Cyolo

Driving Digital Business with **Modern Authentication**

Securely connect users to just the right assets, with just the right access permissions anywhere, anytime. Delivering and managing secure access and connectivity to technology resources and applications is essential to achieving business goals in today's digital world. Mission-critical assets and applications are accessed by different people from an increasing number of locations every day. As the shift to cloud technologies enables greater business agility and productivity along with increased remote access, IT and security teams are now facing a barrage of complicated challenges. And these challenges are not expected to dissipate as the cyber threat landscape continues to evolve.

Meanwhile, the growing rate of remote user access worldwide has made the network perimeter obsolete. And keeping enterprise IT infrastructure and mission-critical assets secure with Virtual Private Networks (VPNs) and firewalls is just not enough anymore, as these technologies were never designed to support the tremendous strain now placed on them.

Innovative technologies can empower organizations to shift towards secure access and connectivity using modern authentication of a single, digital identity for every user. Access control and management is supported by best practices and the compliance standards of the National Institute of Standards and Technology (NIST) and zero-trust frameworks.

"Challenges are not expected to dissipate as the cyber threat landscape continues to evolve."

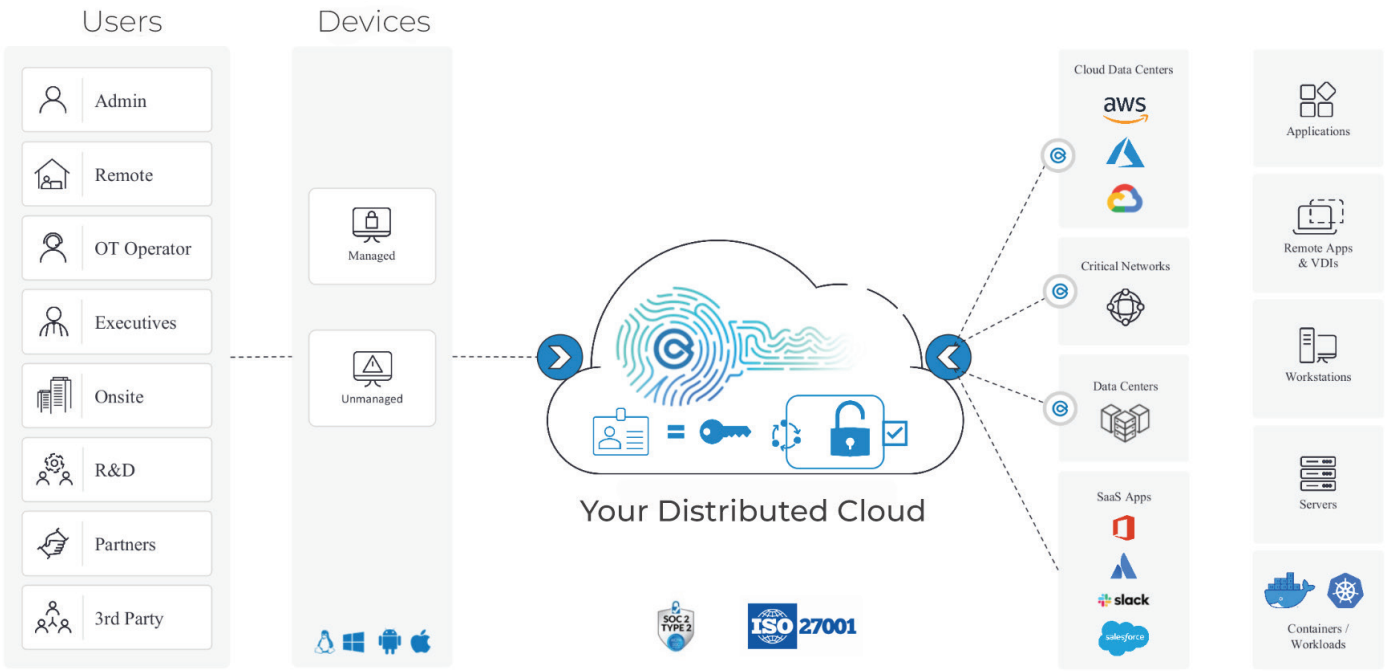
INNOVATIVE TECHNOLOGIES

enable secure access and connectivity using ***modern authentication*** of a single, digital identity for every user.

Enable the Digital Workforce

This work from anywhere model makes plain the need for identity-based access and connectivity. Again, the limitations of traditional remote access tools based on the perimeter security model, like VPNs and firewalls, are now clear. The more people work from anywhere, and the more 'Bring Your Own Device' (BYOD) policies proliferate, the less effective the traditional perimeter-based approach becomes.

The network perimeter has dissolved; people are the new perimeter.



Identity is the New Access Key

Cyolo's identity-based secure access solution connects users to the necessary resources with just the right permissions, based on individually authenticated identity. Click on the needed application, whether on-premises, private cloud, or public cloud, and connect securely following identity verification. Admins grant specific users access to specific content, applications, and resources, connecting to each with a single set of credentials. Cyolo's identity authentication ensures users access only what they need, and that precise permissions and policies are enforced. By simply and securely connecting entities to applications, the attack surface is minimized, and users easily comply with security controls.

Modern Authentication for the Digital Enterprise

- User identity is authenticated for secure application access
- Each device is verified to ensure adherence to access policies
- Deploy Single Sign On (SSO) and Multi-Factor authentication (MFA) for legacy applications

Cyolo helps organizations meet modern compliance and security regulations, extending cloud 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. Organizations stay compliant and ready for security assessments and qualify for cyber insurance with greater ease.

Confidence and Control for the Digital Enterprise

Cyolo's Identity-Based Access Control Solution Aligns with NIST and Zero-Trust Initiatives.

Cyolo's identity-based access control solution addresses both zero-trust and National Institute of Standards and Technology (NIST) requirements, with security focused on identity, instead of networks. Aligning with standards, Cyolo's solution continuously monitors all user access requests to any resource, on-premises or in the cloud. Enforcing compliance requirements and policies is made simple with audit trails and session recording identifying anomalies and minimizing risk.

Cyolo's true zero-trust architecture is founded on the principle *never trust, always verify*. Customer data and traffic is never visible to the platform or stored in the Cyolo cloud. Customers are never asked to trust Cyolo with their data and traffic. Any data stored in the Cyolo cloud remains encrypted and Cyolo never has the decryption key. What happens if Cyolo is breached? Customer data remains secure and in their hands.

Fast, Simple & Secure Access

Cyolo connects users to local or remote resources from anywhere, in any way needed, and across any device. Cyolo will seamlessly converge networks during M&As and other digital transformation transitions, powering connectivity for onsite and remote workers. Agentless and agile, Cyolo extends modern authentication to legacy and native client applications, deployed near effortlessly in any environment. Working with the existing tech stack allows deployment to be ***simple and secure.***

With Cyolo you get immediate secure access and connectivity with one line of code, a few clicks, and a 10-minute deployment. Now users can connect safely to work without compromising security or access controls.