DRAGOS

SOLUTION BRIEF

Exposure Management

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

Overview

Dragos Exposure Management Module integrates with and extends the tools already in your tech stack. It combines data from existing CMDBs, endpoint platforms, OT asset managers, cloud inventories, and vulnerability scanners to produce a single, continuously updated exposure view across IT, OT, IoT, and cloud environments. No rip-and-replace. No new appliances. No credentials required. Value starts on day one.

The Challenge

The systems that influence physical processes no longer sit neatly inside a plant network. Engineering workstations, cloud services, and remote access all extend the operational footprint that now defines the xOT environment. Conventional discovery tools rely on agents and credentials that cannot safely touch OT devices. Point products cover one layer and leave the rest unprotected, scattering asset data across disconnected consoles. Security and asset tools accumulate over time, each holding a partial view of the environment and none of them connected to the others. The gaps between those consoles are where blind spots form, unintentionally, and without anyone noticing.

- ✓ **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.
- ✓ **Regulatory pressure is accelerating.** NIS2, DORA, NERC CIP, and NIST CSF require a current inventory of critical assets.
- ✓ **The skills gap is structural.** Organizations cannot hire their way to complete visibility. Existing tech stacks can be leveraged to do more of the work.

THE DRAGOS INTELLIGENCE FABRIC

The Intelligence Behind Every Exposure

Over a decade of xOT-specific telemetry, asset and protocol research, adversary research, and frontline practitioner expertise, codified into a continuously updating data lake. 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

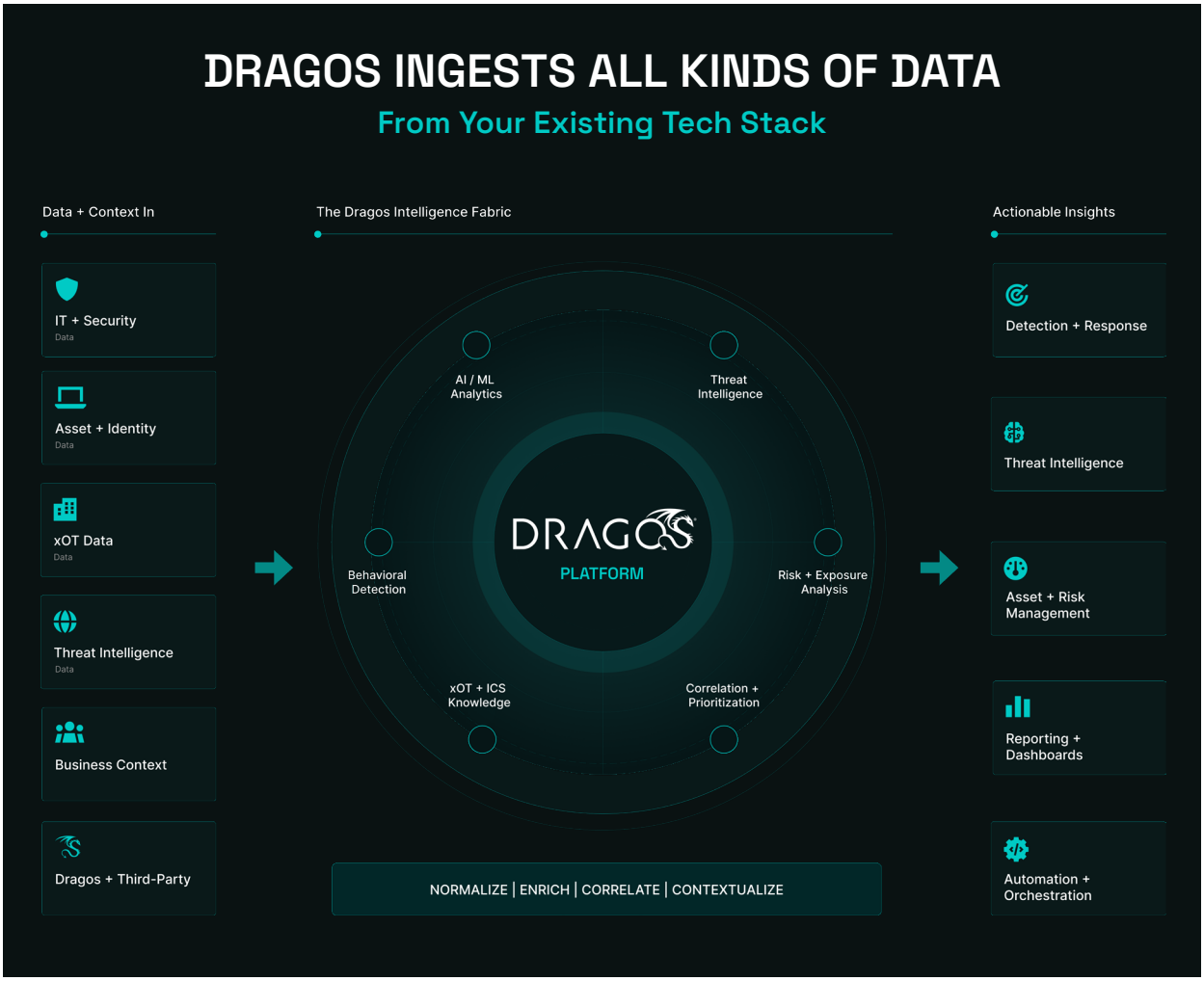
02
High-Fidelity Asset Fingerprinting

03
Cross-Environment Aggregation Across the Existing Tech Stack

04
Context-Based Exposure Prioritization

05
Attack Path & Segmentation Insight

06
Dragos Intelligence Fabric Enrichment



How Dragos Delivers

01

Complete Discovery Without Disruption

The Dragos Exposure Management Module combines three discovery approaches: safe active scanning, always-on passive discovery, and pre-built integrations that pull asset data from the tools already deployed across your tech stack. The result is a complete asset inventory built in minutes, not months, with no agents, credentials, or appliances required.

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 not just what exists, but what it does.

03

Aggregation Across Any Source

Asset data is ingested from existing tools across your 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

Exposure Prioritization Built on Context

The Dragos Exposure Management Module 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 & Segmentation Insight

Research from the Dragos Exposure Management Module 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.

06

Connected to the Intelligence Fabric

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

How the Dragos Exposure Management Module Works

Safe Active Scanning

The Dragos Exposure Management Module's safe active discovery engine 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. Passive and active data are automatically correlated into a single asset record, so teams see one inventory, not two separate datasets that have to be reconciled manually.

Integrations and SDK

Pre-built integrations connect the Dragos Exposure Management Module 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 integrations with any additional source the organization operates. Asset data 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.

OT-Specific Discovery: What Others Miss

Most organizations operate under a "segmentation illusion," assuming 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. The Dragos Exposure Management Module leverages specific discovery capabilities that no conventional tool can match.

01

Peering Behind Protocol Gateways

The Dragos Exposure Management Module 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 capability 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.

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 an adversary 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

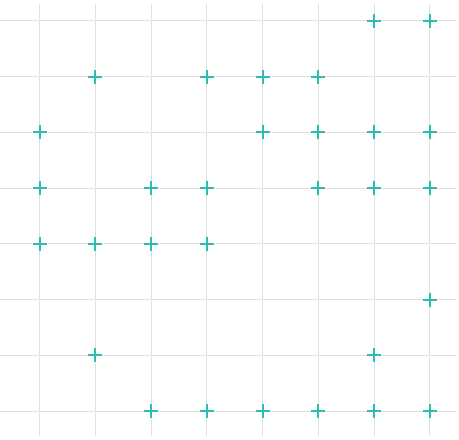
OT Asset Taxonomy

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.

The Dragos Exposure Management Module operates alongside the Dragos Platform, trusted by 600+ customers globally protecting 7.8 million assets across hundreds of industrial facilities, and was recognized as part of the platform named a Leader in Gartner® Magic Quadrant™ for CPS Protection Platforms.

Benefits

- ✓ **Value on day one.** The Dragos Exposure Management Module 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.
- ✓ **One source of truth.** Security, engineering, and operations teams work from the same continuously updated inventory across the full operational environment.
- ✓ **Act on what matters.** Contextual prioritization cuts through alert noise so teams fix the exposures adversaries would actually use first.
- ✓ **Demonstrate posture to regulators and boards.** Audit-ready inventory and exposure reporting supports NERC CIP, NIS2, DORA, and NIST CSF.
- ✓ **Start anywhere, grow into full xOT security.** Exposure management is a natural first step toward network monitoring, threat detection, and OT Watch managed hunting.



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 is the solution, and Universal Exposure Management ensures no part of that environment stays unseen, whether a sensor is in place yet.

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