How Cyolo Helps You Achieve Compliance: ISA/IEC 62443

ISA/IEC 62443 is a series of international standards that specify requirements and processes for implementing and maintaining industrial automation and control systems (IACS). Organizations will have varying levels of risk and fall into different security levels (SL), but each foundational requirement (FR) in ISA/IEC 62443 is widely recognized and adopted by industry professionals and organizations around the world. The system requirements (SR) apply to control systems in IACS environments, and implementing these controls will extend robust security to all operational technology (OT) systems and critical infrastructure.

Cyolo can help organizations achieve any security level of ISA/IEC 62443 compliance by providing reliably fast connections, granular access control, multi-factor authentication (MFA), encryption, continuous monitoring, and compliance reporting capabilities.

HERE ARE SOME WAYS THAT CYOLO SUPPORTS ISA/IEC 62443 COMPLIANCE:

Access Management: Cyolo deploys granular access controls to ensure that only authorized identities can access IACS. The Cyolo solution provides dynamic, context-based access control policies that can adapt to changing circumstances, such as the user’s location, device type, and the sensitivity of the information being accessed.

With its secure remote access solution, Cyolo delivers three layers of controls to better manage scenarios in which user access could cause enormous damage to the business. Deploying Cyolo materially helps support ISA/IEC 62443 standards.

Multi-Factor Authentication: Cyolo implements multi-factor authentication (MFA) to ensure that all identities are properly verified and authenticated before being granted access to IACS. Even legacy and offline systems that do not natively support modern authentication protocols can be retrofitted by Cyolo with MFA capabilities.

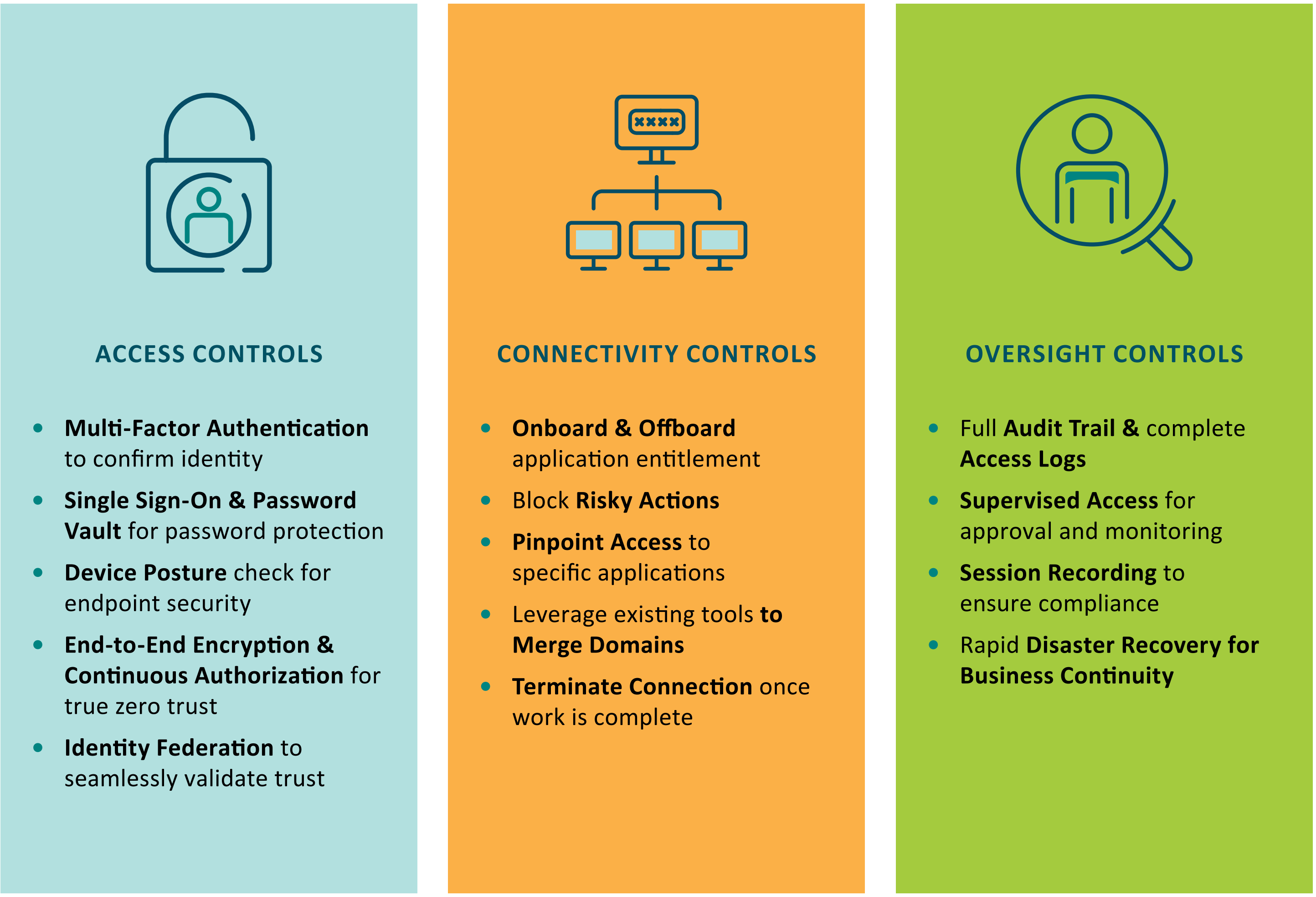
Encryption: Cyolo encrypts data from end-to-end and never decrypts the traffic in its cloud. This makes Cyolo a truly trustless zero-trust access solution, ideal for protecting access to IACS.

Continuous Monitoring: Cyolo continuously monitors and logs user activity to ensure that access to IACS is being used in accordance with applicable corporate policies and regulations.

HOW CYOLO HELPS

The Cyolo solution is built to support the real world, empowering organizations to securely connect users to the resources they need to do their jobs — and nothing more. Secure access is protected, and IACS remain safe and operational.

Cyolo is a member of the ISA Global Cybersecurity Alliance (ISAGCA).



ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools **to Merge Domains**
- **Terminate Connection** once work is complete

OVERSIGHT CONTROLS

- Full **Audit Trail &** complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery for Business Continuity**

Figure 1. Access, connectivity, and oversight controls in the Cyolo solution support compliance with ISA/IEC 62443 standards.

CYOLO ALIGNMENT WITH ISA/IEC 62443

62443-3-3.5 **FR 1 – IDENTIFICATION AND AUTHENTICATION CONTROL**	
SR 1.1	Human user identification and authentication
SR 1.2	Software process and device identification and authentication
SR 1.3	Account management
SR 1.4	Identifier management
SR 1.5	Authenticator management
SR 1.6	Wireless access management
SR 1.7	Strength of password-based authentication
SR 1.8	Public key infrastructure (PKI) certificates
SR 1.9	Strength of public key authentication
SR 1.10	Authenticator feedback
SR 1.11	Unsuccessful login attempts
SR 1.12	System use notification
SR 1.13	Access via untrusted networks

62443-3-3.6 **FR 2 – USE CONTROL**	
SR 2.1	Authorization enforcement
SR 2.4	Mobile code
SR 2.6	Remote session termination
SR 2.8	Auditable events
SR 2.9	Audit storage capacity
SR 2.10	Response to audit processing failures
SR 2.11	Timestamps
SR 2.12	Non-repudiation

62443-3-3.7 **FR 3 – SYSTEM INTEGRITY**	
SR 3.1	Communication integrity
SR 3.2	Malicious code protection (SL-2)
SR 3.8	Session integrity
SR 3.9	Protection of audit information (SL-3)
62443-3-3.8 **FR 4 – DATA CONFIDENTIALITY**	
SR 4.1	Information confidentiality
62443-3-3.9 **FR 5 – RESTRICTED DATA FLOW**	
SR 5.1	Network segmentation
SR 5.2	Zone boundary protection
SR 5.3	General purpose person-to-person communication restrictions
SR 5.4	Application partitioning
62443-3-3.10 **FR 6 – TIMELY RESPONSE TO EVENTS**	
SR 6.1	Audit log accessibility