

Redefining Secure Connectivity

About Cyolo

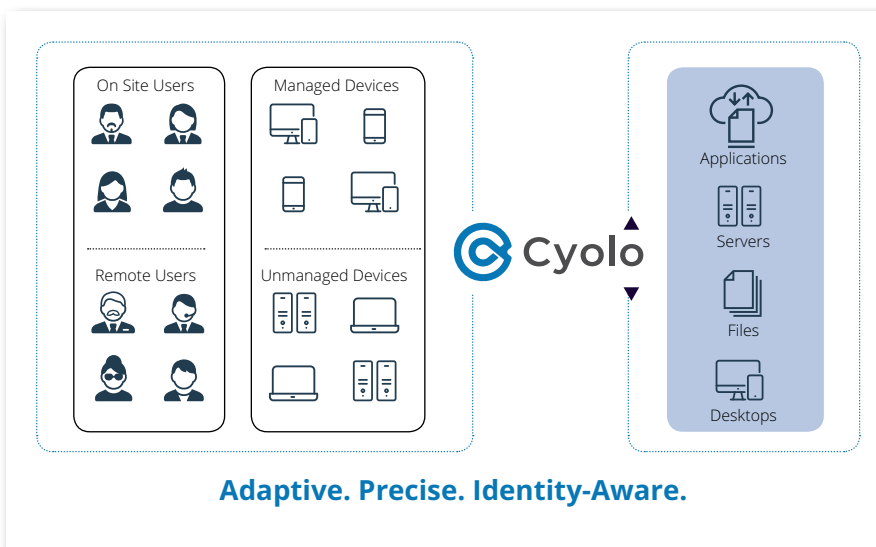
Cyolo's Zero Trust Network Architecture takes secure connectivity to the next level, enabling on-site and remote users to rapidly and securely connect to their working environments.

With **one unified solution** for an increasingly complex cyberspace, Cyolo provides the global workforce with the ability to securely access applications, files, servers, and desktops from any device on their local network or in the cloud.

Optimize Security. Reduce Risk. Facilitate Business Operations.

Cyolo operates as a hybrid broker between users and devices, employing dynamic risk-based access for maximum security. Risk is calculated according to user ID, device ID, time, location and multi-factor authentication, and actionable insights based on AI. The platform enhances visibility and control by applying granular policies and enabling real-time supervised access and actions.

In order to minimize the attack surface and prevent malicious access, Cyolo provides narrow access and service segmentation, to ensure that access is granted to the authorized asset and not to the network itself. Cyolo can be deployed instantly on-site or as a SaaS solution, and is easy to onboard and scalable.



Key Benefits

Real Zero Trust

Cyolo is the only broker that offers true zero trust. In most cases, the ZTNA provider holds the encryption keys, policy, control, and execution of the access policies. The customer is forced to trust the provider and its providers.

Cyolo's customers don't need to put their trust in another system with their data or traffic as all the sensitive information stays with them. With Cyolo no user data, credentials or encryption keys are kept in the cloud and there is no IPSEC tunnel to the assets.

Agility

The Cyolo platform is agile and scalable. It is network and platform agnostic and can be run on premise or on IaaS and SaaS platforms. There is also no need to connect to the users' networks or Network Access Controls.

With Cyolo, users can rapidly and easily expand to new locations – no infrastructure or hardware required. Making it easier for organizations to remain agile and respond to business needs, without compromising on security.

Boundless

Cyolo offers secure access to applications on any network: internal, external, offline and IoT. It supports any protocol and delivers a secure and transparent user experience. Customers can also receive actionable insights based on its AI and self-calibrating functionality.



Key Features

Set up in Under 10 Minutes

Cyolo can be set up in less than ten minutes with a simple one liner installation. Cyolo is platform agnostic and integrates fully with existing infrastructures (such as Okta, Active Directory, ADFS etc.) Cyolo is agentless, low touch and doesn't require any installations on the user's environment or the system's resources, supporting self-service enrollment for users to save the admin's time.

Secure Remote Access to Organizational Assets

Cyolo enables access to the users' desktop, files and more. Users are granted secure access to web applications on-premise or in the cloud, such as Azure, AWS and GCP, including secure access to rich client applications (ERP, PLM, XRM etc.)

The platform enables secure access to servers with multiple protocols, such as RDP, VNC, TELENET, DB, and SSH.

Privileged User Access (Devops, Admin & Suppliers)

The Cyolo vault eliminates the need for potentially risky actions like passing passwords and password rotation. Users login to the platform and it securely connects them to the servers - without the need to know or store the password.

Cyolo's Privileged Access Management minimizes the attack surface, by only giving access to what's needed to the specific user.

Multi-Factor Authentication

Cyolo's IDAC (Identity Access Control) provides granular control per application, based on user ID, biometric (fingerprint and face) authentication, geo-location, timing, one-time password access, and risk-based assessments based on its AI functionality.

Device Authentication and Health Check

It also authenticates devices & runs a full health check, ensuring that it has the latest security policies, including all the controls like the latest anti-virus signature and the correct security patch level. In addition to providing a client certificate for users' devices, Cyolo also supports corporate certificates (X.509)

Protection from Internal Threat

Zero Trust dictates that you shouldn't trust any entity either outside or inside the perimeter at any time. While many providers secure your system from external attacks, Cyolo is the only solution that also protects you from internal threats.

Cyolo protects key areas inside your network by activating supervised access to sensitive assets and hiding them from internal attackers, securing access to critical networks and subnets, and securing connectivity between critical networks.

Cyolo Edge protects assets in offline environments, providing an 'out of the box' solution for offline networks. It also provides secure access from within the network, via LAN or VPN.

Application Security

Cyolo offers full access and action visibility and control. The platform disallows risky actions like copy-paste and file transfers for servers and desktops to mitigate malware and data leakage risks. It also controls and restricts access to specific paths and directories and enables WAF (web app firewall) capabilities for managed applications.

Load Sharing for High Availability

Cyolo enables organizations to deploy as many IDACs as necessary and activate load sharing between them, eliminating the risk of a single point of failure, ensuring high and optimized availability without the need for additional infrastructure. It maximizes the utilization of your existing resources and removes the need for additional infrastructure as the IDAC immediately goes into action upon installation.

Auditing & Recording

With Cyolo, customers can run supervised access in real-time. Supervisors can view precisely what a user is doing live and log and record all activities. This provides organizations with a full audit trail, enabling them to perform thorough post-incident investigations. Cyolo enables inclusive and event-driven activity recording, supports 3rd party recording solutions, and fully integrates with SIEM systems.