DRAGOS

SOLUTION BRIEF

xOT Cybersecurity for Oil & Gas

Detect every asset. Protect every system.

INDUSTRY OVERVIEW

Oil & Gas: Safety, Uptime, and the Cost of Getting It Wrong

Oil and gas sits at the center of global critical infrastructure. From upstream exploration through midstream pipelines to downstream refining, every stage depends on OT environments running safely and without interruption. These environments were built for reliability, not security. Decades-old control systems, proprietary protocols, and a culture that prioritizes physical safety over digital defense create conditions threat actors exploit.

A cyberattack on oil and gas xOT can halt production, damage equipment, trigger environmental incidents, and endanger workers. In 2021, ransomware forced a six-day pipeline shutdown across the US East Coast. In 2017, TRITON/TRISIS targeted safety instrumented systems at a Saudi Arabian petrochemical facility — the first known malware built specifically to disable industrial safety systems.

In oil and gas, the consequences reach further than any other sector: worker safety, environmental integrity, and operations that generate millions of dollars a day. The organizations that understand this treat xOT security as an operational resilience imperative.

26+

OT threat groups tracked by Dragos

507M

lives depending on infrastructure Dragos protects

7.8M

OT assets protected across facilities globally

→ Source: Dragos 2026 Year in Review

© 2026 Dragos, Inc. All Rights Reserved.

OT/ICS CHALLENGES

Challenges Unique to Oil & Gas

Oil and gas xOT presents a combination of complexity and consequence unlike almost any other sector.

01

Legacy Infrastructure Running Critical Processes

Refineries and pipeline control systems were built to run 20 to 40 years. PLCs, DCS, and RTUs deployed decades ago remain in active service, often without vendor support, patches, or modern authentication. These systems were never designed to be networked, and retrofitting security without affecting operations requires deep OT expertise.

02

Always-On Operational Requirements

Pipelines run continuously. Refineries operate in interdependent process cycles where an unplanned shutdown causes physical damage, safety hazards, and seven-figure losses per hour. Standard security practices which often include network scanning, patching, rebooting, can trigger the very incidents they are meant to prevent.

03

Geographically Distributed and Remote Assets

Upstream sites, compressor stations, metering points, and offshore platforms span vast geographies with limited connectivity and no on-site security staff. Hard to monitor, they are high-value targets.

04

IT, OT, and Third-Party Networks

OT environments now connect to more locations, more assets, and third-party vendor systems. Each connection provides a potential new pathway for adversaries into operational networks.

05

Protocol Complexity and OT-Specific Attack Surfaces

Oil and gas runs on dozens of industrial protocols each with its own security limitations. Standard IT tools cannot parse them, cannot distinguish normal from anomalous process behavior, and cannot safely operate on OT networks.

© 2026 Dragos, Inc. All Rights Reserved.

06

Safety Systems as Targets

Safety Instrumented Systems such as fire and gas detection, emergency shutdown, pressure relief, are the last line of defense before a cyber event becomes a physical one. TRITON/TRISIS proved that sophisticated adversaries specifically target SIS to disable safety protections. Standard IT security has no playbook for this.

07

People and Environmental Safety

A cyber incident in oil and gas does not stop at the network boundary. Process disruptions can trigger gas releases, fires, pressure failures, or loss of safety shutdowns. Regulators, insurers, and boards treat environmental and worker safety as non-negotiable. A security program that ignores the physical consequences of control system compromise is not fit for this environment.

08

Operational Cost and Efficiency Pressure

Operators face constant pressure to extract more value from aging infrastructure against volatile commodity prices. A single process upset can cost hundreds of thousands to millions of dollars per hour in lost output and restart costs. Security that generates noise or disrupts operations compounds the problem. Operators need security that works around their processes and contributes to operational intelligence rather than adding overhead.

KEY SECTOR REALITY

In oil and gas, the gap between what organizations think is on their OT network and what is actually there is consistently one of the widest of any sector Dragos assesses.

THE xOT CHALLENGE

The Expanding The Control Loop

Extended operational technology (xOT) encompasses traditional OT alongside IoT, edge devices, and IT assets operating in or adjacent to the operational network. In oil and gas, this expansion has created new categories of risk.

© 2026 Dragos, Inc. All Rights Reserved.

Oil & Gas Refining — End To End OT/ICS Asset Map

xOT / Enterprise IT · OT / ICS · Data / Connectivity · Physical Flow (Material)

	Exploration & Extraction	Gathering & Transportation	Refining Facility	Storage & Terminal	Distribution & Transportation	Retail Delivery
						
xOT / Enterprise IT Assets Business & IT Systems that connect, manage, and support operations.	▪ Corporate WAN ▪ Geoscience Servers ▪ Data Historians ▪ Email / Collaboration ▪ IT Workstations ▪ Security Operations Center	▪ SCADA / Pipeline Control Center ▪ GIS / Mapping Systems ▪ Weather Systems ▪ Data Analytics Platforms ▪ IT Asset Management ▪ Remote Access / VPN	▪ MES / LIMS / ERP ▪ Engineering Workstations ▪ Plant Data Historians ▪ Data Lake / Analytics ▪ Identity & Access Management ▪ Patch Management ▪ Backup / DR Systems	▪ Terminal Management Systems (TMS) ▪ Inventory Management ▪ Scheduling / Logistics ▪ ERP / Finance ▪ Remote Monitoring Apps ▪ Security / Surveillance Systems	▪ Fleet Management Systems ▪ Transportation Mgmt Systems (TMS) ▪ Order Management ▪ Customer Portals / EDI ▪ Telematics Platforms ▪ Business Intelligence	▪ Payment Systems ▪ CRM Systems ▪ Store Management Systems ▪ Remote Site Monitoring ▪ Corporate Reporting ▪ IT Helpdesk / Support
OT / ICS Assets Operational Technology & Industrial Control Systems.	▪ Wellhead Controllers (RTU/PLC) ▪ Subsea Controls (SCADA) ▪ Flow Computers / Meters ▪ Remote Telemetry Units (RTU) ▪ Compressor Units ▪ Local HMI / Operator Panels ▪ Safety Instrumented Systems ▪ Gas Detectors / Analyzers ▪ Electrical Control Panels	▪ Pipeline SCADA Systems ▪ RTUs / PLCs at Stations ▪ Flow / Pressure / Temp Sensors ▪ Cathodic Protection Systems ▪ Compressor / Pump Controls ▪ Metering & Custody Transfer ▪ Leak Detection Systems ▪ Safety Shutdown Systems (ESD) ▪ Remote Terminal Units	▪ Distributed Control Systems ▪ PLCs (Process / Discrete) ▪ Safety Instrumented Systems ▪ Advanced Process Control ▪ Analyzers (Gas, Liquid) ▪ Boilers / Furnaces Controls ▪ Turbine / Compressor Controls ▪ Electrical Substation / Switchgear ▪ Motor Control Centers ▪ HMI / Operator Stations	▪ Tank Level Gauging Systems ▪ Terminal Automation Systems ▪ PLCs / RTUs ▪ Pump / Valve Controls ▪ Loading Arm Controls ▪ Overfill Prevention Systems ▪ Fire & Gas Detection Systems ▪ CCTV / Surveillance ▪ ESD Systems	▪ SCADA / Terminal Control Systems ▪ Pump / Compressor Controls ▪ Valve Actuators / Controls ▪ Flow / Pressure Monitoring ▪ Tank Level Monitoring ▪ Railcar / Truck Load Systems ▪ Pipeline Monitoring Systems ▪ Leak Detection Systems ▪ ESD / Shutdown Systems	▪ Tank Level Sensors ▪ Leak Detection ▪ Fuel Dispenser Controllers ▪ Electronic Price Signs ▪ POS Terminal Controllers ▪ Payment Terminals ▪ CCTV Video Systems ▪ Environmental Sensors ▪ Emergency Stop Systems

Connectivity & Networks

Fiber Optic • Microwave • Satellite • Cellular (4G/5G) • Radio • Leased Lines
Industrial Ethernet • Secure Remote • Access • DMZ / Firewalls • IDS / IPS

Physical Flow (Material)

Crude Oil / Natural Gas → Gathering Pipes → Refined Products → Storage / Terminals → Distribution (Ship / Rail / Truck) → Fuel at Retail

Cross Cutting Systems

- Cybersecurity (SOC, SIEM, NDR)
- Backup & Disaste Recovery
- Vulnerability Mgmt & Patch Mgmt
- Asset Discovery & Inventory
- Identity & Access Mgmt
- Compliance & Reporting

This diagram highlights common xOT and OT assets across the oil and gas refining value chain. Actual environments may vary by organization.

© 2026 Dragos, Inc. All Rights Reserved.

xOT REALITY CHECK

xOT environments now include assets that don't look like traditional industrial equipment: cloud workloads, managed IoT gateways, edge computing platforms, and vendor-managed endpoints.

Standard OT monitoring misses them entirely.

01

Industrial IoT and Smart Field Devices

Sensors, flow meters, pressure transmitters, and condition-monitoring devices now connect directly to corporate networks and cloud platforms. These endpoints often lack authentication, run unpatched firmware, and communicate over protocols built for reliability, not security. Every connected device is a potential entry point.

02

Remote Operations Centers and Cloud Historians

Operating companies are centralizing monitoring into remote operations centers and cloud historian platforms. This concentrates xOT data and control pathways in ways the original security architecture never anticipated. A compromised historian exposes process data; a compromised remote access path reaches the control system directly.

03

Third-Party Remote Access

Vendors and OEMs routinely need remote access to OT systems. These paths are frequently unmonitored, use shared credentials, and bypass segmentation that would otherwise limit an attacker's movement. Dragos has observed threat actors targeting vendor remote access as a primary initial access vector.

04

Operational Technology in the Cloud

Digital twins, AI optimization, and predictive maintenance platforms pull live OT data into cloud environments, creating continuous data flows across IT/OT boundaries; often without the monitoring or controls that would apply in either environment alone.

05

Expanded Operational Surfaces Without Expanded Visibility

The core xOT problem: visibility and controls have not kept pace. Most organizations have significant blind spots in their xOT inventory, limited detection for threats crossing IT/OT boundaries, and IR plans built for IT that do not reflect OT constraints.

© 2026 Dragos, Inc. All Rights Reserved.

Compliance Requirements For Oil & Gas

The regulatory environment for oil and gas OT cybersecurity has intensified significantly. Organizations must navigate a complex set of mandatory requirements and voluntary standards that increasingly carry enforcement consequences.

TSA Security Directives

UNITED STATES

Following the Colonial Pipeline incident, the Transportation Security Administration issued mandatory security directives for oil and natural gas pipeline operators. Current requirements include:

- ✓ Designating a cybersecurity coordinator available 24/7
- ✓ Reporting cybersecurity incidents to CISA within 12 hours
- ✓ Conducting vulnerability assessments and developing remediation plans
- ✓ Implementing specific cybersecurity measures including network segmentation, access controls, and continuous monitoring...

NIST Cybersecurity Framework and SP 800-82

While not mandatory for most oil and gas operators, NIST's CSF and SP 800-82 (Guide to ICS Security) are widely referenced in regulatory guidance, insurance requirements, and contractual obligations. Many operators use the CSF as the organizing framework for their OT cybersecurity programs.

NDAA Section 889

UNITED STATES — SUPPLY CHAIN RESTRICTIONS

Section 889 of the FY2019 National Defense Authorization Act prohibits federal agencies, contractors, and grant recipients from procuring or using covered telecommunications and video surveillance equipment or services from Huawei, ZTE, Hytera, Hikvision, and Dahua (and their affiliates). Oil and gas operators that hold federal contracts, operate on federal or offshore leases, or supply the U.S. government must ensure covered equipment is not present as a substantial or essential component of any system. This obligation extends to OT and IoT devices (cameras, sensors, and networking gear) deployed across production and pipeline environments, where prohibited vendor status must be validated against discovered devices rather than assumed inventories.

© 2026 Dragos, Inc. All Rights Reserved.

OTCC

SAUDI ARABIA / GCC OPERATIONS

Operators in the Kingdom of Saudi Arabia are subject to the National Cybersecurity Authority's Operational Technology Cybersecurity Controls (NCA OTCC-1:2022). OTCC sets mandatory minimum cybersecurity requirements for OT/ICS environments in critical facilities, explicitly including refineries, gas plants, and pipeline networks, and covers ICS, SCADA, DCS, and PLC assets. Given the concentration of upstream and downstream oil and gas operations in the Gulf, OTCC is a material requirement for operators and their suppliers working in the region.

IEC 62443

INTERNATIONAL STANDARD FOR INDUSTRIAL CYBERSECURITY

IEC 62443 provides the globally recognized framework for OT/ICS security. Oil and gas operators and their suppliers are increasingly required to demonstrate compliance with relevant IEC 62443 levels; particularly for safety-critical systems and new project delivery. The standard defines security levels, zone and conduit models, and security requirements for components, systems, and processes.

API Standards

API 1164, API 1163

The American Petroleum Institute's pipeline security standards specifically API 1164 (Pipeline Control Systems Cybersecurity) and API 1163 (ICS Cybersecurity Lifecycle), provide sector-specific security guidance that regulators and auditors reference. API 1164 covers network architecture, access control, monitoring, and incident response specifically for pipeline control systems.

NIS2 Directive

EUROPEAN UNION

Organizations operating in EU member states must comply with the NIS2 Directive, which significantly expands the scope of mandatory cybersecurity requirements for critical infrastructure including oil and gas. NIS2 requires risk management measures, incident reporting within 24 hours, and supply chain security obligations with potential fines up to €10 million or 2% of global turnover.

SEC Cybersecurity Rules

PUBLICLY TRADED COMPANIES

Publicly traded oil and gas companies must comply with SEC cybersecurity disclosure rules requiring material cybersecurity incident reporting within four business days and annual disclosure of cybersecurity risk management, strategy, and governance. OT incidents that materially affect business operations trigger these obligations.

© 2026 Dragos, Inc. All Rights Reserved.

TSA Directives	Network segmentation, continuous monitoring, 12-hour incident reporting
IEC 62443	Zone/conduit architecture, security levels for OT systems and components
API 1164	Pipeline control system security, access controls, incident response
NIS2 (EU)	24-hour incident reporting, risk management, supply chain security
SEC Rules	Material incident disclosure, annual cybersecurity governance reporting
OTCC	Mandatory cybersecurity controls protecting oil, gas refineries, plants, pipelines
NIST CSF	Risk-based framework; referenced in audits, insurance, and contracts
NDAA Section 889	Banned use of network and surveillance equipment made by certain Chinese manufacturers

ABOUT DRAGOS

xOT Cybersecurity Built for What's at Stake

What Dragos Does: Dragos delivers cybersecurity for industrial and extended operational technology (xOT) environments, advancing its mission to safeguard civilization. We combine OT-native technology, the industry's deepest threat intelligence, and expert services to give practitioners what they need to see threats, prioritize action, and keep operations running.

Dragos is the global leader in xOT/ICS cybersecurity. Not a general IT security company with an OT module. Every part of what we do was built for operational technology environments, by people who know the difference between an alert that needs investigation and one that will shut down a compressor station.

We serve organizations across electric, oil and gas, manufacturing, water, transportation, mining, and government, operating globally from our headquarters in Hanover, Maryland, with direct presence across North America, EMEA, and APAC.

© 2026 Dragos, Inc. All Rights Reserved.

The Dragos Platform

Named a Leader in the 2026 Gartner Magic Quadrant for CPS Protection Platforms, the Dragos Platform delivers asset inventory, network monitoring, vulnerability management, and real-time threat detection, engineered for environments where a wrong move can stop a turbine or trip a safety system.

Three interconnected capabilities:

- ✓ Visibility with full situational awareness into your xOT environment: comprehensive asset discovery across OT, IT, and IoT, with segmentation validation that maps what is actually on the network versus what diagrams say should be there.
- ✓ OT context to prioritize and automate action: vulnerability management with "Now, Next, Never" prioritization, surfacing the 3–6% of vulnerabilities that require immediate action. Threat detection backed by behavioral analytics linked to expert response playbooks.
- ✓ The expertise to extend your team: OT Watch Complete for 24/7 managed platform service, Neighborhood Keeper for collective defense, WorldView for finished threat intelligence, and Dragos EmberAI for AI-assisted investigation.

The Dragos Intelligence Fabric

Powering everything Dragos does is the Dragos Intelligence Fabric; the living knowledge engine built from over a decade of OT-specific telemetry, adversary research, and frontline incident response. Over 5 petabytes of daily OT telemetry. More than 26 tracked OT threat groups. Partnerships with government agencies and intelligence communities that surface signals no single organization can observe on its own.

It feeds continuously into Platform detections, analyst playbooks, and Dragos EmberAI so what Dragos learns in the field reaches customers in hours, not months.

DRAGOS EmberAI

Dragos EmberAI is the AI specifically built for xOT

Built on the Dragos Intelligence Fabric, EmberAI activates over a decade of OT-specific telemetry, adversary research across 26+ tracked threat groups, vulnerability analysis, and frontline incident response expertise — making that intelligence immediately accessible to every analyst, regardless of their OT background.

© 2026 Dragos, Inc. All Rights Reserved.

Dragos Expert Services

Dragos Expert Services provide direct access to the practitioners deployed in real OT incident response globally and areas of concentration include security assessments, red team exercises, OT tabletops, and 24/7 rapid response from people who have seen real OT incidents.

OT Watch Complete

For organizations that need continuous OT coverage without building an internal SOC, OT Watch Complete delivers 24/7 managed platform service which includes Dragos analysts monitoring, hunting, and escalating with OT-informed context.

HOW DRAGOS HELPS

Protecting Oil & Gas Operations End to End

Dragos protects oil and gas environments upstream, midstream, and downstream. The threat groups we track, protocols we parse, and playbooks we deploy come from what we have observed in real oil and gas OT networks.

01

Asset Visibility Across the Entire OT Footprint

The Platform builds and continuously maintains asset inventory across 600+ industrial protocols, with Active Collection for segmented or legacy environments and data import from engineering systems. In oil and gas:

- Discovery of field devices, RTUs, PLCs, DCS controllers, historians, physical security and safety systems across distributed sites
- Granular device detail, make, model, firmware, OS, and communication patterns, to support vulnerability prioritization and change detection
- Continuous inventory updates without active scanning that could disrupt process operations

02

Threat Detection Tuned for Oil & Gas Protocols

The Platform parses the protocols that matter such as Modbus, DNP3, OPC-UA, PROFIBUS, EtherNet/IP, Foundation Fieldbus. Detection is not generic anomaly flagging. It is behavioral analytics mapped to how real threat actors operate in OT, with response playbooks from Dragos experts who have investigated actual oil and gas incidents.

Tracked groups with demonstrated interest in oil and gas include XENOTIME (behind TRITON/TRISIS), COVELLITE, RASPITE, and others. When the Dragos Platform detects behaviors consistent with known adversary tradecraft, it surfaces that context directly alongside the alert.

© 2026 Dragos, Inc. All Rights Reserved.

03

Vulnerability Management Without Operational Risk

Vulnerability management in oil and gas OT requires a fundamentally different approach than IT patching. Systems cannot be rebooted during operations. Vendors may not release patches for years. The Dragos Platform applies xOT-corrected vulnerability scoring and "Now, Next, Never" prioritization to identify the small fraction of vulnerabilities that actually require immediate action — cutting through thousands of CVEs to focus on what poses real operational and safety risk in your specific environment.

Only 3–6% of OT vulnerabilities require immediate action. That precision separates a manageable remediation program from one that overwhelms engineering teams.

→ Source: Dragos 2026 Year in Review

04

Network Segmentation Validation

Oil and gas environments accumulate segmentation drift. Emergency changes, vendor access paths, and undocumented connections create gaps between the architecture on paper and the one on the network. The Platform analyzes firewall, router, and switch configurations to identify unintended communication paths continuously, not just at audit time.

05

Incident Response for xOT Environments

xOT incident response must account for process state, safety implications, and operational continuity simultaneously. Dragos Expert Services provide 24/7 rapid response from practitioners who have worked real OT incidents. The Platform's Investigation and Response capability gives on-site teams the network history, asset context, and xOT-informed playbooks to investigate safely without disrupting operations.

06

Protecting People and the Environment

SIS, fire and gas detection, and emergency shutdown systems are the last controls before a cyber event becomes a physical incident. Dragos tracks adversary groups that specifically target these systems including XENOTIME, responsible for TRITON/TRISIS. The Dragos Platform provides visibility into SIS communications, detects anomalous safety system behavior, and surfaces threat context so teams know when a network event carries physical consequence before it becomes an emergency.

© 2026 Dragos, Inc. All Rights Reserved.

07

Supporting Operational Efficiency and Cost Reduction

OT visibility is not only a security driver. Operators using the Platform surface operational intelligence they were not previously capturing: rogue communications explaining intermittent faults, undocumented connections causing bandwidth saturation, configuration drift maintenance teams can act on before failures occur. In oil and gas, Dragos contributes directly to uptime, reliability, and root cause analysis. Security that pays for itself in operational outcomes is how the best operators justify the investment.

08

Compliance Support Across Regulatory Frameworks

The Platform generates audit-ready documentation for TSA directives, IEC 62443, API 1164, and NIS2. Continuous monitoring provides evidence retention regulators require. Segmentation validation maps to IEC 62443 zone and conduit requirements. Network Monitoring directly addresses SANS ICS best practices.

INDUSTRY-SPECIFIC DEPTH

Dragos analysts have conducted assessments at upstream production facilities, offshore platforms, pipeline control environments, and downstream refineries.

The detections, playbooks, and protocols in the Platform reflect that experience directly.

© 2026 Dragos, Inc. All Rights Reserved.

OUTCOMES & BENEFITS

What Dragos Delivers

Dragos customers in oil and gas see measurable improvement across visibility, detection, vulnerability management, and compliance without disrupting operations.

01
Visibility and Asset Intelligence

- Complete, continuously maintained asset inventory across OT, IoT, and xOT including field and dormant devices that prior tools may have never discovered
- Granular device context such as firmware, OS, patch level, communications, enabling informed vulnerability prioritization and procurement
- Continuous baselining that immediately surface deviations such as adversary activity, misconfiguration, or unauthorized change

02
Threat Detection and Response

- Detection of adversary activity earlier in the kill chain, before operational impact occurs
- xOT-informed alert context that enables analysts to make confident triage decisions without requiring years of OT expertise
- xOT-aware response playbooks so investigators know what they can safely do and what carries operational risk
- Reduced MTTR through Investigation and Response workflows that consolidate alerts, asset context, and forensic data in one view

03
Vulnerability Management

- “Now, Next, Never” prioritization that cuts thousands of CVEs down to the handful requiring action thereby preventing remediation program paralysis
- OT-corrected vulnerability scoring that reflects actual exploitability in operational environments, not CVSS scores designed for IT software
- Vendor coordination context which inform for example, whether patches exist, workarounds are available, or segmentation is the right primary mitigation

© 2026 Dragos, Inc. All Rights Reserved.

04
Compliance and Audit Readiness

- Continuous monitoring provides the evidence retention required by TSA directives, NIS2, and API 1164
- Segmentation validation maps network reality to IEC 62443 zone and conduit requirements, identifying drift between intended and actual architecture
- Audit-ready reporting reduces the manual documentation burden for regulatory assessments

05
Operational Continuity

- Multi detection engine methodologies monitoring delivering full network and asset visibility with zero operational risk to process systems
- xOT-native deployment that does not require changes to control system configurations or network architecture
- Expert guidance from practitioners who design security measures around operational constraints

06
People and Environmental Safety

- Visibility into Safety Instrumented System communications, enabling detection of anomalous behavior before it reaches physical consequence
- Threat intelligence on adversary groups targeting SIS, fire and gas, and emergency shutdown systems, with detection logic mapped to their specific tradecraft
- Security decisions informed by physical process context, so response actions account for operational and safety implications before they are taken

07
Operational Efficiency and Cost Reduction

- xOT network visibility that surfaces operational anomalies, not just security threats, enabling engineering teams to identify and resolve process issues faster
- Reduced unplanned downtime through early detection of configuration drift, rogue communications, and network anomalies that precede equipment failures
- Accelerated root cause analysis when process faults occur, combining network history, asset context, and traffic patterns into a single investigation view

© 2026 Dragos, Inc. All Rights Reserved.

Collective Defense Through Neighborhood Keeper

Neighborhood Keeper enables oil and gas operators to share anonymized threat intelligence across the sector without exposing sensitive operational data. When one operator detects a novel behavior, it updates detections across the community presenting a sector-wide defense network that gets stronger as threats evolve.

600+

customers globally

3-6%

of OT vulns require immediate action

#1

Gartner Magic Quadrant Leader, CPS Protection Platforms 2026

→ Source: Dragos External Pitch Deck 2026; Gartner Magic Quadrant for CPS Protection Platforms 2026; Dragos 2026 Year in Review

© 2026 Dragos, Inc. All Rights Reserved.

From the Field
Customer Story

Keyera Corp.

Midstream Oil & Gas • Canada

Keyera is a Canadian midstream energy company operating natural gas gathering and processing facilities, fractionation infrastructure, and storage and transportation assets across western Canada. Their iso-octane production facility is a high-value, continuously operating site. Unplanned downtime is not an abstract cost. It is measured in real time, in lost barrels and disrupted supply commitments.

A recurring fault in the Advanced Process Control system was taking a critical module offline every three days. The facility generates roughly $1.5 million in daily revenue. Each unplanned outage meant not only lost production but a complex, time-consuming restart sequence that added risk to every cycle. Engineers from two different vendors, one based in Finland, one in Korea, were each pointing at the other's equipment. Months passed. Losses mounted into the hundreds of thousands. No one had objective evidence of what was actually happening on the network.

Keyera deployed the Dragos Platform. The network dashboards and traffic visualizations did what months of vendor escalation could not: they showed exactly what was happening on the wire. The APC system was retrying communications 45% of the time, saturating available bandwidth and cascading into the module failures that had been shutting down production on a three-day cycle. The evidence was objective, timestamped, and undeniable by either party.

Both vendors agreed on the fault. The root cause was identified and remediated. The APC system has run cleanly since. The production disruptions stopped. And Keyera now has continuous OT network visibility across the facility, so the next anomaly, whether operational or adversarial, surfaces before it becomes an outage.

INDUSTRY

Oil & Gas

LOCATION

Canada

> "We proved it because we saw it on the wire."
>
> — Keyera Corp.

WHY THIS MATTERS

This is an operations story that security enabled. In oil and gas, that is what OT visibility, security and control actually delivers.

© 2026 Dragos, Inc. All Rights Reserved.

About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Washington DC, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com

© 2026 Dragos, Inc. All Rights Reserved.