Cyolo

Driving Digital Business with **Identity-Based Connectivity**

The explosion of connected things and remote workers is challenging digital enterprises in all industries. This emerging reality requires a new security strategy and a coordinated approach across IT and OT, as the threat from bad actors exploiting weaknesses in existing authentication infrastructure is increasing.

With users connecting from everywhere, it has become apparent that IP white listing or even the device can no longer support the level of security required. Identity has become the new key, and as such needs to be supported by all connected resources. Unfortunately, upgrading existing resources to support modern authentication can be expensive and time consuming.

> "Cyolo helps your organization meet modern compliance and security regulations, extending clould SSO and adaptive MFA to traditional applications, cost-effectively, quickly, and easily."

Adding Multi Factor Authentication (MFA) to VPN authentication as a quick access tool helps alleviate remote connectivity pressure but does not provide the required visibility and control.
Cyolo retrofits existing systems with modern authentication infrastructure to confidently identify and quickly connect users to the resources they need to do their jobs in today's complex digital environment. After the new infrastructure is installed, the path toward identity-based access and connectivity can be easily taken.

Cyolo helps your organization meet modern compliance and security regulations, extending clould SSO and adaptive MFA to traditional applications, cost-effectively, quickly, and easily. The identity-based access solution works with your existing tech stack and active directory to streamline uniform security policies across all systems, reducing overhead with minimal time to deploy, implement, and enforce IT security. The platform provides real-time user-to-application access and control with continuous authorization and end-to-end encryption.

Three Easy Steps to Ensure Connectivity

With Cyolo's identity-based access solution, it's easy for any type of user to securely gain access to all the organizational resources they need.

Deploy and Scale in Minutes

Cyolo is agentless and can be deployed within 10 minutes.

Establish secure connectivity without IP conflicts, architecture changes, or additional resources.

Modernize Identity Infrastructure

Use Cyolo to retrofit every existing system with modern authentication to make use of MFA and SSO for secured connectivity.

Connect Securely

Onsite & remote users can connect securely to their apps, resources, workstations, servers & files through user and device ID, MFA and biometric authentication.

Architecture Reference

Cyolo understands that every organization is at a different stage in their Zero Trust journey. That's why ZTNA2.0 is a completely agnostic platform.

- Connect your existing IdP – cloud, on-premise, SaaS, LDAP, exactly how you've already been doing it. No need to establish directory trust with other organizations to provide secure access to 3rd parties or during M&A transactions.

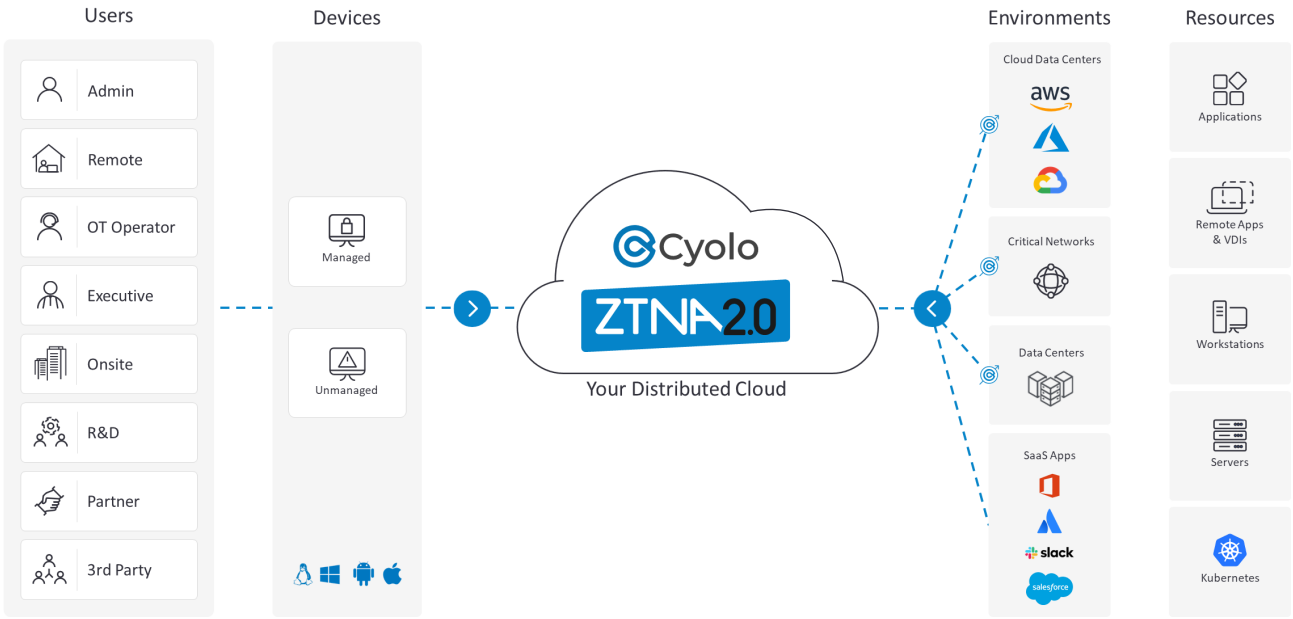
- Deployment is quick and nearly effortless with Cyolo. Both components of the solution, the IDAC (Identity Access Controller) and Edge live as lightweight containers and can be run on hardened operating systems on minimal hardware.

- The IDAC establishes an outbound-only TLS connection to the closest Cyolo PoP. The IDAC requires no public network access, communicates over native protocols, and publishes the resource URLs.

- Think of the Edge as your private Cyolo cloud, connecting to your IDACs. Like the IDAC, the Edge establishes an outbound-only TLS connection to Cyolo and will route user URL requests to the correct IDAC. This means for internal users accessing on-prem resources, there is no Internet round trip for better performance. The Edge, effectively, allows you to create a completely private solution – for an isolated OT deployment, no Internet connection is needed in an Edge deployment.

- Our Zero Trust approach goes farther than any other solution on the market. Cyolo does not store any customer data. We'll never ask for your encryption keys or anything sensitive. Even our employees have incredibly restricted access to your tenant. Even if Cyolo were to be breached, your data would remain 100% secure and untouched.

How it Works



Key Benefits

Connect Everything

Full visibility and control over who connects to where and what has occurred

Ability to integrate with different IdPs (on-premise and cloud)

Protect all applications regardless of protocol or location (on-premise, IaaS, SaaS)

Increase Operational Productivity

Seamless access of all users to accommodate support and critical business processes

Consolidate multiple siloed access tools into a single, overarching platform

Provide better user and admin experience without agents or additional software

Reduce Risk of Breach

Complete, real-time user to application access control and end-to-end encryption

Hide application credentials from trusted and untrusted connected users

Minimize the attack surface, moving public network access to all applications behind ZTNA

Secure Access for All Populations

Remote Employees

Securely connect remote employees to their working environments

Device, multi-factor, & biometric authentication

Agentless access via eb portal

Prevent risky actions like file transfer and copy paste to avoid malware spread and data leaks

3rd Party Users

Enable contractors and 3rd party users to securely access organizational assets

Avoid full network access
Seamless access for native application support

Full audit trail, visibility and session recording

Real-time supervised access and actions, for sensitive roles and areas

Privileged Users

Give privileged users extended access without compromising on security

Avoid passwords with built-in vault

Answer compliance with supervisor mode

Full audit trail, visibility and session recording

Native source code protection