Cyolo

At a Glance

Achieving Safe and Secure Access for the Oil & Gas Industry

Cyolo PRO for Oil & Gas

The oil and gas (O&G) sector provides vital resources that enable countless other industries to operate and allow society as we know it to function. Unfortunately, an increasing number of adversaries also recognize the value of the O&G sector. These threat actors are accelerating their attacks on industrial control systems (ICS) and other operational technology (OT) in order to disrupt operations, commit espionage, and generally wreak havoc.

At the same time, remote work, automation, progress toward Industry 4.0, and rising connectivity between operational technology (OT) and information technology (IT) are creating new opportunities as well as new vulnerabilities for O&G companies.

Remote connectivity, as one example, reduces costs, improves operational agility, and lowers safety risks by enabling maintenance on offshore drilling rigs or distant oil fields to be conducted without traveling to these far-off locations. However, remote access creates its own security and safety risks.

If proper access, connectivity, and supervisory controls are not in place, a security incident could potentially occur at any point across the three major stages of O&G operations: upstream, midstream, or downstream. Attacks could be the result of espionage, cyber-terrorism, ransomware gangs seeking a quick, high-value payout, or critical cybersecurity vulnerabilities affecting the aging infrastructure and legacy systems that characterize OT environments.

And the stakes simply could not be higher when it comes to protecting O&G facilities and the critical infrastructure within them. A cyberattack against these targets could cause immense damage, including financial loss and economic disruption, threats to human safety and the environment, and even the destabilization of nation states.

Cyolo PRO (Privileged Remote Operations) is an advanced Secure Remote Access (SRA) solution tailored for OT, empowering O&G organizations to safely connect remote workers, third-party vendors, and privileged employees to even the most sensitive assets and environments.

72%

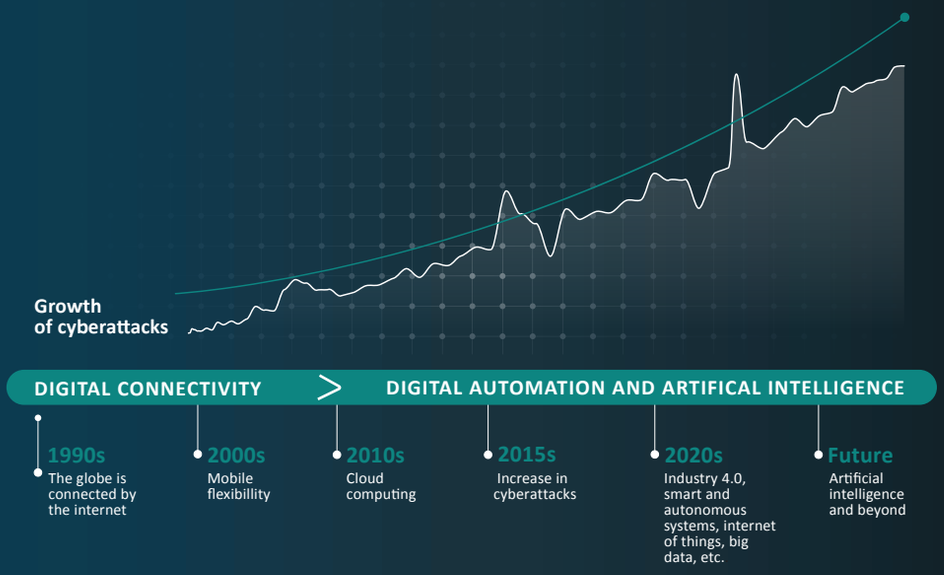
of oil & gas organizations are currently pursuing some level of IT/OT convergence.

Ponemon Institute, 2024

Oil & Gas Security Risks

The O&G industry is deeply dependent on systems that are becoming more digitally connected. Connectivity lowers costs, increases efficiency, and decarbonizes the sector, but it also introduces new risks.

Robust cybersecurity will enable O&G companies to fully enjoy the benefits of digital transformation and IT/OT convergence. But there is work to do, as 69% of O&G professionals worry their organization is more vulnerable to cyberattacks now than in the past.



Source: World Economic Forum

Oil & Gas Cybersecurity: Statistics and Risks

21% of customer engagements in the O&G sector had findings of poor remote access security.

47% of customer engagements in the O&G sector had inadequate asset visibility and ICS network monitoring.

41% of customer engagements in the O&G sector identified inadequate or lacking OT-specific incident response plans in 2023.

26% of customer engagements in O&G sector had findings related to defensible architecture in 2023.

Source: Dragos

Case Study: How a Leading Energy Provider Ensures Secure Access to OT and SCADA Systems

The Need: Remotely connect global partners and third-party suppliers to critical systems

Top Challenges

- Required a single solution to enable secure access for global support teams, third-party suppliers, and customers
- Needed to meet strict internal and external security regulations
- Sought to reduce friction and improve user experience for frustrated employees and support teams

Business Outcomes

- Fastest deployment in company history
- Fast, secure, and seamless access for all users to IT, OT, and SCADA systems
- Months of work reduced to hours
- Hundreds of thosands of dollars saved, plus significantly reduced travel costs
- Improved productivity and user satisfaction

"No solution gives me as much conrol and security as Cyolo. It's everything I need in one solution."

Shlomo Kamilyan
CIO, Rapac Energy

Multiple Needs, 3 Security Layers , 1 Unified Solution

PRIVILEGED ACCESS

- Safeguard Credentials → Vault
- Establish Audit Trail → Session Audit & Recording
- Track Privileged Activities → Supervised Access

IDENTITY MODERNIZATION

- Protect the Last Mile → Zero Trust for Devices
- OpEx Reduction → End User Self-operation Tools
- Device Security → Internal IDP/MFA/SSO for Legacy Systems

ZERO TRUST SECURITY

- Mitigate Asset Vulnerabilities → Application Security
- Mitigate Risk of Phishing Attacks & Ransomware → Zero Trust for Users
- Implement Robust Access Controls → Access & Action Management

THE OUTCOMES

- Advanced Security
- Better User Experience
- Oil Rig and Refinery Safety
- Reduction of Compliance Headaches
- Increased Production Reduced Cost & Complexity
- Enterprise-ready Deployment

Managing Access and Risk in Oil and Gas Companies

51% **Failure to prioritize OT security. Just 51%** of O&G companies identify securing access to OT environments as a high priority.

74% **No accurate asset inventory. 74%** of O&G companies do not maintain an accurate, up-to-date inventory of the industrial assets in their OT environments.

47% **Underprotected. 47%** of O&G companies lack confidence that they're effectively protecting their OT environments.

60% **Insecure OEM Vendor and Third-Party Access. 60%** of O&G companies grant OT systems access to more than 50 different vendors, and 25% give such access to more than 100 vendors.

Source: Ponemon Institute, 2024

Key Remote Privileged Access Use Cases

Facilitate Third-Party Remote Access

Safely connect third parties to your OT environments for enhanced productivity.

Provide OEM Access For Fast, Secure Support

Ensure rapid, secure, and safe support and maintenance for your factory floor and OT environments.

Manage Critical and Risky Access

Secure all access points to your mission-critical assets, whether on-prem or remote.

Achieve Regulatory Compliance

Implement segmentation, supervision and other requirements of industry and regional compliance mandates.

5 Critical Controls

For World-class OT Cybersecurity

- **ICS Incident Response**
- **Defensible Architecture**
- **ICS Network Visibility Monitoring**
- **Remote Access Security**
- **Risk-based Vulnerability Management**

Source: SANS Institute

The Cyolo Ecosystem Addresses All 5 Critical Controls for Oil & Gas Cybersecurity

Case Study: The Cyolo/Dragos Partnership

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

ICS Incident Response - which integrates operational insights into incident handling, enhancing system integrity and recovery (Dragos)

Defensible Architecture - ensuring robust visibility, segmentation, and enforcement mechanisms to bridge technological and human aspects of security (Dragos and Cyolo PRO)

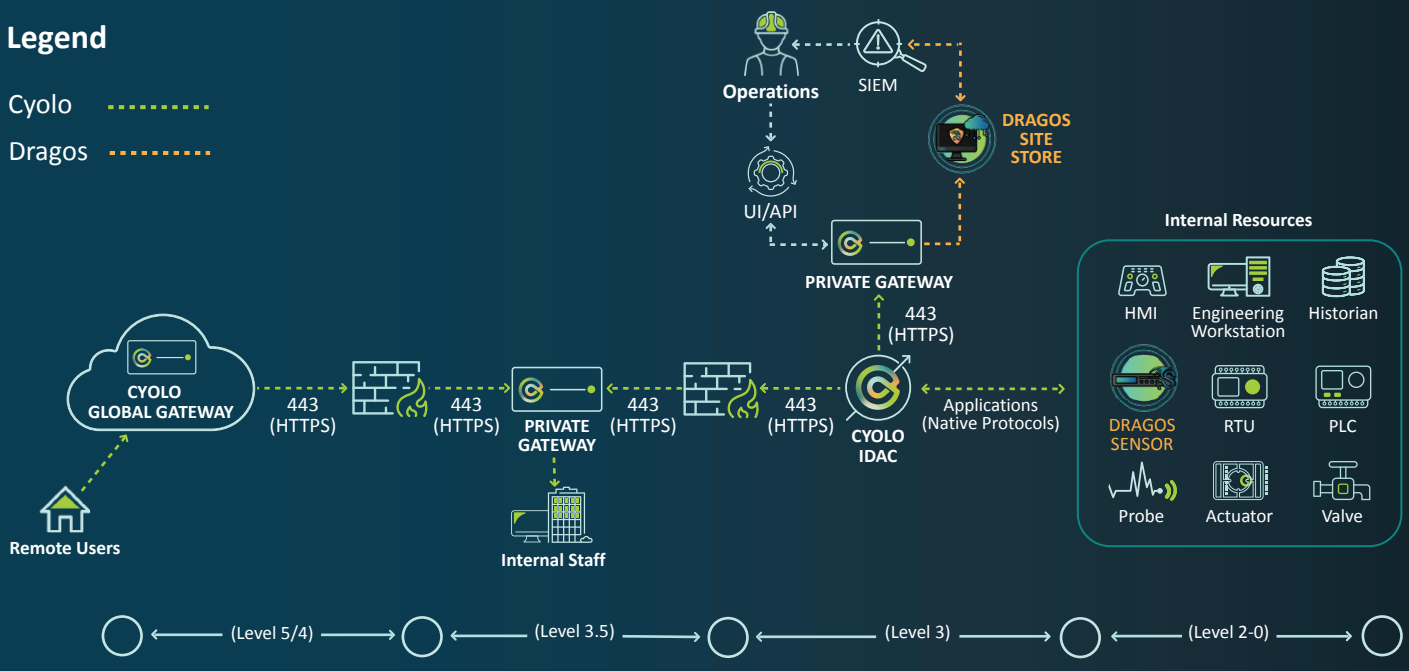
ICS Network Visibility Monitoring - employing continuous monitoring and protocol-aware tools to detect and address potential vulnerabilities (Dragos)

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

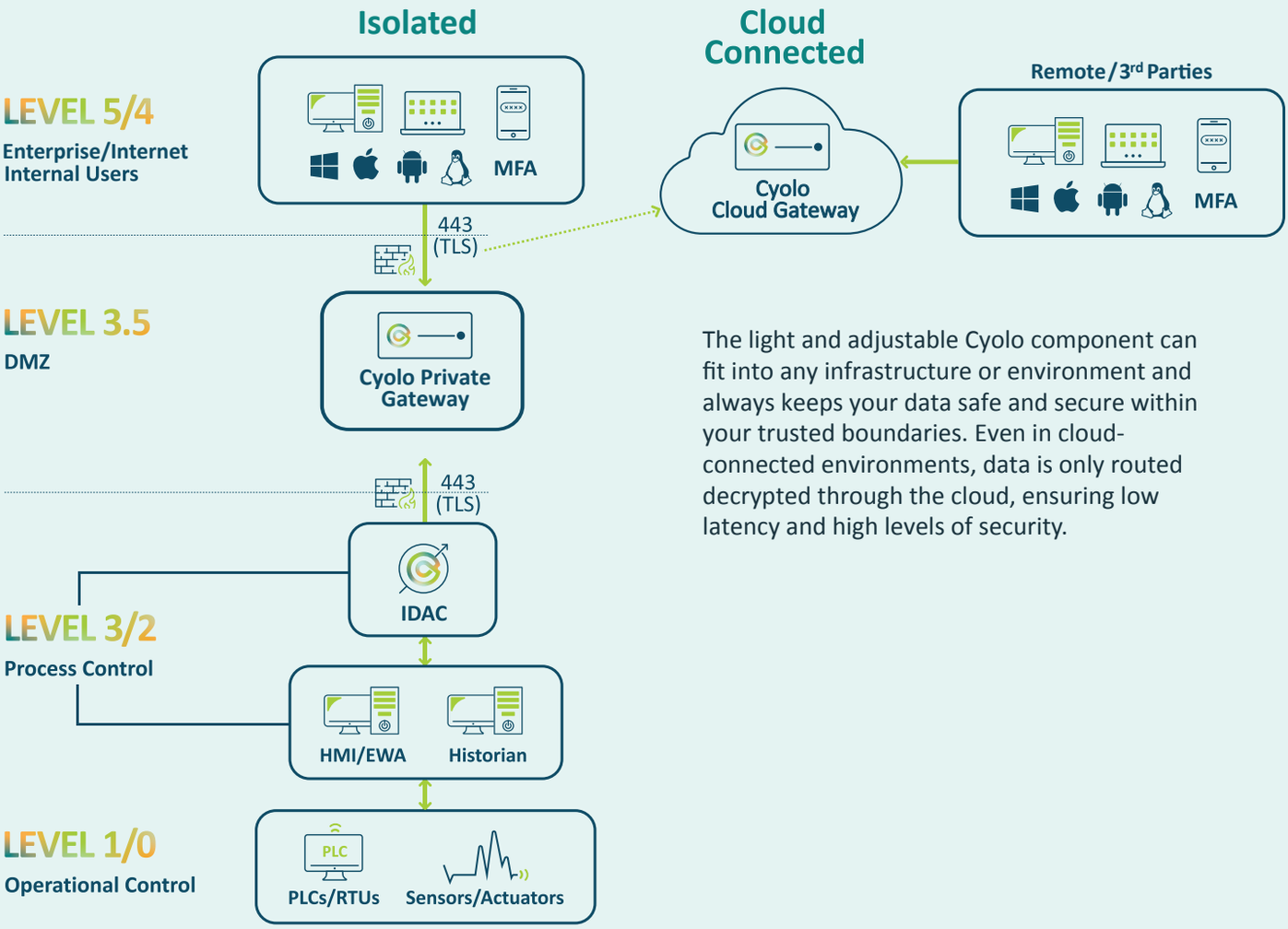
Risk-based Vulnerability Management - prioritizing and addressing vulnerabilities based on their potential to pose significant operational risks, thereby ensuring proactive prevention, response, and recovery actions (Dragos and Cyolo PRO)

UNIFIED INDUSTRIAL CYBERSECURITY CONTROL

HOW IT WORKS



Cyolo PRO's Unique Architecture Enables a Flexible Solution to Fit Any Environment



The light and adjustable Cyolo component can fit into any infrastructure or environment and always keeps your data safe and secure within your trusted boundaries. Even in cloud-connected environments, data is only routed decrypted through the cloud, ensuring low latency and high levels of security.

Cyolo PRO Benefits

Secure

- Keep your data inside your trusted boundaries
- Granular identity-based controls & supervision
- Full activity/audit trails

Flexible

- Deploy on-prem, on-cloud & hybrid—simultaneously
- Extend identity authentication and security to legacy applications
- Centralized governance & site-based administration

Fast and Easy

- Agentless deployment
- Consolidated access controls with modularity
- Low-latency/High-availability

Cyolo is a leading cybersecurity innovator dedicated to providing cutting-edge access solutions. With a focus on security, operational agility, and user experience, Cyolo is fostering a transition from merely enabling access to empowering operations, productivity, and compliance.

www.cyolo.io

Cyolo