Cyolo

Faster, Smarter, Better Secure Access to Everything

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running.

Cyolo was founded by a former CISO and two ethical hackers to solve the challenge of securely connecting high-risk users to business-critical applications within every kind of environment — cloud-connected, cloud-averse and offline.

Cyolo provides the only trustless zero-trust access solution and gives organizations visibility and access control over the users who leave them most exposed to risk.

Common high-risk access scenarios include:

- **Operational Technology (OT)** is crucial to many companies, and any interruption can lead to physical risk and lost revenue – making these systems a valuable target for cybercriminals. As OT systems undergo digital transformation and are increasingly targeted by bad actors, it is more important than ever to secure every connection and keep operations running safely and smoothly.
- **Connecting third parties**, like vendors, partners, and contractors, to sensitive systems is standard practice today. However, security teams have little control over these third-party users or their devices, making it difficult to manage or monitor their access. Third-party access has led to many recent cybersecurity incidents, revealing that current tools are not sufficient to protect against this growing risk.
- **Migrating employee access** can take months or even years to complete. After an M&A, giving new employees access to shared systems can leave the organization vulnerable to cyberattacks. Additionally, migrating users to cloud-based applications can leave many users frustrated by poor access policies. The common workaround of giving wide permissions to internal users makes it easier for attackers to enter and move within the network.

To address these challenges, Cyolo built the first and only Zero Trust Access platform designed to enhance organizations' security, operational agility, and user experience. Our unique technology securely connects strong identities to applications with continuous authorization, in contrast to traditional solutions that only connect users to networks.

Beyond enabling secure access to all environments, the Cyolo solution empowers organizations to take back control of their data and resources. Only Cyolo gives security and IT leaders the access, connectivity, and oversight controls they need to securely enable their business while simultaneously lowering the risk of the most complex access scenarios.

Cyolo Key Visibility and Access Controls

ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- Control **Activity Permissions**
- **Terminate Connection** once work is completed

OVERSIGHT CONTROLS

- Full **Audit Trail** & complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery** for **Business Continuity**

Cyolo is on a mission to prevent the high-risk access nightmares that can cause enormous damage to businesses. With Cyolo as not just a vendor but a true partner, organizations gain the power to secure all types of users and enable their business for whatever lies ahead. Securely connect everyone to everything they need, from anywhere – no exceptions.

> "Since we changed to Cyolo, we're much more agile. I get people on quicker; I can secure my platforms and my estates much easier, and I've got much more control over who can get on, who's doing what, and then we've got more visibility into what's happening."
>
> **— Jason Ozin**
> *Group Information Security Officer, PIB Group*