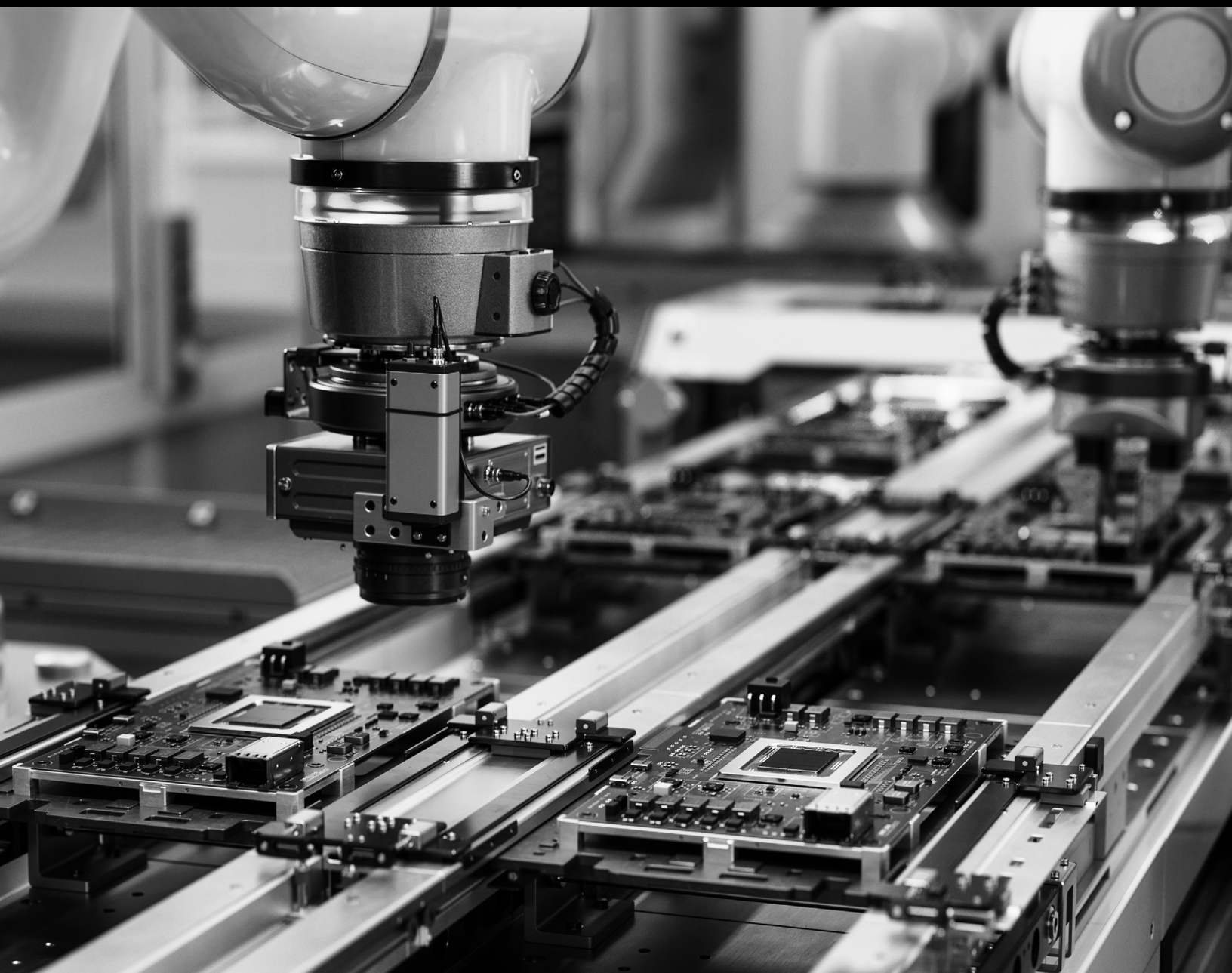
DRAGOS

SOLUTION BRIEF

Software & Supply Chain

Know what is inside the software your operations depend on, before it is deployed and before it is exploited.



Overview

xOT risk does not begin at the network boundary. It begins in the supply chain of firmware and software, long before a device reaches the operational environment. Dragos Software and Supply Chain Module extends the visibility, security and manageability with binary-level analysis of compiled firmware and software, surfacing embedded risks inherent in the code that runs the devices and assets xOT environments depend on.

The Challenge

Modern software is assembled, not just built. Roughly 80% of the code in a vendor's software is written by open-source contributors the buying organization does not employ and has no visibility into (NetRise, 2026). AI-assisted development compounds the problem: code produced with AI tooling routinely pulls in libraries, packages, and dependencies that no developer on the project ever vetted, and those components ship into production alongside everything else. Vendor SBOMs and attestations routinely miss what is actually in compiled artifacts, and regulations including the EU Cyber Resilience Act, NERC CIP, NIS2, and TSA directives increasingly require organizations to demonstrate software component transparency.

- ✓ **Supply chain incidents move faster than manual review.** A backdoor cultivated over years, a library weaponized within hours of disclosure: defenders could not answer where it was.
- ✓ **One compromised component reaches many organizations at once.** The same open-source libraries and vendor packages are deployed across operators, sectors, and geographies. When a single component is poisoned, adversaries can gain a foothold and establish a path to command and control in every environment that uses it.
- ✓ **The xOT environment runs on firmware never designed for inspection.** Every system that influences a physical process depends on software most organizations cannot see inside.
- ✓ **Most organizations cannot demonstrate transparency.** Regulatory frameworks increasingly require it, and most cannot produce the evidence.

How it Works

OT network monitoring tells you what is communicating across your environment. The Dragos Software and Supply Chain Module tells you what's actually running inside the devices themselves.

The platform analyzes compiled binary code in firmware, XIoT devices, containers, and applications without requiring source code access — which in xOT environments almost never exists for the PLCs, RTUs, and network appliances practitioners to depend on. Through Binary Composition Analysis, it generates a verified software bill of materials (SBOM) for every device. Identifying components the vendor may not even know are present.

From there, reachability analysis identifies which vulnerable code executes at startup, cutting through lists of thousands of CVEs to surface what's actually exploitable. A single query via AI powered search can then trace impacted assets across an entire device fleet, compressing investigations that would otherwise take days.

The result is verified visibility into the software running south of the firewall — not vendor self attestation, not assumptions. Ground truth.

Key Capabilities

01
Compiled Code & Firmware Binary Analysis

02
SBOM Generation, Ingestion & Enrichment

03
Open-Source Provenance & Contributor Risk

04
Blast Radius Scoping in Minutes

05
Pre Compile and Pre-Deployment Weakness Identification

06
Dragos Intelligence Fabric Enrichment

THE DRAGOS INTELLIGENCE FABRIC

The Intelligence Behind Every Component

Over a decade of xOT-specific telemetry, asset and protocol research, adversary research, and frontline practitioner expertise, codified into a continuously updating loop. Findings from Software and Supply Chain Module feed the same living knowledge engine that powers intelligence and depth of the Dragos Platform.

How Dragos Delivers

01

Firmware & Software Binary Analysis

Compiled code is analyzed directly, generating and enriching SBOMs for OT and xoT devices. Findings include embedded vulnerabilities, exposed credentials, and misconfigurations.

02

Open-Source Provenance & Contributor Risk

Every component's origin, maintainers, and repository health are assessed, identifying nation-state contributors and dependency poisoning risks source-based tools miss.

03

Blast Radius in Minutes, Not Months

When a component or maintainer is compromised, exposure is scoped upstream and downstream so teams remediate with evidence instead of guesswork.

04

Pre-Deployment Weakness Identification

Weaknesses in compiled software are identified before devices enter the operational environment, including risk introduced by AI-generated code.

05

Policy Enforcement at Intake

Non-compliant or malicious packages are stopped in the build pipeline before they land in production artifacts.

06

Connected to the Intelligence Fabric

Supply chain findings feed the Dragos Intelligence Fabric, sharpening defense across the full operational environment.

Proof Points

<1 min

to identify the blast radius of a compromised open-source component, versus days of manual tracing

0 days

of reverse engineering. Behavioral analytics flag abnormal activity before a CVE exists, and binary analysis names every affected asset the moment it does.

44%

of AI-generated code fails security testing, a rate unchanged across four years and 100+ models*

This capability is backed by the organization with over a decade of OT-specific incident response experience, more than 5 petabytes of daily OT telemetry feeding the Dragos Intelligence Fabric, and recognition as a Leader in the 2026 Gartner Magic Quadrant for CPS Protection Platforms.

* Source: NetRise incident analyses and platform data, 2026 (XZ Utils and Log4Shell case analyses).

Benefits

- ✓ **Know your application risk before it becomes an incident.** Findings embedded in device software and firmware are surfaced before those devices are deployed.
- ✓ **Compress incident response from days to minutes.** When the next supply chain compromise emerges, query the environment, map the exposure, and act with confidence.
- ✓ **Verify vendors with evidence.** Before accepting vendor software, know what is actually inside it, not just what was declared.
- ✓ **Demonstrate posture to regulators and boards.** SBOM management and audit-ready documentation support EU CRA readiness, NERC CIP, NIS2, and TSA directives.
- ✓ **Start before the network, grow into full xOT security.** Supply chain intelligence engages organizations before any OT program exists, opening a path to exposure management, asset visibility, and OT Watch managed hunting.

The xOT Standard, Secured from the Source

The operational environment begins with the supply chain of firmware and software and extends inward through connected systems to the operational core. xOT is the standard for defending that full environment, and the Dragos Platform is the solution.

The Platform works across that entire footprint: the code inside firmware and software, the assets running the process, the IT and cloud systems that touch operations, and the security tools already in place. Behind it sits the Dragos Intelligence Fabric, built from over a decade of OT-specific telemetry, adversary research, and frontline incident response, alongside Dragos WorldView threat intelligence, OT Watch managed threat hunting, and Dragos Expert Services when teams need people working next to the technology. No other organization brings xOT-specific technology, intelligence, and services together under one roof.

The Software & Supply Chain Module secures that environment from the earliest point risk can enter: the code itself.

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