Cyolo

At a Glance

Achieving Safe & Secure Access for the Maritime Industry

Cyolo PRO for Maritime, Shipping & Transportation

It's no exaggeration to say that the shipping and maritime industry serves as the backbone of the global economy. Unfortunately, an increasing number of adversaries also recognize the enormous value of this vital sector. Even as cyberattacks increase across a wide range of industries, maritime is particularly vulnerable due to its reliance on technology for navigation, communications, and logistics.

Recognizing this vulnerability, threat actors are acclerating their attacks on industrial control systems (ICS) and other operational technology (OT) and cyber-physical systems (CPS) in order to disrupt international commerce, steal sensitive data, and generally wreak havoc. Attacks could result from many spheres, such as ransomware gangs seeking a quick, high-value payout, or critical cybersecurity flaws affecting the aging infrastructure and legacy systems that characterize OT environments.

At the same time, digitization, automation, remote work, and rising connectivity between operational technology (OT) and information technology (IT) are creating both new opportunities and new vulnerabilities for companies in the martime space. Remote connectivity, as one example, reduces costs, improves operational agility, and lowers safety risks by enabling maintenance on vessels at sea to be conducted from port, with no need to travel to distant and potentially dangerous locations. However, remotely accessing critical systems creates its own security and safety risks, especially when third-party vendors and technicians are part of the equation.

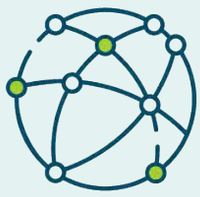
Simply put, if proper access, connectivity, and supervisory controls are not in place, a cyberattack against maritime targets could cause immense damage, including not only financial loss and severe economic disruption but even threats to human safety and the environment.

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

71%

of transportation and logistics organizations are currently pursuing some level of IT/OT convergence.

Ponemon Institute, 2024



Maritime Cybersecurity: Too Much Access, Too Little Control

28% of vessels allow crew to have local admin access for onboard machines.

63% of vessels provide crew access to more functionality of computer systems than they need for day-to-day operations.

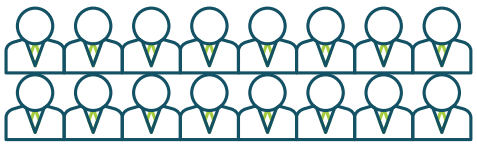
58% of vessel computers use obsolete operating systems.

37% have robust controls in place on what software can be uploaded onto the vessel computers.

Source: CyberOwl, 2023

Case Study: Fortune 500 Conglomerate

150 global sites



100,000 employees across **70** countries

Top Challenges

- Supply remote access to isolated and rugged environment (shipping containers)
- Unable to provision an asset with fixed IP to multiple policies
- Ensure worker safety at all times

Business Outcomes

- Improvement in remote access security and ease of use
- Ability to deploy on extremely small form factor hardware/ VM/ ruggedized
- Ability to freely attach multiple access policies to users/applications to ensure granularity and safety

Multiple Needs, 3 Security Layers , 1 Unified Solution

PRIVILEGED ACCESS

Safeguard Credentials → Vault

Establish Audit Trail → Session Auditing & 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

Improved User Experience

Safety on Land and at Sea

Reduction of Compliance Headaches

Reduced Cost and Complexity

Enterprise-ready Deployment

Managing Access and Risk in the Increasingly Connected OT Environment

45% believe their organization is **not effectively mitigating risks and security threats** to their OT environments.

77% of organizations **do not maintain an accurate, up-to-date inventory** of the assets in their OT environment.

73% of organizations **allow third-party vendors to access their OT environment**, and 60% grant such access to more than 50 different vendors.

71% **IT teams are partially or fully responsible for OT security at 71% of organizations**, but just 39% report strong or significant collaboration between IT and OT.

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 OT environments.

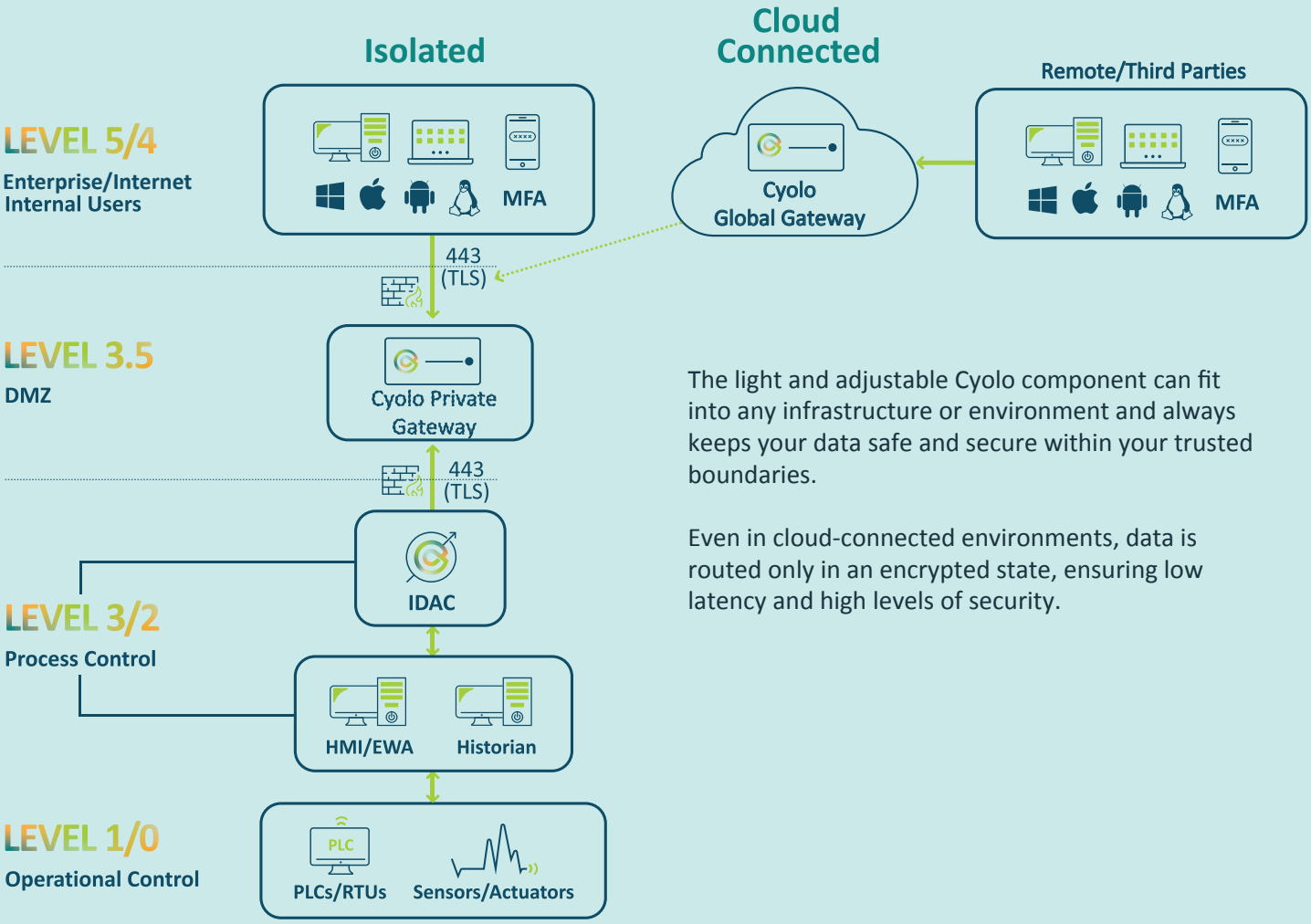
Manage Critical and Risky Access

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.

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