Cyolo

No Change Management Needed: Securely Connect People to Work from Anywhere

In many instances, deploying a new security solution is not only difficult but also potentially disruptive. Typical deployments require multiple security and IT groups to coordinate for a synchronized go-live. Even with the best laid plans, new tools come with challenges, such as connectivity issues, downtime or business disruption.

Cyolo was founded by a veteran Chief Information Security Officer (CISO) and two ethical hackers. With a deep understanding of the daily work of security and IT teams, they know the many disruptions that come with new processes and technologies. They have lived the reality of good projects going wrong – so they designed Cyolo to be different.

> "Change management is the enemy of security."
>
> **Almog Apirion,**
> CEO & Co-Founder, Cyolo

Deploying the Cyolo Zero-Trust Access platform requires no change management. It is self-contained, deployed within firewall boundaries, and takes around 10 minutes to get started. A typical Cyolo installation does not require special expertise and can be performed by anyone familiar with a Linux prompt.

- Guided User Installation (GUI) with minimal operator input
- The license, delivered by Cyolo ahead of time, includes all the product options/variants, domain information, etc.
- Unique scripting provides DNS changes and SSL certificate generation
- Where required, operator input is supported by highly accurate (99% match) suggested default values
- As opposed to DMZ deployed solutions, Cyolo is designed to run behind the organizational Firewall and does not require any open incoming port
- Typically, no new Firewall rules, or any Firewall team involvement, are needed.

Change management is also important to consider from a user perspective, as any change to users' normal workflow can have a serious impact on productivity. Cyolo simplifies adoption of security tools for users by enforcing policy without requiring changes in their workflow.

- One-time multi-factor authentication (MFA) identity validation
- Comprehensive single sign-on (SSO) to their needed tools
- Access to all applications and systems needed for work (and nothing more)
- No new logins or passwords to remember

From a technical perspective, solving the change management challenge can significantly improve organizational security. The best tools are those that easily integrate with the existing security stack and are easy for security teams to operate. Below are common technical change management challenges and how Cyolo's unique approach eliminates them.

TYPICAL CHANGE MANAGEMENT CHALLENGES	THE CYOLO DIFFERENCE: NO CHANGE MANAGEMENT REQUIRED	IT CM NEEDED WITH CYOLO?
Technical Expertise Needed	Cyolo is simple to deploy and does not require hiring, contracting, or training additional staff.	No
Installation Timelines	The Cyolo platform installation typically takes less than 10 minutes and does not require a maintenance window.	No
Firewall Rules Update	As a 'Reverse Proxy,' Cyolo sends traffic out Port 443 and does not require configuration from the firewall team.	No
Routing Table Changes	Cyolo uses Server Name Indication (SNI) to route traffic, so no changes are needed to core routing tables.	No
DNS Query Configuration	Cyolo has an internal DNS server and does not require additional configuration.	No
Planned Upgrade Downtime	Cyolo is deployed in high availability clusters and upgrades are scheduled for minimal impact to operations.	No
Endpoint Agent Installation	Agentless deployment with no changes to MDM or Group Policy needed to connect devices.	No
Device Posture Assessment	User self-installs agent to run device health check and then it quietly launches and runs when needed.	Minimal
Identity Provider Integration	Cyolo integrates and can federate multiple IdPs into a single user validation workflow.	Minimal