

# Unique Value Proposition

Companies using Virtual Private Network (VPN) technology should consider shifting to Zero Trust Access (ZTA). ZTA offers granular control over who gets access to what and when, unlike VPNs which grant users access to the whole network. This means that businesses can authenticate and authorize users based on their credentials and determine exactly which resources they should be permitted to access.

## What's the difference between ZTNA and VPN?

Virtual Private Network (VPN) and Zero Trust Network Access (ZTNA) each offer secure network access options but differ in the way they are implemented. VPNs use encrypted tunneling to establish a secure connection between two points while ZTNA leverages user authentication and authorization processes to limit access to approved networks or applications.

VPNs provide users with access to an entire corporate network, while ZTNAs provide targeted access depending on user identity verification. This means that instead of granting a user access to the whole network, with ZTNA you can determine which resources the user should have access to based on their credentials. Overall, ZTNA offers more granular control over who gets access and when, making it a more secure option for those looking for heightened security measures for their networks.

# Major Key Differentiators that separate Cyolo from the competition:

## Who's got the keys?



What is zero trust? Well, trusting any third party with your encryption keys definitely isn't zero trust. In fact, it's antithetical to zero trust, as it makes whoever holds such keys the logical target of bad actors. Cyolo's architecture is definitively differentiated on this point. It's why the company was created. To be clear, Cyolo isn't ZTNA (Zero Trust Network Access). It is ZTA (Zero Trust Access). The network is physically and logically air-gapped.

## Coverage for the tough stuff – legacy infrastructure



Whether we're talking ZTNA or ZTA, Cyolo's best competitors are optimized for modern, cloud-based SaaS –and that's not a bad thing. However, why can't you have your cake and eat it too? While Cyolo is also optimized for cloud-based apps, its architecture was developed to ensure coverage for legacy applications. This is a huge point of differentiation. It allows Cyolo room to prove its mettle in the areas its competitors don't support. Put simply, it supports a land and expand strategy.

## Less network latency than competition



Cyolo is typically 30% faster than its competitors for the reasons stated above. In fact, Cyolo's competitors generally have reseller agreements with network service providers, as their solutions require the client to acquire more bandwidth.

## More granular controls and policies



All of the best solutions support more granular controls, policies, etc. But they're only as good and/or only extend to covered systems. Context is important –and policies governing who needs to access what should be relevant across the entire infrastructure –not different sets of rules for multiple infrastructural segments.

## Fast and easy to deploy



For most companies, Cyolo installs in under an hour. For larger enterprises with wildly distributed infrastructure and multiple, disparate user groups –including third parties– Cyolo can still be up and effectively running in hours. Bottomline, there is almost no change management required from both user and administrative perspectives.

## Cyolo vs competition:

	Cyolo	Zscaler	Palo Alto Networks	Umbrella - Cisco	Perimeter 81	Cato	Traditional VPN
Doesn't require customer encryption keys	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Covers the last mile (legacy) applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Session recording and supervision	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fast and easy to deploy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Internal Workforce remote access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Extended workforce remote access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Bring Your Own Device	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Privileged Remote Access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## Complementary Solutions

**MFA** - Many companies are using Okta for Multi Factor Authentication. While MFA demonstrably helps to ensure secure access, it does not provide actual connectivity to most systems and applications. Cyolo connects directly to Okta for identity verification, giving verified users access to your network.

**EDR (Endpoint Detection & Response)** companies like CrowdStrike or Carbon Black ensure real-time, continuous monitoring of endpoints with data analytics and rule-based automated responses, and is quickly becoming an industry standard. While EDR solutions do not offer network access, they do offer endpoint specific protection in case authenticated users download malicious software.

### About ALPS

Acadia Leadership Partners, INC (ALPS) is a network of industry professionals bringing vetted technologies to the market. To learn more about our B2B Marketplace, visit [acadialps.com](http://acadialps.com), or contact [Sales@acadialps.com](mailto:Sales@acadialps.com)