

# Achieving Safe & Secure Access for the Mining Industry

## Cyolo PRO for Mining 4.0

The mining industry is undergoing a transformation. As Industry 4.0 or, more precisely, "Mining 4.0," integrates modern technologies like automation, robotics, the Industrial Internet of Things (IIoT), and advanced data analytics into traditional processes, both new opportunities and new risks are emerging.

More specifically, rising connectivity between operational technology (OT) and information technology (IT) is reshaping mining operations, driving greater efficiency, improving resource utilization, and reducing safety risks. However, this same connectivity expands the attack surface that cybercriminals can use to wreak havoc on mining sites, mineral processing plants, and all related facilities. Each new connected device — from programmable logic controllers (PLCs) to autonomous vehicles — represents a potential entry point for malware, ransomware or other threat vectors. And the sector's growing reliance on cloud and automation technologies (including for those used in efforts to achieve decarbonization targets) only increases its vulnerability.

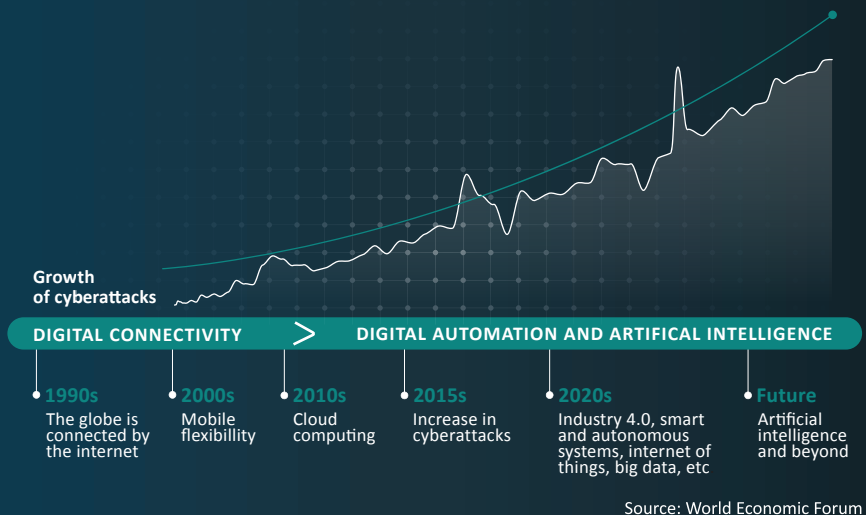
According to Ernst & Young's 2022 Global Information Security survey, 54% of mining and metals companies have suffered significant cyberattacks, and 71% saw an increase in disruptive attacks during the previous year.

**Against this backdrop of threats, it is crucial for mining companies to implement a proactive cybersecurity strategy that starts with protecting remote access to their most critical systems and assets.** Monitoring and controlling access will help organizations to maintain profitability and competitive advantage, prevent operational disruptions, keep equipment and workers safe above and below ground, and comply with emerging regulations.

**Cyolo PRO (Privileged Remote Operations) is an advanced Secure Remote Access (SRA) solution tailored for operational technology (OT). Cyolo PRO empowers mining companies to safely connect remote workers, third-party vendors, and privileged employees to even the most sensitive assets and environments.**

## Mining 4.0 Security Risks

As with every revolution, Mining 4.0 brings new challenges. Increased connectivity (and in particular, remote connectivity) heightens the risk that key components of an organization's OT network could come under cyberattack, potentially leading to downtime, financial loss, and safety hazards. To mitigate such risk, cybersecurity must become an essential part of industrial control systems.



## State of Cybersecurity in the Mining Industry: Key Statistics

- 74%** of mining and metals executives say integrating technology is a key cybersecurity challenge, compared with 37% for all sectors.
- 61%** say "too many potential attack surfaces" is a key challenge, compared with 52% for all sectors.
- 48%** are very concerned about technology infrastructure risks. 43% are very concerned about intellectual property protection risks, and 39% are very concerned about financial risks.
- 70%** are outsourcing more functions and capabilities to third-party specialists to help solve the skills gap. Interestingly, the same percentage are very concerned about supply chain risks.

Source: EY, 2024

# Case Study: Leading Chemicals Provider

**The Need:** Provide secure remote access to OT and IT networks for employees, vendors, and contractors



## Top Challenges

- Need a single solution to provide access to multiple types of environments (OT & IT, offline & online)
- Legacy OT systems did not support multi-factor authentication (MFA)
- With workers underground and potentially at-risk 24/7/365, safety is key and downtime is not an option



## Business Outcomes

- Safe, secure, and tightly controlled remote access for badged employees and third parties into critical environments
- No infrastructure changes needed in order to add modern security and access controls to legacy systems
- Ability to monitor and record sessions, improving post-connection visibility and oversight

"Tata Chemicals has benefited a great deal from Cyolo's platform. We're able to more easily provide remote access to systems to both to internal users and external users. The management overhead of all of these remote access connections has been greatly reduced."

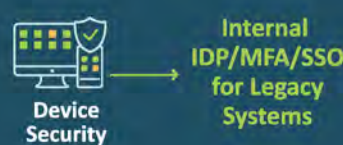
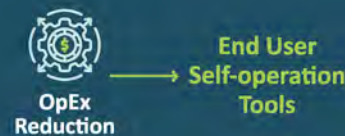
- Senior Systems Administrator, Tata Chemicals

## Multiple Needs, 3 Security Layers , 1 Unified Solution

### PRIVILEGED ACCESS



### IDENTITY MODERNIZATION



### ZERO TRUST SECURITY



## THE OUTCOMES



Advanced Security



Better User Experience



Operational Safety



Reduction of Compliance Headaches



Increased Production  
Reduced Cost & Complexity



Enterprise-ready  
Deployment



# Managing Access and Risks in Connected OT Environments

- 45%** of security professionals believe their organization is not effectively mitigating risks and security threats to the OT environment.
- 73%** of industrial organizations do not maintain an accurate, up-to-date inventory of the assets in their OT environment.
- 60%** of industrial organizations grant OT systems access to more than 50 different vendors, and 25% give such access to more than 100 vendors.
- 72%** of industrial organizations are pursuing some level of IT/OT convergence, but just 33% have policies, tools, governance and reporting in place to control and monitor connectivity between IT and OT systems.

Source: Ponemon Institute, 2024

## Key Remote Privileged Access Use Cases

### Facilitate Third-Party Remote Access

Safely connect third parties to OT environments for enhanced productivity without VPNs or jump boxes.

### Provide OEM Access For Fast, Secure Support

Ensure rapid, secure, and safe support and maintenance of diagnostics for OT systems.

### Manage Critical and Risky Access

Secure, monitor, and control all connections to 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 SANS Critical Cybersecurity Controls

### 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)

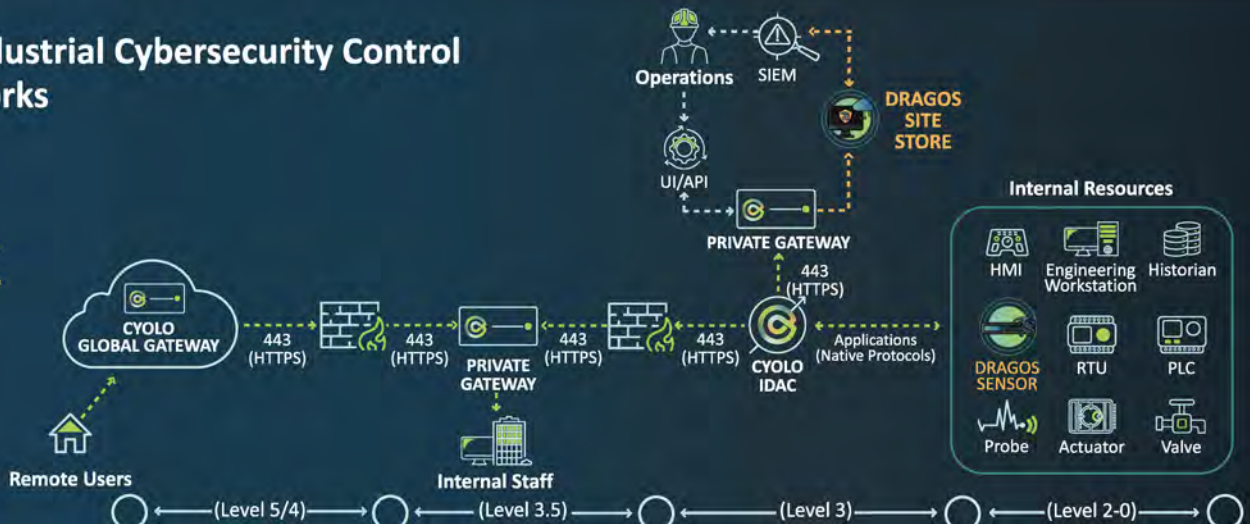
**Remote Access Security** - ensuring safe and secure stringent access control in the face of evolving hybrid work environments (Cyolo PRO).

**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).

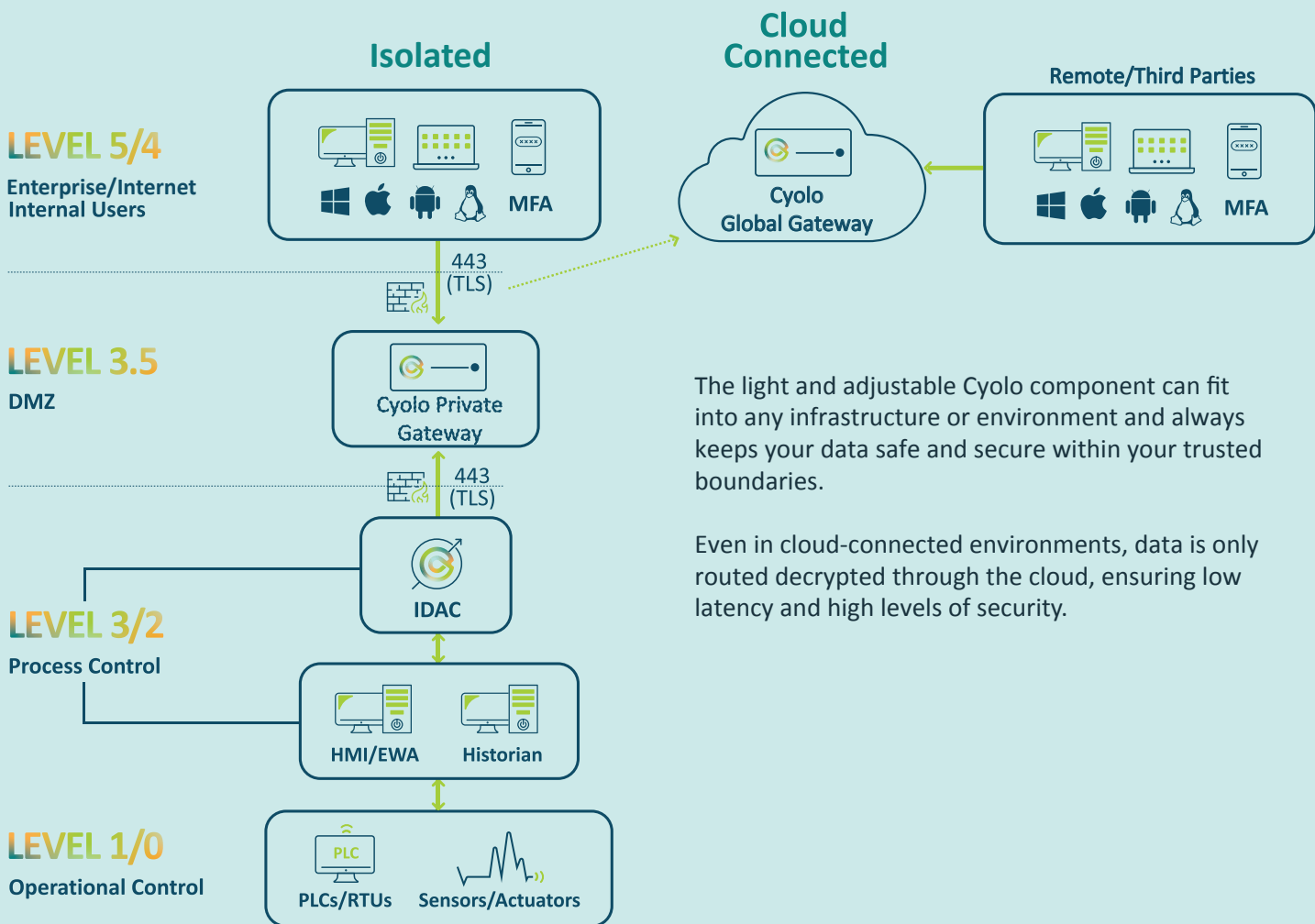
## Unified Industrial Cybersecurity Control How IT Works

### Legend

- Cyolo
- Dragos



# Cyolo PRO's Decentralized Architecture Enables Maximum Adaptability



## 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](http://www.cyolo.io)

