Cyolo

At a Glance

Achieving Safe & Secure Access for the Automotive Industy

Cyolo PRO for Automotive Manufacturing

The advent of Industry 4.0 has transformed the automotive industry by integrating innovative technologies like automation, artificial intelligence (AI), manufacturing execution systems (MES), and advanced data analytics into more traditional industrial systems and processes. Technologies that boost connectivity and efficiency are generating substantial ROI for automotive manufacturers,[1] but they also heighten cybersecurity risks and expose organizations to new safety and security threats.

As smart factories grow more dependent on interconnected systems and devices, the attack surface for potential cyberthreats continues to expand. According to 2022 research from Upstream Automotive, the automotive industry experienced a staggering 225% increase in cyberattacks over the previous three years.

If proper access, connectivity, and supervisory controls are not in place, cyberattacks targeting the automotive industry can exploit a variety of entry points, including factory machines, auto dealers, finance companies, and original equipment manufacturers (OEMs) and parts manufacturers throughout the supply chain. And as vehicles themselves come to rely increasingly on software and digital interfaces, they may also serve as a target in their own right. Protecting vehicles and the systems used to build and distribute them is crucial to ensuring the physical safety of workers, drivers, and passengers as well as the operational integrity of the broader transportation infrastructure.

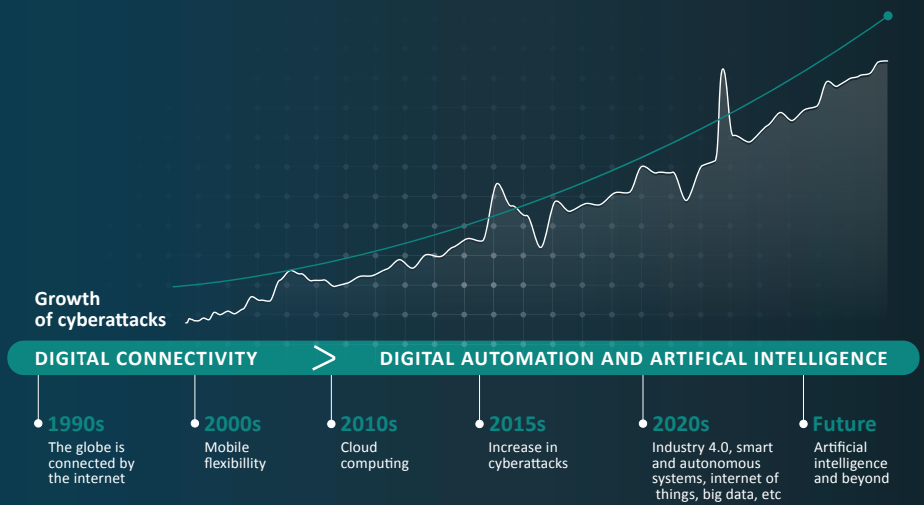
Cyolo PRO (Privileged Remote Operations) is an advanced Secure Remote Access (SRA) solution built to meet the the distinctive needs of operational technology (OT) and industrial control systems). **Cyolo PRO empowers organizations across the automotive industry to safely connect remote workers, third-party vendorsand OEMs, and privileged employees to even the most sensitive assets and environments.**

97%

of automotive manufacturers and their suppliers are either using or evaluating smart manufacturing technology.[1]

Smart Factory Security Risks

As with every great revolution, Industry 4.0 brings new challenges. Increased connectivity heightens the risk that key components of a manufacturer'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

Automotive Cybersecurity: Statistics and Risks

#1 Automotive manufacturers ranked cybersecurity risk as their top external obstacle in 2024 – up from #9 the previous year.[1]

295 cyber incidents targeting the automotive and smart mobility industries were disclosed to the media in 2023.[2]

64% of attacks against the automotive and smart mobility industries in 2023 were conducted for personal gain, financial gain, or for malicious purposes.[2]

36% of automotive manufacturers plan to invest in a zero trust cybersecurity architecture in 2024.[1]

[1] Rockwell Automation, 2024
[2] Upstream Security, 2024

Key Remote Privileged Access Use Cases

Facilitate Third-Party Remote Access

Safely connect third-party vendors to OT environments for enhanced productivity.

Provide OEM Access For Fast, Secure Support

Ensure rapid, secure, and safe support and maintenance of diagnostics (M&D) 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.

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

Case Study: Top Global Manufacturer

100 Global sites

2000 Remote maintenance and support engineers

The Need: Simplify secure access for third parties to the factory floor

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

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)

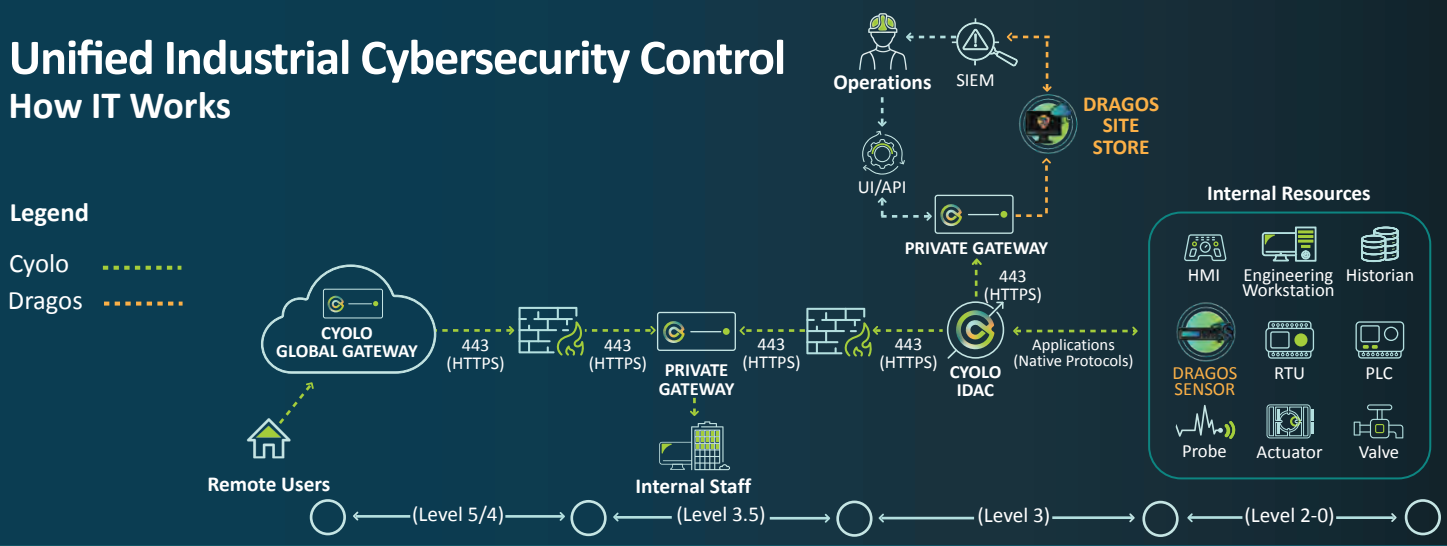
Defensible Architecture - ensuring robust visibility, segmentation, and enforcement mechanisms to bridge technological and human aspects of security (Dragos and Cyolo PRO)

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

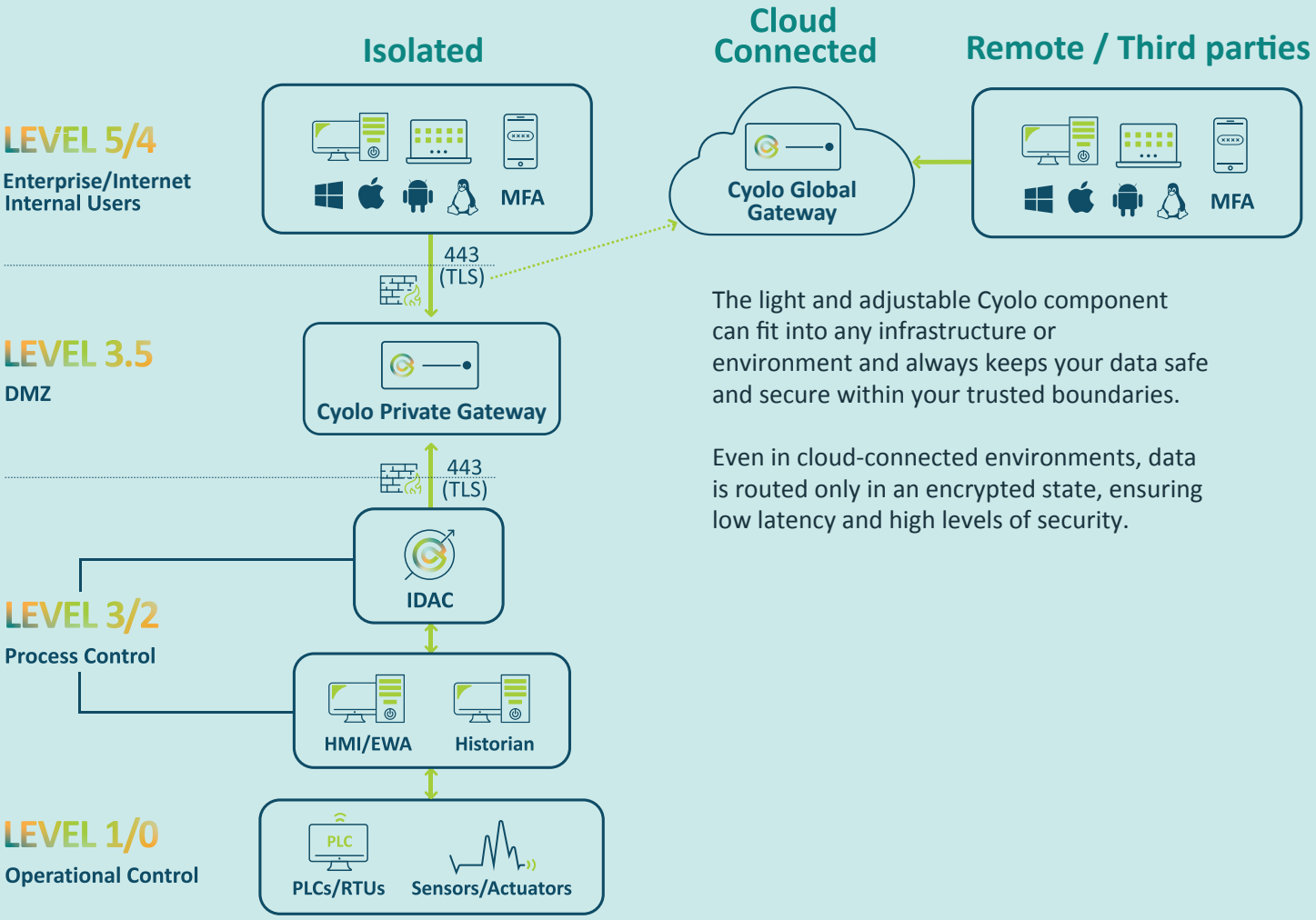
Remote Access Security - ensuring safe and secure stringent access control in the face of evolving hybrid work environments (Cyolo PRO).

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