SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

OT Cybersecurity Solutions for Defense Manufacturers

What You Need to Protect Your Industrial Infrastructure

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 dozens of global manufacturers, amidst an ever-changing threat landscape.

Five Reasons to Choose Dragos

1) OT Cybersecurity is Different from IT Cybersecurity

OT environments include different systems, network traffic, adversaries, and vulnerabilities than IT environments. When manufacturers modernize their operations, the IT network becomes 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 manufacturing 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. Seventy-two percent of those attacks targeted manufacturers – making threat intelligence a higher priority than ever before. Dragos WorldView threat intelligence arms your company with in-depth visibility to the threats targeting industry 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 pinpoints malicious behavior on your networks.

3) Our Approach – from Monitoring to Vulnerability Management – Keeps Your Facility Operating and Producing at the Highest Levels

The Dragos approach to risk management, focused on identifying and protecting your crown jewels, requires a deep understanding of your architecture. While other technologies flag everything and flash every potential vulnerability, we carefully prioritize and help you make sense of what's urgent and what can wait. Our vulnerability management approach is effective because it reflects business risk at the asset level – considering an asset's identity, purpose, and potential impact within your architecture.

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 producing the materials that help defend American interests around the world.

5) Rave Reviews

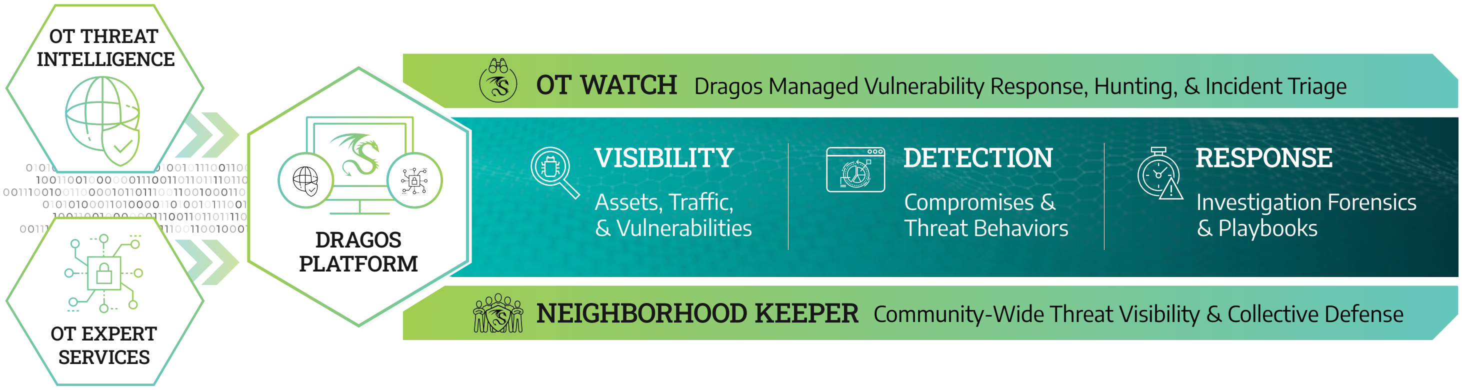
The Dragos team comes highly recommended, with hundreds of cybersecurity experts serving within government and in critical industry sectors like defense manufacturing, aerospace, energy, and oil and gas.

How We Help Defense Manufacturers

Dragos technology protects everything from commercial manufacturing plants to power grids to facility related control systems. Our unparalleled understanding of these 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 helps you visualize, protect, and respond to cyber threats.


OT THREAT INTELLIGENCE
OT EXPERT SERVICES
DRAGOS PLATFORM
OT WATCH Dragos Managed Vulnerability Response, Hunting, & Incident Triage
VISIBILITY
Assets, Traffic, & Vulnerabilities
DETECTION
Compromises & Threat Behaviors
RESPONSE
Investigation Forensics & Playbooks
NEIGHBORHOOD KEEPER Community-Wide Threat Visibility & Collective Defense

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.

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

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 into 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 about 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, enabling you to 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.

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.

Rely on Dragos to Defend Your Critical Manufacturing Facilities and Keep Your Operations Productive

Cyber incidents disrupt operations; threaten health and safety of the community; 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 your unique environment and cyber maturity level
- Accurate and uncontestable information prevents additional trips for data
- Contextualized and prioritized vulnerability recommendations enable maximum uptime
- Efficient, real-time identification of malfunctioning components and devices improves output and reduces maintenance costs across your enterprise

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 Service Component Objectives and NDAA requirements including cyber terrain mapping, critical asset continuous threat monitoring, creating an OT zero trust framework, and ensuring OT asset visibility across multiple facilities
- Conduct tabletop exercises, establish baselines, and track progress
- Enable accurate briefings to customers and government agencies; simplify reporting

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.

DRAGOS
SAFEGUARDING CIVILIZATION
COMMUNITY DEFENSE
DRAGOS PLATFORM
OT THREAT INTELLIGENCE
OT EXPERT SERVICES

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**.