



SOLUTION BRIEF

# Vulnerability Management for xOT Environments

Focus on the 3–6% that need attention now.



## The Challenge

### Thousands of Vulnerabilities. One Maintenance Window.

OT security teams face thousands of vulnerabilities each year, and the environment they are responsible for keeps growing. It now reaches past controllers into engineering workstations, remote access, cloud and AI systems, automation, and facility infrastructure: what Dragos calls Extended Operational Technology, or xOT.

Most of those vulnerabilities are not critical. The hard part is knowing which ones are, and how to respond without risking operations. Published CVSS scores do not take into account asset criticality or reachability and IT vulnerability tools inherit a similar blind spot, flooding defenders with noise and guidance that is unsafe to apply in OT.

## The Dragos Platform

### Risk-Based Vulnerability Management, Built for xOT

The Dragos Platform provides risk-based xOT vulnerability management with prioritization guidance to help defenders mitigate vulnerabilities without disrupting operations. It aligns hardware, software, and OS vulnerabilities to the assets you actually run, applies OT-specific context, and provides clear “Now, Next, Never” guidance, so the 3 to 6 percent of xOT vulnerabilities that require immediate action (Dragos 2026 OT Cybersecurity Year in Review) become a working list rather than a statistic.

Weekly Knowledge Packs ensure defenders work from continuously updated data and recommendations. Purpose-built for xOT, the Platform combines analyst-reviewed vulnerability data, clear prioritization, and operationally safe guidance to protect critical environments.

#### IN THE PLATFORM

## One Record, From Detection to Proof of Fix



### 01

#### Asset Inventory and Network Mapping

Every device profiled by make, model, firmware, OS, and lifecycle status. Passive monitoring across 600+ OT protocols, Safe Active Discovery, and file import feed one inventory, and network mapping shows which vulnerabilities are reachable.



### 02

#### Continuously Updated Vulnerability Matching

Each vulnerability is matched to the assets in your inventory, by hardware, firmware, OS, and software, with match confidence on every finding. Weekly Knowledge Packs deliver new vulnerabilities, scoring, guidance, and detection.



03

**OT-Corrected Scoring**

Dragos researchers correct published CVSS scores against four questions: Is it reachable here? Are ICS-targeting groups exploiting it? What controls are already in place? What would exploitation do to the process?



04

**"Now, Next, Never" Prioritization**

What to address inside the current operational window, what to plan for the next maintenance window, and what to document and monitor. Filtering to Now produces the working list; a crown jewel insight surfaces the matches that matter most.



05

**Operationally Safe Guidance**

Expert-developed guidance for every vulnerability: immediate patching or alternatives such as segmentation, access controls, configuration changes, and detection coverage, so risk drops before the maintenance window arrives.



06

**Centralized Tracking and Dispositions**

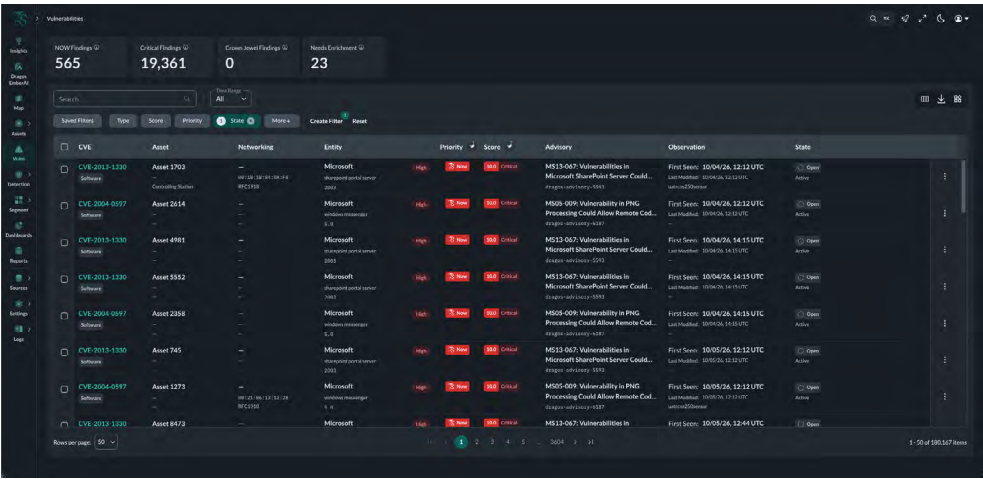
One record from identification through resolution. Six states with dispositions underneath that capture what is actually happening: waiting on a vendor patch, scheduled for the next outage, or risk-accepted with controls and a review date.

## The Foundation

### An Inventory The Vulnerability List Can Trust

Prioritization is only as good as the inventory it runs on. The Dragos Platform profiles every asset by vendor, model, firmware, operating system, zone, and hardware lifecycle status, so a vulnerability is tied to the exact equipment it affects and devices nearing end of support are visible before an advisory lands.

Passive monitoring across 600+ OT protocols is the foundation; Safe Active Discovery adds firmware and patch-level detail in segments that carry little traffic, and file import covers sites that monitoring cannot reach. Crown jewel tagging carries through to prioritization, so the assets whose compromise matters most are never buried in the list.

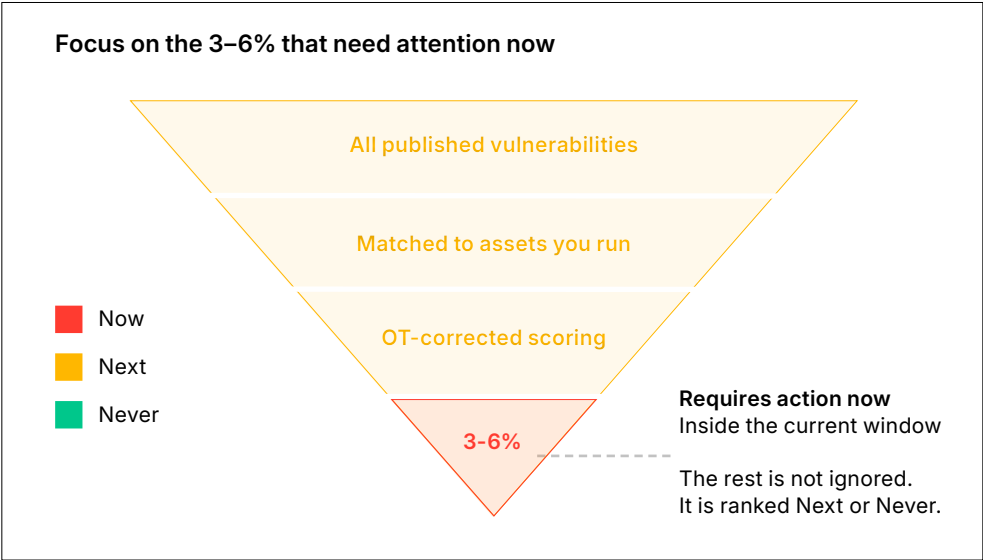


Vulnerabilities view in the Dragos Platform: every finding tied to the asset, vendor, model, and firmware version it affects, with “Now, Next, Never” priority, match confidence, the related Dragos advisory, and lifecycle state on the same row.

The Model

Now, Next, Never

Every published vulnerability is the starting universe. Matching to real assets removes what is not deployed. OT-corrected scoring removes what cannot be reached or exploited in this architecture, and raises what sits closer to the process than its published score suggests. What survives is the Now tier. The remainder is ranked, not discarded.



Source: Dragos 2026 OT Cybersecurity Year in Review



Each stage narrows the list against a different question. Only the vulnerabilities that survive all three earn the current operational window.

Now

Actively exploited, reachable in your environment, and tied to crown jewel assets or safety systems.

Act within the current operational window. Patch where possible; apply compensating controls where it is not yet feasible.

Next

Significant but not immediately exploitable: not yet actively exploited, partially mitigated by existing architecture, or constrained by operational access.

Plan remediation for the next maintenance window. Track and monitor; review if intelligence shows the risk profile changing.

Never

Will not materially improve the security posture of the device or environment even if fully remediated.

Deprioritize and document the rationale. Do not spend a maintenance window on remediation that produces no risk reduction.

PRIORITY, SCORE  
AND CONFIDENCE

What an  
Analyst Sees  
on Every Row



01

Priority Beside Severity

The tier sits alongside the published CVSS score rather than replacing it, so an analyst sees generic severity and OT-corrected priority on the same row. The record shows the threat analysis behind the correction: exploitation status, reachability, and what exploitation would do to the process.



02

Match Confidence

High confidence means the Platform has confirmed the vulnerability affects that specific asset. Medium indicates a partial match that needs qualification before the finding is worked.





03

Dispositions, Not Open and Closed

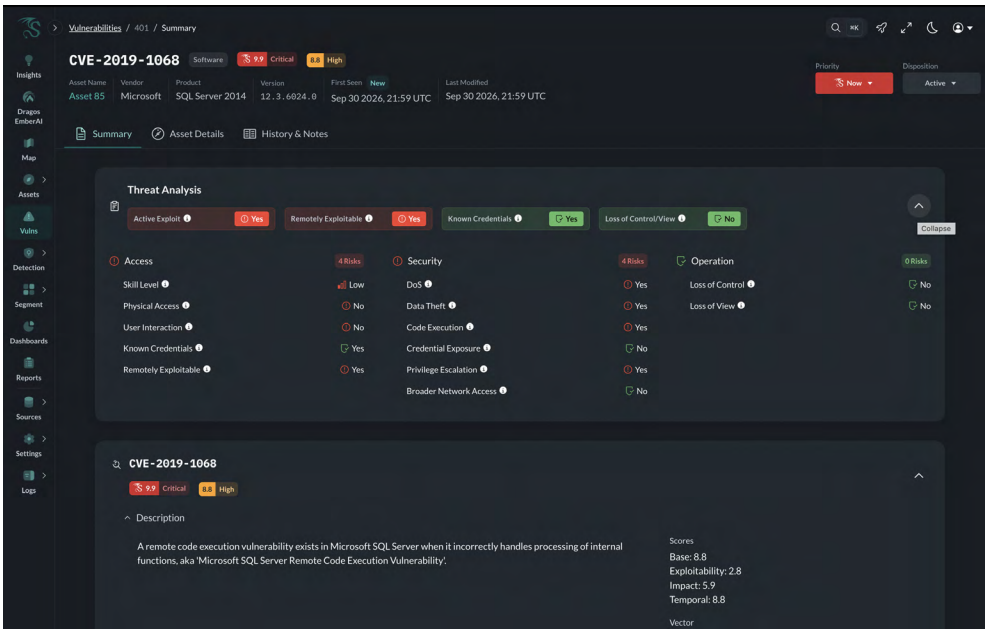
Every disposition rolls up to a parent state, so risk acceptance carries its compensating controls and a review date, and service level clocks attach to real movement rather than a binary status. Set through the interface or API; add custom dispositions where a workflow needs one.



04

Crown Jewel Insight

Where crown jewel assets are tagged, a dedicated insight counts Now-priority vulnerabilities with high-confidence matches on them and links to a filtered view.



A single vulnerability record: priority and disposition set at the top, with threat analysis (active exploitation, remote exploitability, known credentials, loss of control or view), access, security, and operational risk factors, scores, and the related advisory in one view.



## Why Dragos

# Built For The Environment You Actually Run



### 01

#### Built for The Full xOT Environment

Vulnerability matching runs against every system that can influence the process, whichever team owns it and whichever category it was filed under, not just the traditional OT core.



### 02

#### Grounded in The Dragos Intelligence Fabric

Vulnerability research is connected with adversary activity across the 26+ OT threat groups Dragos tracks by name, so priority moves when adversary behavior changes, not when a catalog updates.



### 03

#### Triage at The Speed of The Window

Dragos EmberAI puts that same intelligence in the hands of every analyst, through expert-built Skills for crown jewel analysis and vulnerability prioritization that run the triage a Dragos analyst would.



DRAGOS  
EmberAI

**Dragos EmberAI is the AI specifically built for xOT**

Built on the Dragos Intelligence Fabric, EmberAI activates over a decade of OT-specific telemetry, adversary research across 26+ tracked threat groups, vulnerability analysis, and frontline incident response expertise — making that intelligence immediately accessible to every analyst, regardless of their OT background.

## About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil and gas, manufacturing, water, and transportation.

Learn more: [dragos.com](https://dragos.com)

