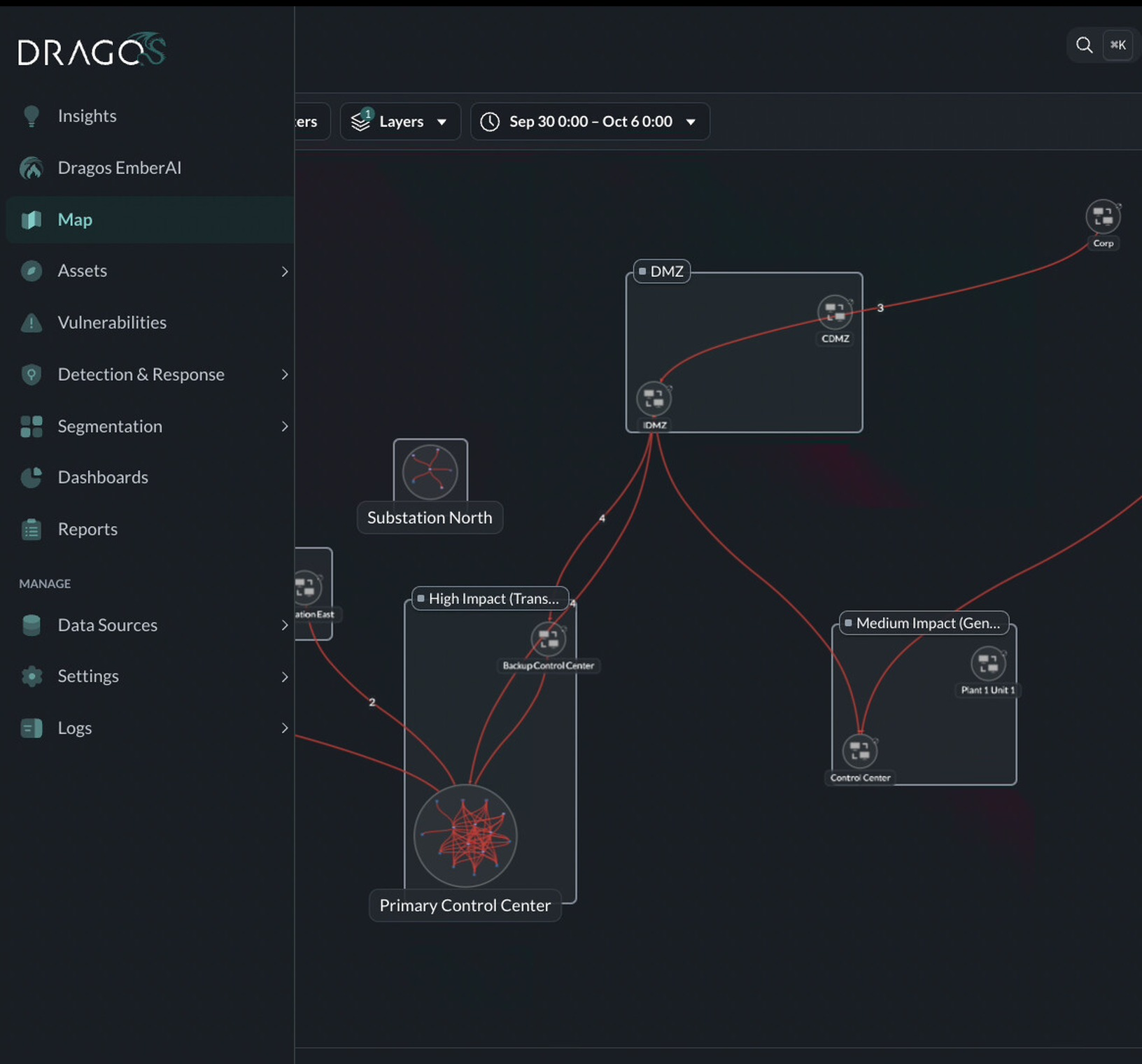




BROCHURE

The Dragos Platform

A Cybersecurity Platform Built for xOT Environments



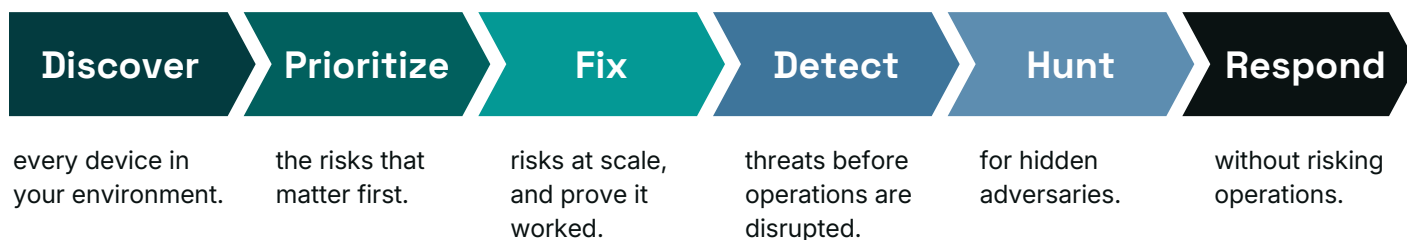
THE DRAGOS PLATFORM

Protecting the infrastructure civilization depends on.

The operational environment is no longer just PLCs and SCADA. It spans engineering workstations, remote access, cloud and AI systems, facility infrastructure, and the data centers that keep operations running. This is Extended Operational Technology (xOT). Adversaries operate across all of it, and a disruption anywhere can stop production or put safety at risk. Defending xOT takes technology, intelligence, and expertise built specifically for it.

Securing operations requires knowing what you have, how it connects, and what puts it at risk. The Dragos Platform brings xOT visibility, segmentation, vulnerability management, threat detection, and investigation together with the Dragos Intelligence Fabric, so your team can understand exposure, prioritize work, and respond with the operational context each decision requires.

Dragos helps you:



What your organization gains:



Full situational awareness

Know every asset in your xOT environment, how it communicates, and what your segmentation actually permits, so nothing operates in a blind spot.



Prioritized risk reduction

Focus remediation on what matters most with "Now, Next, Never" prioritization, without disrupting operations.



Operational resilience

Find and stop threats before production or safety systems are affected, with monitoring that never puts operations at risk.



Faster incident resolution

Scope the blast radius, then contain and recover faster with playbooks, intelligence, forensics, and practitioners who have responded to major attacks.



Regulatory confidence

A defensible program backed by documentation and continuous monitoring that satisfies regulatory requirements and withstands board and auditor scrutiny.



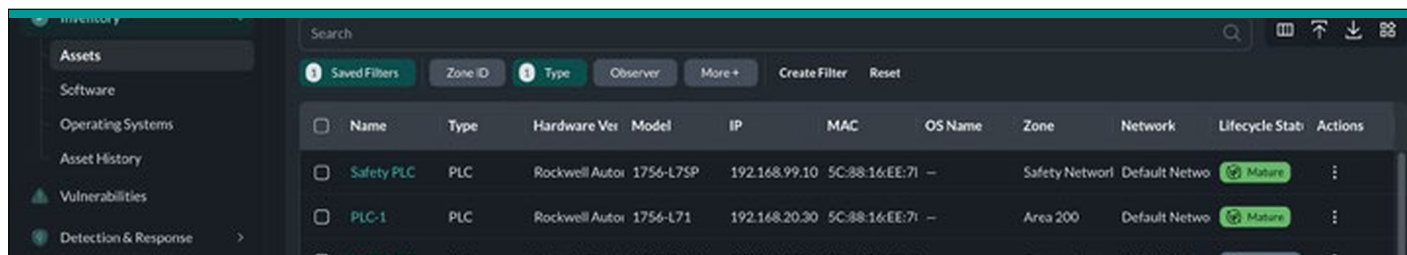
Expanded team capacity

Extend a lean team with OT expertise: Dragos EmberAI guides every analyst, and Dragos OT Watch Complete adds 24/7 hunting, triage, and tuning.

ASSET VISIBILITY

Know every device in your xOT environment.

DISCOVER



The screenshot shows the Dragos Asset Visibility interface. On the left is a sidebar with navigation options: Assets, Software, Operating Systems, Asset History, Vulnerabilities, and Detection & Response. The main area displays a table of assets with columns: Name, Type, Hardware Ver, Model, IP, MAC, OS Name, Zone, Network, Lifecycle Stat, and Actions. Two assets are visible: 'Safety PLC' and 'PLC-1', both identified as Rockwell Automation 1756-L75P and 1756-L71 respectively, with IP addresses 192.168.99.10 and 192.168.20.30. Both have a 'Mature' lifecycle status.

Name	Type	Hardware Ver	Model	IP	MAC	OS Name	Zone	Network	Lifecycle Stat	Actions
Safety PLC	PLC	Rockwell Auto	1756-L75P	192.168.99.10	5C:88:16:EE:71	—	Safety Network	Default Netwo	Mature	
PLC-1	PLC	Rockwell Auto	1756-L71	192.168.20.30	5C:88:16:EE:71	—	Area 200	Default Netwo	Mature	

Build a complete, continuously updated inventory of your xOT assets, from PLCs and engineering workstations to remote access pathways and connected facility systems.

- **Trust your inventory.** Passive monitoring discovers assets automatically and keeps the inventory current, so it does not go stale like manual records.
- **Reach every part of your environment.** Active collection can be deployed in segmented, low-traffic, and legacy environments to safely add firmware, OS, and patch-level detail that passive monitoring cannot see.
- **Plan with confidence.** Make, model, firmware, revision, and product lifecycle detail support patching, modernization, and spare inventory decisions, and show exactly which devices a new vulnerability affects.

EXTEND YOUR VISIBILITY

SOFTWARE SUPPLY CHAIN SECURITY

Know your software risk before it becomes an incident.

DISCOVER

Dragos Software Supply Chain Security analyzes compiled binary code in firmware, xOT devices, containers, and applications to generate a verified software bill of materials for every device.

- **See what is inside your devices.** Embedded vulnerabilities, exposed credentials, and open-source components the vendor may not know are present.
- **Fix what is exploitable.** Reachability analysis identifies which vulnerable code actually executes at startup, cutting through thousands of CVEs.
- **Surface risk with no CVE.** Hard-coded secrets, stored key pairs, expired certificates, and accounts without passwords never appear in a vendor SBOM or scanner result.
- **Scope the blast radius in under a minute.** When a component is compromised, match it against every device in the environment to see exactly which assets are affected.

SEGMENTATION

Prove your segmentation holds.

DISCOVER

TO →	10.10.99.0/24 2 assets Corp-fw1 +1	169.254.50.0/30 0 assets Mfg-firewall.root	172.16.50.0/30 2 assets Mfg-firewall.root	10.10.0.0/24 1 asset Corp-fw1	10.10.98.0/24 1 asset Corp-fw1
↓ FROM					
10.10.99.0/24 2 assets Corp-fw1 +1		UNKNOWN	UNKNOWN	IP/ANY 1 SVC	IP/ANY 1 SVC
169.254.50.0/30 0 assets Mfg-firewall.root	DENIED		UNKNOWN	DENIED	DENIED
172.16.50.0/30 2 assets Mfg-firewall.root	UNKNOWN	UNKNOWN		UNKNOWN	UNKNOWN
10.10.0.0/24 1 asset Corp-fw1	IP/ANY 1 SVC	UNKNOWN	UNKNOWN		1 SVC
10.10.98.0/24 1 asset Corp-fw1	IP/ANY 0 SVC	UNKNOWN	UNKNOWN	UNKNOWN	
10.40.80.0/24 4 assets Corp-fw1	IP/ANY 1 SVC	UNKNOWN	UNKNOWN	1 SVC	1 SVC

Dragos Segmentation delivers configuration-based segmentation policy validation. It reads firewall, router, and switch configurations offline, with no agents, scans, or traffic on the OT network, and reveals every access path they permit.

- **Trust your segmentation.** Stop assuming barriers hold. See exactly what your configurations permit, including paths no traffic has ever used.
- **Find what is wrong before it is used maliciously.** Misconfigurations, overly permissive rules, and unjustified access surface as findings, not incidents.
- **Walk into an audit with evidence.** Generate segmentation and NERC CIP-005 reports from the configurations running in your environment today.

VULNERABILITY MANAGEMENT

Don't just find vulnerabilities. Fix them.

PRIORITIZE

FIX

Type	Title	Name	Vendor	Asset	CVE	CVSS	Priority	Confidence	Resolution	First Detected
Hardware	Multiple Vendors In	BMXNOC04	Schneider El	PLC-3	CVE-2021-2	9.8	Never	Medium	Not Set	05/28/26, 01
Hardware	Multiple Vendors In	BMXNOC04	Schneider El	PLC-3	CVE-2021-2	9.8	Never	Medium	Not Set	05/28/26, 01

Turn an overwhelming advisory backlog into a short, defensible action list, then fix what matters.

- **Know the 3-6% that need action now.** "Now, Next, Never" prioritization shows which OT vulnerabilities require immediate action, so teams stop chasing every advisory.
- **Risk corrected for OT, not IT.** Dragos analysts correct CVSS scores for OT context, reviewing exploitability, exposure, and operational impact.
- **Act confidently without waiting for a maintenance window.** Alternative mitigations include configuration changes, network controls, and detections when patching is not viable.
- **Focus on what adversaries are exploiting.** Threat context flags the vulnerabilities adversaries are actively using.

FURTHER YOUR RISK REDUCTION

EXPOSURE MANAGEMENT

Surface the risks adversaries would use first.

DISCOVER

PRIORITIZE

Dragos Exposure Management produces a single, continuously updated exposure view across IT, OT, IoT, and cloud, so you find the assets and exposures your other tools miss.

- **Connect what you already have.** Pre-built integrations, safe active discovery, and always-on passive discovery build a unified inventory without agents, credentials, or appliances.

DEVICE REMEDIATION

Fix weaknesses at scale, and prove it worked.

DISCOVER

FIX

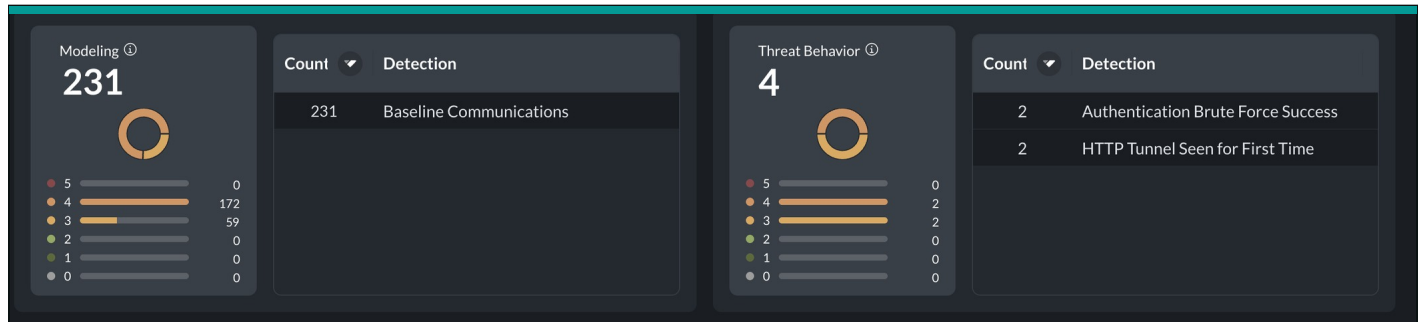
Dragos Device Remediation covers credential rotation, firmware updates, certificate management, and configuration change control across xOT devices, with deeper device profiling.

- **Rotate credentials at scale.** Replace default and shared credentials across xOT devices.
- **Keep firmware and certificates current.** Firmware updates and certificate management across the fleet.

THREAT DETECTION

Detect threats before operations are disrupted.

DETECT



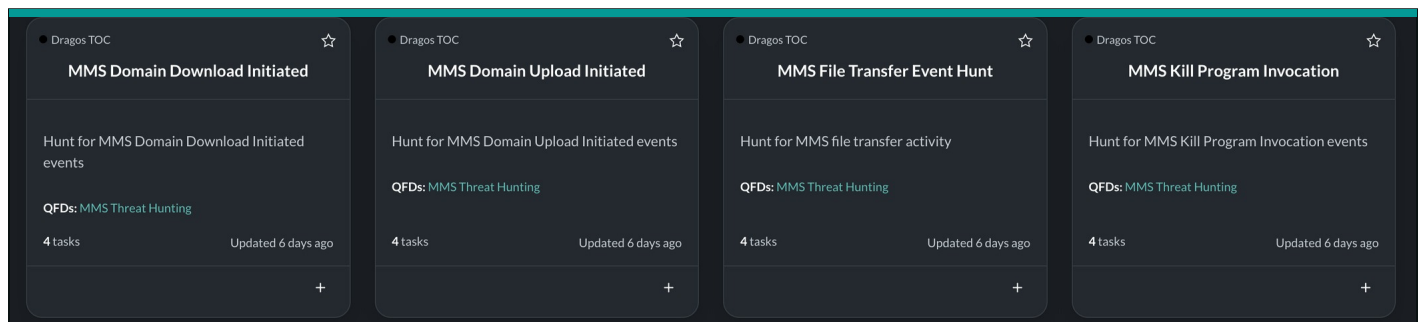
Tell a real threat from an operational anomaly. Detections are built on adversary behavior Dragos tracks in the field.

- **Detect the adversary, not just an anomaly.** Threat behavioral detections correlate observed behavior with the adversary tactics, techniques, and procedures Dragos tracks in the field, alongside modeling, configuration, and indicator detections.
- **See the whole attack, not isolated alerts.** Composite Detections correlate findings across time and data sources into one analyst-ready narrative.
- **Stay ahead of new threats.** Weekly Knowledge Packs add new detections, indicators, and playbooks, mapped to MITRE ATT&CK for ICS.

INVESTIGATION & RESPONSE

Know what to do next, without risking operations.

RESPOND



Move from alert to answer fast, with playbooks written by Dragos experts to guide each step.

- **See everything in one place.** The Insights Hub brings alerts, asset data, vulnerability context, and AI-powered recommendations into one dashboard.
- **Keep the whole investigation together.** Case management holds activity logs, forensic data, threat intelligence, and timelines in one case.
- **Respond the way an OT expert would.** Response Playbooks give step-by-step guidance for specific adversary behaviors.

BEHIND THE PLATFORM

The Dragos Intelligence Fabric.

The living knowledge engine behind the Dragos Platform. It codifies over a decade of OT-specific telemetry, asset and protocol research, adversary research, vulnerability data, and frontline practitioner expertise into a continuously updating loop, so defenders get the context to act fast and get it right.

Built from five interconnected elements (data, people, partnerships, systems, and AI), it reaches you through the Platform's ongoing content, including Knowledge Packs, and you can query it directly through Dragos EmberAI.

5+ petabytes of OT telemetry analyzed daily

26+ OT threat groups tracked and named by Dragos

10+ years of frontline incident response and adversary intelligence

DRAGOS EMBERAI

The AI that actually knows OT.

DISCOVER

PRIORITIZE

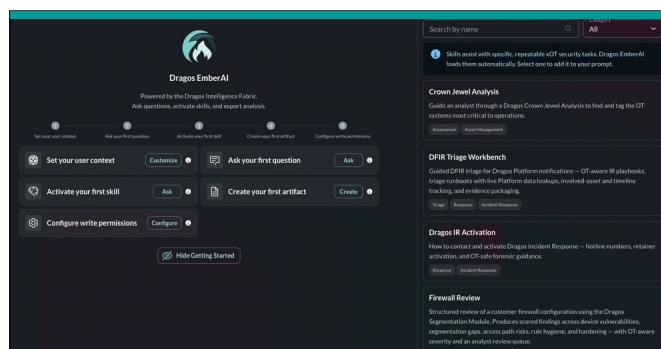
FIX

HUNT

RESPOND

Dragos EmberAI is an xOT-native AI agent built on the Dragos Intelligence Fabric and grounded in your environment. It applies Dragos expert methods to the work analysts already do.

- **Follow the experts.** Guided Skills built by Dragos analysts take your team from scoping to a final report.
- **Get findings, not raw output.** Structured tables and visuals ready for leadership updates and compliance evidence.
- **Turn decisions into action.** Analysts approve every change, and Dragos EmberAI never acts on xOT devices directly.



DRAGOS EMBERAI AS AN EXTENSION OF YOUR TEAM

QUERY

"Is my environment exposed to the recent reporting on Rockwell device exploitation?"

SKILL

"Run a structured threat hunt for VOLTZITE activity in my OT environment."

ACTION

"Tag these five newly identified systems as Criticality 10 so I can track them as crown jewels going forward."

ARTIFACT

"Build a heat map of vulnerability exposure across my crown jewel assets."

EXPERTS AND COMMUNITY

You aren't defending alone.

EXPERTS ON YOUR TEAM

Dragos xOT Threat Intelligence

PRIORITIZE DETECT HUNT

Finished OT threat intelligence from the largest private ICS/OT intelligence team in the industry, including 26+ tracked threat groups and corrected CVSS scores.

OT Watch

HUNT

Expert-led threat hunting that surfaces stealthy OT threats and validates what matters.

OT Watch Complete

DETECT HUNT RESPOND

24/7 expert monitoring, hunting, triage, and tuning, so you get a mature OT security program without building one in-house.

Expert Services

Frontline OT practitioners for incident response, assessments, architecture reviews, and tabletop exercises.

A COMMUNITY BEHIND YOU

Neighborhood Keeper

PRIORITIZE DETECT HUNT

Anonymized telemetry shared across participants, so behavior validated in one environment surfaces in others.

Community Defense Program

Free Dragos Platform access for eligible small utilities. 100+ customers protected at no cost. Apply today at dragos.com/community.

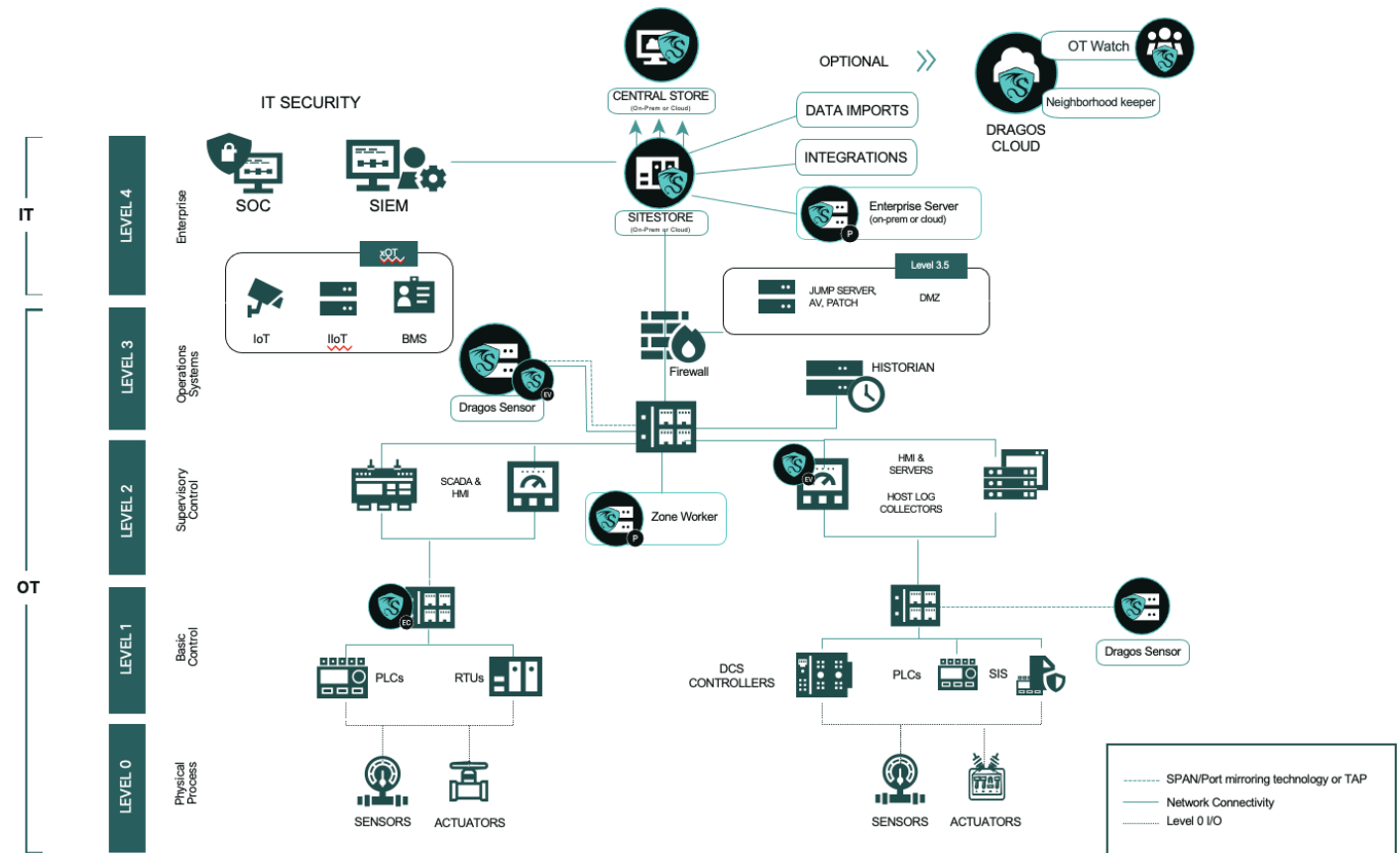
OT-CERT

Free OT security training and resources for asset owners and operators. 3,035 members worldwide.

DEPLOYING THE DRAGOS PLATFORM

Deploys your way.

The Dragos Platform deploys on-premises, hybrid, virtual, or in the cloud, to fit each organization's architecture and operational constraints.

**Passive monitoring**

Dragos Sensors, physical or virtual, passively decode 600+ industrial protocols.

Active collection

OT-safe, protocol-aware queries enrich the inventory, reach isolated or low-traffic assets, and add device-level detail.

Import and integrate

Import project files, and exchange data with SIEM, SOAR, ITSM, Microsoft Defender, and Sentinel.

Aggregation

SiteStores aggregate data across sensors. An optional CentralStore adds multi-site management.

For architecture, sizing, and additional capabilities, contact your Dragos account team.

DRAGOS BY THE NUMBERS

26+

named threat groups tracked

600+

organizations protected, including 22 of the top 25 electric utilities and 7 of the top 15 oil and gas companies, plus top manufacturers and water utilities

4.2B

actions logged annually



A LEADER IN
2026 Gartner® Magic Quadrant™
for CPS Protection Platforms



A LEADER IN
The Forrester Wave™, Q3 2026
Operational Technology Security Solutions

WHY THE DRAGOS PLATFORM

Built for xOT.

Deep packet inspection of 600+ industrial protocols, designed for environments where operations cannot afford disruption.

Intelligence that lives in the Platform.

The Dragos Intelligence Fabric turns over a decade of xOT-specific telemetry, adversary research, and incident response into detections and content that ship directly to the Dragos Platform.

You don't defend alone.

The Dragos Customer Success team helps you reach value faster and see measurable results, with Dragos Expert Services available from security assessments to 24/7 incident response.

A partner to operations teams.

Gives operations teams the visibility and context to understand what is happening across their OT environment, a trusted foundation for troubleshooting, resilience, and informed decisions.

Start where you are.

Enter at any stage of the maturity journey and see a clear path to the next one. No prerequisite blocks you from getting value from Dragos.

See the Dragos Platform in action.

dragos.com/request-a-demo

REQUEST A DEMO

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 & gas, manufacturing, water, and transportation.