Cyolo

Preventing Your High-Risk Access Nightmares

As cyberattacks have grown more sophisticated, hackers no longer break into systems; they log in with stolen credentials.

The threat is real, even to organizations with strong security measures in place. There are certain connections the business needs even though they present substantial risk. These are known as High-Risk Access scenarios, and they pose a challenge to companies everywhere. To prevent potentially catastrophic damage, security and IT teams urgently need greater visibility and control over these high-risk connections.

Some common High-Risk Access scenarios include:

- **Connecting third parties**, like vendors, partners, and contractors, to sensitive systems is standard practice today. However, security teams have little control over these external users and their devices, making it hard to manage or monitor their access. This has led to many recent cybersecurity incidents, revealing that current tools are not enough 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 can make it easier for attackers to enter and move within the network.
- **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 become digitized and more frequently targeted by bad actors, it is important to secure every connection to keep operations running safely and smoothly.

To address these challenges, Cyolo built the fastest and most secure Zero-Trust ~~Network~~ Access (ZT~~N~~A) solution. Leveraging the expertise of its founders – a seasoned CISO and two ethical hackers – the team designed a powerfully simple access platform, capable of meeting the unique needs of any environment. With Cyolo, security and IT leaders finally have the controls they need to securely enable their business and lower 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 high-risk access nightmares. Cyolo Zero Trust ~~Network~~ Access gives security and IT teams the power to securely enable their business for whatever lies ahead. It's the only true zero-trust access solution that securely connects 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*