S&P Global
Market Intelligence

451 Research Market
Insight Report Reprint

# Dragos highlights depth and operational clarity in latest cybersecurity platform release

October 29, 2025

by Johan Vermij

The company has released version 3.0 of its industrial cybersecurity platform, emphasizing usability, incident prioritization and cost-effective deployment while strengthening its focus on core OT security functions before expanding into a broader platform model.

## Introduction

The operational technology cybersecurity market continues to evolve as industrial organizations seek to defend against an increasing array of threats with limited skilled resources. In response, Dragos has released Platform 3.0, an update designed to make cybersecurity defenses in OT environments easier to deploy, manage and operationalize. The release underscores the vendor's commitment to enhancing the usability and quality of its platform, addressing skill shortages across industrial sectors, and ensuring that foundational security use cases are executed effectively before expanding into more advanced features.

## THE TAKE

Dragos Platform 3.0 introduces significant changes in usability, deployment flexibility and service integration. Central to the release is a redesigned user interface that is intended to simplify workflows and lower the learning curve for customers with limited in-house expertise. A consolidated Insights Hub provides contextualized information about vulnerabilities and adversary activities, reducing the cognitive burden on analysts. While rivals are pursuing aggressive platform consolidation, Dragos is emphasizing depth and operational quality in core OT security. Its success will depend on whether this focus resonates with organizations prioritizing operational reliability over broad, one-stop-shop integrated coverage in the current phase of OT cybersecurity maturity.

## Context

Founded in 2016 and headquartered in Hanover, Maryland, Dragos specializes in cybersecurity for industrial control systems, cyber-physical systems and broader OT environments. The company integrates threat intelligence, incident response and cybersecurity technology into a combined offering that addresses industrial risk. Dragos is widely recognized for its adversary research, contributing regularly to public- and private-sector understanding of state-affiliated and criminal actors targeting OT networks. Its platform is deployed across industries such as energy, utilities, manufacturing and transportation where operational resilience is closely tied to national security and economic stability.

The vendor has raised approximately $440 million in funding. Its most recent round came in 2023 and was a $74 million extension of its series D led by WestCap. The series D dates back to 2021 and was led by Koch Disruptive Technologies, an investment arm of Koch Industries, with funds and accounts managed by BlackRock Inc. Other investors include AllegisCyber Capital, Canaan Inc., DataTribe, Emerson Electric Co., Energy Impact Partners, Global Reserve Group, Hewlett Packard Enterprise Co., National Grid Partners, Schweitzer Engineering Labs and Rockwell Automation Inc.

## Technology

With the recent launch of Platform 3.0, Dragos is highlighting usability. The platform's UI has been redesigned to reduce complexity and make navigation more intuitive. This redesign directly responds to one of the sector's largest challenges: a shortage of skilled OT cybersecurity professionals. By simplifying workflows, Dragos is aiming to allow smaller or less experienced teams to operate effectively without being overwhelmed by excessive data or requiring specialized expertise.

In terms of functionality, the company has prioritized improving the quality and comprehensiveness of existing use cases rather than aggressively expanding into new ones. Many industrial organizations remain in the early stages of their security journeys, focusing on asset discovery, threat detection and vulnerability management. Platform 3.0 addresses these core areas by bolstering asset inventory capabilities via both passive and secondary active discovery techniques, integrating vulnerability contextualization within the new Insights Hub, and streamlining remediation guidance. The vendor's stated goal is to excel at these foundational elements, creating operational stability for customers before layering on advanced or experimental features.

Along with the existing deployment options, Dragos has added passive network traffic analysis in a single consolidated component, lowering deployment costs and reducing the complexity of managing multiple tools. This adjustment makes it easier to roll out the platform at small or remote sites, while also lowering the total cost of ownership across larger environments.

Furthermore, the enhanced OT Watch Complete service now offers 24/7 monitoring and triage, giving customers the option to fully outsource ongoing management to Dragos experts. This directly addresses resource shortages, giving organizations with minimal staff access to managed detection and incident triage that they can plug into existing security operations center or managed detection and response partnerships.

Dragos remains cautious in its adoption of artificial intelligence. While AI features are being incorporated in the back end to support analysis and contextualization, the company has avoided introducing disruptive front-end AI functionality until customer environments and capabilities are better aligned. With this strategy, Dragos is viewing AI as a force multiplier for human analysts, rather than a replacement. It also allows customers to retain full ownership and control over their data.

The newly launched AI features are designed to alleviate the shortage of skilled analysts — future additions will likely include model context protocols, analyst assistants, and broader AI-driven automation to boost detection, investigation and efficiency. This measured approach reflects the company's emphasis on operational continuity and conservative integration of new technologies.

## Competition

The cybersecurity space is undergoing consolidation, with several companies pursuing platform strategies that combine OT and information security functions under unified frameworks. Armis, bolstered by its acquisition of OTORIO, has expanded its coverage to include IT, OT, and internet of things asset visibility and security. Nozomi Networks, recently purchased by Mitsubishi Electric Corp., has integrated its OT visibility tools into a larger industrial automation ecosystem. Claroty continues to pursue its own platform expansion, with partnerships and acquisitions aimed at bridging IT and OT security domains. Tenable Holdings Inc. has primarily expanded its reach through integrations and partnerships.

Dragos has adopted a different approach, concentrating on operational quality and usability in core OT functions rather than moving aggressively toward broad platform consolidation. While its competitors are emphasizing comprehensive coverage and cross-domain integration, Dragos has deliberately focused on addressing foundational challenges that organizations encounter when building or advancing their OT security programs. By prioritizing enhancements in user experience, threat contextualization and foundational deployments, Dragos is positioning itself as a pragmatic alternative to consolidation-driven rivals, especially for customers seeking depth and operational clarity rather than breadth.

## SWOT Analysis

### STRENGTHS

With the revamp of its UI, Dragos is addressing a critical pain point by making the system more accessible to resource-limited teams. Its focus on augmenting existing use cases ensures reliability for customers still evolving their OT security programs. Expanded OT Watch services with OT Watch Complete also enhance the vendor's ability to serve organizations without sufficient staff.

### WEAKNESSES

Its conservative adoption of new technologies, including AI, could position Dragos as slower to innovate compared with competitors that stress automation. Its strategy to emphasize quality over breadth could also leave gaps in environments requiring consolidated IT and OT functionality.

### OPPORTUNITIES

The continuing shortage of OT cybersecurity professionals is creating growing demand for managed services, positioning OT Watch Complete as potentially enticing for SMEs.

### THREATS

M&A in the OT security sector presents a challenge as Dragos' rivals increasingly deliver unified IT/OT tools. Armis, Nozomi, Claroty, Tenable and XM Cyber are pursuing integration strategies that could attract enterprises seeking a single-vendor approach.

**CONTACTS**

**Americas:** +1 800 447 2273
**Japan:** +81 3 6262 1887
**Asia-Pacific:** +60 4 291 3600
**Europe, Middle East, Africa:** +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html