Cyolo

Redefining Secure Connectivity

The organization’s cyberspace has become almost impossible to secure, as users, applications, resources and data are spread across networks and in the cloud.

Control, visibility and management is cumbersome and too often inefficient. Maintaining multiple secure environments with different solutions and policies, is a challenge to every organization and a window of opportunity for cyber attackers.

Secure business connection that is not network bound

Cyolo’s Secure Access Service Edge (SASE) platform securely connects **onsite and remote users** to authorized assets, in the organizational **network, cloud or IoT** environments and even offline networks, regardless of where they are or what device they are using.

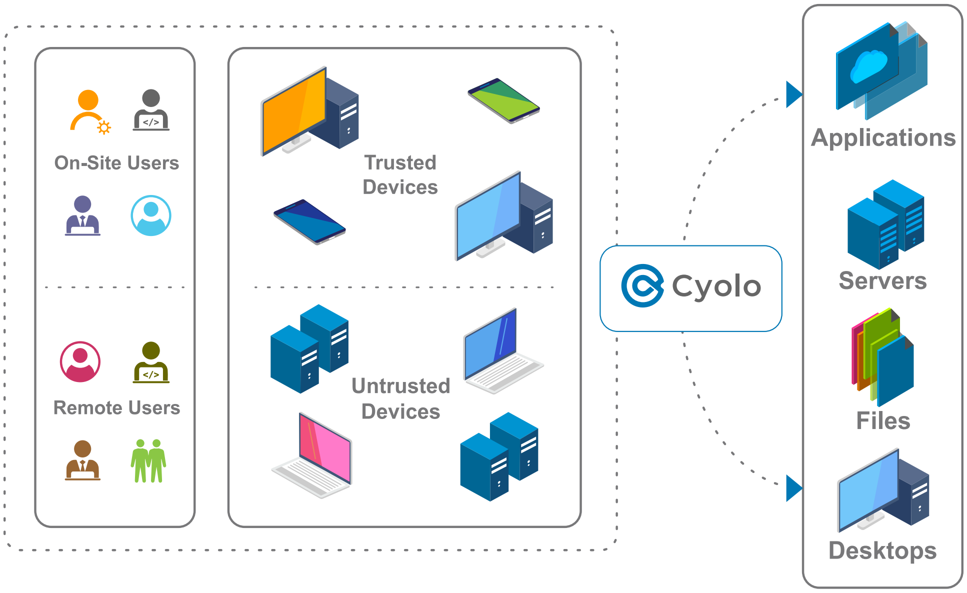
Cyolo ensures secure access to **applications, resources, workstations, servers and files,** without granting risky network access to information assets.

Solution Highlights

- Ensure **business continuity** with controlled access and secure remote access
- Facilitate **collaboration** with secure cross organizational connectivity
- Employ dynamic risk-based access to improve **security** and user experience
- Increase accuracy of secure access with granular **visibility** and **control**
- Apply easy-to-use **MFA**, touch and face ID and endpoint certificates support for **identity** accuracy
- Optimize management with easy **deployment** and **scaling** abilities

Securely connect any user from any device with trusted access to any system on any network and platform

- ✓ Network and platform agnostic
- ✓ Secure access to sensitive areas and assets
- ✓ Support for rich client applications
- ✓ File transfer inspection for malware and data leakage



For more information visit www.cyolo.io or contact us: info@cyolo.io, 866.918.1143

Cyolo

Secure Access to Support your Business

Controlled Access

Protect assets against insider threats and external attacks and ensure business continuity.

- Full visibility and control over users' access and actions over sensitive applications and mission-critical environments, on-premises and in the cloud
- Controlled access for DevOps, developers, administrators and privileged users

Collaboration and M&A

Facilitate cross organizational connectivity during collaboration and M&A projects, by securely connecting users to shared applications.

- Avoid costly infrastructure investments
- Eliminate requirements for network integration or trust relationship, between users' directories
- Lower the risk to information assets

Remote Access

Securely connect employees and 3rd parties to applications, desktops, servers and files, over the Internet – VPN and network free.

- Gain control with device authentication, multi factor and biometric authentication
- Real-time supervised access and actions, for sensitive roles and areas
- Avoid malware spread and data leaks with prevention of risky actions such as file transfer and copy-paste

Compliance Readiness

Enhance privacy and improve compliance readiness with end-to-end encryption of the entire traffic.

- Users' traffic and information is never exposed
- Encrypted traffic and secure access for client-server and proprietary applications
- Multi factor and biometric authentication for specific actions or roles
- Covering legacy applications and systems

Optimize security, reduce risk, facilitate business operations

Resilient

- Enforce granular & action-based policy
- Minimize the attack surface with no access to the network
- Reduce risk of internal and external threats with risk-based access

Agile

- Network and platform agnostic - on premise, IaaS and SaaS platforms
- Remove the need to connect to users' networks, NACs etc.
- Easily expand to new locations with no infrastructure or hardware required

Boundless

- Unified secure access to applications on any network: internal, external, offline and IoT
- Deliver a secure and transparent user experience
- Get self-calibrating actionable insights

Cyolo enhances **visibility and control** by applying granular policies that are based on user ID, device ID, application, time and action, and by 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's technology enables to ensure security without compromising business needs. Cyolo's **dynamic risk-based access** employs AI powered policy suggestions and self-calibrating actionable insights to reduce the risk of unauthorized access, and visualized users' risk profiles, to set policies and optimize mitigation.

Cyolo's unified SASE platform was designed for **easy deployment and scale,** to support business needs, growth and expansion. Its on-boarding processes are straight-forward and are built to facilitate management without special skills requirements.

For more information visit www.cyolo.io or contact us: info@cyolo.io, 866.918.1143