TP Research

Vendor SITREP

CYOLO

Snapshot

Founded – 2020

HQ – Tel Aviv, Israel

Funding - $85.2M

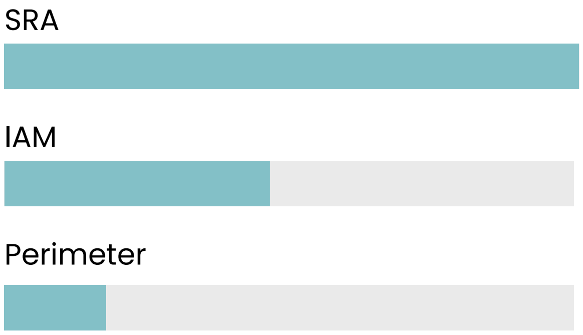
Primary Category: Secure Remote Access

Employees ~90

Website LinkedIn

GTM: Direct and Channel

Solution categories



Cyolo Overview

Cybersecurity threats now pose a risk to operational safety. This inspired Cyolo to build a zero-trust access platform that functions across all deployment scenarios (including fully offline) and enables OT and security professionals to prevent access-related threats. The Cyolo solution was built by the CISO of a manufacturing company and two ethical hackers to solve real-world problems, like securing third-parties and connecting users to OT systems without requiring downtime or network changes. Cyolo offers the visibility and control you need to operate your business safely.

Cyolo's Technology Adoption: I-SRA

Remote Access to ICS/OT assets within the production/operations environment

Who		From where	
Internal - Company employees	External - Vendor, OEM & third-party Access	Local production (Purdue L0-3.5) or Enterprise Network (L4-5)	Cloud Access, Internet, dial-up/modem, mobile.

Some of the solution's main features include:

- Enabling businesses to change policies and access controls in real-time to address emerging threats and vulnerabilities.
- Providing secure remote access and Industry 4.0 capabilities, allowing businesses to collect and analyze critical data for process improvement.
- Minimizing access risk by allowing only authorized users to access critical infrastructure, based on role, application, and device identity.
- Strengthening security controls across the entire environment and recording everything — making it an excellent tool for compliance and auditing.
- A small footprint that includes a password vault and is designed for remote access locations.
- Full auditability to meet compliance mandates.
- Simple deployment that requires no IT expertise and can seamlessly fit into any environment, thanks to the 'no footprint' design.
- Adding a secure overlay to all current SRA solutions which can also be phased out slowly, with upgrades planned and trained for.
- Minimizing the inherent risks of digital transformation, connectivity, IIoT, and smart manufacturing.

Platform/Solution Overview

Cyolo is a zero-trust access platform purpose-built for OT environments. Deploying the Cyolo solution allows you to embrace the zero-trust framework for these critical infrastructures without forklift changes or severe environmental disruptions. Cyolo can also add multi-factor authentication (MFA) and single sign-on (SSO) capabilities to ICS systems that do not natively support modern authentication. With a unique trustless architecture, Cyolo empowers critical infrastructure operators to safely connect their systems and enable the benefits of digital transformation.

Here is how they do it:

1. **Verifying every connecting user** - Using existing Identity Providers (IdP) or the Cyolo IdP, every user, including external users, is validated before accessing any resource. Additionally, health checks can be assessed on the device used to connect.

2. **Assigning policies that limit application access** - By enforcing dynamic policy-based MFA and SSO, users can only access the applications, tools, and resources needed to perform their work. Once the work is complete, the access is rescinded.

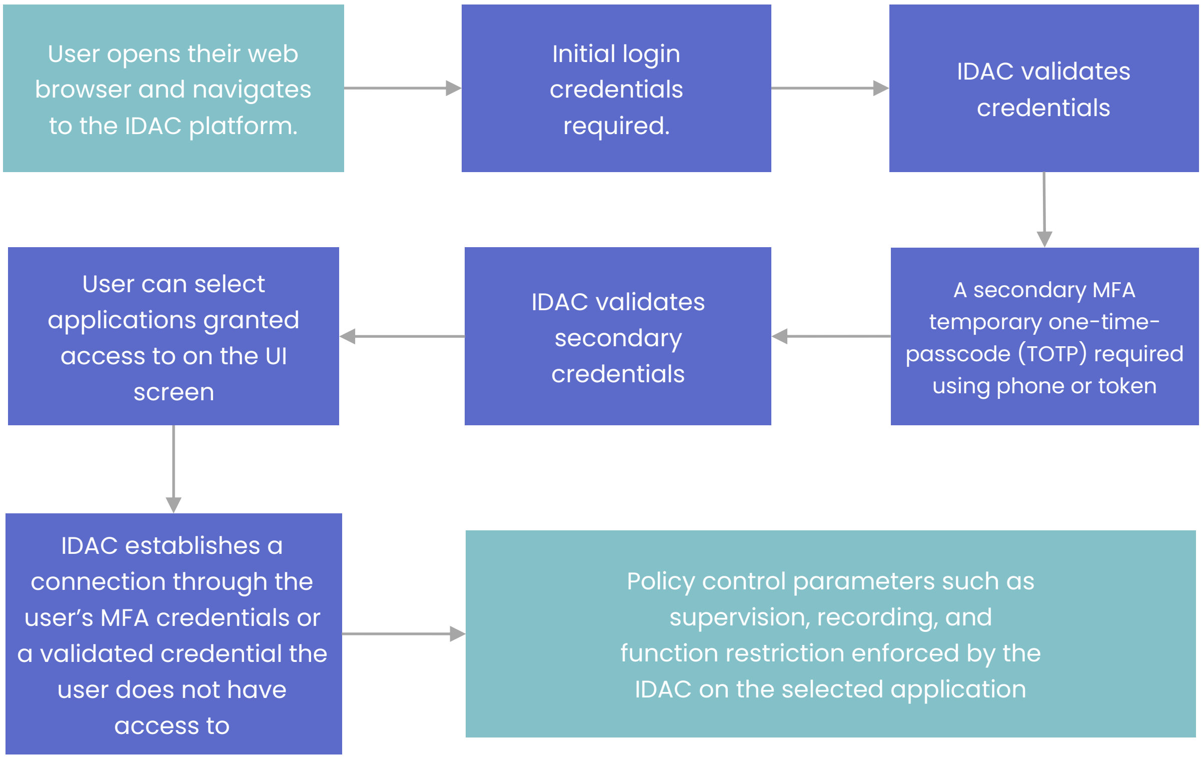
3. **Full activity reporting** - Every session is monitored, and a full audit trail is generated for all activities to support reporting needs and compliance goals.

The Cyolo platform consists of two primary components:

Identity Access Controllers (IDACs)	The Cyolo Edge
These connectors reside close to the application servers they publish, either in your private data center, your IaaS provider, or a combination of the two. IDACs never communicate with each other directly, only through Edge routers (Cyolo's cloud or your own). IDACs communicate with the application servers in native protocols such as RDP, SSH, and HTTP. IDACs terminate the Transport Layer Security (TLS) communication from users and instead enforce the access policies configured by the Cyolo administrator.	This Edge broker routes users' requests based on a Server Name Indication (SNI) header to the relevant IDAC. In any situation, regardless of cloud, hybrid, or isolated deployment, Edge brokers have the same functionality – routing traffic between the users to the IDACs and amongst the IDACs to keep the operational state between them in continuous sync.

How Does It Work

Cyolo recognizes that even the best security tool will not be effective unless it is simple to use, and that user experience is critical to product adoption.



User opens their web browser and navigates to the IDAC platform.

Initial login credentials required.

IDAC validates credentials

A secondary MFA temporary one-time-passcode (TOTP) required using phone or token

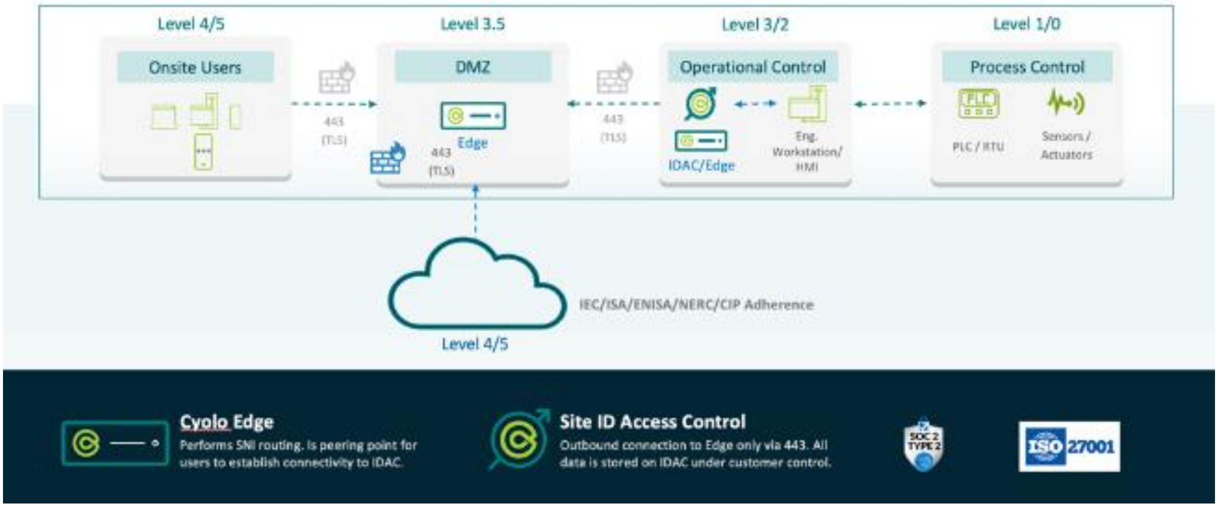
IDAC validates secondary credentials

User can select applications granted access to on the UI screen

IDAC establishes a connection through the user's MFA credentials or a validated credential the user does not have access to

Policy control parameters such as supervision, recording, and function restriction enforced by the IDAC on the selected application

Deployment scenario



Cyolo Edge
Performs SNI routing. Is peering point for users to establish connectivity to IDAC.

Site ID Access Control
Outbound connection to Edge only via 443. All data is stored on IDAC under customer control.

What I-SRA capabilities does Cyolo offer?

Technical Requirements

- ☑ Support access from third-party owned laptops, using native applications with or without using Jump servers.
- ☑ Provide agent-based or agentless methods of implementation.
- ☑ Supports High Availability (redundant) operation of critical components.
- ☑ Cause no downtime when upgraded.
- ☑ Remote access does not interfere with how OT/ICS systems are accessed/used locally.

Integration Requirements

- ☑ Support integration to Security Information and Event Management (SIEM) solutions or to general log management
- ☑ Built-in integration to multifactor authentication mechanisms
- ☑ Support Active Directory for user/group integration
- ☑ Provide all types of reports as relevant to remote access and usage
- ☑ Support reporting and extraction of session specific logs

Functional Requirements

- ☑ Provide setup and automatic enforcement of time-limits on remote access sessions.
- ☑ Support launching RDP and SSH sessions to target devices.
- ☑ Provide a method of session logging or log collection for each access method and activity.
- ☑ Provide a method for real-time viewing of active sessions.
- ☑ Support the emergency termination of remote access sessions.

Support & Maintenance Requirements

- ☑ Support software updates and expert services
- ☑ Provide expert training for key/administrative users as necessary.
- ☑ Provide on-site support for ultra-critical industrial infrastructure and processes
- ☑ Provide perpetual licensing model that supports uninterrupted connectivity

Some Factors to Consider About Cyolo

When evaluating Cyolo, it is important to consider several elements such as:

- They are a startup and hence a certain amount of risk.
- They have a new innovative approach, not widely deployed.
- They have an evolving solution; an approach required to combat systematic cyber risks

TP Research Recommendations

The actions needed to increase I-SRA maturity must always be weighed against the cost and efficacy of each step and how much risk is reduced or eliminated. Some OT assets and environments can endure what we perceive as a “greater” risk due to the cost effects or because the operation is less critical than others. You can find more information on balancing costs and risks in TP’s full report on Industrial Secure Remote Access. TP recommended you read the full report alongside this SITREP to conclude the suitable vendor for your business.