SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

OT Cybersecurity Solutions for Maritime Environments

What You Need to Protect Your Industrial Applications

Based in the Washington, DC area, Dragos is the only US-owned OT cybersecurity technology, intelligence, and services company. Dragos protects the enterprises of more than 500 customers, including maritime transportation and logistics companies, amidst an ever-changing threat landscape.

Maritime industrial control systems (ICS) and operational technology (OT) contain similar systems and software components to what is seen in land-based critical infrastructure installations, such as building management, power, manufacturing, and oil and gas (ONG). Maritime vessels, ports, and waterways continue to adopt new technology to improve GPS, propulsion, safety, and traffic management capabilities, but these developments dramatically increase security risks. Dragos industrial cybersecurity technology and professional services can help protect your ICS/OT maritime applications against increasingly capable adversaries.

How Dragos Helps Maritime Fleets and Ports

Dragos technology protects everything from landside facilities to shipboard systems and offers protection across ONG/LNG port entities, as well as electric and chemical shoreside assets and facilities. Our technology also offers monitoring across standard ICS/OT systems and devices found onboard ships such as safety management systems like those found in FRCS, and cargo management systems. Our unparalleled understanding of OT systems and environments strengthens the readiness and resiliency of your teams, enables secure modernization and innovation, and facilitates compliance while minimizing risk.

The Dragos Platform

The industry's most advanced ICS/OT cybersecurity software to help you visualize, protect, and respond to cyber threats.

Top Five Use Cases for the Dragos Platform

Asset Visibility

A comprehensive and real-time understanding of all assets in your environment is essential for network monitoring, threat correlation, and effective vulnerability management. Our customers use the Dragos Platform to identify crown jewel assets, create asset inventories, and identify unusual activity across thousands of devices.

Vulnerability Management

OT cybersecurity teams are overwhelmed by hundreds of vulnerabilities that potentially need to be remediated. Without simple, accurate, prioritized guidance, you'll waste time and money patching vulnerabilities that aren't important – and you can easily miss those that are truly critical. Dragos customers use the platform to simplify compliance and reporting, prioritize vulnerabilities that matter most, and maximize remediation resources.

Threat Detection

Adversaries evolve their tactics, techniques, and procedures with subtle behaviors that are easily lost in the noise of your environment. Without actual intelligence, your team can easily suffer from alert fatigue and begin to ignore or undervalue relevant alerts while devoting unnecessary time and productivity to false alarms. Our platform customers immediately see any unauthorized IT-OT traffic across complex networks, analyze file downloads quickly and easily, and detect potential adversaries in the environment in real time.

Top Five Use Cases for the Dragos Platform

Incident Investigation

When faced with a potential incident, clear and carefully vetted guidance can be the difference between quickly restoring operations or making the situation worse. Dragos Platform users can analyze changes and forensic records, efficiently manage response and recovery, and leverage prescriptive playbooks with proven, tested response protocols.

Cross-Functional Operations Insights

Monitoring assets and properly dissecting and inspecting network traffic requires in-depth protocol coverage; otherwise, threats and asset details remain hidden. Dragos customers use the platform to detect operational process errors quickly and efficiently, monitor ICS/OT network and device health, support ATO/RMF artifacts, and integrate active defense via SIEMENS Siber Protect.

WorldView Threat Intelligence

Actionable Threat Intelligence and Defensive Recommendations

The latest research from Dragos highlights a new threat group targeting ONG and maritime assets. Bentonite seeks to exploit vulnerable remote access or internet-exposed assets that can facilitate access to the broader enterprise. Maritime environments are specifically targeted by the group, and Dragos is closely monitoring their activities, reporting defensible, action-oriented advice via our threat intelligence subscription program. Backed by a team of industrial control systems cybersecurity experts with deep industry knowledge, Dragos WorldView threat intelligence offers in-depth visibility of threats targeting OT environments AND defensive recommendations to combat them. WorldView threat intelligence is an annual subscription service, providing access to regular reporting, critical alerts, executive insights, webinars, and more.

Use these WorldView tools to proactively defend your ICS networks and stay ahead of threats:

- Critical alerts, weekly reports, threat perspectives, quarterly insights, and dedicated threat feeds provide comprehensive insight of threats to your ICS
- Actionable defensive recommendations from a dedicated team of ICS intelligence analysts and practitioners to help you prepare for and combat cyber attacks
- Detailed information of global industrial adversary behaviors, including TTPs and victimology to understand ICS attackers and prevent them from going undetected on your networks
- The latest Indicators of Compromise (IOCs) to help you thwart potential attacks
- Partnerships with companies like Crowdstrike, ThreatQuotient, eclectic iq, ThreatConnect, Anomoli, Recorded Future, and others provide enhanced threat intelligence capabilities – and all of WorldView's threat intelligence reporting references MITRE ATT&CK for ICS TTPs

ICS/OT Incident Response

Proactive and Responsive Service to Prepare for, Combat, and Respond to ICS/OT Attacks

The Dragos Rapid Response Retainer is the cornerstone of your OT cybersecurity program, ensuring can respond quickly and recover confidently when attackers strike. Having a retainer in place is a proactive approach that bolsters your security posture and provides access to incident responders who have been on the front lines of cyber-attacks globally, are familiar with your environment, and are highly skilled at OT cybersecurity crisis management. A Rapid Response Retainer pairs perfectly with the Dragos Platform, because the Platform provides a powerful investigation workbench with detailed forensics records and prioritized guidance for vulnerabilities and risk mitigation.

1 24 X 7 ACCESS TO INDUSTRY-LEADING RESPONDERS

- ✓ When you're in crisis mode, you need experienced incident responders who understand your technology, have situational awareness and exercise good judgement.
- ✓ The Dragos team of experts are industry leading supporting customers with OT cybersecurity incidents on an international scale.
- ✓ Ensure you have the necessary support from a team that can analyze and investigate industrial cyber events, and consult with you on important executive, legal, regulatory, and insurance communications that may be necessary.

2 RAPID RESPONSE WITH THE DRAGOS PLATFORM

- ✓ While a subscription to the Dragos Platform is not required to purchase a retainer, it is highly recommended.
- ✓ Because the Dragos Platform provides continuous visibility to OT devices, profiles, traffic patterns, vulnerabilities and threats, sites with the Platform installed are eligible for expedited response times (SLA) based on the number of retainer hours purchased.
- ✓ With our technology in place, responders are better equipped to analyze, investigate, and perform root cause analysis on historical data within your environment when an event occurs.
- ✓ Non-retainer incident response or sites not equipped with the Dragos Platform receive our best-effort response time.

Five Reasons to Choose Dragos

1) ICS/OT Cybersecurity is Different From IT Cybersecurity

OT environments include different systems, network traffic, adversaries, and vulnerabilities than IT environments. When ports and vessels modernize their operations, the IT networks become part of the control system – and control systems have very different latency requirements to ensure employee and public safety. You need a team with process-level expertise to support your cybersecurity programs, and Dragos has a full bench of ICS/OT cyber experts with deep experience in maritime environments.

2) We Make it Our Business to Stay Ahead of the Adversaries

According to the latest Dragos research, ransomware attacks against industrial organizations increased 87 percent over the last year, and a new threat group is specifically targeting maritime operations – making threat intelligence a higher priority than ever before. Dragos WorldView threat intelligence arms vessels and ports with in-depth visibility to the threats targeting assets globally and provides tried-and-true defensive recommendations for your team to implement. Plus, everything we learn from WorldView is incorporated into our leading technology platform, which rapidly pinpointing malicious behavior on your networks.

3) We Enable Compliance and Simplify Reporting to Government Agencies and Insurers

Cyber regulations like the International Maritime Organization's Resolution MSC.428(98) and the US Coast Guard's Navigation and Vessel Inspection Circular (NVIC) require a new level of analyzing and reporting on OT cybersecurity risk. Shipping and cruise companies have a broad threat landscape, requiring efficient and effective asset identification and monitoring, vulnerability management, and threat intelligence. Your systems will be more reliable – and more secure – because of our expertise.

4) Community Matters

Dragos provides the connective tissue between government, civilian agencies, and commercial customers, leveraging threat intelligence and lessons learned to optimize results for all stakeholders. Dragos is the only US-owned ICS/OT cybersecurity company – and that matters when you're transporting people and machinery that help defend American interests around the world. Plus, we work closely with partners like ABS Group to deliver customized solutions for maritime environments.

5) Rave Reviews

The Dragos team comes highly recommended, with hundreds of cybersecurity experts serving within government and in critical industry sectors like transportation, defense manufacturing, aerospace, energy, and oil and gas.

Rely on Dragos Technology and Services to Defend Onshore, Port, and Vessel Operations

Cyber incidents disrupt timelines and logistics; threaten health and safety of crews and communities; and shake the trust of customers and stakeholders. Put our team of researchers, hunters, and defenders to work on your mission – you'll dramatically lower your risk AND you'll experience benefits like these.

Save Money

- Focused threat hunting and cybersecurity engagements, custom-built to suit maritime's unique challenges and your operation's cyber maturity level
- Accurate and uncontestable information prevents additional trips for data
- Contextualized and prioritized vulnerability recommendations enable efficient, documented risk management
- Real-time identification of malfunctioning components and devices reduces maintenance costs and lowers operational risk across geographies

Save Time

- Run automated, continuous inventory cycles
- View live data without lengthy site interactions
- Identify process errors quickly and continuously
- Begin collecting data during the Dragos pre-site assessment and hit the ground running

Simplify Compliance and Reporting Requirements

- Meet the latest compliance requirements including cyber terrain mapping, critical asset continuous threat monitoring, developing an ecosystem that supports a framework of access control inspired by zero trust, and ensuring OT asset visibility across diverse assets
- Conduct tabletop exercises, establish baselines, and track progress
- Enable accurate briefings to customers and government agencies; simplify reporting for insurance companies

Minimize Risk and Improve Mission Resiliency

- Prioritized vulnerability management ensures exploitable risks are addressed first
- Intelligence-informed threat detection based on adversary tactics, techniques, and procedures allows earlier identification and remediation

Next Step: Learn more about Dragos and our technology, services, and threat intelligence – book a meeting today.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.