DRAGOS

WHY **OT VISIBILITY** IS CRUCIAL FOR **INDUSTRIAL CYBERSECURITY**

info@dragos.com

@DragosInc

Dragos, Inc.

ABSTRACT

Fully understanding the operational technology (OT) environment — what assets are running on the OT network, what traffic looks like, which vulnerabilities exist within assets, and which potential threat behaviors might be lurking within — is fundamental to strong industrial cybersecurity. Without solid OT visibility, it becomes nearly impossible to fully understand the risk posture of industrial control systems (ICS) and OT networks. Threat detection becomes an exercise in uncertainty, and organizations face an uphill battle in deciding the most effective security controls for their OT deployments.

Unfortunately, many industrial organizations today still operate with considerable blind spots across their OT environments. As many as eight in 10 organizations have extremely limited to no visibility into their OT assets and nearly half of them are not even sure if they've had a security incident impact their OT systems in the past year. If you are unsure whether your organization is among these, consider the following questions:

- Do you know exactly what OT assets you're running, including versions they're operating?
- Do you know which vulnerabilities exist in those assets — and which ones introduce the most risk to the OT environment?
- Do you know what alternate mitigations you can make if you can't patch those vulnerabilities?
- Would you know if you were compromised?

If your organization struggles to answer any of these questions, odds are that it could stand to improve its OT visibility. Take heart — OT blind spots are not necessarily a failing on the part of an industrial organization, let's examine why.

Organizations running these networks have traditionally been able to operate efficiently and safely without these detailed views of cybersecurity risk before the days of the Industrial Internet of Things (IIoT) and digital connectivity. What's more, establishing and maintaining good OT visibility takes considerable effort, meticulous planning, and specialized OT security technology to carry out. But now as OT cybersecurity attacks grow and risks pile up due to the increased interconnectedness and remote access of ICS systems, things need to change.

Here's why OT visibility is crucial, what it takes to achieve it, and how to partner with a vendor who can not only provide the kind of OT cybersecurity expertise needed to get started, but more importantly also walk that journey with you.

OT VISIBILITY BY THE NUMBERS

86%

of Dragos's services customers have **EXTREMELY LITTLE TO NO VISIBILITY** into the assets in their OT environment when they were first engaged

48%

of organizations with OT systems **DID NOT KNOW WHETHER THEY HAD A SECURITY INCIDENT** impact those assets in the past year

63%

of organizations **HAVE EXPERIENCED AN ICS/OT CYBERSECURITY INCIDENT** in the past two years

$50B

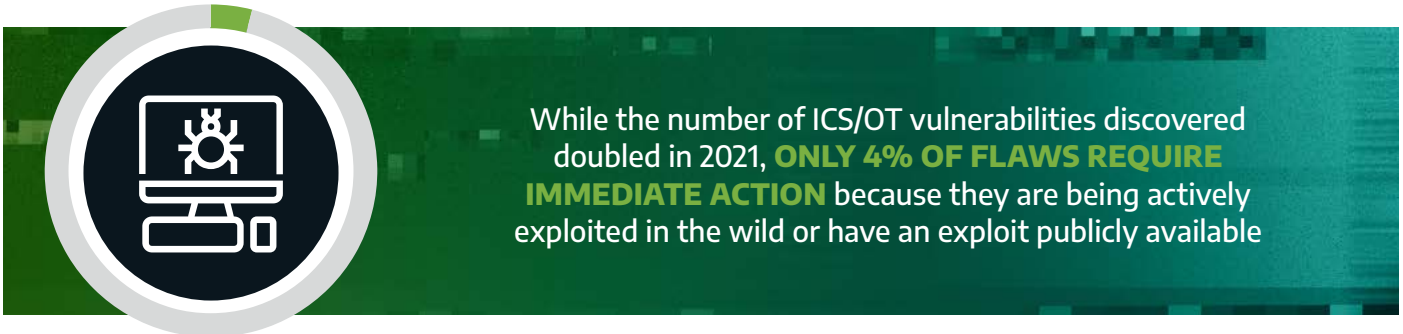
By 2023 the impact of OT cyber-attacks will reach **$50 BILLION**

70%

External connections to OT more than doubled in 2021, with **70% OF ORGANIZATIONS RUNNING OT ASSETS THAT CAN BE ACCESSED REMOTELY**

49%

of ICS and OT vulnerability advisories in 2021 **COULD CAUSE BOTH A LOSS OF VIEW AND LOSS OF CONTROL** in an OT system



THREE COMPONENTS OF OT VISIBILITY

OT visibility requires a great deal of planning and careful execution to fully come to fruition. At the heart of OT visibility are three major components: asset visibility, threat visibility, and vulnerability management.

ASSET VISIBILITY

WHAT IT IS

Organizations achieve OT asset visibility through the discipline of discovering, inventorying, and classifying the systems that run operational processes in industrial facilities. OT asset visibility tracks configuration states of assets, versions used, and maps relationships between assets. Asset visibility is first established with an inventory of assets, which can then be used to prioritize which assets to monitor on a continuous basis for threat detection, vulnerability management, and change control.

WHY IT MATTERS

When organizations fully identify and inventory their OT assets, every cybersecurity process becomes easier, whether leveraging threat detection, actively managing assets for vulnerabilities, implementing overarching strategic OT security initiatives, or responding to an incident.

HOW IT HELPS OT CYBERSECURITY

A clear and continuously updated view of the industrial assets in use within an environment helps OT cyber professionals make better, more informed decisions. OT asset visibility gives them a blueprint of the environment to know where to look for:

- remote connections and network communications operators didn't expect,
- active threats operating quietly in the environment,
- insecure configurations,
- embedded vulnerabilities, and
- rogue assets in place within OT networks.

ASSET VISIBILITY IN ACTION

A major provider of wind power in North America, NaturEner uses Dragos Platform to maintain OT visibility across its wind farm networks and energy management system (EMS) networks. The assets are spread across subnets that have a massive physical footprint — with locations hundreds of miles apart. Before partnering with Dragos, NaturEner struggled to maintain an up-to-date view of what was running on all of their OT networks, including windfarm ICS networks. Now the team can see those devices mapped and logically grouped with traffic summaries. This new level of asset visibility makes it much easier to understand and improve the firm's security operations.

> We've been able to track who is talking to whom over what ports, and most importantly, see traffic from our warranty vendor's various sites and systems. Over time, as we've monitored the infrastructure and learned how our devices are talking, we have a better sense of what is happening in our network. Girded with that knowledge and the Dragos Platform, we hunt for issues, intrusions and improperly configured devices, thereby increasing our security footprint across the organization.
>
> **— A NaturEner representative**

THREAT VISIBILITY

WHAT IT IS

Organizations achieve threat visibility through the combination of thorough, relevant OT threat intelligence and threat detection mechanisms that identify active threats in an environment.

OT threat intelligence is collected by expert ICS cybersecurity researchers who actively hunt for and observe industrial-specific adversaries on a range of industrial networks worldwide. They categorize the tactics, techniques and procedures (TTPs) of the threat actors and provide advisories that include attack details and technical indicators of compromise (IOCs) tied to them.

OT threat detection codifies advisory information about threats operating elsewhere into technical mechanisms that look for clues of similar threat activity inside an OT environment. Detection depends on monitoring of OT assets and network traffic in the context of threat intelligence.

WHY IT MATTERS

As security processes mature, adversaries adjust their tactics to circumvent new safeguards put in place, often going undetected. Greater threat visibility can be achieved by assessing the capabilities of threat groups and connecting this information with what is happening in an organization's OT environment. This paves the way for early warning and detection of threats and facilitates threat hunts within an organization's infrastructure.

HOW IT HELPS OT CYBERSECURITY

Threat visibility makes it possible to prioritize cybersecurity controls that protect against the threats most likely to put an environment's high-value OT assets at risk.

A platform that leverages IOCs identified through threat intelligence directly into the security monitoring of OT assets adds additional assurance that a security team will quickly be alerted to threats operating within an environment. Other cybersecurity benefits of solid threat visibility include:

- Better situational awareness and data to fuel threat hunts and incident response activities
- Improved vulnerability mitigation patch prioritization based on which flaws attackers are currently attacking
- Sector-specific data to understand what the OT threat landscape looks like for the business
- Relevant, contextualized information to fuel clear reporting to the C-suite on industry relevant threats and cyber headlines
- Compelling evidence to justify additional resources to combat relevant threats

THREAT VISIBILITY IN ACTION

Orlando Utilities Commission (OUC) is a public water utility that serves more than 250,000 households. The municipal entity was initially drawn to Dragos Platform for its automated passive asset discovery

capabilities, along with its mapping and zoning functions. But as they dug into the capabilities of the platform further, OUC experts recognized that it could greatly strengthen their threat visibility.

They previously utilized threat intelligence sources that couldn't give deep enough OT-specific intelligence. By pairing Dragos WorldView threat intelligence with Dragos Platform, the firm can get relevant, detailed threat visibility to automate the blacklisting of malicious industrial-themed domains, as well as to ensure that their OT network is configured to better defend against the tactics and techniques of determined adversaries.

> **"We did receive notices from the sector-specific information sharing services (before Dragos), but it was like someone telling us that a person (threat) was about to enter America somewhere along the U.S.-Canada border. Unfortunately, this information wasn't as specific or as actionable as we needed. These types of alerts even led to confusion and panic. The combination of Dragos WorldView and the Dragos Platform gives us much better information.**
>
> **— Joe Reilly, OUC Director of Operational Technology**

VULNERABILITY MANAGEMENT

WHAT IT IS

OT vulnerability management is the practice of identifying and remediating vulnerabilities in OT assets that put them at risk of a cyber attack. Software flaws can exist in operating systems, applications, industrial firmware or protocols and are classified based on risk of exploitation. Remediation can either come through patching vulnerable assets or implementing compensating controls that mitigate the risk of a flaw.

WHY IT MATTERS

Just as with information technology (IT) systems, OT assets such as industrial control systems (ICS) contain a range of software and configuration flaws that can be exploited by criminals to carry out attacks. Discovery of these vulnerabilities grows by the day, and so do the attacks. In 2021 the number of ICS/OT system vulnerabilities doubled, and some 63% of organizations have experienced an ICS/OT cybersecurity incident in the past two years.[iii]

HOW IT HELPS OT CYBERSECURITY

Effective OT vulnerability management can greatly reduce the attack surface of the OT network, cutting off potential avenues for threat actors to compromise OT assets and impact physical safety. Ideally an OT vulnerability management program prioritizes remediation not only on based on vulnerability classification but also the business context in which a vulnerable asset operates — including the criticality of the asset and the risk of loss of view or control. It can also improve prioritization by layering in threat intelligence about how the flaw is being exploited in the wild. Dragos found that only 4% of OT flaws require immediate action because they are being actively exploited in the wild or an exploit is publicly available. The key is figuring out which 4% that is.

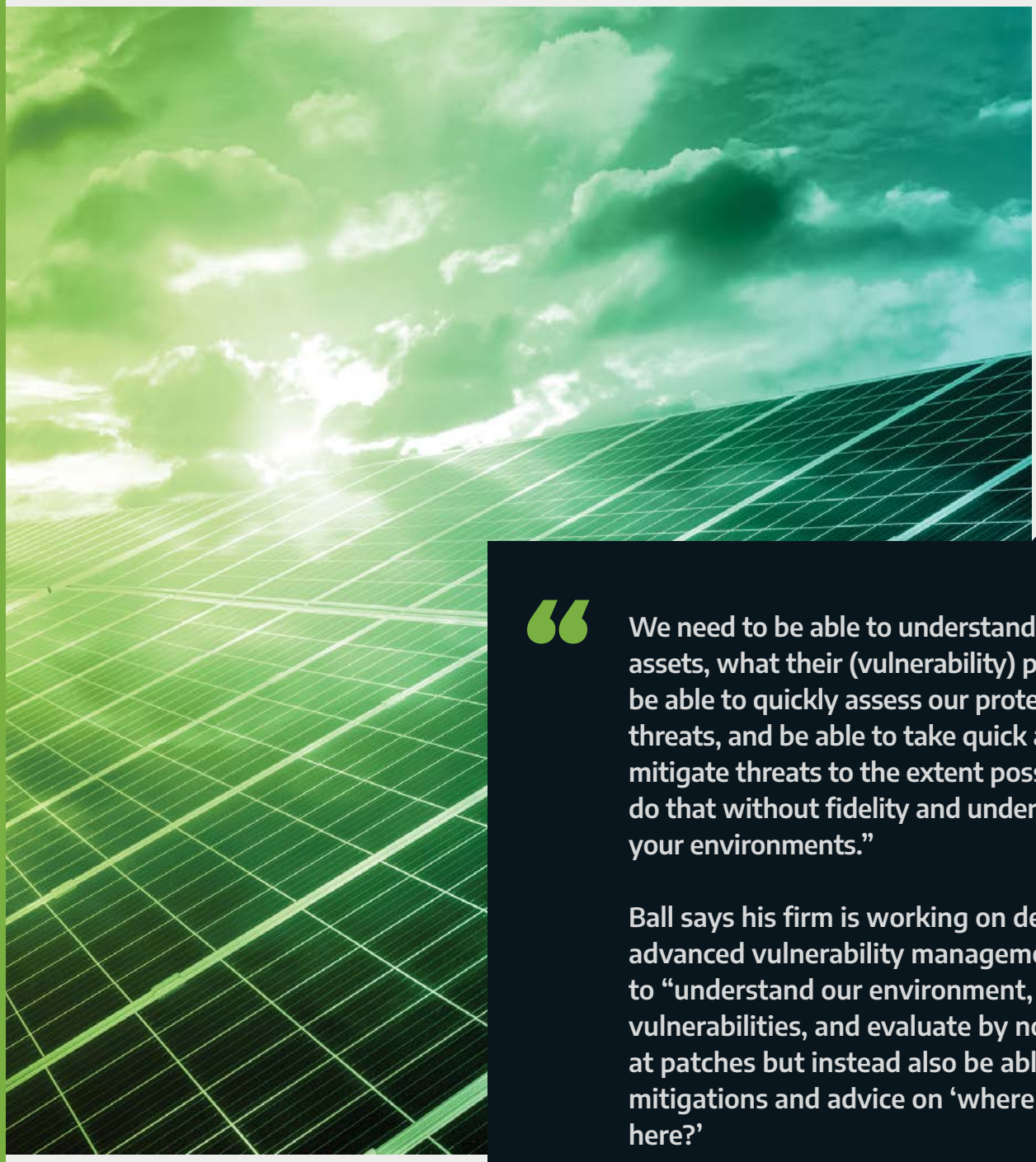
Effective OT vulnerability management can help an OT cybersecurity program:

- Simplify compliance by effectively documenting vulnerabilities and their disposition (patched, remediated, or risk-accepted)
- Prioritize action around vulnerabilities based on importance of the asset, downtime risks, and evidence of in-the-wild exploits against them
- Maximize remediation resources to get the most out of cybersecurity budgets
- Provide a unifying view of vulnerabilities across assets for both OT operators and cybersecurity stakeholders

VULNERABILITY MANAGEMENT IN ACTION

According to the Berkshire Hathaway Energy CSO Michael Ball, one of the biggest cybersecurity challenges for his firm is that his team and other stakeholders “must know everything in our environment.” The company operates 10 locally run energy companies across 28 states in the United States. Ball says he’s currently on a mission to getting “more comprehensive and unified” OT visibility so his organization can have better

situational awareness about the state of their OT assets as they make business and security decisions across the organization. A big part of that is improving the way his firm discovers and assesses OT vulnerabilities.



> We need to be able to understand all of our assets, what their (vulnerability) posture is, to be able to quickly assess our protections against threats, and be able to take quick action to mitigate threats to the extent possible. You can't do that without fidelity and understanding of your environments."
>
> Ball says his firm is working on deploying advanced vulnerability management capabilities to "understand our environment, prioritize vulnerabilities, and evaluate by not just looking at patches but instead also be able to look at mitigations and advice on 'where do we go from here?'

— Michael Ball, CSO
Berkshire Hathaway Energy

BRINGING **ALL THREE COMPONENTS** TOGETHER

All three components of OT visibility are interdependent on one another.

ASSET VISIBILITY provides the framework around which vulnerability management and threat visibility can be conducted. Without understanding which assets are deployed within an environment, it can be nearly impossible to know where to look for flaws, let alone active threats operating within them.

THREAT VISIBILITY can provide valuable data to help vulnerability management programs prioritize remediation efforts based on exploit activity in the wild.

VULNERABILITY MANAGEMENT, especially information on the disposition of various flaws in an environment, in turn can be used to decide where to actively hunt for threats using threat visibility and also to continuously update an asset inventory.

THE ROLE OF VISIBILITY IN AN OT CYBERSECURITY PROGRAM

ASSET VISIBILITY	THREAT VISIBILITY	VULNERABILITY MANAGEMENT
• Create asset inventory • Identify crown jewel assets • Change management	• See unauthorized IT-OT traffic • Analyze file transfers • Detect adversary behaviors	• Simplify compliance • Prioritize vulnerabilities • Maximize remediation resources

When all three components are well-integrated together to provide end-to-end OT visibility, they can be leveraged to fuel effective and more efficient incident response. OT visibility makes it possible to analyze changes to infrastructure and provides forensic records to reconstruct threat activity. This makes it easier to efficiently manage response and recovery efforts.

MAINTAINING **VISIBILITY THAT MATTERS** FOR OT ENVIRONMENTS

One of the biggest challenges of establishing and maintaining good OT visibility is that the tools, processes, and goals differ from what many cybersecurity experts may be used to. Asset visibility, threat visibility, and vulnerability management are all traditional areas of discipline around which IT visibility is also realized. However, because OT risks and operational considerations are very different than those in IT, the path to achieving OT visibility follows a different course.

Whereas IT's biggest risks are around confidentiality, integrity, and availability, OT's biggest risks are around physical safety and the loss of operations of things like the electrical grid, water systems, safety systems, pipeline or plants. Environmental considerations are different as well, with different systems in play, different network traffic and protocols in use, and a different set of adversaries.

IT & OT: Cyber Risks are Different

IT

OT

IT		OT
MANAGE INFORMATION Servers, laptops, mobile devices, cameras, point-of-sale devices	**SYSTEM TYPES**	**OPERATE PHYSICAL PROCESSES** PLCs, RTUs, HMIs that run actuators, sensors & valves
Patch/update software	**MANAGE VULNERABILITIES**	Patching production systems means plant or system shutdown; need alternatives
DNS, HTTPS, RTP, MP4 video	**NETWORK TRAFFIC**	Hundreds of industrial system communications protocols
Loss of data, intellectual property, network services	**MAJOR INCIDENT IMPACT**	Loss of electrical grid, pipeline or plant operations; loss of control of safety systems

This introduces the following challenges in the three areas of OT visibility:

OT CHALLENGES IN ASSET VISIBILITY

- IT asset visibility tools and tactics do not translate well to OT environment
- The protocols used in OT aren't as well covered by IT vendors
- Network scanning for asset discovery could disrupt OT processes
- Facilities can be geographically dispersed and difficult to manually inventory

OT CHALLENGES IN THREAT VISIBILITY

- Downtime tolerance is limited and the risk of a patch disrupting system stability can sometimes outweigh the risk of it being exploited
- OT/ICS contracts often dictate that organizations must get approval from OT vendors before patching systems
- OT systems are often run continuously, with months or years before a maintenance window allows for patches to be administered
- Public vulnerability notices often don't include enough context about OT risk or alternative mitigations beyond patching

OT CHALLENGES IN VULNERABILITY MANAGEMENT

- Indicators are only obtained retroactively and do not scale well between victims.
- Configuration and anomaly detections are unreliable and difficult to maintain in dynamic environments.
- Detecting threat behaviors is highly effective but difficult to implement and are not fully reusable across all industries.
- Limited asset visibility and coverage reduces the effectiveness of detection in OT environments.

All of these considerations mean that an OT cybersecurity program needs OT visibility technologies and processes that are built specifically for the environment. Not only does the visibility afforded need to provide OT-relevant information, but it must be gathered in a way that doesn't threaten the stability of OT processes.

HOW **DRAGOS PLATFORM** DRIVES OT VISIBILITY

The Dragos Platform is the most effective OT security solution for gaining comprehensive OT visibility, with knowledge built into it from the largest and most experienced team of ICS security specialists in the world. Dragos Platform drives OT visibility in all three key areas:

ASSET VISIBILITY

- Establish asset profile baselines for connected integrations with firewall and CMDB systems
- Group assets in a visual map with customizable zones for easier cyber-ops management
- See historical changes with timeline views to spot unexpected activity

THREAT VISIBILITY

- Industry specific analysis, correction, and enrichment of known vulnerabilities
- Alternative mitigation advice, prioritized with "Now, Next, Never" guidance
- Disposition tracking for full lifecycle management and to simplify audits

VULNERABILITY MANAGEMENT

- Curated Indicators of Compromise (IOCs), malicious IPs, domains, and hashes from Dragos Intelligence
- Anomalous traffic patterns and baseline deviation alerts
- Composite detections from TTP analysis of threat groups and attacks

> "We were initially focused on anomaly detection software and originally thought that we would benefit from the ability to see and react to alerts. But we quickly realized that the majority of those solutions just weren't as mature as we needed. This awareness led us to consider OT visibility platforms in general, and the conversation pretty much started and stopped with Dragos.
>
> **— Electric & Water Utility Partner**

DRAGOS PLATFORM

Dragos Platform provides OT threat intelligence and expertise at machine speed and scale. It codifies learning and research gained by Dragos analysts and field consultants. This means that the asset visibility afforded by the platform's inventorying, mapping, and continuous monitoring is contextualized by the ongoing work done by Dragos Global Services. Dragos Platform leverages and enables the following to create more complete OT visibility for customers:

OT THREAT INTELLLIGENCE

- Research about threat groups and attack campaigns against OT targets
- Analysis about true operational impact of vulnerabilities, CVE enhancement for OT and alternative mitigation recommendations
- Adversary research, including IOCs, TTPs, and threat behaviors

OT EXPERT SERVICES

- Threat hunting and vulnerability analysis
- Architecture assessments and capability maturity assessments
- Incident response planning and services

NEIGHBORHOOD KEEPER

- Collective but aggregated ICS threat, asset, & vulnerability intelligence across participating Dragos Platform organizations
- Industry, regional, & system-wide view shared between asset owners & community defenders
- Request for Assistance between participant peers or Trusted Advisors

OT WATCH

- Curated visibility of your OT environment
- Detection - proactive threat hunting
- Response - incident triage

Interested in learning more? Check out any of the following whitepapers (click to download) or contact **info@dragos.com** to start a discussion.

10 Ways Asset Visibility Builds The Foundation For OT Cybersecurity

Understanding the Challenges of OT Vulnerability Management

How to Prepare for and Respond to Ransomware in OT Environments

IT Threats Impacting OT Infrastructure

ABOUT DRAGOS, INC.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities,energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

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 DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT www.dragos.com.