PARTNER SOLUTION BRIEF

Dragos and Cyolo

OT-Native Network Visibility & Monitoring with Secure Remote Access

HIGHLIGHTS

- Provide comprehensive ICS/OT asset visibility, threat detection, and vulnerability management with investigation playbooks best-practice guidance, with secure controlled access.
- Define and manage user roles, application permissions and credentials.
- Control application access and resource access at a granular level including geolocation, time, supervision, and auditable recordings.
- Deliver a comprehensive ICS/OT security framework based on the Five ICS Cybersecurity Critical Controls

As digital transformation is reshaping industries worldwide, Secure Remote Access (SRA) is now a critical component in modern industrial control systems (ICS) and operational technology (OT). Together, Dragos and Cyolo, strengthen your organization with a coalescence of OT network visibility & monitoring and identity-based secure connectivity solution, to provide comprehensive ICS/OT asset visibility, threat detection, and vulnerability management, allowing users to leverage this data to update access polices.

THE CHALLENGE

The digitalization of ICS, along with the global pandemic, has necessitated increased remote connectivity, providing significant business and operational value. However, this shift has also introduced substantial risks, including the connection of existing infrastructure that runs highly vulnerable end-of-life operating systems, legacy applications without support for modern authentication or connectivity methods, strict regulations, and third-party remote access in an evolving threat landscape.

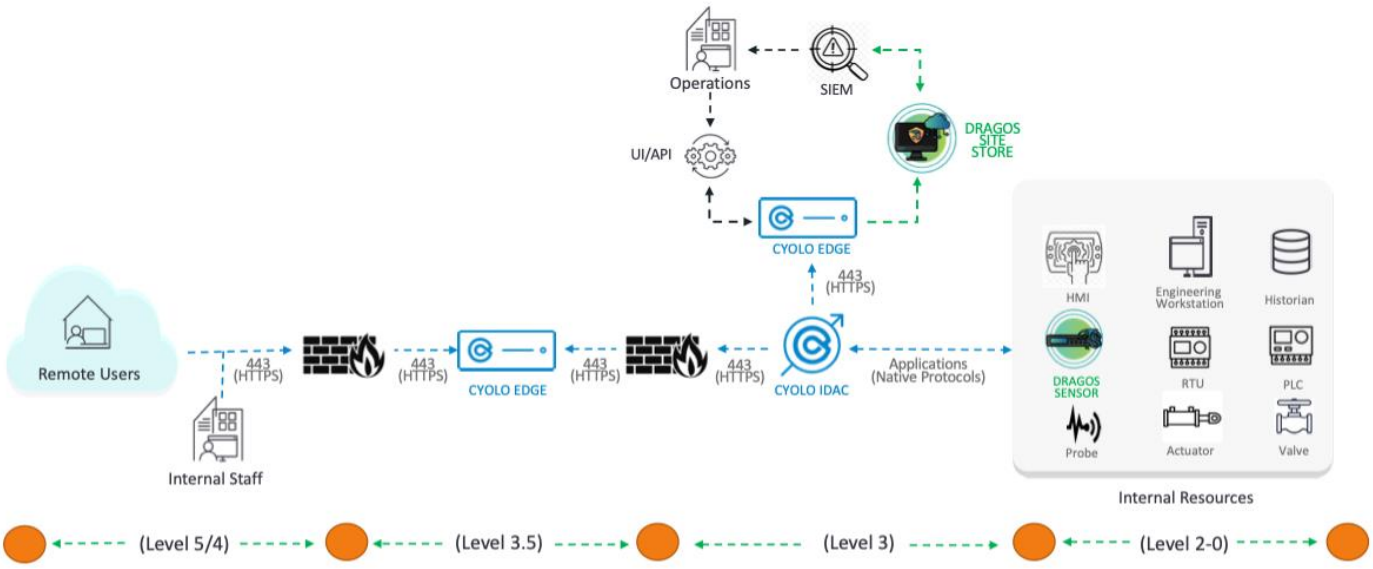
This increased connectivity has attracted adversaries who target remote access methods directly, often IT network vendors, maintenance personnel, integrators, and equipment manufacturers to pivot into the OT networks.

Secure remote access, highlighted by SANS's **The Five ICS Cybersecurity Critical Controls**, is a necessary control in modern industrial cybersecurity. Multi-Factor Authentication (MFA), a secure remote access control, can be safely applied to most ICS environments, significantly reducing adversary attack paths. Putting a focus on externally accessible connections, with priority given to remote connections traversing shared private networks, public networks, and the internet. Industrial organizations are now trying to solve for the risk around increased remote connectivity, while improving their OT cybersecurity, which typically requires more than one best-of-breed technology.

THE SOLUTION

Dragos and Cyolo have partnered to deliver a combination of secure remote access and OT-native network visibility and monitoring that provides industrial organizations a robust and interoperable solution to protect their critical infrastructure against cyber threats.

Bringing the Cyolo PRO platform alongside the Dragos OT-native network visibility and monitoring offerings gives unparalleled advantages. The **Dragos Platform** enables organizations to scale protection, the threat intelligence to keep on top of current threats, and the tools to respond quickly to incidents. With Cyolo's robust role-based access, application, and policy control, in the future the Dragos Platform will be able to manage Cyolo's Identity-based parameters (users, applications, resources, policy) in accordance with SOC / IR policies and guidelines.



The combined power of the Dragos Platform and Cyolo Pro platform provides organizations with transformative Industry 4.0 and MITRE ICS ATT&CK Framework capabilities as well as aligning with the Five ICS Cybersecurity Critical Controls to help implement ICS Incident Response, Defensible Architecture, ICS Network Visibility Monitoring, Remote Access Security, and Risk-based Vulnerability Management. Allowing teams to investigate and respond to threats before they cause significant operational impacts to the safety and security of their people, process, and technologies.

HOW IT WORKS

The Dragos Platform's interoperability with Cyolo's robust role-based access, application, and policy control, can handle Cyolo's Identity-Based parameters (users, applications, resources, policy) in line with Security Operations Center (SOC) and Incident Response (IR) policies and guidelines.

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.

The Operations Staff, armed with enriched multi-sourced operational environment information, can now facilitate auditable remediation or response actions through the Cyolo PRO Platform. The Cyolo PRO Platform can quickly and efficiently take corrective actions for any functions that break user, policy, or application parameters within the environment. These actions include session intervention, lateral movement, improper command execution, malware mitigation, device-based threats and the enabling or disabling of firewall ports and network access.

ADVANTAGES OF THE CYOLO AND DRAGOS PARTNERSHIP INCLUDE:

- Gain context rich asset visibility across your ICS/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 ICS/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 dragos.com/partner/cyolo/
or contact us at info@dragos.com