Cyolo

At a Glance

Achieving Safe and Secure Remote 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 intotraditional 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, thissame 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.

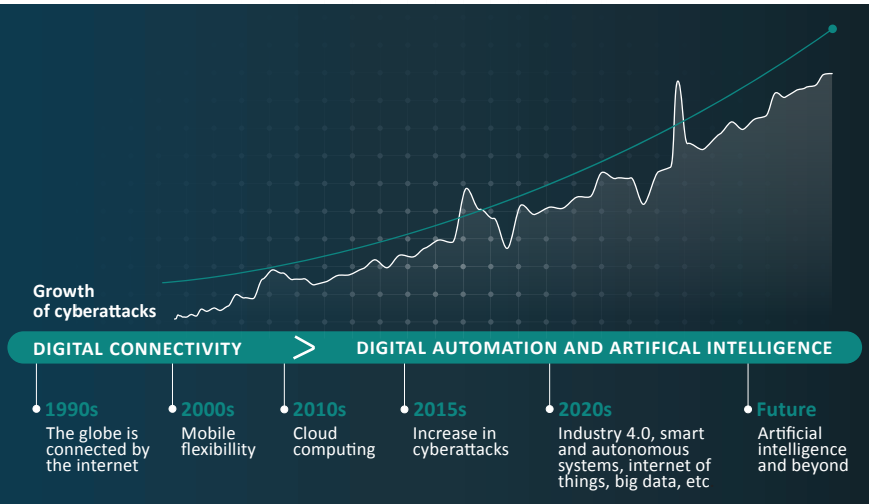
According to Ernst & Young’s 2022 Global Information Security survey, 54% of mining and metals companies have suffered significant cyberattacks, and 71% saw an increase in disruptive attacks during the previous year.

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.



Source: World Economic Forum

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 percentrage are very concerned about supply chain risks.

Source: EY, 2024

Case Study: Leading Chemicals Producer

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

Top Challenges

- Complex login processes on both the user side (7 logins for an RDP!) and admin side (excessive ticketing)
- Needed secure file transfer within the OT environment
- Needed to allow emergency fix access for an OEM vendor

Business Outcomes

- Simple, secure, and agentless remote access for employees, third party contractors, and OEM vendors
- File scanning (ICAP) integration within the policy
- No need to change existing network topology
- Fast and secure remote OEM support
- Under 90 days to deploy

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

- Safeguard Credentials → Vault
- Establish Audit Trail → Session Audit & Recording
- Track Privileged Activities → Intelligent 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
- Operational Safety
- Increased Production
  Reduced Cost & Complexity
- Better User Experience
- Reduction of
  Compliance Headaches
- 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 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 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)

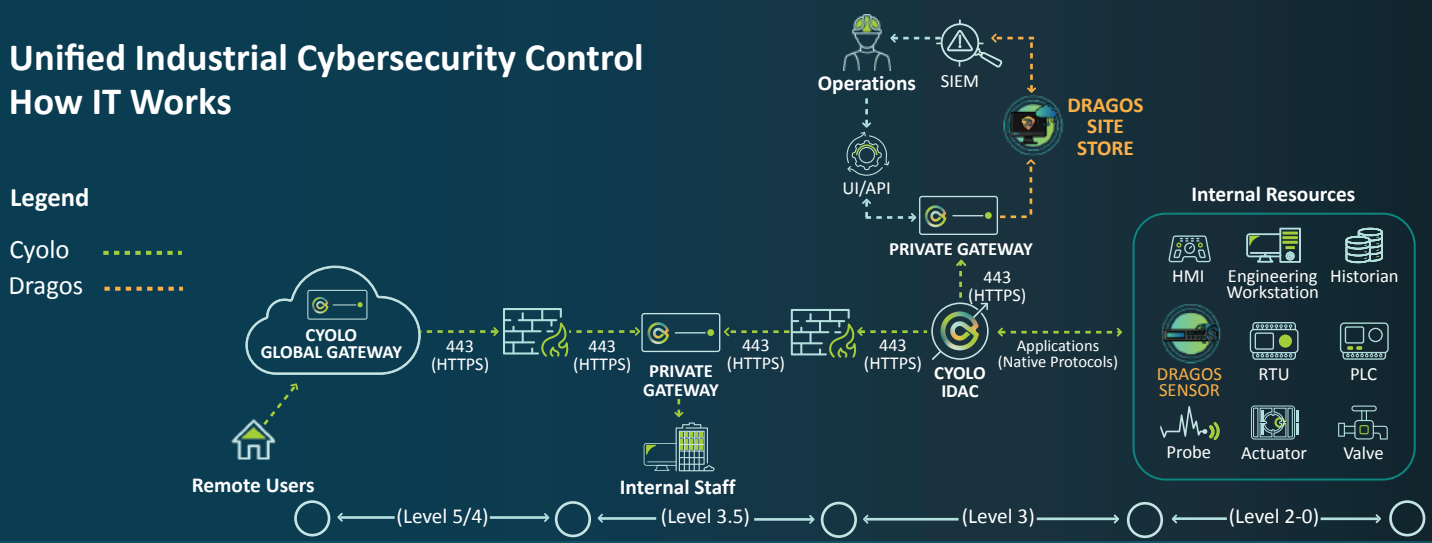
Defensible Architecture - ensuring robust visibility, segmentation, and enforcement mechanisms to bridge technological and human aspects of security (Dragos and Cyolo PRO)

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

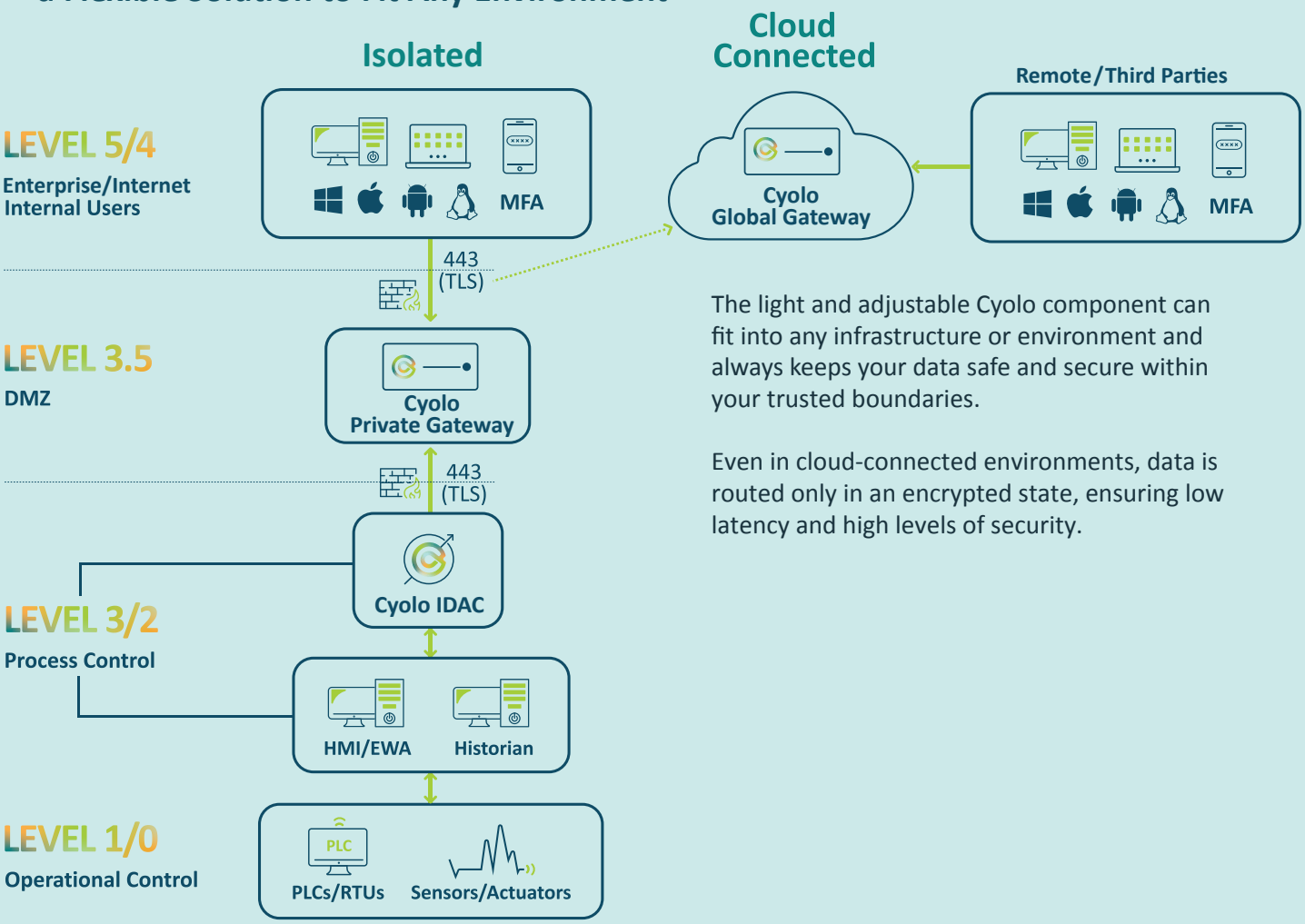
Remote Access Security - ensuring safe and secure stringent access control in the face of evolving hybrid work environments (Cyolo PRO).

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



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 routed only in an encrypted state, 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
- Intelligent supervision eases operational burden

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. Learn more at **cyolo.io**.

Cyolo