DRAGOS

# 10 REASONS WHY INDUSTRIAL ORGANIZATIONS NEED BETTER ASSET VISIBILITY

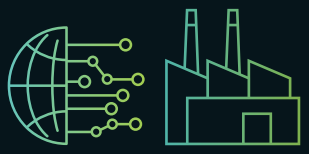
A key defense against increasing industrial cyber threats is to fully identify and inventory all your operational technology (OT) assets, including communication pathways. Every cybersecurity process becomes easier and more effective, when you have good asset visibility.

**Here are 10 ways OT asset visibility lays the foundation for your industrial cybersecurity program and activities -- today and in the future.**

## 01 UNDERSTANDING NORMAL

*An aggressive trend towards connected digital operations is accelerating a need to have centralized views across OT environments.*

Asset visibility of your operational technology offers a full view of how processes and workflows execute in the operational environment. It accelerates cybersecurity activities such as threat detection and incident response by providing valuable context and a higher fidelity of information about your industrial operations.



**ONLY 10%**
of enterprises have a **COMPLETE INVENTORY OF THEIR OT ASSETS COVERED** by their SOC
— SANS Institute 2019 SOC Survey

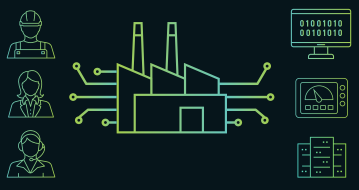
## 02 ASSET VERIFICATION

*Knowing the state of an asset allows operations teams to work more efficiently and with the speed they require, particularly during an unplanned outage or potential security incident.*

Asset visibility can provide insight into not just the existence of an asset but also its version, firmware status, and configuration state. A complete asset database allows industrial asset owners and operations to clearly identify misconfigurations, vulnerabilities, and other weaknesses across an industrial control environment.


## 03 IDENTIFY & VISUALIZE ASSET RELATIONSHIPS

*If an engineering workstation suddenly starts sending commands to a controller in Zone 2 when it is only supposed to talk to devices in Zone 1, then investigation is needed.*



Mature asset visibility capabilities make it easier to monitor an organization's OEM and third-party management communication channels to ensure they're not introducing unnecessary risk to the ICS ecosystem. This includes knowing that communication paths aren't touching other systems, only doing work during approved change control windows, and so on.

## 04 THREAT DETECTION

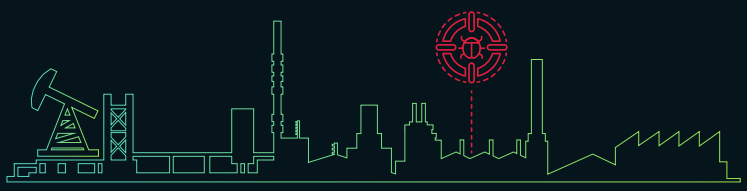
*Visibility and an established baseline for asset inventory and behaviors adds crucial contextual clues to speed up threat detection.*

Environmental information coupled with threat behavior data, provides valuable additional context on whether changes are related to adversary tactics, techniques and procedures (TTP), as opposed to planned infrastructure changes.

## 05 SPOTTING ROGUE ASSETS

*Adversaries can gain an advantage by targeting assets that organizations aren't managing properly, like undocumented engineering workstations, as a way to quietly persist on a network.*

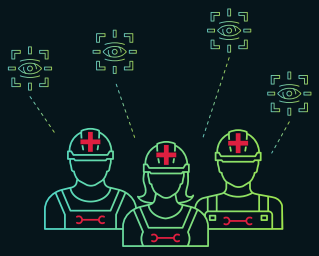
Companies with remote sites or large sprawling facilities with varying levels of physical security may not be aware of the rogue or hidden assets that open the environment to risk.



Automated asset identification for rogue assets can make a big difference in continuously hardening your OT environments.

## 06 INCIDENT RESPONSE

*Responders armed with accurate asset inventories can confirm threats and identify incidents faster.*



When investigating an incident, asset visibility can make all the difference in accurately scoping the spread of an incident and fully understanding the systems affected by the adversary's actions. Greater visibility gives responders a stronger vantage point to determine whether a threat is fully eradicated.

## MITIGATING NEW CRITICAL VULNERABILITIES & THREATS 07

*Can you quickly answer executives when they want to know whether your infrastructure is impacted by a new vulnerability or a new threat group's TTPs?*


A searchable, easily accessible asset inventory can help to quickly rule out irrelevant threat intelligence or calm fears of a named new vulnerability. It can also help teams pinpoint where relevant assets are if they need to be patched — or secured through compensating controls if a patch is not available or impractical to deploy for operational reasons.

## 08 SUPPLEMENTING CHANGE MANAGEMENT WITH CONFIGURATION DETECTION

*Configuration drift is inevitable in a dynamic industrial network and it can be difficult to track and manage changes as they occur in real-time.*

The right asset visibility capabilities can make it easier to detect changes in configurations that make infrastructure weaker or even knock it out of compliance with internal or external regulatory standards. They provide the building blocks for improving change management and asset management maturity — a key element not just for security but also operational integrity.

**90%**

**of Dragos's professional services engagements find that industrial organizations have EXTREMELY LOW OR NO VISIBILITY into the assets in their OT environment**

— Dragos 2020 ICS Cybersecurity Year in Review

**+60%**

**Increase in OT CONNECTEDNESS in last 4 years**

- 2020 IDC Survey

## MINIMIZE IMPACT OF COMPLIANCE REPORTING 09

*Industrial operations are increasingly under tremendous pressure to meet regulatory mandates such as NERC CIP and standards like ISA 99/IEC-62443.*

This process often requires a significant amount of manual labor and can be disruptive to daily work. Automated discovery, analysis, and mapping of assets can minimize the impact of compliance reporting effort for the entire team and free up resources for other security or operational improvements.

## 10 JUSTIFYING SECURITY INVESTMENTS

*In order to conduct a robust risk assessment, security strategists must understand the complexity of their OT asset portfolio to effectively identify gaps in controls and processes.*

Asset inventories and mapping provide the security team with an essential source of information for adjusting cybersecurity programs and offer a clear line of sight to investment coverage.

Contact Us at sales@dragos.com or request a demo at dragos.com/request-a-demo.

DRAGOS