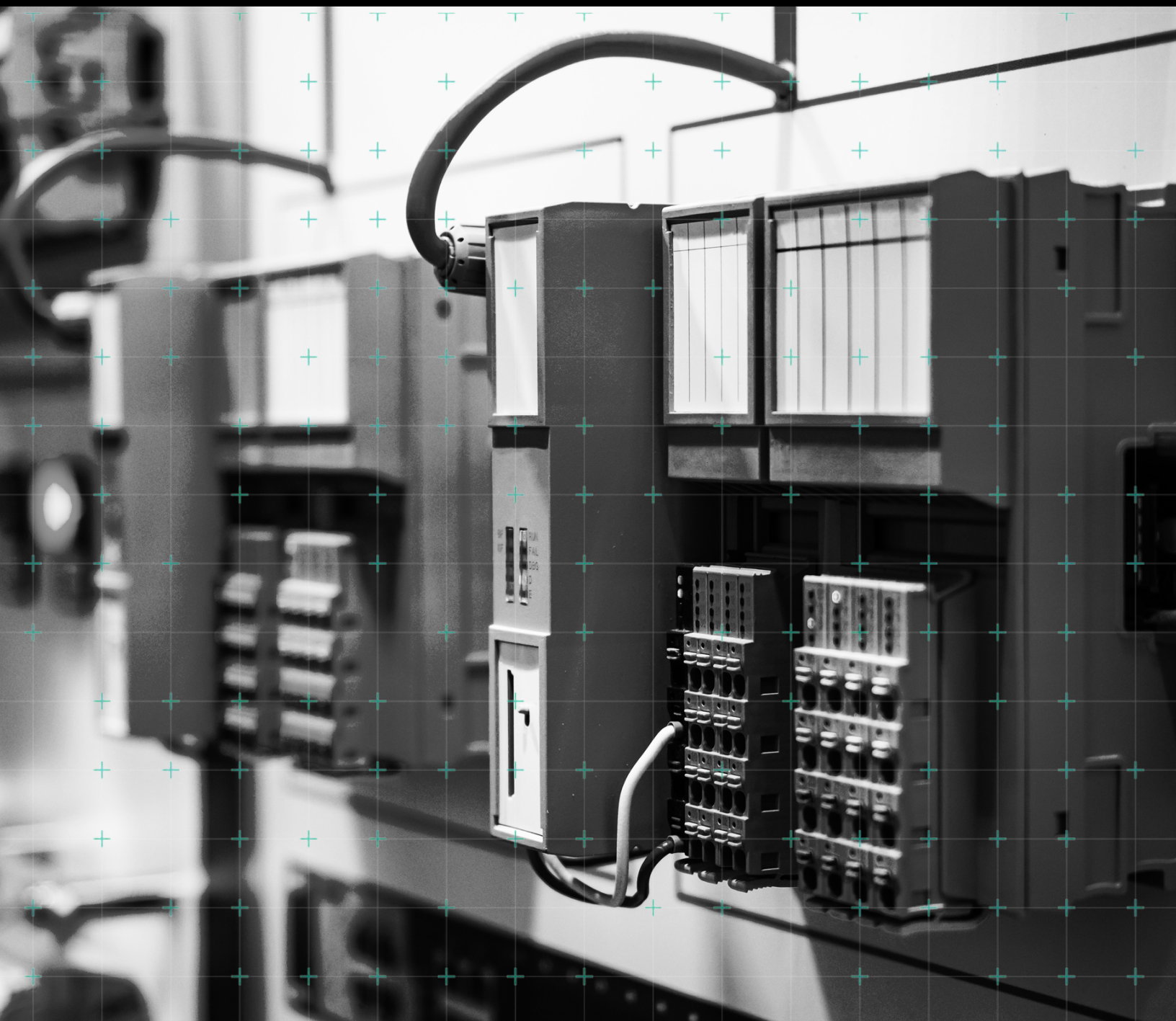
DRAGOS

WHITEPAPER

Resilience at xOT Scale

Defending every system operations depend on,
not just the ones labeled OT.



What OT Used to Mean

You can't protect what you can't see. Most organizations can't see nearly as much of their operational environment as they think they can. Resilience starts with closing that gap.

The industrial security community has gone by a lot of names over the years: industrial automation control systems, process control networks, and industrial control systems. The name that stuck was operational technology, or OT, and for good reason. OT was never really about a device category. It was about the control loop, the connection between a digital system and something physical in the real world. It was about physics, not an operating system.

That mission hasn't changed. What has changed is the size of the environment physics now touches.

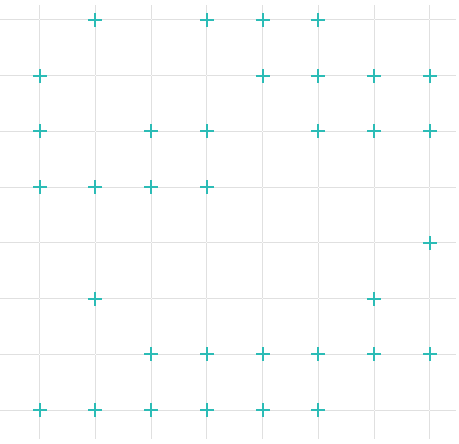
What Runs Operations Today

Picture a manufacturing facility running at full capacity. On the floor, PLCs control the line, and HMIs give operators a real-time view of what's happening. That's the OT most people picture, and it still matters as much as it ever did.

Now widen the view. A production order comes through the ERP system and goes straight to the line, no person in the loop. A machine vision system inspects every unit and feeds quality data upstream to adjust the process in real time. A historian aggregates that data and sends it to a cloud analytics platform, which recommends process changes overnight. A vendor logs in remotely to tune the robots. Walk across the facility itself, and the HVAC system is holding the temperature the process needs to stay in spec, sharing a network with the production floor it serves.

If any one of these systems goes down or is compromised, production stops. Not because the line itself broke, but because the conditions required for it to run no longer exist.

The same logic travels to operations that look nothing like a factory. At an oil and gas facility, it reaches the cloud-connected analytics platform, recommending changes to how a carbon cracker runs. In a data center, it reaches the environmental sensor, which feeds the cooling controls that keep racks within their thermal envelope; if that sensor reports an invalid temperature, the cooling system makes the wrong decision with total confidence. On the grid, it reaches the optimization system, recommending setpoints across a generation fleet. None of these were built as OT, and none of them used to show up in a security review. All of them can now stop operations if they fail.



DRAGOS CALLS THIS EXPANDED SCOPE XOT, EXTENDED OPERATIONAL TECHNOLOGY:

The standard for defining and defending the full operational environment. It is not a rebrand of OT, nor another name for IT/OT convergence or the Internet of Things. IoT describes a subset of connected devices. xOT is defined by consequence: what stops running when those devices, the systems around them, and the processes that depend on them fail.

The Boundary Test

Category, network segment, and org chart cannot be used to draw this boundary; too many systems that matter sit outside traditional OT ownership, and too many that don't sit inside it. The test that actually holds is operational influence: does the system influence a physical process, or drive a high-impact operational outcome? If yes, it's in scope, regardless of what it's called or who bought it.

An industrial label printer that a manufacturing line depends on to run sits squarely inside that boundary; if it goes down, the line stops with it. A cloud analytics platform that collects historical data for later review sits outside it, since production continues even if it fails. The same test applies further up the stack. A programmable logic controller that commands a machine naturally draws attention because its connection to physical output is obvious. A manufacturing execution system coordinating production across an entire plant often doesn't, because nothing about it looks like control. But if that system becomes unavailable, production can stop across multiple lines at once.

Where Labels Undercut Resilience

That context problem runs deeper than a single overlooked system. A Windows-based HMI, the operator screen directly controlling a physical process, often gets inventoried as an IT asset simply because it runs a familiar operating system. It gets patched on an IT schedule, monitored by IT tools, and managed by an IT team, even though it is controlling a physical process the moment it's asked to. The label is wrong, and the label is the gap. It is exactly the kind of gap adversaries are trained to find.

In practice, that gap shows up furthest from the traditional OT core. Most security programs cover control devices, engineering workstations, and historians well. Coverage thins fast from there: environmental sensors feeding data to control systems, IIoT devices embedded in production processes, and building automation platforms sharing network infrastructure with industrial controllers. The further a system is from the traditional core, the less likely it is to appear in the device inventory, be actively monitored, or be considered an asset critical to operations in an organization's security program.

The Five Functional Categories of xOT

Control Systems & Engineering Define & execute physical processes	PLCs, DCS/SCADA, SIS, RTUs, HMIs, engineering workstations, historians, config repositories
Data, Analytics & AI Inform & drive operational decisions	IIoT sensors, edge devices, cloud analytics, AI optimization models, predictive maintenance
Automation & Execution Execute automated process actions	Industrial robots, AGVs, machine vision, automated production and assembly systems
Access & Connectivity Enable interaction with OT systems	VPN gateways, jump servers, vendor remote access pathways, identity & access management
Operational Support & Infra Sustain the operational environment	ERP & production planning, building automation, BMS, physical security, data center infrastructure

Closing that gap starts with an honest accounting of the operational environment an organization is actually running, not the definition it inherited or the inventory it built five years ago. Every system that touches the control loop, every dependency that could be exploited to disrupt operations, and every team that owns a piece of the environment that influences a physical outcome, has to be part of that accounting. The point is to find the gaps before an adversary does.

Why Devices, Systems, and Controls Each Need a Different Approach

Once operational influence, not category, defines the boundary, the security problem ceases to be a single problem. It becomes at least three, and each one breaks a different assumption on which IT security tools were built.

01

Devices

The physical endpoints inside this boundary, sensors, controllers, IP cameras, badge readers, industrial label printers, building automation controllers, and traditional ICS hardware, are proprietary, cannot run a conventional agent, and were never designed for centralized management. An inventory tool built for laptops and servers cannot classify them, and a vulnerability scanner built for IT cannot safely probe them. They must be discovered, assessed, and hardened using their own native protocols, safely, without disturbing the process that depends on them.

02

Systems

The control systems and platforms that orchestrate those devices, DCS, SCADA, building automation, and the safety systems layered around them, exist to keep a physical process running with near-perfect uptime. A monitoring approach that risks disruption is not a viable option here. Visibility into these systems must be passive-first by default, with safe, active techniques reserved for the moments an organization deliberately chooses to use them. And visibility into the systems themselves is not always enough; some processes depend on the accuracy of the data flowing through them just as much as the systems that carry it.

03

Controls

The configurations, policies, and safeguards that govern how devices and systems behave, password policy, firmware currency, certificate trust, services enabled, segmentation rules, and safety interlocks, drift constantly: a password reset here, a firmware rollback there, a segmentation rule quietly bypassed during a maintenance window. The patch-and-audit cadence built for IT compliance cycles cannot keep pace with that rate of drift across an environment this large and this diverse.

A generic IT security stack, however well relabeled, cannot govern all three layers at once. That's what xOT is, as a standard: a more accurate definition of operational risk, not just a bigger inventory to worry about, that requires a purpose-built way to defend it. Governed together, these three layers turn a monitored environment into a resilient one.

How Adversaries Already See It This Way

Defining the category correctly matters because adversaries have already done it themselves. Sophisticated threat groups do not draw the boundary at the control system either. They study an organization's full operational environment for months, sometimes years, before they ever act, and the model they build looks much more like xOT than a traditional OT asset inventory.

An inventory can tell you what's there. It takes an operational model to explain why any of it matters. To maintain long-term access, an adversary needs to know what normal looks like well enough to blend into it. To collect intelligence, they need to know which systems carry meaningful operational context. To cause disruption, they need to know where they can create the greatest physical effect for the least effort. In every case, that requires understanding how the operation actually works: which systems communicate across boundaries, where credentials grant access, and which technologies sit between a business decision and a physical outcome.

01

Learning The Environment: VOLTZITE

Dragos has tracked VOLTZITE, a threat group that overlaps with Volt Typhoon, collecting GIS data, OT network diagrams, SCADA configurations, operating instructions, and process details from the critical infrastructure organizations it targets. More recently, Dragos observed VOLTZITE accessing engineering workstations to extract configuration and alarm data while investigating the exact conditions that would trigger a process shutdown. That is an adversary building an operational model, not collecting a list of devices.

02

Finding The Weak Link: AKIRA AND THE CAMERA

Since the start of 2025, Dragos has tracked 628 incidents tied to Akira, one of the most consistently active ransomware operations targeting manufacturing and industrial organizations. In one 2025 incident, endpoint detection and response tools blocked Akira's attempts to deploy ransomware on Windows systems. The adversary then found a vulnerable, internet-connected camera on the network, a device outside EDR coverage, and used it to deploy ransomware to network shares instead. The camera never touched the manufacturing process. Its position on the network did the damage.

That story is not really about a camera. It is about every device on an environment's edges that cannot run a conventional agent and is too easily overlooked for anyone to manage centrally: a default password never changed, firmware never updated, a certificate that expired and was never replaced, end-of-life hardware nobody retired, and a configuration nobody hardened. Basic controls like these fall to manual effort precisely because these systems are too diverse and too numerous to manage by hand, and every gap that effort leaves behind is a low-cost way in that adversaries count on.

03

Manipulating The Data: FROSTYGOOP

In the 2024 FrostyGoop malware attack on a Ukrainian municipal energy company, the adversary manipulated ENCO controllers to report false temperature readings. The district heating system depended on those readings to make operational decisions, and it failed not because a controller was disabled, but because the data flowing through it became unreliable. An organization watching only the controllers would have missed the dependency entirely. Understanding the process meant observing the devices producing that data, the values they reported, and the relationship between them.

The Pattern Adversaries Already Understand

None of these adversaries started by hunting for an organization's single most important asset. They learned about the environment first: how engineers access systems, which hosts talk to each other across boundaries, where credentials open doors, and which unglamorous system a critical process quietly depends on. They are also counting on weaker security hygiene in exactly the systems this paper has been describing, the ones sitting outside the traditional OT perimeter, because the lack of basic security hygiene makes initial access faster, easier, and quieter.

What Changes When the Boundary Is Right

Attack groups now number in the hundreds, with demonstrated capability to disrupt operational environments, and they are not limiting themselves to traditional OT assets; they are targeting the full range of systems that influence physical operations. A security program that monitors a fraction of that environment will detect a fraction of that activity, no matter how good its tools are.

AI is accelerating both sides of this at once. It is being built into industrial decision-making in ways that will keep expanding the xOT environment, and into adversary operations in ways that compress the time between an initial IT compromise and a targeted move against OT, lowering the skill and time it takes to find exactly the systems this paper has been describing.

Defined correctly, though, that same environment becomes defensible. Visibility, and a deep situational awareness across every system that influences operations, prioritization that reflects operational consequences, and detection tuned to the behaviors adversaries actually use are what enable an operation to absorb an intrusion and keep running. That is resilience at xOT scale: not the absence of threats, but an operation that keeps running while it deals with them.

The Question Worth Asking

Every organization defending critical infrastructure eventually has to answer an uncomfortable question: does our security program reflect the environment we are actually running, or the one we think we are running? xOT is Dragos's answer to how that question should be framed: a standard, not a product, built to define the full operational environment so it can actually be defended.

xOT is the Standard

The Dragos Platform is how organizations secure the devices, systems, and controls that make up their xOT environments.

Recognizing the category is the first step. Building a program that can defend devices, systems, and controls together, at scale, is the work that follows, and no two organizations start that work from the same place.

Contact Dragos

We will meet you where you are and help you build a program that strengthens the resilience of your full xOT environment, starting with an honest look at where that program stands today and what it would take to defend the environment you are running.

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