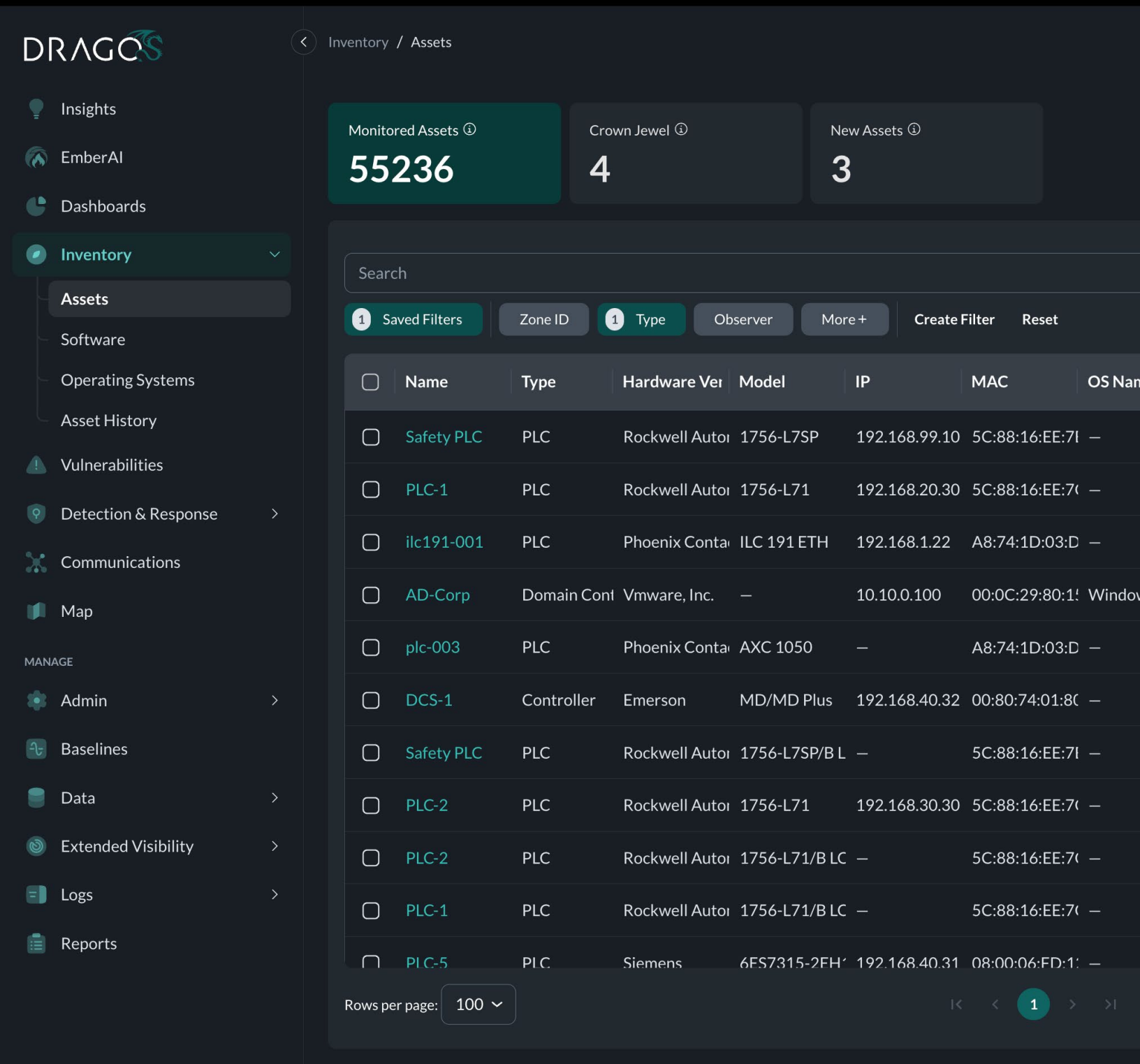
BROCHURE

# The Dragos Platform

## A Cybersecurity Platform Built for OT Environments



## Overview

The Dragos Platform monitors the operational environment to deliver complete visibility south of the firewall, prioritizes actions with OT-specific context, and extends security teams with expert guidance. With the Dragos Platform, organizations identify assets, discovers and prioritizes vulnerabilities, validates segmentation, detects threats, and expedites investigations to protect the critical infrastructure the world depends on.

## The Challenge

The operational environment is no longer just PLCs and SCADA. It now spans engineering workstations, enterprise IT, remote access, cloud and AI systems, automation and robotics, facility infrastructure, and the data centers that keep operations running. This is Extended Operational Technology (xOT). Adversaries operate across all of it. IT tools weren't built for it. Tools focused on the control layer alone don't cover it.

## Key Capabilities:

- Asset Visibility
- Threat Detection
- Vulnerability Management
- Investigation and Response
- Segmentation Validation
- Network Monitoring
- EmberAI

## Why The Dragos Platform:

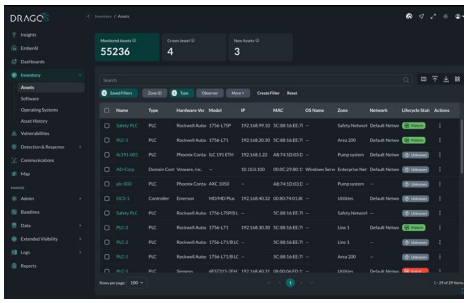
- **OT-Native:** Designed for OT environments where IT tools cannot safely operate. Deep packet inspection of 600+ OT protocols
- **Threat Detection:** The leading threat detection in OT. Detections built on tracked adversary behavior, not generic anomalies.
- **OT Context to Prioritize Action:** OT-corrected vulnerability scoring with "Now, Next, Never" prioritization focuses teams on the 3-6% requiring immediate action
- **Built by Practitioners:** Detections, response playbooks, and vulnerability guidance authored by the Dragos experts who respond to OT incidents in the field
- **Recognized Industry Leader:** Named a Leader in the Gartner® Magic Quadrant™ for CPS Protection Platforms (2026)

### The Dragos Intelligence Fabric: The Intelligence Behind The Dragos Platform

Over a decade of OT-specific telemetry, asset and protocol research, adversary research, vulnerability data, and frontline practitioner expertise, codified into a continuously updating loop that gives defenders the context to act fast and get it right. Built from four interconnected elements: data, people, partnerships and systems.


© 2026 Dragos, Inc. All Rights Reserved.

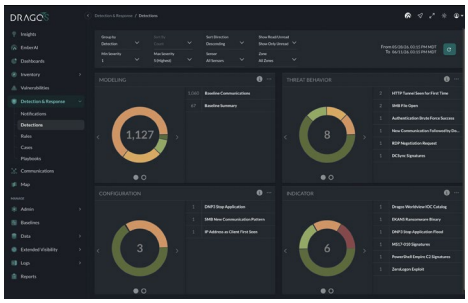
# Key Features



## 01.

### Asset Visibility

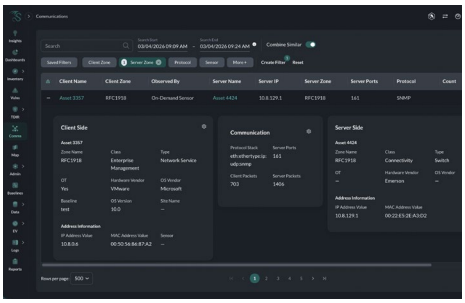
Build a complete, continuously updated inventory of xOT assets, from PLCs and engineering workstations to remote access pathways and connected facility systems. The Platform delivers passive-first discovery and safe active collection to support risk-based decisions.



## 02.

### Threat Detection

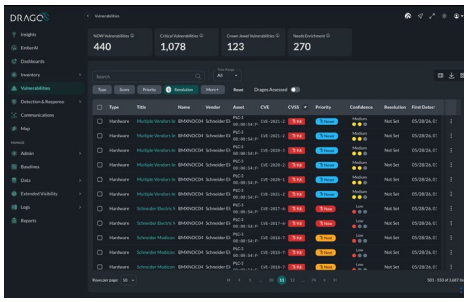
Four detection types work together: modeling against baselines, configuration change monitoring, indicators of compromise, and behavioral detections built on tracked adversary TTPs. Composite Detections correlate findings across time and data sources into a single analyst-ready narrative.



## 03.

### Network Monitoring

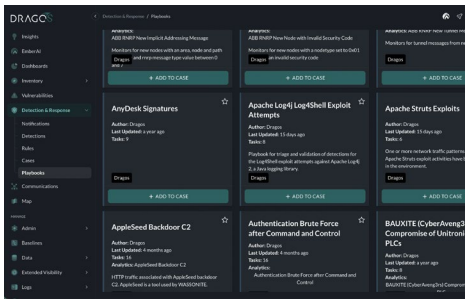
Deep packet inspection of 600+ OT protocols establishes baselines, identifies communication patterns, and visualizes traffic over time to reveal a clear network topology.



## 04.

### Vulnerability Management

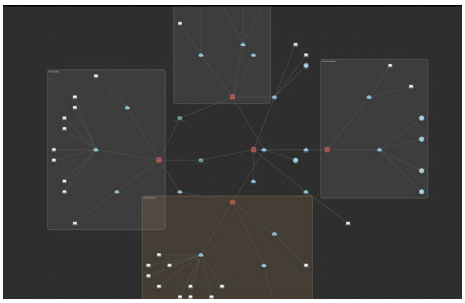
Corrected, enriched, prioritized guidance to manage the full lifecycle of hardware, software, and OS vulnerabilities. “Now, Next, Never” mitigation guidance focuses teams on the 3-6% of OT vulnerabilities that require immediate action. Authored and updated by Dragos vulnerability analysts.



## 05.

### Investigation and Response

Create cases that pull in activity logs, forensic data, threat intelligence, and timeline views. Reference response playbooks written by Dragos experts to investigate confidently and reduce time to response.



## 06.

### Segmentation Validation

Analyzes firewall, switch, and router configurations to validate segmentation policies, map topologies and access routes, and surface drift between intended and actual segmentation to support compliance and improve posture.


© 2026 Dragos, Inc. All Rights Reserved.

# The Dragos Platform Offers Flexible Monitoring to Address Customer Requirements

### Dragos Platform Inputs

- **Sensor and Virtual Appliances:** Passive monitoring via physical sensor appliances and virtual sensors, with deployment options that cover diverse OT architectures without disrupting the network.
- **Active Collection:** Lightweight software for active collection on Windows and Linux devices. Discovers isolated or low-traffic assets and enriches inventories with software and OS detail to enable vulnerability matching.
- **Containerized Traffic Forwarding:** Edge Collector deployed in containerized and edge computing environments captures east-west traffic locally, then deduplicates, filters, compresses, and forwards data to sensors.
- **Data and Project File Import:** Import and enrich asset inventories from existing data sources, vendor files, and third-party tools.

### Integrations

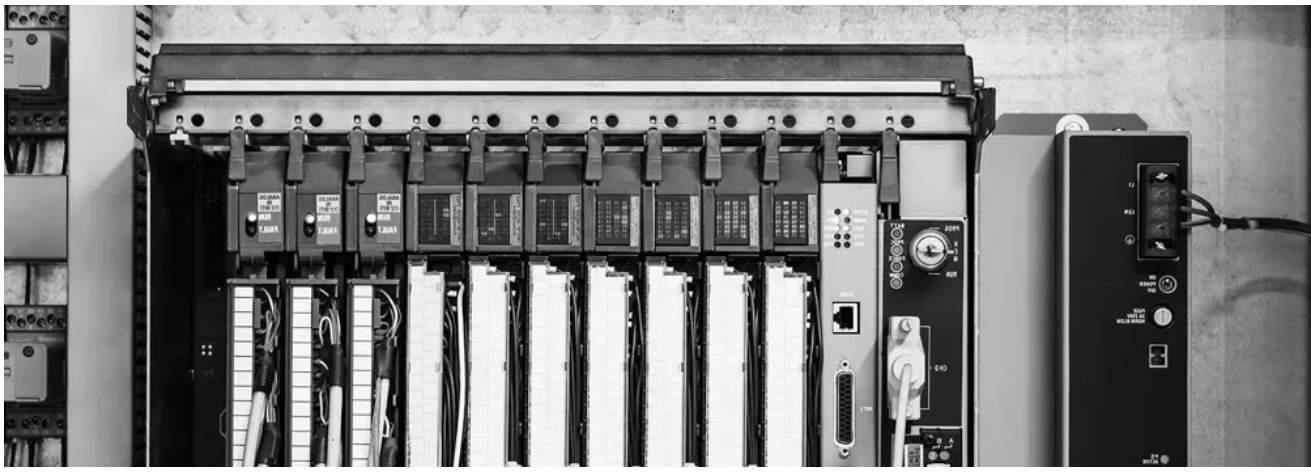
Integrates directly with leading firewall vendors including Fortinet, Cisco, CheckPoint, and Palo Alto Networks; SIEM systems like Microsoft Sentinel; endpoint tools including CrowdStrike; CMDB systems like ServiceNow; and AI models via Model Context Protocol (MCP) servers.

### SiteStore

Aggregates Dragos sensor asset, vulnerability, and threat information across connected sensors, including key workflows such as alert management, vulnerability tracking, and investigation tools.

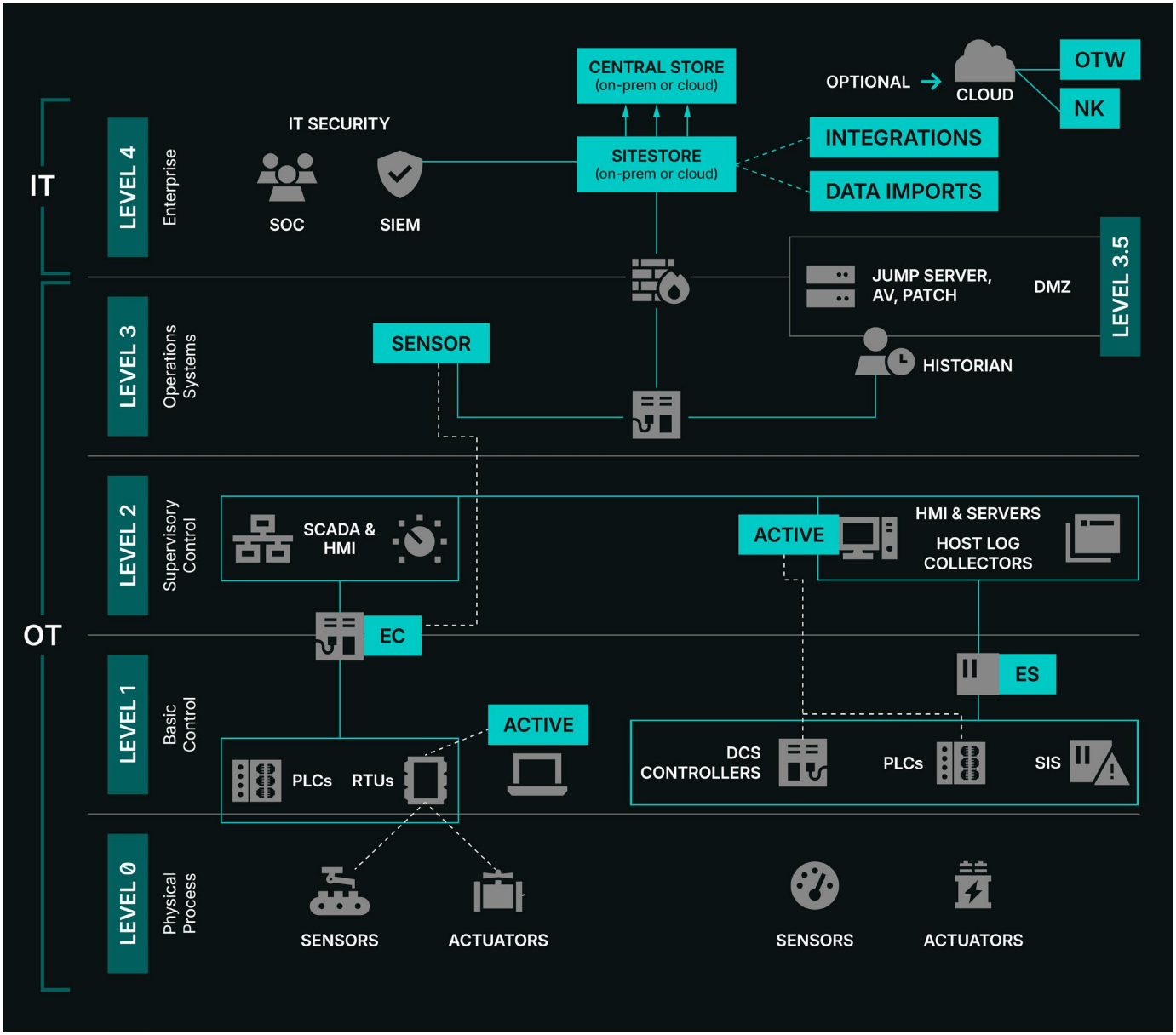
### CentralStore

Optional component that offers SiteStore management, enabling a central location for multi-enterprise aggregation, central dashboards, searching, and reporting.




© 2026 Dragos, Inc. All Rights Reserved.

# Dragos Deployment Diagram




**Gain Visibility Through Flexible Monitoring**

Preserve operational uptime with a “Do No Harm” monitoring approach. OT organizations need visibility south of the firewall, at Levels 1, 2, 3, and 3.5 (the OT/IT interface) of the Purdue Model.


© 2026 Dragos, Inc. All Rights Reserved.

## The Power of the Dragos Ecosystem

The Dragos Platform is supported by industry-leading expertise, meeting customers where they are in their OT cybersecurity journey.

- **OT Watch:** Dragos experts behind the Platform. OT Watch adds expert-led threat hunting that surfaces stealthy OT threats, validates what matters, and acts with OT-specific context, informed by the Dragos Intelligence Fabric. OT Watch Complete extends this with 24/7 monitoring, SLA-backed alert triage, continuous platform tuning, vulnerability reporting, and expert-led hardening, for organizations that want a mature OT security program without building one in-house.
- **Neighborhood Keeper:** An opt-in collective intelligence network that enables Dragos Platform users to benefit from anonymously shared intelligence. Neighborhood Keeper aggregates data and intelligence across organizations to provide a view of threat activity and trends.
- **WorldView:** The only threat intelligence built exclusively for OT. Finished, analyst-validated, and continuously updated by the largest private ICS/OT threat intelligence team in the industry. Dragos tracks 26+ OT-specific threat groups, tests ICS vulnerabilities on physical devices, and corrects CVSS scoring that's wrong 30% of the time for OT. Findings are reported in WorldView and integrated into the Dragos Platform.
- **Supporting Services:** From technical account managers who help customers operationalize key platform use cases, to experienced OT incident responders, to consultants who assess broader OT cyber defense architectures, Dragos services focus on helping customers achieve their key OT cybersecurity outcomes.
- **Integrating with Security Operations:** The Dragos Platform integrates with a wide range of complementary technologies to expand visibility and reduce time to respond and recover across OT and IT, including leading SIEMs, firewalls, and EDR.
- **Partnerships:** Dragos partners across the technology ecosystem, from firewalls and SIEMs to industrial automation OEMs, to extend Platform value into the tools customers already use. System integrators, resellers, and OEM partners expand deployment reach.

**See the full list of Dragos Partners:** www.dragos.com/partners/


Built on the Dragos Intelligence Fabric, EmberAI brings a decade of OT cybersecurity expertise into every analyst workflow.

- **Understand Your Environment:** "List all assets first seen in the last 7 days, grouped by zone, and which sensors detected them."
- **Apply Threat Intelligence:** "Is my environment exposed to the recent reporting on Rockwell device exploitation?"
- **Triage Without Manual Work:** "Which Dragos advisories published in the last 30 days apply to assets and software versions in my environment?"
- **Cut Investigation Time Dramatically:** "Create a timeline of notifications on the source and destination assets."


© 2026 Dragos, Inc. All Rights Reserved.

## See the Platform in Action

Request a demo: dragos.com/request-a-demo

## 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


© 2026 Dragos, Inc. All Rights Reserved.