SOLUTION BRIEF

DRAGOS | INDUSTRIAL DEFENDER

Integrated Cybersecurity Technology from Dragos and Industrial Defender

Comprehensive ICS/OT Asset Visibility and Configuration & Change Management

HIGHLIGHTS

- Achieve comprehensive inventory and visibility of ICS/OT assets, devices, and vital details in OT environments.
- Understand endpoint configurations and automatically collect, normalize, and report changes in the OT environment, regardless of vendor or location.
- Ensure secure configuration of systems and evaluate any changes for potential security risks and compliance issues.
- Manage and prioritize vulnerabilities in the environment to mitigate risk and allocate resources.
- Rapidly pinpoint malicious behavior in your ICS/OT network with threat behavior analytics and receive context rich alerts, to aid in faster response times.

With the increase in connectivity and accessibility required to improve operational efficiency, industrial organizations must manage cybersecurity risks to their industrial control systems (ICS) and operational technology (OT). Together, Dragos and Industrial Defender strengthen your organization's defensive capabilities by offering comprehensive ICS/OT asset inventory along with advanced configuration and change management capabilities.

THE CHALLENGE

The shift toward modernization in OT infrastructure underscores the critical role of cybersecurity tailored to these complex environments. Security teams across the electrical utility, oil and gas, and manufacturing industries have the complicated responsibility to manage assets within these critical environments, address and respond to risks and vulnerabilities, and adhere to audit and compliance programs. This complexity makes it difficult for organizations to fully identify, monitor, and manage their OT environments effectively.

THE SOLUTION

The Industrial Defender and Dragos technology integration easily incorporates into an organization's broader security and enterprise ecosystem, also empowering IT/Security teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Ensuring organizations can protect the availability and safety of these systems, while also simplifying compliance requirements.

The Dragos Platform, recognized as the most trusted solution in OT cybersecurity, provides comprehensive asset visibility, vulnerability management, and the industry's most effective threat detection in ICS and OT environments. By analyzing a broad range of data sources, including protocols, network traffic and logs, it rapidly pinpoints threats with reduced false positives. The platform offers in-depth contextual alerts, enriched risk scores, and prioritized guidance to enable teams to effectively manage the full lifecycle of vulnerabilities and respond decisively to security incidents. This approach ensures a high level of preparedness and protection against operational threats, safeguarding critical processes and infrastructure.

The Industrial Defender Platform delivers the OT asset data you need to protect your critical operations. By providing deeper-level asset data, Industrial Defender helps you achieve goals for OT asset management, change and configuration management, vulnerability management, and policy compliance.

Configuration management focuses on maintaining the integrity of all configurable elements of a piece of hardware or software, including capturing a baseline build or settings for any specific asset, detecting new configurations, and managing deployment of new builds or configurations.

By integrating the two technologies, customers now have comprehensive ICS/OT asset coverage via active, agentless, and passive data collection methods for connected assets, plus manual import capabilities for disconnected assets.

HOW IT WORKS

The Industrial Defender Platform and the Dragos Platform integration can be configured within the Dragos Platform. Start by configuring the Dragos Platform using the REST-based API and syslog to transfer information between the two solutions. Industrial Defender integrates network data with endpoint configuration data for a more detailed and comprehensive view of system states.

Once configured, the integration allows the Dragos Platform to automatically synchronize and reconcile assets within the Industrial Defender Platform per the defined frequency interval providing users with an accurate inventory that can be used to serve many different functions.

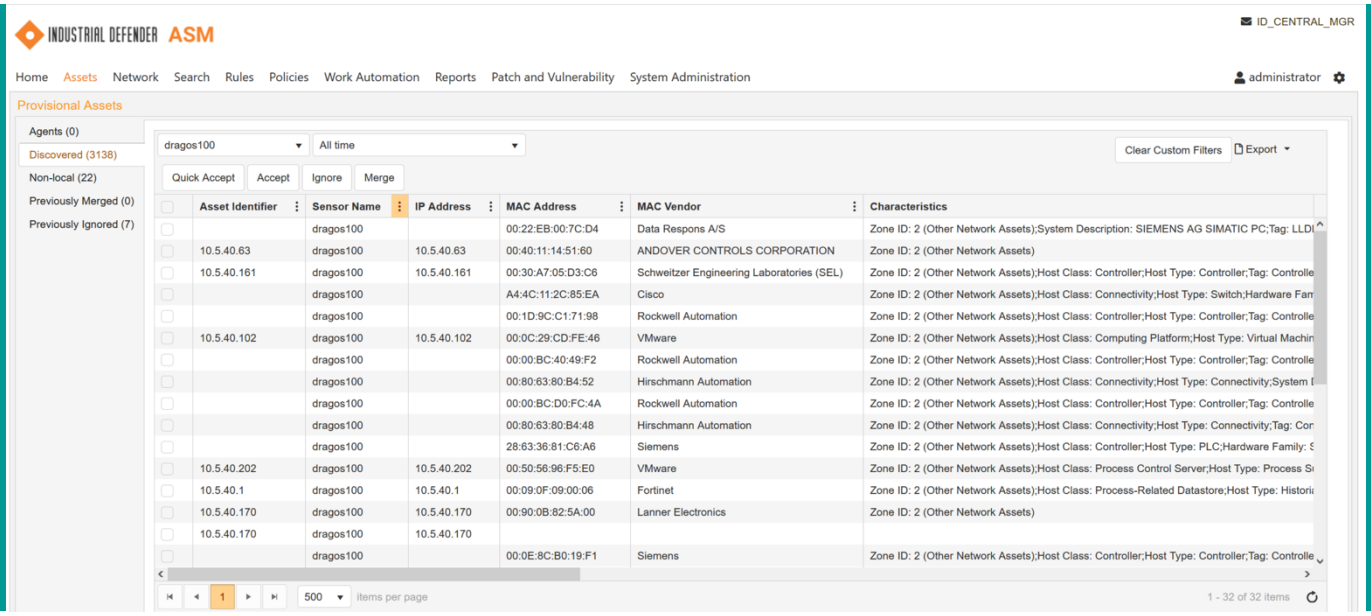


Figure 1. Asset data from Dragos Platform shown in the Industrial Defender ASM dashboard.

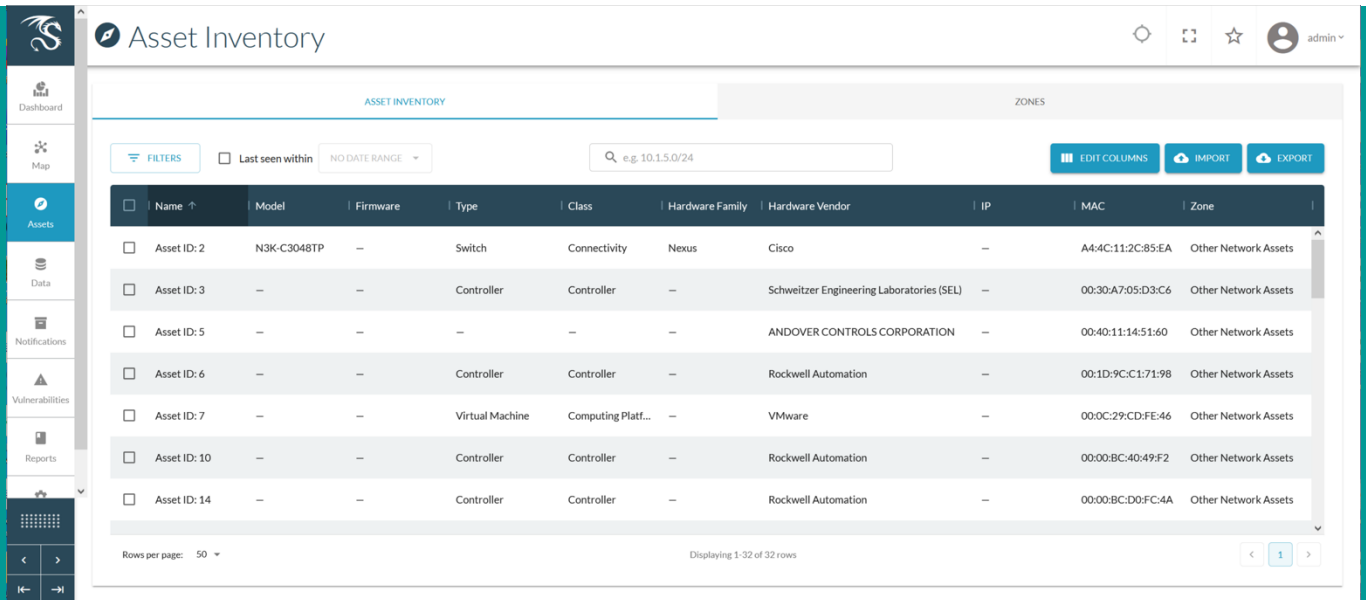
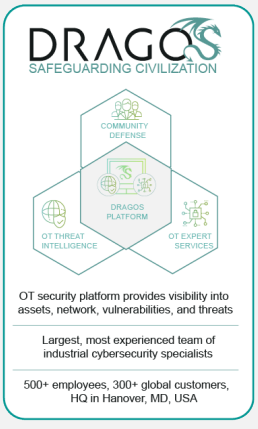


Figure 2. Asset inventory in the Dragos Platform.

ADVANTAGES OF THE INTEGRATED INDUSTRIAL DEFENDER AND DRAGOS SOLUTIONS INCLUDE:

- Gain context rich asset visibility across your OT network, including PLCs, HMIs, SCADA systems, Historians, and other assets.
- Easily create asset baseline configurations that the change detection engine compares with actual asset configuration data including ports and services, users, software, and patches and firewall rules.
- Utilize detailed visibility and insight from both connected and non-connected devices to allow organizations to detect and respond to security and operational risks.
- Easily determine the status of OT infrastructure and automate reporting for relevant regulatory programs and industry standards like NIST CSF, NERC CIP, ISA/IEC 62443, CFATS, ANSI/AWWA G430, GxP, IT-SIG 2.0, and many others.

For more information, please visit http://www.dragos.com/partner/industrial-defender/
or contact us at info@dragos.com



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.