

The screenshot displays the Dragos Platform interface. At the top, there's a 'BROCHURE' header on the left and the 'DRAGOS' logo on the right. Below the header, there's a 'Map' section with filtering options like 'Zones: Public Networks + 32 more', 'Links: Physical', 'Assets: Only Active, IP/MAC Required', 'Asset Limit: 1,500', and 'Protocols: DNS + 4 more'. The main area is split into 'EXPLORE MAP' and 'STRUCTURED MAP'. Below the maps, there's an 'Inventory / Assets' section with a search bar and filters for 'Zone ID', 'Type', 'Observer', 'Network ID', and 'Hardware Vendor'. A table lists assets with columns for Name, Type, Hardware Vendor, MAC, Zone, Network, Model, Last Seen, Device Connections, and Actions. Below the table, there's a 'Welcome User' section with three main cards: 'Visibility' (2 Sensors, Configuration Needed 1/2, Up-to-Date 2/2, Ingest, Avg: 41.26 MB/s Last 7 days), 'Security' (6,116 Internal Assets, Missed Internal Assets, Open Critical NOW Vulnerabilities, New Sev. 4+ Alerts), and 'Integrations' (1 Service, Active Integrations, Neighborhood Easier, Q1 Watch). At the bottom, there's a 'Recommendations' section with a list of items to review.

The Dragos Platform

A Cybersecurity Platform Built for OT Environments

The Dragos Platform monitors OT networks to deliver complete visibility south of the firewall, prioritizes actions with OT-specific context, and extends security teams with expert guidance. Purpose-built for OT and powered by industry-leading cyber threat intelligence, the Platform identifies assets, discovers and prioritizes vulnerabilities, validates segmentation, detects threats, and expedites investigations to protect the critical industrial infrastructure that powers our world.



THE CHALLENGE

Industrial organizations face escalating cyber threats while managing complex OT environments with limited visibility. Specialized expertise is scarce, operational disruption is unacceptable, and the unique requirements of OT systems demand purpose-built security solutions.



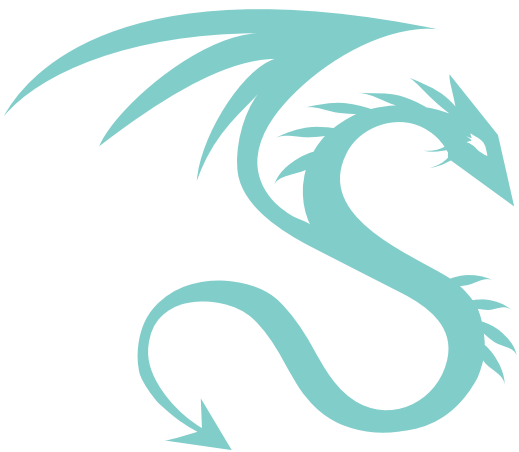
THE SOLUTION

The Dragos Platform enhances the cybersecurity posture in these critical environments through network monitoring, asset visibility, vulnerability management, segmentation validation, threat detection, and investigation and response.



KEY CAPABILITIES

- Asset Visibility and Inventory
- OT Network Monitoring and Deep Packet Inspection
- Risk-Based Vulnerability Management
- Segmentation Policy Validation
- Intelligence-Driven Threat Detection
- Investigation and Response

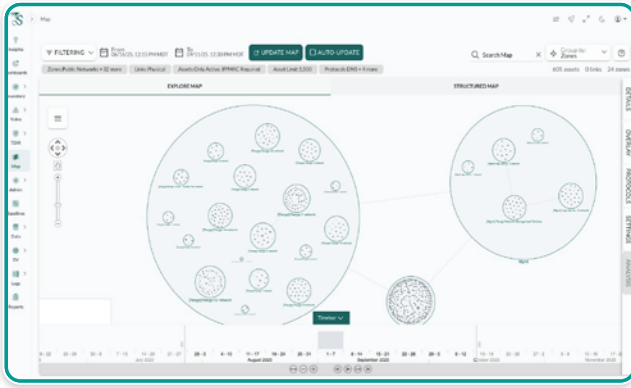


WHY THE DRAGOS PLATFORM

- ✔ **OT-Native Platform** - Purpose-built specifically for OT and industrial control systems (ICS) environments.
- ✔ **Recognized Industry Leader** - Named a Leader in the Gartner® Magic Quadrant™ for CPS Protection Platforms (2026).
- ✔ **Intelligence Fabric** - Real-world operational experience, threat research, and collective defense continuously feed threat, vulnerability, and asset insights directly into the Platform.
- ✔ **Threat Detection** - Industry-leading OT threat intelligence powers high-fidelity threat detection in the Platform.
- ✔ **Monitoring & Visibility with OT Watch** – 24/7 platform coverage, with expert threat hunting, tuning, and hardening, led by Dragos.
- ✔ **Commitment to Customer Success** - Dedicated professional services and ongoing support ensure measurable cybersecurity outcomes.

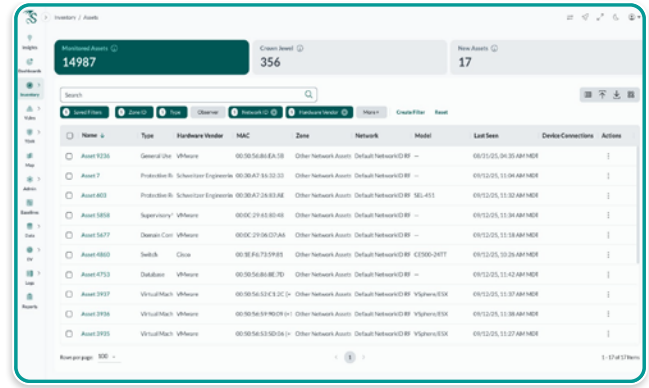
Key Features

OT Network Monitoring



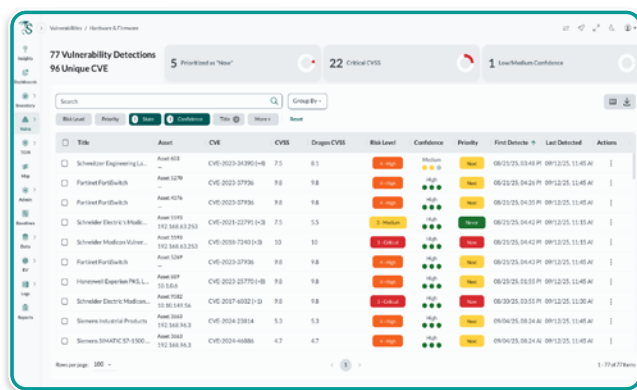
Monitors network traffic to enable both cybersecurity and operations. The Platform performs deep packet inspection (DPI) to establish baselines and identify communication patterns. This enables a comprehensive understanding of the environment and allows users to visualize communications over time to provide a clear network topology.

Asset Inventory



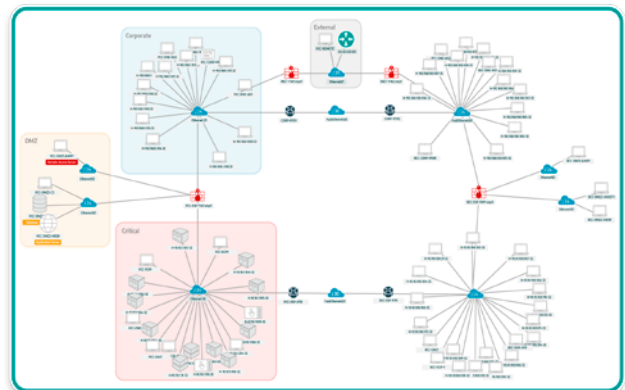
Build a complete, continuously updated OT asset inventory with detailed attributes supporting key security and operational use cases. The Platform delivers passive-first discovery and safe active collection when needed to build comprehensive visibility and support risk-based decisions.

Risk-Based Vulnerability Management



Provides corrected, enriched, prioritized guidance that allows you to manage the full lifecycle of hardware, software, and OS vulnerabilities in your environment. With "Now, Next, Never" mitigation guidance, teams can prioritize resources, minimize downtime, and mitigate risks. Guidance authored and updated by Dragos vulnerability analysts and incorporated back into the Platform to keep up with the changing threat landscape.

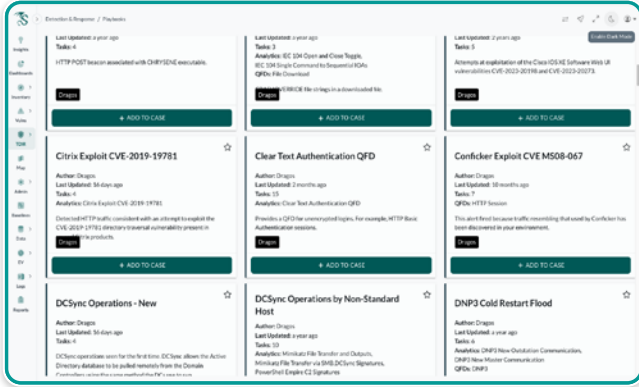
Segmentation and Policy Validation



Dragos NP-View analyzes configuration of firewalls, switches, and routers to validate segmentation policies, map topologies and access routes, and evaluate firewall policies to streamline compliance reporting and improve cybersecurity posture.

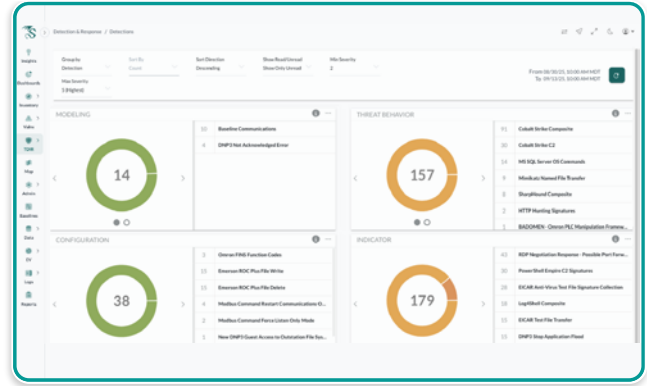
Key Features (cont.)

Investigation and Response



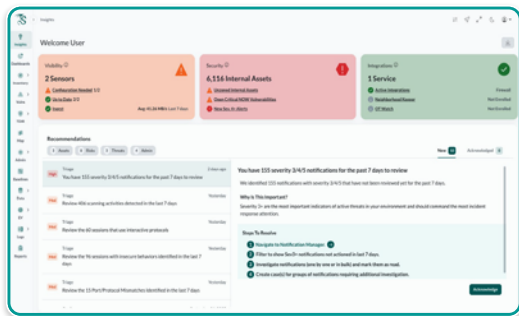
Dragos Platform users can easily create cases to initiate investigations by pulling in relevant activity logs, forensic data, threat intelligence reports, timeline views, and reference response playbooks written by Dragos experts for a comprehensive approach to investigating incidents and reducing crucial time to response.

Intelligence-Driven Threat Detection



The Dragos Platform offers the leading threat detection capability in the industry. Rapidly pinpoint malicious activity with four types of threat detection – modeling, configuration, indicators, and behavioral detections. Dragos incorporates cyber threat intelligence continuously, enabling up-to-date and contextualized analytics to provide deeper detection of threats.

INSIGHTS HUB



Your Central OT Security Dashboard

Unifies alerts, vulnerabilities, asset insights, operational status, and recommendations in one dashboard, plus AI-powered analysis infused with the Dragos Intelligence Fabric. Your starting point to see what matters, prioritize exposures, accelerate investigations, and reduce risk.

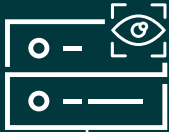
KNOWLEDGE PACKS

Dragos pushes regular content updates to the Dragos Platform content via Knowledge Packs including:

- Detections and threat analytics for new and evolving threats to include threat activity groups, ransomware, malware, and targeted exploits.
- Vulnerability advisories, detections, and guidance to the industry's largest vulnerability database.
- Protocol characterizations including updated ICS, equipment, and vendor protocols to expand dissection.
- Playbooks to guide cyber analysts to enable response and threat hunting efforts.



THE DRAGOS PLATFORM OFFERS FLEXIBLE MONITORING TO ADDRESS CUSTOMER REQUIREMENTS



DRAGOS PLATFORM INPUTS



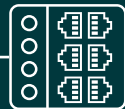
Sensor and Virtual Appliances:

Comprehensive passive monitoring via physical sensor appliances and virtual sensors, ensuring extensive coverage, minimal network disruption, and flexible deployments across diverse environments.



Active Collection with Dragos Agent:

Lightweight, purpose-built software executable for active data collection on Windows and Linux-based devices. Discovers isolated or low-traffic assets and connected devices to enrich inventories and enable software and OS 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

Seamlessly integrates with leading firewall vendors such as Fortinet, Cisco, CheckPoint, Palo Alto Networks, SIEM systems like Microsoft Sentinel, endpoint solutions including CrowdStrike, CMDB systems like ServiceNow, and AI models via Model Context Protocol (MCP) servers, enhancing asset enrichment, threat detection, and response capabilities.



SITESTORE

Aggregates Dragos Sensor asset, vulnerability, and threat information across connected sensors, including key workflows.



CENTRALSTORE

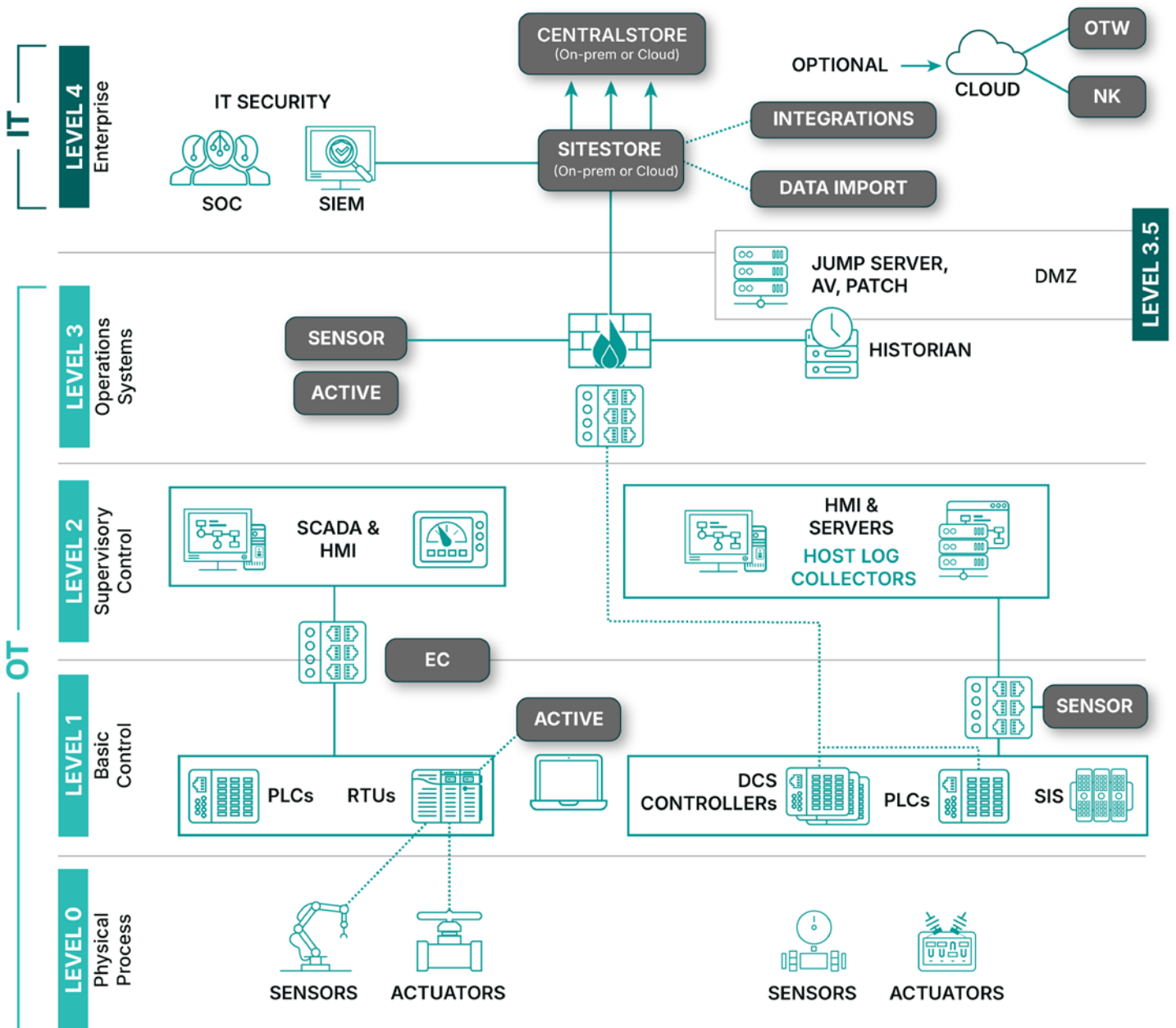
Optional component that offers SiteStore management enabling a central location for multi-enterprise aggregation, central dashboards, searching, and reporting.

DEPLOYMENT OPTIONS

Gain Visibility Through Flexible Monitoring

Preserve operational uptime with a “Do No Harm” monitoring approach. Industrial organizations need to monitor deep within the OT environment, at Levels 1, 2, 3, & 3.5 (the interface of OT/IT) of the Purdue Model.

THE DRAGOS PLATFORM DEPLOYMENT DIAGRAM



The Power of the Dragos Ecosystem

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

OT Watch

We put Dragos experts behind your Platform. Offered as scheduled threat hunts or as 24/7 managed platform coverage with OT Watch Complete, you get an OT security program that overcomes staffing constraints and delivers measurable outcomes sooner.

Neighborhood Keeper

An opt-in collective intelligence data network that enables Dragos Platform users to benefit from anonymously shared intelligence Neighborhood Keeper aggregates data and intelligence across organizations providing a view of threat activity and trends.

WorldView

Dragos fields the largest civilian OT-focused cyber threat intelligence operation. Adversary hunters research threat groups, their campaigns, and tactics. Vulnerability researchers conduct primary OT vulnerability discovery and analyze third-party vulnerabilities, providing OT risk and impact analysis. All findings are reported in Dragos WorldView and integrated into the Dragos Platform.

Supporting Services

Dragos offers critical services to operationalize an effective OT cyber defense. From technical account managers that help customers operationalize key platform use cases, to experienced OT incident responders, to consultants that help you assess your broader OT cyber defense architectures – we focus on helping you achieve your key OT cybersecurity outcomes.

Integrating with Security Operations

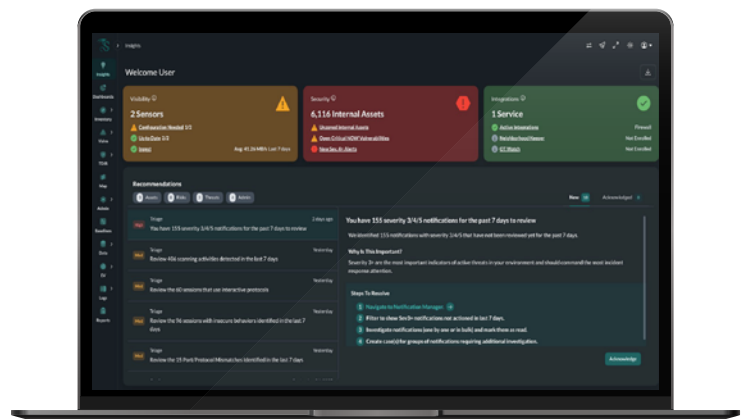
The Dragos Platform integrates with a wide variety of complementary technologies to enable customers to expand visibility and reduce time to response and recover across OT and IT environments while achieving maximum value from the investments made in their existing ecosystem including leading SIEMs, Firewalls, EDR and more.

Industrial OEM Partnerships

Dragos partners with industrial OEMs to validate interoperability of the Dragos Platform within industrial environments and help with development of new content to improve visibility and detections. Furthermore, our industrial OEM partners provide additional value to customers by providing an option to procure from, deliver, and support Dragos Platform into their OT operations.

See the full list of Dragos Partners:

www.dragos.com/partners/



ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**Learn more about our technology, services,
and threat intelligence offerings:**

[Request a Demo](#)

[Contact Us](#)