Cyolo

How Cyolo Helps You Achieve Compliance: TSA SD2021-02C

In July 2022, the United States implemented Transportation Security Administration (TSA) Directive SD2021-02C. This directive was specifically designed for owners and operators of hazardous liquid pipelines, natural gas pipelines, and liquefied natural gas facilities that have been deemed critical by the TSA.

The directive aims to ensure the security of these facilities by mandating compliance with a range of security controls aimed at avoiding any potential disruptions or degradation to the infrastructure. These controls include:

- Multi-Factor Authentication (MFA)
- Network Segmentation
- Network Monitoring
- Traffic Filtering

HOW CYOLO HELPS

Purpose-built for use in operational technology (OT) environments, Cyolo is a comprehensive solution designed to assist organizations in meeting stringent security and compliance requirements while also addressing the practical challenges posed by the oil and gas environment. These challenges, such as the deployment of technology in remote and harsh locations where computational infrastructure may be non-existent and bandwidth is limited, can be effectively overcome with the Cyolo zero-trust access solution.

SECURE SOLUTION

With its zero-trust 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 TSA SD2021-02C compliance during an audit.

Cyolo was created to give users access to the resources they need while maintaining the zero-trust model. It is built to support the real world, enabling companies to protect their entire network and all critical infrastructure. With Cyolo, you can securely access the resources you need to get your work done, while keeping your network and data safe.

ACCESS CONTROLS

- **Multi-Factor Authencation** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Contiunuous 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**
- Control **Activity Permissions**
- **Terminate Connection** once work is completed

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. Cyolo Z*ero-Trust *Access controls that support compliance with TSA SD2021-02C)*

CYOLO ALIGNMENT WITH TSA SD2021-02C

SECTION	MEASURE	CYOLO CAPABILITIES	CONTROL TYPES
III.C.2	Multi-Factor Authentication	Extend MFA to all user accounts (service, shared, individual, etc.) in isolated, hybrid or cloud environments.	Provides
III.C.3	Least privilege access rights and separation of duties	Provide user access rights based on individual, group, role or location.	Provides
III.C.4.a	Shared accounts limited through least privilege and separation of duties	Provide shared account access rights based on individual, group, role or location.	Provides
III.C.4.b	Access to shared account credentials restricted	Deny direct access to shared account credentials	Provides
III.D.4	Incident isolation controls	Restrict access to users or resources provisioned within the platform, manually via operational staff or in an automated manner via a Security Orchestration, Automation, and Response (SOAR) or other tools	Supports
III.E.3	Patching deficiency mitigation	Allow operational staff to apply controls and restrictions to resources to mitigate risks while maintaining operational availability	Provides
IV.C.2.e.i	Compliance attestation - Log files	Retain log files of platform usage and is configured to feed into other log aggregation platforms	Validates
IV.C.2.f	Compliance attestation - Other	Enable session recording to create fully auditable user session information	Validates

Table
Provides: *Provides information to give directly to auditor or feeds data into an artifact*
Vali*dates:* *Can be used to prove whether another control(s) is present and/or work*ing
Supports: *Feeds information into another system or processes which serve the requirements*