

CYOLO AND DRAGOS PROVIDE OT-NATIVE NETWORK VISIBILITY MONITORING WITH SECURE REMOTE ACCESS



Cyolo and Dragos have partnered to deliver a safe and secure Industrial Control System (ICS)-focused connectivity solution with the Cyolo PRO Secure Remote Access Platform's interoperability with the Dragos Platform, the most effective OT-native cybersecurity monitoring and visibility solution. This collaboration is designed to provide Operational Technology (OT) customers visibility and management of their asset inventory and enhance asset vulnerability detection and remediation capabilities through a seamless secure controlled access platform.

CHALLENGE

The industrial landscape is rapidly changing. While the operation may not be changing, recent technology is helping a legacy OT world to improve business operations and reduce overall mean-time-to-resolution (MTTR). The benefits of digitization are many, but the deployment in ICS and OT environments pose unique risks including:

- Cyber adversaries are increasingly targeting critical infrastructure recognizing the high-impact potential to disrupt these essential services.
- Connecting highly vulnerable end-of-life and legacy platforms to transformative Industry 4.0 environments.
- Legacy applications lacking modern authentication or connectivity methods.
- Complying with increasing regulatory response and reporting requirements for an evolving threat landscape.
- Uncontrolled and unsupervised Third Party Remote Access.

JOINT SOLUTION OVERVIEW

Together the Cyolo PRO and the Dragos Platform architecture deliver unsurpassed visibility and control of critical digital assets through secure identity-based access. Together, both companies will deliver simpler, stronger, and more efficient security controls that lay the foundation for Zero Trust (NIST 800-207) and other regulatory requirements.

Balanced priorities are essential to effective ICS/OT security, as made clear by the SANS Institute whitepaper, "The Five ICS Cybersecurity Critical Controls" to respond and provide mitigation impacting Operational Technology (OT) environments:

Together Dragos and Cyolo deliver a comprehensive ICS/OT security framework based on the five critical controls:

1. **ICS incident response** - which integrates operational insights into incident handling, enhancing system integrity and recovery (Dragos).
2. **Defensible architecture** - ensuring robust visibility, segmentation, and enforcement mechanisms to bridge technological and human aspects of security (Dragos and Cyolo PRO).

3. ICS network visibility monitoring - employing continuous monitoring and protocol-aware tools to detect and address potential vulnerabilities (Dragos).

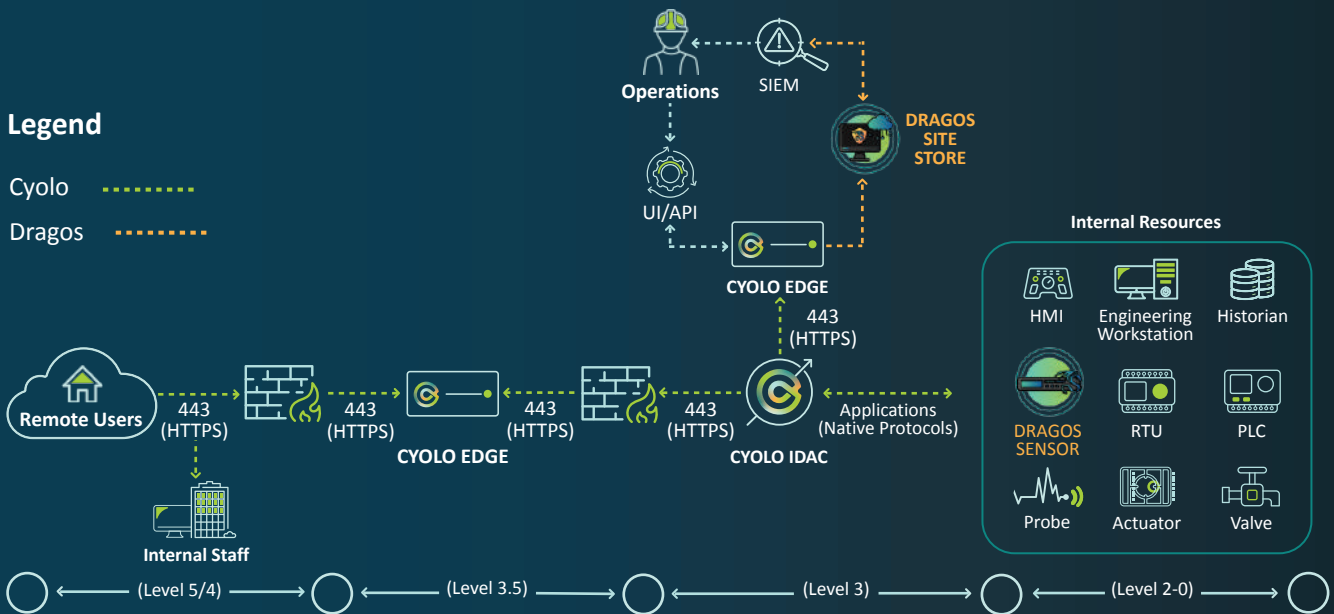
4. Remote Access Security - ensuring safe and secure stringent access control in the face of evolving hybrid work environments (Cyolo PRO).

5. Risk-based vulnerability management - prioritizing and addressing vulnerabilities based

on their potential to pose significant operational risks, thereby ensuring proactive prevention, response, and recovery actions (Dragos and Cyolo PRO).

Additionally, the combined Cyolo PRO and Dragos Platform gives an unparalleled advantage to helping get boots on the ground, in minutes, not hours, reducing the scope and impact to an organization experiencing a cyber event or incident.

UNIFIED INDUSTRIAL CYBERSECURITY CONTROL HOW IT WORKS



The Dragos Platform provides automated asset discovery and monitoring capabilities, delivering asset inventory and visibility across the network. Powered by Dragos OT Cyber Threat Intelligence, the Platform accurately detects threats, providing actionable insights. With a risk-based vulnerability database and risk scoring system, users efficiently prioritize security actions considering operational needs. Expertly crafted OT Response Playbooks streamline investigations in complex operational

environments, leveraging insights from the largest ICS/OT practitioner team to effectively respond to adversaries.

Armed with enriched multi-sourced operational environment information, operations staff can now facilitate auditable remediation or response actions through the Cyolo PRO Platform. Staff can quickly and efficiently take corrective actions for any functions that break user, policy, or application parameters within the environment.

BENEFITS

Unifying the Cyolo PRO Secure Remote Access Platform with the Dragos OT-native network visibility and monitoring offerings gives unparalleled advantages. The Dragos Platform enables organizations with the threat intelligence to keep on top of current threats, and the tools to respond quickly to incidents before they cause significant operational impacts to the safety and security of their people, process, and technologies. The unified platform provides organizations with a wide range of granular controls and managed response capabilities including:

- Defining and managing user roles, application permissions and credentials.
- Controlling application access and resource access at a granular level including geolocation, time, supervision, and auditable recordings.
- Initiating threat mitigation / incident response activities including session intervention or the disabling of user or network access.
- Isolating asset vulnerabilities / zero-day threats indefinitely (or until remediated).
- Comprehensive ICS/OT assets visibility and discovery.
- Operational playbooks that align to the MITRE ICS ATT&CK Framework and Industry 4.0 best-practice guidance.
- Micro-segmentation to prevent lateral movement by enabling or disabling firewall ports and network access.



SUMMARY

Together, Dragos and Cyolo deliver simpler, stronger, and more efficient security controls for critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the world that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

ABOUT CYOLO

Cyolo provides secure remote privileged access for cyber-physical systems (CPS). Our solution enables industrial enterprises to simply connect employees and third-party vendors to critical assets.

Cyolo meets the needs of both security and operational technology (OT) teams with a solution that's adaptable to any environment and deploys without causing disruptions or requiring change management. To learn more, please visit: www.cyolo.io

ABOUT DRAGOS

Dragos has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The Dragos Platform offers the most effective industrial cybersecurity technology, giving customers visibility into their ICS/OT assets, vulnerabilities, threats, and response actions. The strength behind the Dragos Platform comes from our ability to codify Dragos's industry-leading OT threat intelligence, and insights from the Dragos services team, into the software. Our community-focused approach gives you access to the largest array of industrial organizations participating in collective defense, with the broadest visibility available. To learn more, please visit: www.dragos.com

