DRAGOS

SOLUTION BRIEF

Exposure Management

Use your existing tech stack to discover where you are exposed.
One source of truth for the full operational environment.

See everything, regardless of what you have deployed.

Every asset. Every exposure. Discover and rank everything across OT, IT, and cloud by ingesting the data your existing tools already produce. No new agents, credentials, or hardware required.

Overview

You can't protect what you can't see. Businesses operate in multiple environments. On-prem. Hybrid. Cloud. Each with assets and exposures that must be seen and identified to secure your total attack surface.

Dragos Exposure Management provides a single source of truth for assets and exposures across your entire attack surface: IT, OT, IoT, and cloud. It gives you a single, continuously updated exposure view, with no rip-and-replace and no new appliances or credentials required. It extends the asset discovery and classification the Dragos Platform is known for beyond sensor-covered OT networks into IT, cloud, and remote infrastructure, with a unified exposure view from day one.

Value starts on day one. You can discover assets and exposures immediately, without waiting to deploy hardware.

The challenge

Systems that influence physical processes are no longer just inside plant networks. Engineering workstations, cloud services, and remote access all extend the operational footprint that now defines the xOT environment.

Conventional discovery tools that rely on agents and credentials miss many OT devices. Point products cover one layer and leave the rest unprotected, scattering asset data across disconnected consoles. As security and asset discovery tools accumulate over time, the view becomes more fragmented, because none of them connect to or share information with the others. Blind spots with unmanaged, unknown, or non-agentable assets accumulate in the gaps between those tools.

Finding those blind spots and consolidating the data into one continuously updated view is what makes it possible to prioritize and respond to vulnerabilities and threats.

- ✓ **xOT environments are under active threat.** Adversary groups move through whatever part of the environment defenders can't see or don't have full situational awareness of.
- ✓ **Regulatory pressure is accelerating.** NIS2, DORA, NERC CIP, and NIST CSF require a current inventory of critical assets.
- ✓ **Organizations hold more isolated vulnerability findings than they can act on.** Existing telemetry rarely comes together in a single asset inventory.

© 2026 Dragos, Inc. All Rights Reserved.

The Dragos Intelligence Fabric

The Intelligence Fabric codifies over a decade of xOT-specific telemetry, asset and protocol research, adversary research, and frontline practitioner expertise into a continuously updating data lake, so exposure data reflects xOT context, not generic vulnerability scoring. Every exposure is enriched by the same living knowledge engine that powers the Dragos Platform.

Key capabilities

01
Complete discovery and deep situational awareness across the full xOT environment

02
High-fidelity asset fingerprinting

03
Cross-environment aggregation across the existing tech stack

04
Prioritization based on exploitability

05
Attack path and segmentation insight

06
Dragos Intelligence Fabric enrichment

07
Eliminate blind spots

08
Immediate risk prioritization and remediation recommendations

© 2026 Dragos, Inc. All Rights Reserved.

How Dragos delivers

01

Complete discovery without disruption

Dragos Exposure Management combines three discovery approaches: safe active scanning, always-on passive discovery, and pre-built integrations that automatically pull asset data from the tools already deployed across your tech stack. Together they identify unknown and unmanaged assets, endpoints, shadow IT, fragile OT, and other devices that static inventories miss. The result is a complete, unified asset inventory built in minutes, not months, with no agents, credentials, or appliances required.

© 2026 Dragos, Inc. All Rights Reserved.

02

High-fidelity fingerprinting

Assets are profiled against thousands of distinct device attributes without credentials or agents, delivering definitive intelligence on make, model, OS, firmware, installed software, open services, and operational role. For OT environments, it identifies sub-assets behind industrial protocol gateways, including field-level devices across Modbus, BACnet, Ethernet/IP, Siemens S7comm, and more than 220 protocols total, surfacing assets that traditional tools never reach. Every device is classified by category (IT, OT, or IoT) and function, so teams know what exists and what it does.

03

Aggregation across any source

Asset data is ingested from existing tools across your entire tech stack through pre-built integrations and a flexible SDK. It pulls from endpoint detection platforms, mobile device management, cloud providers, vulnerability scanners, CMDBs, and OT-specific management tools. Asset data is normalized, deduplicated, and correlated to eliminate conflicting records and fill gaps each source leaves behind.

04

Prioritize based on exploitability

Dragos Exposure Management goes beyond CVE lists. Exposures are ranked by each asset's full attribute profile and operational role, surfacing the risks most likely to lead to an incident rather than flooding teams with noise. Risk scores combine threat intelligence, vulnerability data, and operational context, so teams act on what matters first. Rapid response capabilities allow emerging threats to be assessed across the full inventory without rescanning. Remediation is confirmed by verified rescan, closing the loop from detection to resolution.

05

Attack path and segmentation insight

Research from Dragos Exposure Management shows that in manufacturing environments, roughly 30% of OT assets sit one hop from an internet-exposed device, and 90% within two hops. Interactive topology maps, path tracing, and choke point identification show exactly how an adversary would move through the network. Topology mapping links internal architecture with external exposure, charting the paths an adversary would take.

© 2026 Dragos, Inc. All Rights Reserved.

06

Connected to the Dragos Intelligence Fabric

Exposure data is enriched by more than a decade of OT-specific telemetry, adversary research, and frontline incident response.

07

Eliminate blind spots

Existing tools only see and know what is registered and already protected, leaving shadow IT, unmanaged legacy devices, fragile OT, and more completely invisible. Discover these invisible devices and eliminate inventory blind spots.

08

Immediate risk prioritization and remediation recommendations

Risk prioritization and remediation recommendations for assets and exposures across the entire attack surface. Identify ownership and create tickets for remediation. Track both ticket and exposure status, as well as security posture with goals and improvement metrics.

How Dragos Exposure Management works

No agents, credentials, or appliances required

Dragos Exposure Management uses an agentless combination of active scanning, passive discovery, and API integrations to uncover and safely fingerprint every asset across your internal and external attack surfaces, including unknown and unmanageable devices, with depth and accuracy.

Safe active scanning

The safe active discovery engine in Dragos Exposure Management sends only normal traffic. Scan rates are configurable with per-host pacing controls that protect fragile devices.

Always-on passive discovery

Passive discovery monitors network traffic continuously without sending any probes. It delivers always-on coverage, detailed fingerprinting, and superior data accuracy for the most sensitive devices on the OT floor, including fragile environments where active scanning is not permitted. Passive and active data are automatically correlated into a single asset record, so teams see one inventory, not two separate datasets that must be reconciled manually.

Integrations and SDK

Pre-built integrations connect Dragos Exposure Management to leading cloud providers, endpoint detection and response platforms, mobile device management, vulnerability scanners, and OT asset management tools already in your environment. A flexible SDK enables custom integration with any additional source the organization operates. Asset data

© 2026 Dragos, Inc. All Rights Reserved.

from all connected sources is normalized and correlated automatically, creating one continuously updated inventory. Egress integrations push enriched asset and exposure data back into the workflow tools teams already use for remediation and reporting.

Uncover hidden risks that other tools overlook

Dragos Exposure Management delivers insight into exposures that evade other tools. Its fingerprinting methodology analyzes each asset's attributes and connections to identify hidden risks that traditional tools overlook, pinpointing critical issues instantly without relying on signatures or rescanning. Your security team moves from discovery to mitigation faster, stays compliant, and shrinks the window of exploitability.

OT-specific discovery: what other tools miss

Most organizations operate under a "segmentation illusion," assuming their OT environments are isolated when the evidence says otherwise. Industry research consistently finds that more than a third of organizations have at least one OT asset exposed to the public internet. Dragos Exposure Management uses discovery capabilities that conventional tools lack.

01

Peering behind protocol gateways

Dragos Exposure Management enumerates sub-assets hidden behind industrial protocol gateways, including PLCs, RTUs, and field devices that are not directly addressable on the network. Support for more than 220 OT and IoT protocols, including Modbus, BACnet, Ethernet/IP, KNXnet, Siemens S7comm, and Triconex TriStation, surfaces devices that passive-only tools and traditional scanners never reach.

02

Inside-out attack surface management

Inside-Out Attack Surface Management compares the unique fingerprints of internal assets against a global database of public endpoints, identifying internal systems exposed to the internet that the organization may not know about. This gives practitioners an external attacker perspective on their own environment without requiring a separate external scan tool or a second engagement.

© 2026 Dragos, Inc. All Rights Reserved.

03

Segmentation validation, not segmentation assumption

Interactive attack path mapping and 2D/3D topology views show exactly how IT exposure connects to OT systems. Multi-homed device detection flags assets connected to multiple network segments that bypass firewall controls. Choke point analysis prioritizes the handful of devices that, if compromised, give adversaries access to the broadest set of high-value targets. Anomaly detection flags misplaced assets automatically, such as a Windows laptop inside a production zone, without requiring manual review.

04

xOT asset taxonomy

Every fingerprinted asset is assigned to a category and one or more operational functions from a defined taxonomy: Process Control, Safety, Engineering, Human Interface, Monitoring, Networking, Communications, Power Management, Remote Access, and others. This structured classification allows security teams to slice the asset inventory for operational purposes, not just by IP range, enabling risk analysis and policy enforcement that reflects how the environment actually works.

Dragos Exposure Management operates alongside the Dragos Platform, trusted by 600+ customers globally and protecting 7.8 million assets across hundreds of industrial facilities. The Dragos Platform is named a Leader in the Gartner® Magic Quadrant™ for CPS Protection Platforms. Dragos is also named a Leader in the Forrester Wave evaluation of the OT security market.

600+
customers globally

7.8 million
assets protected across hundreds of industrial facilities

3-6%
of OT vulnerabilities require immediate action

Benefits

- ✓ **Value on day one.** Dragos Exposure Management requires no agents, credentials, or appliances. It integrates with what you already have. Organizations are up and running in minutes, with asset inventory results available immediately. Existing asset data from deployed tools is ingested and correlated on day one, giving practitioners a complete cross-environment view before the first Dragos Platform sensor is placed. Deployment is measured in minutes rather than project cycles, saving teams 20+ hours a week previously spent on manual discovery.

© 2026 Dragos, Inc. All Rights Reserved.

- ✓ **Safe active scanning for IT, OT, and IoT.** Proprietary active scanning technology discovers everything on your network, including unknown and unmanageable devices, providing detailed insight into OSs, services, hardware, and installed software through advanced fingerprinting proven safe for even the most sensitive OT and IoT environments.
- ✓ **Always-on passive discovery.** Passive discovery delivers always-on coverage with faster deployment and immediate results. It provides detailed fingerprinting and superior data accuracy for fragile OT environments where active scanning is not permitted.
- ✓ **One source of truth.** Dragos Exposure Management provides a single source of truth for exposure management across your total attack surface. Security, engineering, and operations teams work from the same continuously updated inventory across the full operational environment, instead of reconciling separate consoles by hand.
- ✓ **Act on what matters.** Contextual prioritization cuts through alert noise so teams fix the exposures adversaries would actually use first. Exposures are ranked by each asset's attributes and role, with remediation confirmed by verified rescan.
- ✓ **Demonstrate posture to regulators and boards.** Audit-ready inventory and exposure reporting supports NERC CIP, NIS2, DORA, and NIST CSF.
- ✓ **Get more from your tools.** Pre-built API integrations, an SDK, and asset intelligence connect you with leading cloud providers, EDRs, MDMs, vulnerability scanners, endpoints, CMDBs, and network tools. Data consolidates into one unified view with complete visibility into every asset and exposure across complex environments, so existing investments cover more ground without rip-and-replace.
- ✓ **Start anywhere, grow into full xOT security.** Exposure management is a natural first step toward network monitoring, threat detection, and OT Watch managed threat hunting.

Proof points

1.3M+
OT, IT, and IoT devices given visibility across 343 public schools

15K
previously unknown assets discovered by a university security team

20+ hours
saved per week while safely discovering fragile OT environments

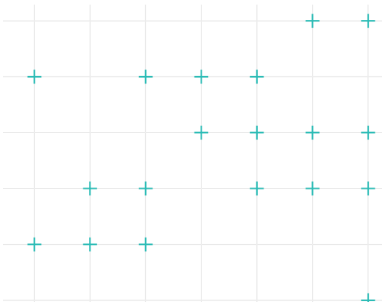
Why Dragos for Exposure Management

Discovery tools built for IT cannot safely touch OT devices. Dragos brings xOT-native discovery together with over a decade of operational context, so ranking reflects what matters.

- ✓ **Safe for fragile OT.** Discovery runs without the agents and credentials conventional tools require, so assets that cannot tolerate active scanning are still identified and profiled.

© 2026 Dragos, Inc. All Rights Reserved.

- ✓ **A path to full xOT security.** Exposure management is a starting point that extends into network monitoring, threat detection, and OT Watch managed threat hunting on the same platform.



The xOT Standard, Secured

xOT is a new standard for defining and defending the full operational environment: any system whose failure affects operations belongs to it. The Dragos Platform secures that environment, and Dragos Exposure Management ensures no part of it stays unseen, whether a sensor is in place yet.

FAQs

Do I need to deploy a sensor to use exposure management?

No. Dragos Exposure Management ingests asset data from tools already in place, including endpoint, CMDB, cloud, EDRs, MDMs, vulnerability scanners, and network sources, and produces a unified exposure view from day one. Sensors add deep xOT network threat detection and protocol-level visibility, and the two work together.

Will this replace the OT security tools we already have?

No, it supplements them. Exposure Management ingests data from a range of platforms, including competitive tools and legacy inventories, so a mixed-vendor stack can be consolidated into one exposure view without rip-and-replace. Existing investments are extended rather than displaced.

How is exposure prioritized differently from a CVSS score?

Exposures are ranked using each asset's attributes and operational role, not severity alone. CVSS was designed for IT and overstates risk in OT context. Dragos applies OT-corrected scoring and "Now, Next, Never" prioritization to identify what genuinely requires action.

Which compliance frameworks does an asset inventory support?

NERC CIP, NIS2, DORA, and NIST CSF all require organizations to maintain a current inventory of critical assets. A continuously updated, cross-environment inventory provides the audit-ready evidence to demonstrate that requirement is met.

© 2026 Dragos, Inc. All Rights Reserved.

Talk to an xOT security specialist.

See how Dragos Exposure Management builds your asset inventory and exposure view across IT, OT, IoT, and cloud.

Request a platform demo Contact us

© 2026 Dragos, Inc. All Rights Reserved.

About Dragos

Dragos is the global leader in xOT cybersecurity and is purpose-built to protect the industrial and critical infrastructure that civilization depends on.

The Dragos Platform delivers visibility, continuous monitoring, and threat detection across expanded xOT environments at scale. It is powered by the Dragos Intelligence Fabric, built from over a decade of xOT-specific telemetry, adversary research, and incident response. Dragos EmberAI puts that intelligence directly in analysts' hands so each can operate like a professional regardless of their experience. Dragos xOT Threat Intelligence delivers finished threat intelligence built exclusively for xOT, produced by the largest private ICS/OT threat intelligence team in the industry. Dragos Expert Services provide direct access to frontline expertise, from security assessments to 24/7 incident response.

No other organization brings xOT-specific technology, intelligence, and services together under one roof.

Dragos protects organizations across electric, oil and gas, manufacturing, water, transportation, mining, and government sectors, operating globally from its headquarters in Hanover, Maryland.

Learn more: **dragos.com**

© 2026 Dragos, Inc. All Rights Reserved.