known for xOT cybersecurity. Beyond its core security capabilities, it also gives plant staff and automation engineers the visibility they need to troubleshoot faster and keep production running.

The Challenge

Operational Blindness

Without visibility into OT communications, you can't answer basic questions when something goes wrong: Who did it? What did they do? Where did it happen? When? Why?

See. Understand. Act.

See what's happening on your network in real time. When production is disrupted or an outage occurs, you have a complete record to find the root cause fast. This visibility enables:

- ✓ Increase operational resilience and preserve business continuity in conjunction with OT threat detection
- ✓ Visibility into operational network activity before it creates unsafe conditions or lost production
- ✓ Improve response time and resolution when production is disrupted or an outage occurs
- ✓ Enable root-cause analyses when an event occurs
- ✓ Accountability for vendor and third-party remote access

How The Dragos Platform Supports Your Operations Team

The Dragos Platform helps operations teams understand network activity, investigate issues faster, and make informed decisions that reduce disruption.

01

Complete Visibility Into Your Communications History

A complete, searchable record of your assets and communications, so you can trace root causes and make informed maintenance decisions.

02

Understand What's Happening on Your Network

See not just that something happened, but what it means, including errors, deviations, and unusual access, before they impact production.

03

Investigate & Respond Fast

Integrated case management and incident playbooks turn investigations into structured workflows.

THE CHALLENGE

Operational Blindness

This is operational blindness, and it costs uptime long before any adversary is involved.

01

Built For Control, Not Visibility

Industrial automation equipment is purpose-built, often running embedded real-time operating systems instead of traditional IT platforms. These devices lack features like group policy and native authentication by design to support deterministic, low-latency control. As a result, systems may operate normally while Operations has little visibility when something goes wrong.

02

No Way To Answer Basic Questions

Without visibility into OT communications, Operations cannot reliably determine who did it, what they did, where it occurred, when it happened, or why. The same gap hides misconfigurations, physical-layer problems, and communication timeouts and latency that can create unsafe conditions or loss of production.

03

Evidence That Disappears

When a fault, error, or event is caused by disrupted or unexpected communications, it typically leaves no record, no audit trail, and no way to reconstruct the root cause of an outage or production loss. Communications are ephemeral: once the event passes, the evidence is gone. Traffic often stays inside an isolated subnet held together by a switch and rarely leaves that smaller network.

04

Low Traffic, High Consequences

Though traffic volume is low, it supports mission-critical functions such as safety control, high-speed motion, and substation relay control. High-speed automation relies on sub-millisecond communications, where even minor traffic spikes or physical layer issues—including cabling deficiencies, electromagnetic interference, and environmental conditions—can introduce latency, trigger timeouts, and increase network inefficiency.

THE SOLUTION

An Ongoing Record of OT Communications

The Dragos Platform provides the visibility and context Operations teams need to understand what is happening across their OT environment. By continuously recording assets and communications, it creates a trusted foundation for troubleshooting, resilience, and informed decision-making.

Asset Characterization

Naturally, the Dragos Platform performs asset characterization to identify the often unknown assets found in OT environments, obtaining Make, Model, Family, Firmware, Serial Number, and Revision, and correlates these to Dragos-adjusted vulnerabilities, as well as providing product lifecycle information to make informed decisions positioning for modernization or assisting with spare inventory.

A Dynamic System of Record

This automated, dynamically updating asset record capability serves as an advanced alternative to manually created spreadsheets or OT-unaware enterprise asset management, serving as a system of record for not only assets but also communications. This applies not only to expected assets, but to recordkeeping of transient or rogue assets that may have been involved in any events.

Communications With Context

The Dragos Platform provides an ongoing record of all communications, whether the cause is malicious, simple error, or entirely benign. Awareness of the traffic matters, but so does the context of what that traffic is doing. Understanding the function behind specific communications helps surface activity, malicious or not, that may be compromising the performance, efficiency, and resilience of ICS networks.

Stronger Troubleshooting and Continuity

This also allows users to rule out the health of the network as the cause of an event, with the previously missing communications now included in troubleshooting analysis. These often-overlooked capabilities support business continuity, maximize uptime, and give Operations a foundational record to work from.

Protocol Behavior Analytics

The Dragos Platform classifies protocol activity so Operations can interpret what is happening on the network, not just that something happened.

Classification	What It Covers	Operational Examples
Control & Execution	Locking, unlocking, stopping, and manipulation of control	Identify key states (Run / Remote / Program) and CPU lock state without physically observing devices, which often sit in locked cabinets that require a powerdown to evaluate.
Configuration, Activation & Setup	Device misconfigurations, exceptions, and invalid functions	Highlight erroneously assigned IP addresses in legacy hardware forcing gateway addresses. Locate program calls to devices that are no longer relevant.
Diagnostic Monitoring & Analysis	Protocol error codes	Discover faulted I/O suggesting latency from oversubscribed interfaces and subsequent TCP retransmissions, indicating deterioration of improper physical media in rugged environments.
Programming & Logic	Firmware updates, program downloads and uploads	Record unexpected program changes by internal or external users. Log the inadvertent transfer of a program to the incorrect PLC. Identify when programs are changed.
Communication Patterns	New communications, new devices	Capture transient or rogue assets in insufficiently locked down facilities. Identify poorly hardened equipment running unneeded services. Capture external network communications where none should be present.
File Operations	Unexpected file and data transfers	Isolate movement of data that may be valid but can consume network bandwidth and create latency. Identify unrecorded, unscheduled, or forgotten file backups that may no longer be necessary.

Baselining, Remote Access, and Human Error

Baselining. A baseline configuration helps track and trace detailed behavior that deviates from expected communications, making new or unusual behavior easier to spot.

Remote access. Regulating, controlling, and monitoring remote access remains a high risk in industrial networks. Where hardware is vendor-supplied and maintained, methods to restrict access are often limited. Records and logging of communications can determine whether an outside party was responsible for an outage or downtime and confirm whether they operated within policy.

Human and machine error. Much production loss, downtime, and outages are not caused by a malicious actor, but by human or machine error. The Dragos Platform provides visibility into both, reducing risk from mean time to resolution (MTTR) as well as from adversaries.

Managing Events

Case Management. Many facilities lack the ability to track, record, and manage operational incidents in the context of OT, or lack the security apparatus with awareness and context of the differences in OT environments. The Dragos Platform provides an embedded Case Management system out of the box that allows users to centralize investigation of the event — assets involved, hypothesis, evidence, and notifications associated with the event.

Playbooks. The Dragos Platform offers a path forward to investigation and response to any incident, regardless of source, providing next steps beyond the alerting. These are based on real-world scenarios that Dragos Incident Responders and Dragos Threat Intelligence have developed based on actual events, not theoretical ones.

Key Outcomes for Operations

An ongoing dynamic, searchable record of OT communications for root-cause analysis after a fault, error, or outage.

Faster time to resolution when production is disrupted.

Visibility into misconfigurations, physical-layer issues, and latency before they create unsafe conditions or lost production.

Accountability for vendor and third-party remote access.

Business continuity and maximized uptime, layered on top of OT threat detection.

About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil and gas, manufacturing, water, and transportation.

Learn more: dragos.com