Dragos™ **Platform**

DRAGOS

The industrial control system cybersecurity monitoring platform built for ICS defenders by ICS practitioners and cybersecurity experts

Dragos Platform Overview

The Dragos Platform is the most technologically complete solution in the industrial cyber threat detection and response market today. It provides security teams with unprecedented knowledge of their industrial control system (ICS) assets and activity, the threats and adversaries they face, and the tools and knowledge to defend against them. It is the industry's first and only solution to codify and integrate the knowledge of the industry's most trusted ICS security experts and an intelligence-driven approach with software technology. When you deploy the Dragos Platform, you get not only the features and benefits of advanced software, you get the transfer of knowledge from Dragos Threat Intelligence, Threat Hunting, and Incident Response teams that is integrated right into the Platform.

Why Choose the Dragos Platform?

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**

"The passive, cybersecurity defenses used in most industrial cybersecurity programs may be adequate for low-risk facilities. But operators in critical industries need to recognize that, increasingly, they are on "the radar" of sophisticated attackers and must be able to ensure that their programs can defend against non-traditional, targeted attacks. Active monitoring and management of anomalies by qualified people is essential.

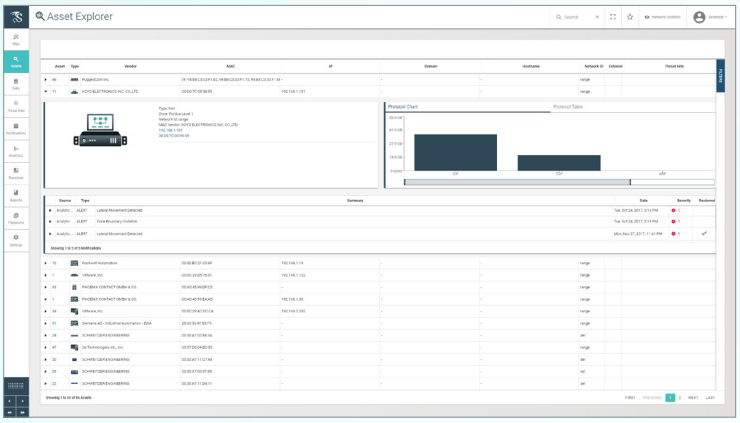
Adopting a context-aware, intelligence-driven approach, like that offered by Dragos, can help ensure that these resources have the information and tools they need to be both effective and efficient."

Arc Advisory Group, December, 2017

Dragos™ Platform

Dragos Platform Modules

The Dragos Platform provides all of the necessary capabilities to gain visibility into industrial networks across the entire industrial cybersecurity framework. It operates as a security incident and event management (SIEM) solution, purpose built for industrial environments, and can be deployed in a security operations center (SOC) model. It is modularly designed so that it can be deployed in whole or in parts to address both immediate and longer-term needs.

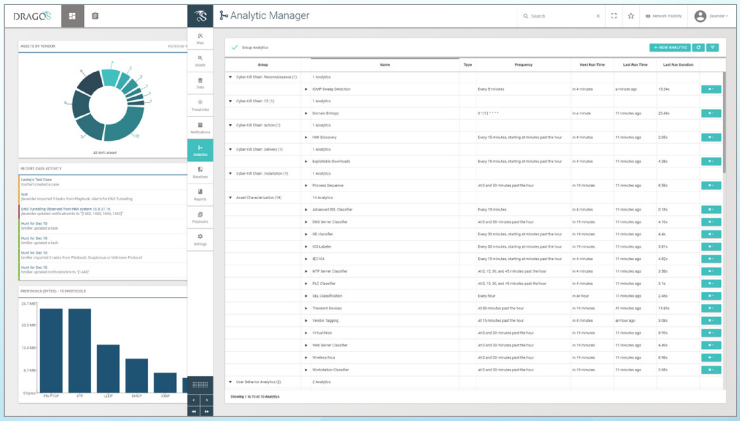


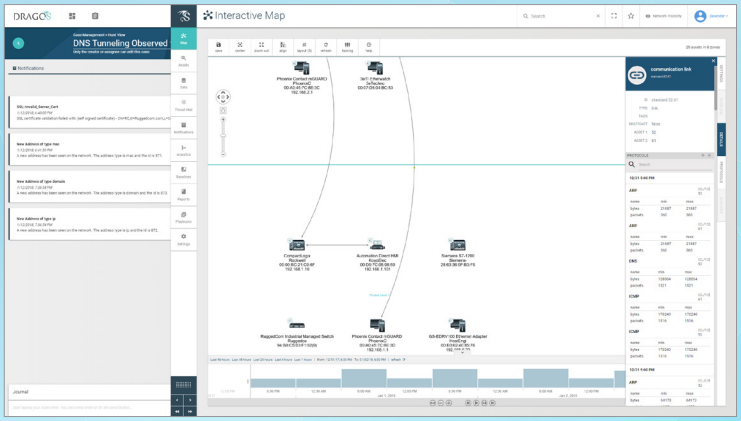
Asset Discovery

- Passively identify all assets and communications on the network
- Visualize and map network security zones and identify attack paths
- Set one or more network baselines against which to monitor changes
- Scalable to hundreds of thousands of assets across multiple sites

Threat Detection

- Dragos threat behavior analytics provide rich context as to what is occurring and what to do next
- Indicator of Compromise and Query-Focused Datasets support threat hunting
- Collects, stores and analyzes logs and data from host systems, logic controllers and data historians, not just data traffic





Investigation Playbooks & Workbench

- Use case management tools to manage incident response case notes, forensics and collaboration
- Playbooks from Dragos experts drive standardized, best practice response
- Automation and orchestration between different security tools reduces workload
- Reporting and Dashboards monitor analyst and system activity

Feature	Benefits
Asset Discovery, Enrichment, Classification and Exploration	■ Significantly reduce the amount of time necessary to identify and inventory all assets and traffic on your network ■ System-generated asset maps and reports enable you to have a consistent, time-driven view that is accurate, up-to-date, and thorough ■ Enrich Asset information to tailor behavioral analytics and improve security profile ■ Automatic classification of assets based on behavior ■ Set one or more baselines, notify when specific changes or anomalies occur in the environment over time ■ Recognize new or rogue assets as they appear; identify assets that have disappeared from the network
Threat Behavior Analytics	■ Powered by human-based intelligence that identifies adversary tradecraft and campaigns ■ No bake-in or tuning period required; behavioral analytics work immediately upon deployment ■ Detect threats not simply as anomalies, but with context that guides effective response
Investigation Playbooks and Workbench	■ Notification filtering provides a risk-based approach to management ■ Playbooks codify incident response and security operations best-practice workflows developed by Dragos experts ■ Manage incidents and cases from the same console cross-team
Reporting and Dashboards	■ Clear Indicator of Compromise reports guide attention to Assets that are vulnerable ■ Easily monitor case, notification, and analyst activity, as well as system-level health and status
Third Party Integrations	■ Firewalls, Alarm Servers, Data Historians, Existing Asset Trackers, Log Storage, and open APIs to extend

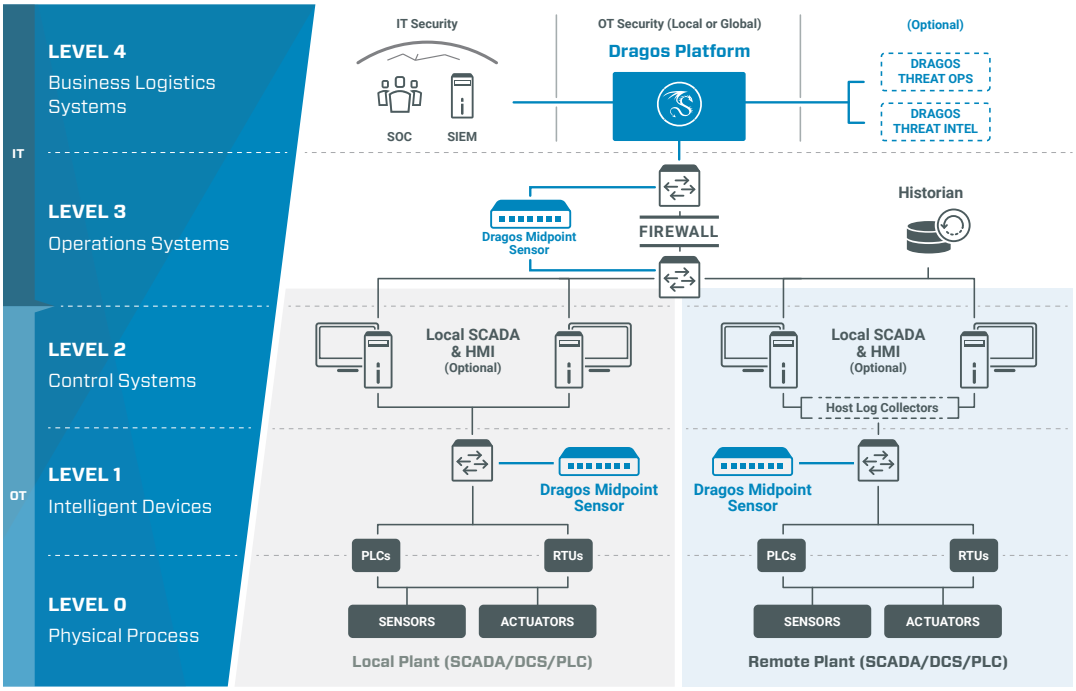
"The Dragos Platform provides us with a level of real-time, situational awareness and monitoring capabilities unparalleled in the industry today, which was never before possible within our Windfarm networks. It has become an integral part of our day-to-day cybersecurity, OT network monitoring, and asset management program and has eliminated a number of manual processes while increasing our speed of incident response. A high-value system for any organization whose operations are dependent upon ICS technology, processes, and protocols."

Marc DeNarie, Chief Information Officer NaturEner USA

NaturEner

Dragos™ Platform

Platform Development and System Requirements



Dragos Sitestore

- 48 CPU / 128 GB RAM
- x6 4TB SSD HD
- Deployable on-premise or in AWS

Dragos Midpoint Sensors

- Hardware-deployed appliance in Small, Medium or Large
- Handles up to 1GB data rates

Sample of Supported Protocols

ModbusTCP, Ethernet/IP, Profinet, OPC, IEC 61850, IEC 104

Licensing

- Hardware appliance – initial fee
- Annual license fee for software
- Support included in license fee

Dragos Solutions Span the Entire Industrial Cybersecurity Best-Practice Framework

Given the developing nature of industrial cybersecurity tools and practices, many organizations find it useful to apply best practice methodologies to better understand, manage and reduce their cybersecurity-related risk. While there are various solid frameworks, Dragos' view is that "know thyself, know thy enemy, and know what to do" covers the core tenets of them all.

	Know Thyself		Know Thy Enemy	Know What to Do	
Frameworks	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
	What processes and assets need protection?	What safeguards are available?	What techniques can detect threats and incidents?	What techniques can contain incident impact?	What techniques can quickly and safely restore capabilities
Dragos Solutions			Dragos ICS WorldView		
	Dragos Threatview			Dragos Incident Response	
	Dragos ICS Cybersecurity Training				
	Dragos Platform				

Dragos provides the only industrial cybersecurity portfolio that spans the entire ICS cybersecurity best-practices continuum. It combines human intelligence analysts, ICS operations experts and advanced technologies to enable asset owners to build and maintain the most effective cyber-defenses possible.

Contact Information

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