Cyolo

SANS | Research Program

Product Briefing

ICS/OT with Cyolo PRO:

The Evolution of Remote Access in ICS/OT Environments

October 2024

In recent years, organizations have increasingly opened their Industrial Control Systems (ICS) and Operational Technology (OT) environments to remote access by employees and internal staff as well as third-party vendors and contractors. As a result of the pandemic and changing work practices, many industrial organizations rapidly deployed new remote access tools. These stopgap solutions kept operations running but also introduced ongoing security risks, as carefully controlled access management practices became ad hoc and reactive. Recognizing this, the SANS Institute identified remote access security as a critical cybersecurity control in 2022. The latest *2024 SANS State of ICS/OT Cybersecurity* report underscores the importance of secure remote access in defending critical systems against evolving threats.

Cyolo PRO: Redefining Secure Remote Access for ICS/OT Environments

Traditional Secure Remote Access (SRA) tools—such as VPNs, Virtual Desktop Infrastructure (VDI), and jump servers—fail to meet the complex needs of today's OT environments. These tools often lack real-time visibility, are difficult to manage, and expose organizations to security risks by granting overly broad access.

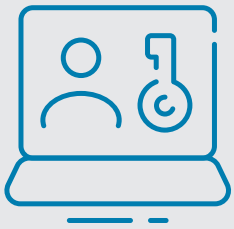
Cyolo PRO (Privileged Remote Operations) is an advanced SRA platform purpose-built for critical industries like manufacturing, energy, and oil & gas. Cyolo PRO secures remote access for employees, third-party vendors, and privileged staff, combining an innovative decentralized architecture with enhanced security, operational agility, and user experience.

Key Findings

Historically, ICS/OT environments were secured primarily through isolation. The recent shift toward connectivity and remote access has necessitated new approaches to security:

Multi-Factor Authentication (MFA)
74.9% of organizations now employ MFA as their primary security measure for remote access.

Jump Boxes
71% use jump boxes to create a secure path into OT systems.



Access Verification and Supervised Access
Less than half (48.3%) regularly verify remote access rights, while only a third (32.9%) employ next-generation solutions for session recording and least-privilege access.

Cyolo PRO Architecture and Key Capabilities

1. **Decentralized, Trustless (Zero Trust) Architecture—** Cyolo PRO operates within the user's own infrastructure, offering organizations full control over their security perimeter. It uses a reverse-proxy model, requiring no inbound network connections and minimizing network changes.
2. **Seamless Integration with Legacy Systems—**Cyolo PRO wraps OT assets in a secure layer that provides MFA, Single Sign-On (SSO), and session recording, allowing organizations to maintain security across diverse devices, from modern PLCs to legacy Windows hosts.
3. **Agentless Access for Third-Party Users—**Cyolo PRO enables secure remote access without the need for agents, eliminating compatibility issues for third-party users and allowing them direct access via a web browser.
4. **Zero Trust and Just-In-Time Access—**Adopting a zero-trust approach, Cyolo PRO uses digital identities with just-in-time creation, granular access policies, and restricted visibility for high-risk environments.
5. **Operational Agility—**Cyolo PRO can be deployed in under 15 minutes, making it easy to integrate into existing network topologies without asset modifications.

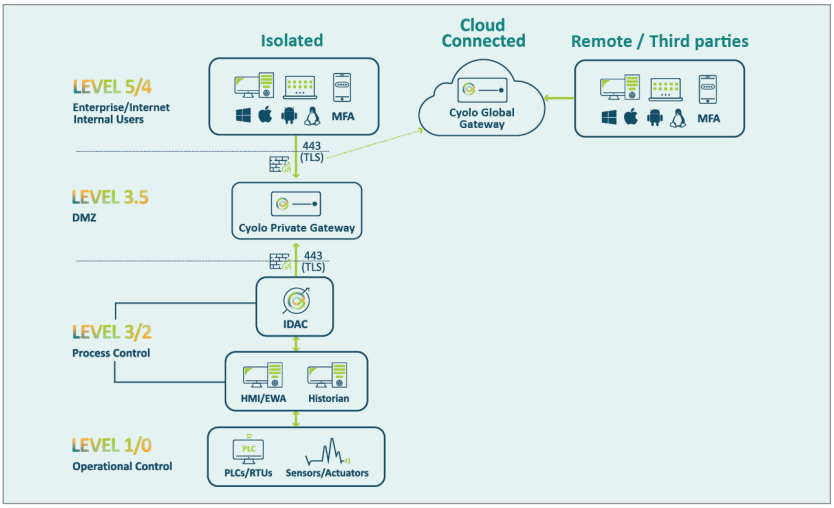


Figure 1. Its unique decentralized architecture allows Cyolo PRO to integrate seamlessly into any environment

Cyolo PRO Solves Major ICS/OT Security Challenges

The 2024 SANS survey highlights pressing challenges in ICS/OT environments, including:

- **Technical Integration of Aging Systems—**65% of organizations report difficulties integrating legacy OT systems with modern IT. Cyolo PRO's agentless architecture addresses these concerns by securely integrating legacy systems without requiring modifications.
- **Knowledge Gaps among IT Staff—**Half of surveyed organizations struggle in the face of IT staff's limited understanding of OT needs. Cyolo PRO simplifies management and offers secure, supervised access tailored to the unique requirements of OT.
- **Skilled Labor Shortages—**As 46% of organizations cope with labor shortages, Cyolo PRO's intuitive and agentless-first approach eases the burden on security teams, making secure remote access efficient and straightforward for all users.

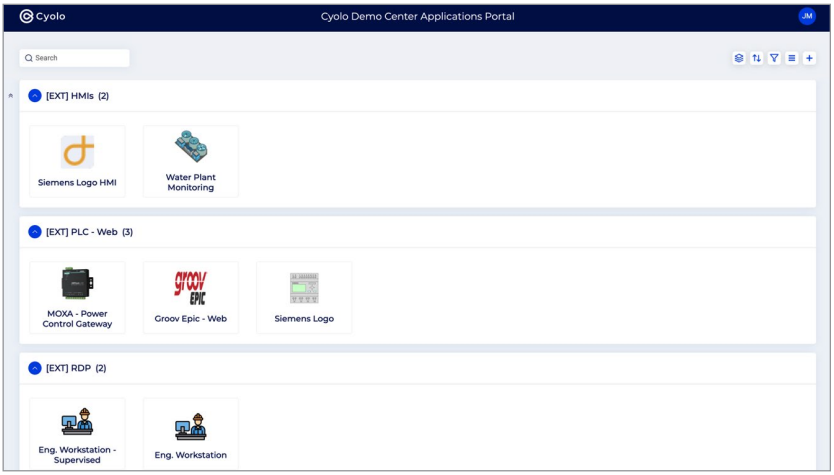


Figure 2. Verified users access authorized assets via the Cyolo PRO applications portal

Operational Benefits of Cyolo PRO

1. **Enhanced Visibility and Security Controls—**Cyolo PRO offers in-depth session monitoring, with granular policies for specific users, times, and geographic locations. It also includes access limitations and real-time supervision, so internal staff and OEMs can receive tailored security controls.
2. **Fast, Reliable Connections for Critical Situations—**Built without reliance on cloud processing, Cyolo PRO delivers rapid connections and low latency, ensuring that critical situations can be managed efficiently, regardless of location.
3. **On-Prem Security for OT Safety—**The on-prem nature of Cyolo PRO allows engineers to remotely access OT assets without compromising safety. This approach supports safe and secure operations, even for remote users handling sensitive ICS/OT assets.

Scan here to get a demo of the Cyolo PRO solution.

Cyolo.io/demo

Conclusion: Why Cyolo PRO is the Future of Secure Remote Access

Cyolo PRO addresses the urgent need for an effective, user-friendly, and highly secure remote access solution in ICS/OT environments. Its unique architecture, zero-trust approach, and agentless deployment enable organizations to overcome the traditional challenges of remote access, especially in environments with aging systems, third-party integrations, and labor shortages. With Cyolo PRO, industrial organizations can achieve the security, agility, and efficiency required to stay resilient in an evolving threat landscape.