Cyolo

At a Glance

Safe and Secure Manufacturing for the Food & Beverage Industry

Cyolo PRO for Smart Manufacturing

The food and beverage industry is one of the largest and most crucial manufacturing sectors and plays a key role in the world economy as well as the wider global culture. The combined food and bev sectors of the United States and the European Union (EU) generate over $3 trillion in annual sales. The US alone employs 1.5 million workers across 22,407 food production facilities,[1] and food and bev is the biggest manufacturing employer in half of EU member states.[2]

The advent of Industry 4.0 has revolutionized manufacturing operations for food and bev by integrating cutting-edge technologies such as automation, Internet of Things (IoT), and data analytics into traditional industrial processes. However, increased connectivity between operational technology (OT) and information technology (IT) has significantly heightened cybersecurity risks and led to new vulnerabilities.

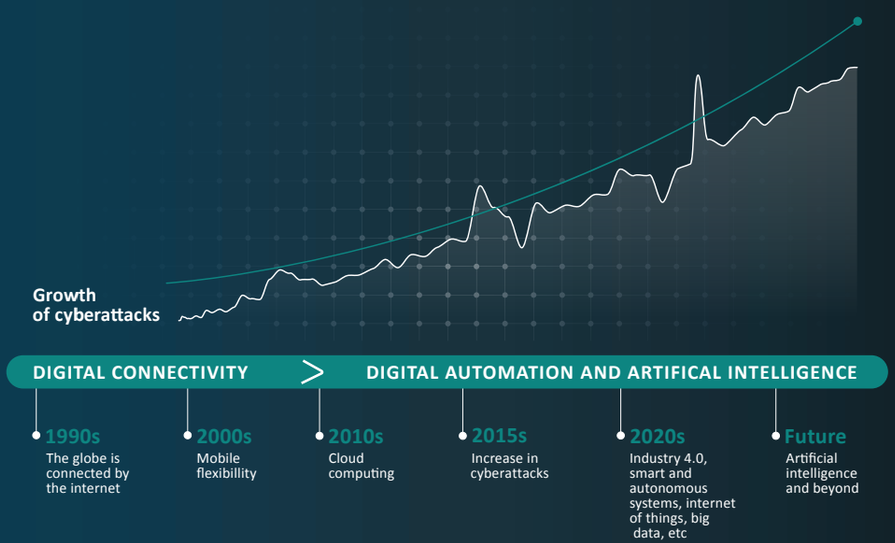
With interconnected systems and devices forming the backbone of smart factories, the attack surface for cyberthreats has expanded exponentially. Greater connectivity and data visibility within the manufacturing ecosystem make it a prime target for cyberattacks, with the sector experiencing the highest number of attacks globally for three consecutive years, comprising 25.7% of all attacks.

Cyolo PRO (Privileged Remote Operations) is a modernized Secure Remote Access (SRA) solution built to empower food and bev organizations to safely connect remote workers, third-party vendors, and privileged employees to even the most sensitive assets and environments.

[1] IndustrySelect, 2023
[2] FoodDrinkEurope, 2023

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

Manufacturing Cybersecurity: Statistics and Risks

60% **Rising Cybersecurity Incidents:** Over 60% of manufacturing companies have experienced cyberattacks, reflecting an escalating risk environment.

$1M **Financial Ramifications:** The average cost of a cyber breach in this sector is around $1 million, signifying substantial financial risks.

30% **IoT Expansion and Risks:** IoT integration exposes new risks, leading to 30% increase in security incidents.

70% **Human Error:** Internal vulnerabilities, primarily due to human error, account for 70% of breaches in manufacturing, and underscore the importance the comprehensive cybersecurity training.

Source: DataGuard, 2024

Case Study: Global Top 3 Food and Beverage 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

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

Better User Experience

Production Floor Safety

Reduction of Compliance Headaches

Increased Production
Reduced Cost & Complexity

Enterprise-ready Deployment

Managing Access and Risk in Connected Manufacturing Environments

43% **Underprotected. 43%** of manufacturing organizations are not effectively protecting their OT environments.

77% **No accurate asset inventory. 77%** of manufacturers do not maintain an accurate, up-to-date inventory of the industrial assets in their OT environments.

57% **Insecure OEM Vendor and Third-Party Access. 57%** of manufacturers grant OT systems access to more than 50 different vendors, and 26% give such access to more than 100 vendors.

50% **Non-compliant.** Shockingly, only **50%** of firms comply with standard cybersecurity protocols, indicating a significant gap in security implementation.

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 Manufacturing

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

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

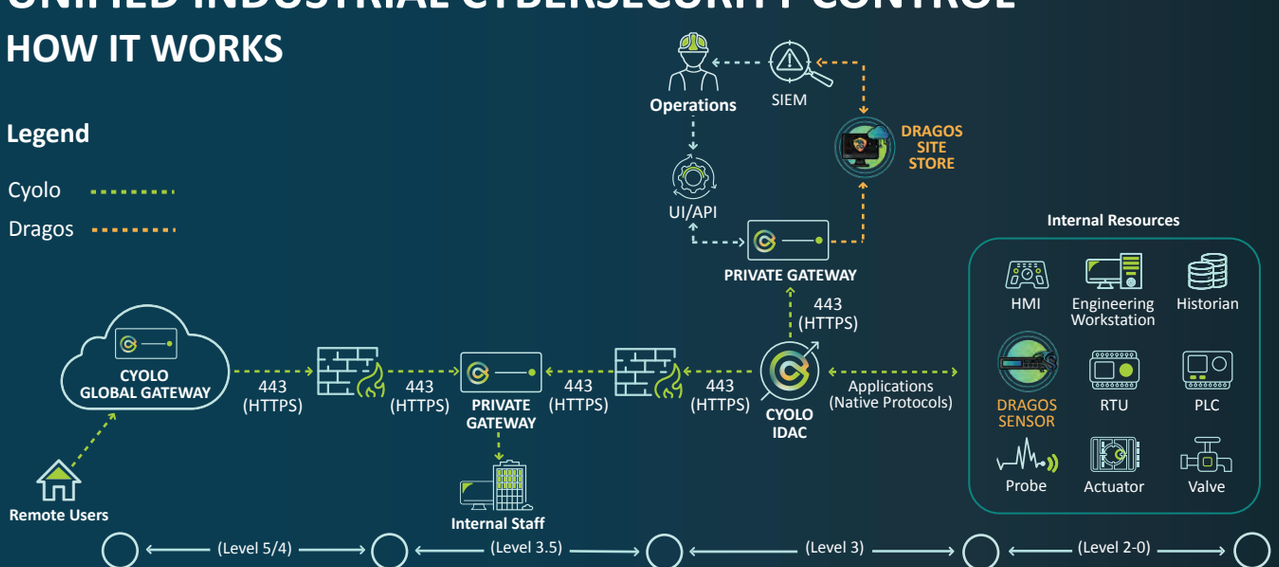
ICS Network Visibility Monitoring - employs continuous monitoring and protocol-aware tools to detect and address potential vulnerabilities (Dragos)

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

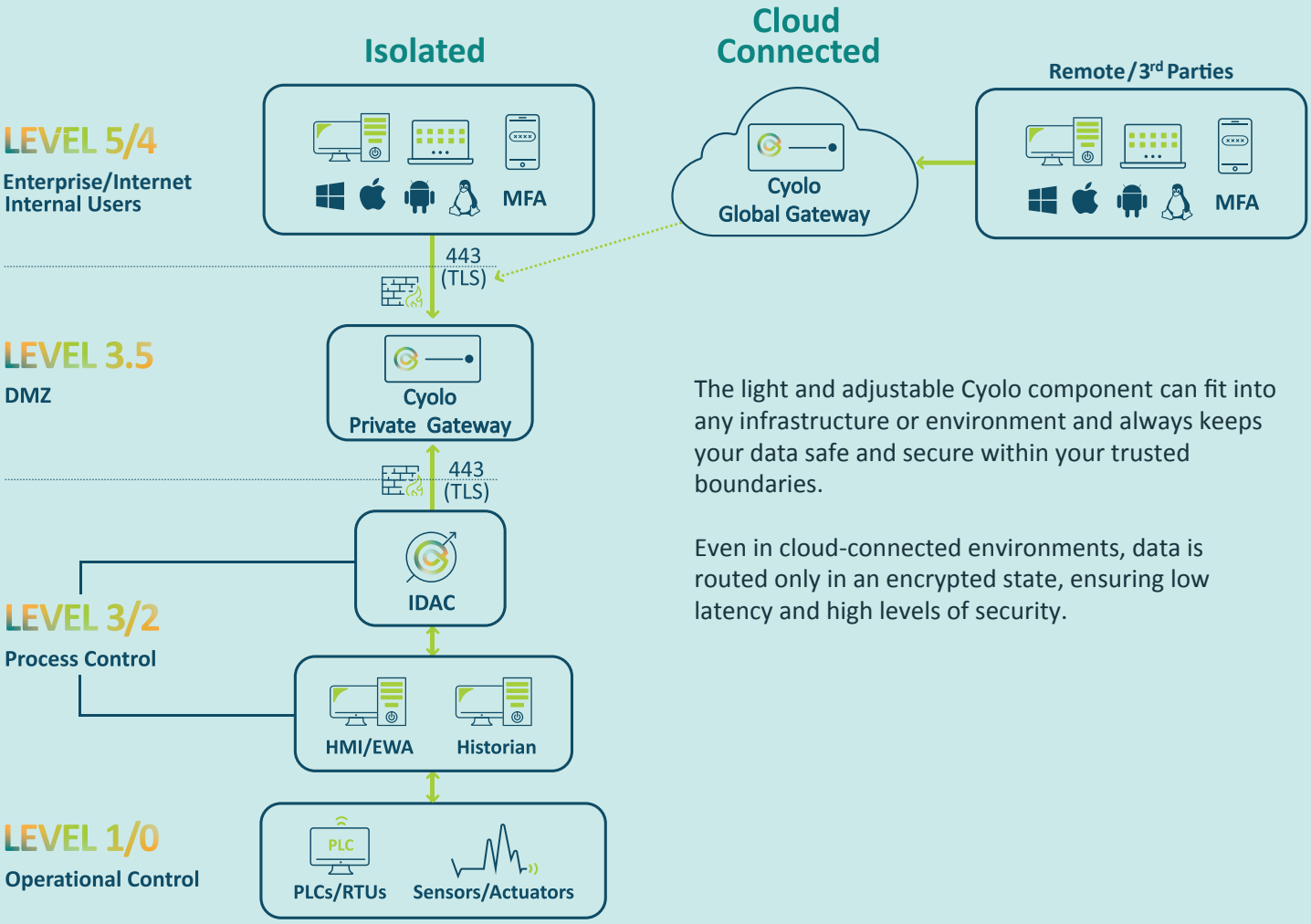
Risk-based Vulnerability Management - prioritizes and addressing vulnerabilities based on their potential to pose significant operational risks, thereby ensuring proactive prevention, response, and recovery actions (Dragos and Cyolo PRO)

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