

Dragos™ Platform & TCO



Dragos' unique threat behavior analytics detection and automated response capabilities enable a lower ongoing cost of ownership than environment-based only solutions

Dragos Platform Overview

The Dragos Platform is a modular Industrial Control System (ICS) cybersecurity solution that provides ICS defenders with unprecedented knowledge and understanding of their assets and activity, the threats and adversaries they face, and the knowledge and tools to respond. **The Dragos Platform codifies the skills and knowledge of the industry's most trusted ICS practitioners and cybersecurity experts, providing all of the capabilities needed for a more scalable, efficient and effective defense.**

Ongoing Operations Costs Drive ICS Cybersecurity TCO

All ICS cybersecurity solutions have upfront costs to acquire and deploy, and across the major providers, including Dragos, in the marketplace today, these upfront costs generally fall within a similar range. The total cost of ownership equation is substantially driven by a solution's ongoing cost of ownership, including maintenance and downtime costs, which is where Dragos stands apart from all others.

How a solution detects threats and the capabilities it provides ICS defenders to respond once it does, significantly impact its ongoing cost of ownership.

The vast majority of ICS cybersecurity solutions have similar ongoing costs of ownership owing to their similar reliance upon detecting threats as anomalies within an ICS environment, with a solution scope that does little beyond alerting operators upon their detection. Dragos employs multiple threat detection techniques including the industry's sole threat behavior analytics-based approach, and provides a range of capabilities beyond alerts that facilitate the most effective and efficient incident response and resolution. As a result of these key differences, the ongoing operating costs, reduced downtime and consequently the TCO of the Dragos Platform can be significantly lower.

Solution Acquisition & Deployment Costs: Prior to Threat Detection

**Environment-Based
Detection Solutions**
(Typical Industry
Approach)



**Threat-Based
Detection Solutions**
(Dragos' Approach)



Ongoing Solution Operating Costs: Responding to Detected Threats



More alerts to investigate, less threat context, longer MTTR, little to no response automation.



Less alerts to investigate, more threat context, shorter MTTR, rich response automation.

**Dragos TCO
Advantage**

Dragos' Threat Behavior Analytics Drive Down Hard and Soft Security Operations Costs

Dragos threat behavior analytics mine the in-depth knowledge, intuition, and insight from expert ICS and cybersecurity sources around the world – most notably the Dragos Threat Operations Center – to weed out the forensic noise and alert fatigue to better prioritize and respond to threats before significant damage or disruption occurs. The Dragos Platform frees up security analysts to focus on the more strategic and sophisticated tasks of hunting for new threats, leading to further efficiencies and optimizations to industrial cybersecurity posture.

Not All ICS Cybersecurity Solutions are the Same

The Dragos Platform was designed and built by recognized ICS security practitioners who have lived the challenges that security teams face securing industrial control systems and their surrounding infrastructure. Our deep understanding of those challenges and the ICS threat landscape is reflected in our differentiated approach to providing a solution to them, as shown below:

	Dragos Platform	Typical Industry Solutions
Principal threat detection method	Threat Behavior Analytics	Anomaly Detection
Ongoing system/training adjustment	Minimal	Significant
Alert/threat response capabilities	Automated/Integrated into Platform	Manual/On Operator
False positives	Few	Many
Threat intelligence	Integrated into Platform	Manual/On Operator
Detailed threat context with alerts	Yes	No
Potential for alert fatigue	Low	High
Ongoing cost of ownership	Low	High

Better Time and Cost Outcomes from Dragos' Comprehensive Approach

ICS cybersecurity solutions are all useful to ICS defenders facing an increasingly complex threat landscape, and while they have some common elements and components, they address the challenge of reducing the time and ultimately the cost of detection and response differently. As shown below, the comprehensive approach taken by Dragos enables faster recovery at less total cost than typical industry solutions.

Time and Cost Benefits of Deploying Dragos versus Typical Industry Solutions

Typical Industry Solutions



Total Adversary Dwell Time and Mean Time to Recovery (MTTR)



Total Cost of Ownership (TCO)



Dragos Platform



Contact Information

1745 Dorsey Road
 Hanover, MD, 21076 USA
dragos.com | info@dragos.com