SOLUTION BRIEF

# Securing Facility Related Control Systems (FRCS)

## Leveraging the Dragos Platform to Address a Common Threat Scenario

Building automation systems, or facility-related control systems (FRCS), provide a centralized way to manage and optimize energy usage, control building access, and monitor environmental conditions. Examples of FRCS include video surveillance, fire alarm systems, access control, HVAC (heating, ventilation, and air conditioning) systems, environmental control, and energy management systems. Typically comprised of interconnected devices, including controllers, sensors, valves, and related networking equipment, these systems can be vulnerable to cyber attacks if they are not properly designed, installed, maintained, and secured.

### A cyber-attack on facility-related control systems in an industrial setting or research can have severe impacts on the operations, safety, and security of the building and its occupants, including:

- **Disruption of Operations:** If the operation of building systems such as HVAC, lighting, and access control are disrupted, the facility or research can incur significant downtime, reduced productivity, and financial losses.

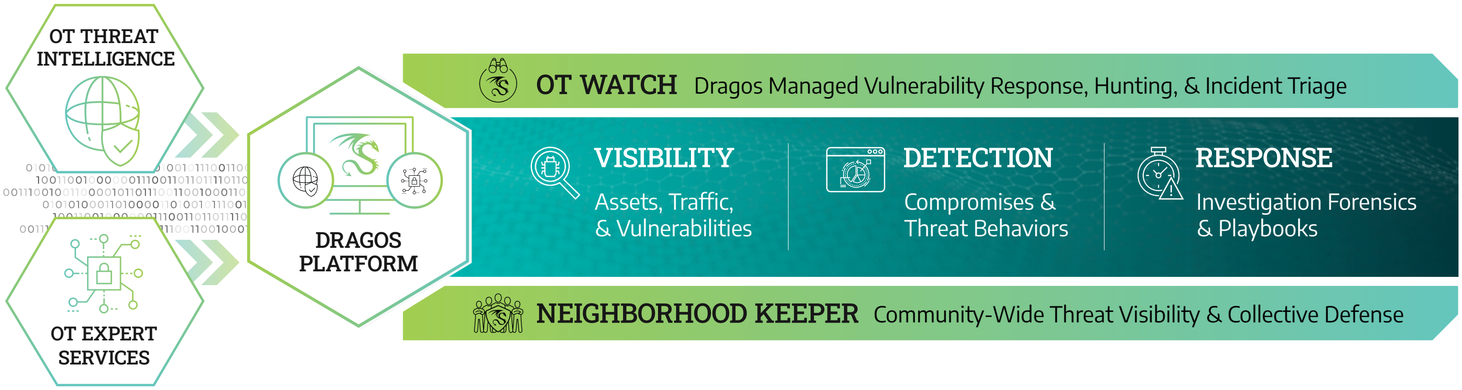
- **Physical Damage and Safety Risks:** An attack on the facility-related control systems could cause damage to equipment and infrastructure or create safety risks. If the attack affects the building's fire alarm or sprinkler systems, it could increase the risk of damage or loss of life.

- **Loss of Data:** An attack could result in the loss of critical data, such as intellectual property, building automation configurations, or occupant data.

- **Regulatory Compliance Issues:** Failing to protect control systems from cyber-attacks could result in the building owner or operator failing to comply with regulations and standards, leading to fines, legal action, or reputational damage.

## The Dragos Platform Monitors and Secures FRCS

The Dragos Platform is developed and managed by the only US-owned OT cybersecurity hardware vendor, intelligence, and services company. Our technology is used around the world to secure large managed data centers, national laboratories, government-owned industrial facilities, and more. The Dragos team is regularly consulted in the design and assessment of network architectures, endpoint protection, and operational resilience. The Platform's protocol support extends to a wide range of protocols present in the 16 federally recognized critical infrastructure sectors, as well as specialized building automation protocols like BACnet and LonTalk.


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

## FRCS 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 within FRCS and beyond.

**Vulnerability Management:** Without simple, accurate, prioritized guidance, you'll waste time and money patching system and device 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, including FRCS, so that you can 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, including those within FRCS, 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 OT/ICS network and device health, support ATO/RMF artifacts, and integrate active defense via SIEMENS Siber Protect.

# Additional Solutions to Safeguard Your Facility-Related Control Systems

## WorldView Threat Intelligence

Backed by the industry's largest and most experienced team of industrial control systems (ICS) cybersecurity practitioners, Dragos WorldView threat intelligence arms your organization with in-depth visibility of threats targeting industrial environments globally and the tried-and-true 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.

## Incident Response

OT-specific response plans are essential for environments that have operations technology. With different devices and communication protocols, OT incident response is distinct from IT, with different attack tactics, techniques, and procedures (TTPs) used by threat groups. Since the potential impact of a cyber-attack can vary based on visibility, the ability to respond, and your organizational security posture, a dedicated ICS/OT incident response plan that considers your needs is crucial to quickly scope, investigate, and respond to incidents.

## Other Professional Services

Dragos is comprised of the industry's largest and most experienced team of ICS security practitioners. We can help you understand your organization's unique environment to build an effective ICS cybersecurity program that's right for you. Our service offerings provide you with visibility and insight into your OT environments, identification of vulnerabilities and threats, education for practitioners, and overall risk mitigation.

### 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**.