PARTNER SOLUTION BRIEF

Dragos and CrowdStrike: Discover, Monitor, and Secure OT Assets

Complete asset visibility and threat detection for ICS environments, pairing the Dragos Platform's xOT-native coverage with CrowdStrike Falcon® endpoint data for one accurate picture of operations.

OVERVIEW

Executive Summary

Extended operational technology (xOT) is the full operational environment: everything that influences a physical process, from traditional control systems to the newest devices on the network. Securing it starts with knowing what is in it, and that is harder than it looks. Even environments with strong endpoint coverage hold devices no agent can reach, and inventories drift the moment operations change. Together, Dragos and CrowdStrike help organizations discover, monitor, and secure OT asset inventory in ICS environments, pairing the Dragos Platform's xOT-native visibility and threat detection with endpoint data from CrowdStrike Falcon® for one complete, accurate picture of the assets that keep operations running.

HIGHLIGHTS

One Accurate Picture of Everything That Influences Operations

01

See Every Asset That Influences Operations

The Dragos Platform discovers every asset, from traditional control systems to the newest devices on the network, with complete visibility and context.

02

Cover The Assets Agents Cannot Reach

Endpoint agents can't be deployed on most devices that influence physical processes. The Dragos Platform monitors them passively, without adding operational risk.

03

Enrich Both Platforms With Two Integration Flows

Dragos asset inventory flows into CrowdStrike Falcon® Discover for IoT, and Falcon endpoint data enriches Dragos assets through operator-approved mapping.

04

Fix The Vulnerabilities That Matter First

"Now, Next, Never" prioritization focuses teams on the 3–6% of OT vulnerabilities requiring immediate action (Dragos 2026 Year in Review).

05

Respond Without Stopping Production

Falcon detections on edge ICS devices pair with Dragos response playbooks built to prioritize operational uptime alongside threat mitigation.

The Challenge

In ICS environments, security starts with a question most organizations cannot answer with confidence: what is actually in the environment? OT asset inventories are difficult to build and nearly impossible to keep current. Assets communicate only during specific operational events, and manual records go stale the moment a system changes. Without an accurate inventory, vulnerability management is guesswork and incident response is blind.

The gap is structural. Most of the devices that influence physical processes, including programmable logic controllers (PLCs), remote terminal units (RTUs), and human-machine interfaces (HMIs), cannot run endpoint agents at all. Security tools built for the enterprise do not speak industrial protocols, cannot safely operate in operational networks, and were not built for environments where a wrong move can stop a turbine. The result is a blind spot covering exactly the assets that matter most.

Adversaries know it. More than 26 threat groups targeting OT environments are now tracked by name (Dragos 2026 Year in Review), continually evolving tactics, techniques, and procedures (TTPs) that use subtle behaviors designed to get lost in the noise. The consequences are measured in downtime, safety risk, and lost production, not just data. Closing the gap starts with one accurate, continuously current picture of the environment.

The Solution: Better Together

The Dragos Platform secures the xOT environment, built to see, detect, understand, and protect everything that influences a physical process. For organizations that also run CrowdStrike Falcon®, two integrations connect the platforms so asset data flows in both directions and both consoles work from the same accurate picture.

What The Dragos Platform Delivers

The Dragos Platform delivers xOT-native network visibility and security monitoring across all levels of the Purdue Model, with deep situational awareness across 600+ industrial protocols. See it: discover every asset, from traditional control systems to the newest devices on the network, passively and with complete context. Detect it: identify adversary TTPs and threats targeting operations using continuous monitoring and behavioral analytics, informed by the team that tracks more OT threat groups by name than any other organization. Understand it: query intelligence in plain language, with expert playbooks and alternative mitigations. Protect it: validate segmentation policy, harden devices at scale, prioritize vulnerabilities with “Now, Next, Never,” and respond with confidence. All of it is powered by the Dragos Intelligence Fabric: a decade of OT-specific telemetry, adversary research, and frontline incident response expertise.

PLATFORM COVERAGE

Where CrowdStrike Falcon® Fits

CrowdStrike Falcon® provides endpoint detection and response where agents can be deployed: the servers, workstations, and edge devices that support operations. CrowdStrike Falcon® Discover for IoT gives Falcon customers a unified console view of the broader device estate. The Dragos Platform complements that coverage, going where agents cannot, so the environment is protected end to end.

Dragos Platform Data Connector

Brings Dragos-discovered OT asset inventory into CrowdStrike Falcon® Discover for IoT. Falcon customers get an accurate, current view of ICS assets, including PLCs, RTUs, HMIs, historians, and engineering workstations, with segmentation context across virtual zones, Purdue levels, and ICS protocols.

Dragos Endpoint Asset Enrichment

Pulls Falcon endpoint asset details into the Dragos Platform. Operators review match evidence and approve each endpoint-to-asset mapping before it's committed. Confirmed Falcon detections generate notifications in the Dragos Platform for coordinated response.

Unified Visibility

OT assets appear alongside the rest of the estate in the console analysts already use. Detections correlate across both platforms, helping investigations move faster with shared asset context and reducing mean time to recovery (MTTR).

SANS ICS 5 Alignment

Integrating asset visibility, vulnerability management, threat detection, and response helps organizations align to the SANS ICS 5 Critical Controls for defending ICS and OT environments.

Availability & Deployment

The Dragos Platform Data Connector and Dragos Endpoint Asset Enrichment for OT are available on the CrowdStrike Marketplace and are configured within the respective platforms.

The Dragos Platform enables network visibility across all levels of the Purdue Model with multiple methods of data capture to assure environment availability and comprehensive coverage.

BETTER TOGETHER

How It Works

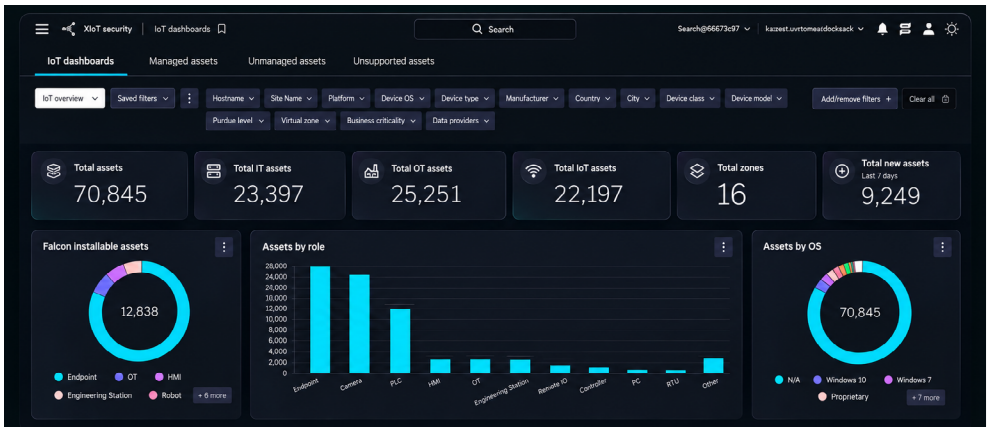
One Accurate Inventory Across Both Platforms

Security and operations teams share one continuously current view of the environment, with automated discovery, management, and monitoring of assets in operational environments.

Protect the complex and diverse assets within your organization's OT environment using asset data from the Dragos Platform integrated into CrowdStrike Falcon® Discover for IoT. Achieve extended visibility and security across ICS networks through CrowdStrike's Unified Threat Console, encompassing devices such as programmable logic controllers (PLCs), remote terminal units (RTUs), human-machine interfaces (HMIs), historian databases, engineering workstations (EWs), and more. By unifying ICS asset information and context, analysts can minimize blind spots and streamline asset management, enabling security operations teams to make better-informed decisions to secure your OT environment.

DIAGRAM 1

CrowdStrike Falcon® Discover For IoT Dashboard Showing ICS Assets From The Dragos Platform



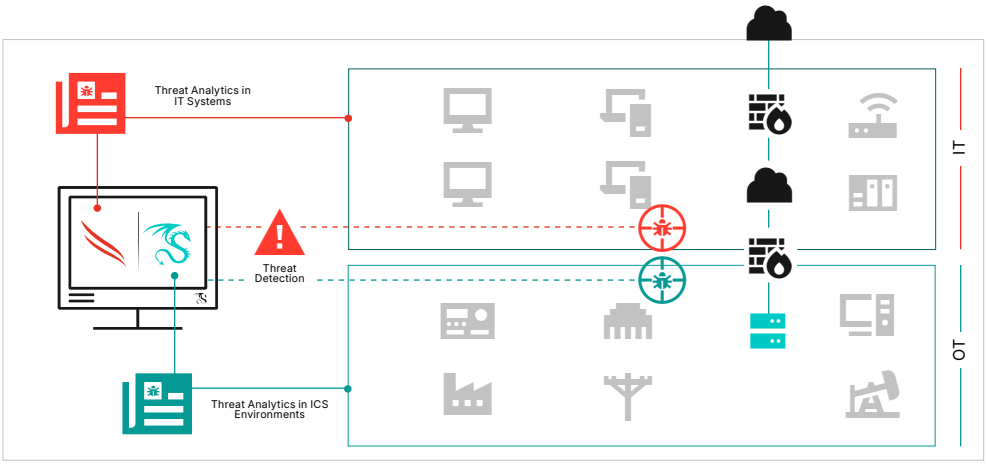
The Dragos Platform automates discovery, management, and monitoring across all assets within the xOT environment, spanning traditional OT, IoT, edge devices, and even IT assets. It utilizes insights from 600+ protocols, network data, and logs, laying a foundation for effective vulnerability management, threat detection, and incident response with superior security and operational efficiency.

Through the Dragos Platform Data Connector, customers bring asset discovery, detections, and vulnerability management details from the Dragos Platform into CrowdStrike Falcon® Discover for IoT. This can be integrated with CrowdStrike Falcon Next-Gen SIEM to centralize log management, enable real-time detection with unified data, facilitate rapid collaboration and search, enhance the SOC with Generative AI, and prevent breaches through workflow automation.

Consolidated SOC Workflows

SOC Teams Can Consolidate Workflows For Better Detection and Coordinated Incident Response

Dragos's OT-specific high fidelity, low noise threat detection enhances CrowdStrike Falcon's detection capabilities allowing SOC analysts to rapidly pinpoint malicious activity in OT networks with in-depth context of alert insights to reduce false positives and provide clear prioritization. Dragos's OT-specific intelligence also helps analysts recognize ICS-targeting threats on enterprise endpoints before they reach operational networks.



Analysts can quickly correlate notifications with a timeline view of historical insights which allows for a comprehensive timeline of events, aiding in the identification and analysis of incidents. Using the MITRE ATT&CK framework, analysts can then easily map detected threats to specific adversary TTPs.

Incident Responders can better coordinate response efforts by using CrowdStrike's extensive detections on edge ICS devices combined with Dragos's in-depth understanding of OT environments with tailored response strategies that prioritize operational uptime alongside security threat mitigation.

The Dragos Platform enhances an organization's response plan to speed up forensics and enable quick resolution with embedded case management and integrated response playbooks developed by OT security experts. Forensic artifacts are abstracted and well organized so incident responders can easily create cases to initiate investigations, accessing relevant activity logs and timeline views. This comprehensive approach ensures thorough and efficient incident investigations.

Endpoint Insight

Enrich OT Assets With Endpoint Insight For Thorough Investigations

Enrich Dragos Platform's asset visibility and detection capabilities further with Windows-based devices managed by CrowdStrike Falcon® Insight XDR. Falcon endpoint data is compared against Dragos assets, and operators review the match evidence and approve each endpoint-to-asset mapping before any change is committed to the asset inventory, keeping inventories accurate and consistent. Confirmed mappings enrich known assets with device details including operating system data, IP addresses, MAC addresses, endpoint hostnames, agent status, associated Active Directory (AD) domains, and additional custom attributes. Falcon-observed address history is retained with full provenance in asset drill-downs, and every confirmed mapping and enrichment is logged in the asset audit trail. This visibility deepens your understanding of the systems that influence operations. Once a mapping is confirmed, CrowdStrike Falcon detections on those assets, informed by CrowdStrike Indicators of Compromise (IOCs), generate notifications in the Dragos Platform for accelerated remediation and coordinated response.

CONCLUSION

Outcomes and Benefits

Together, Dragos and CrowdStrike deliver comprehensive visibility, detection, and response across both IT and xOT environments. By combining industry-leading endpoint security with purpose-built OT cybersecurity, organizations gain a unified approach to protecting critical operations, reducing risk, and improving resilience.

For more information, please visit dragos.com/partner/crowdstrike/

See Every Asset That Influences Operations

The Dragos Platform discovers and profiles OT assets passively, including the devices endpoint agents cannot reach, and Falcon endpoint data enriches them, producing one accurate, continuously current inventory.

Detect Threats Targeting Operations

Continuous monitoring and behavioral analytics surface adversary TTPs across industrial assets, while Falcon detections on edge ICS devices generate notifications in the Dragos Platform.

Act on Asset Data Both Teams Can Trust

Operator-approved endpoint-to-asset mapping, full provenance, and an asset audit trail keep the inventory accurate as both platforms enrich it.

Spend Remediation Effort Where Risk Is Real

"Now, Next, Never" prioritization focuses teams on the 3–6% of OT vulnerabilities requiring immediate action (Dragos 2026 Year in Review), with endpoint context from Falcon sharpening the call.

Keep Operations Running Through Response

Response strategies prioritize operational uptime alongside threat mitigation, built from over a decade of OT-specific incident response experience.

Compliance Alignment

Support compliance with NIST SP 800-82, IEC 62443, ISA/IEC 62443, NERC CIP, ISO/IEC 27001, CIS Controls, and FIPS 199 and 200, with alignment to the SANS ICS 5 Critical Controls.

About Dragos

Dragos delivers cybersecurity for industrial and extended operational technology (xOT) environments, advancing its mission to safeguard civilization. The Dragos Platform, Dragos Threat Intelligence, and Dragos Professional Services deliver comprehensive xOT cybersecurity capability, built by practitioners, for practitioners. Dragos is privately held, headquartered in Hanover, Maryland, and operates globally across North America, EMEA, and APAC.

Learn more: dragos.com
Contact: sales@dragos.com