# Shared Services Security Requires Shared Security Responsibility

Critical applications and workflows are rapidly moving from corporate-owned data centers to the public or hybrid cloud. As a result, security leaders need to reconsider legacy assumptions of trust around people and data center security tools, technologies, processes, and skills.

For this reason, ALPS has partnered with Cyolo, a company whose zero-trust network access (ZTNA) solution is market leading.  In short, because we view ZTNA capabilities as “non-negotiable,” meaning we see its adoption as inevitable, we are recommending Cyolo to our clients for immediate evaluation.

Not only does Cyolo solve the authentication complexities and secure remote access problems for organizations that still use Virtual Private Networks (VPNs), but it delivers access to legacy applications and resources, serving to finish the job of the first generation ZTNA solutions that many of our clients have already implemented.

We are also bullish because ZTNA is foundational to Secure Access Service Edge, also known as SASE -- pronounced "sassy.” SASE is a cloud architecture model that unifies network and security-as-a-service functions as a single cloud service. In other words, ZTNA is not only strategic, but there’s a consensus supporting it as the first logical step in the journey.

Delivering shared services to a growing remote workforce has not only created new cybersecurity risks but magnified old ones.

## The Background

The pandemic has driven cloud adoption and changed how end users gain access to resources. While traditional IT infrastructures were built around perimeter controls, modern approaches require an entirely different approach, as they realize the traditional perimeter is gone. Zero-Trust (ZT) ditches the perimeter-centric security paradigm where everything inside the perimeter is inherently secure (e.g., VPNs, DaaS, Virtual Desktop Infrastructure) in favor of an approach where no device or connection is inherently trusted. Capturing its benefits requires a fresh perspective that acknowledges end-users as the new perimeter.

Put simply, shifting from traditional perimeter-focused security administration to identity-policy-based controls (i.e., ZTNA) is essential to managing secure access by employees and third parties, regardless of how they choose to access resources or from where. In other words, ZTNA's benefits are not limited to remote users. Internal users can be managed the same way.

## Modern Authentication to Prevent Modern Cyberattacks

The idea is to safely connect people to work – everyone, everything, everywhere—which is why we are recommending Cyolo. For companies that rely on the quality, breadth, and security of the resources they make available to internal, external and third party workers, , the value is timely and beneficial on many levels.

## Single Sign On (SSO)

For as long as users have been forced to supply their credentials for the variety of applications and platforms they need to access, vendors have invested in finding ways to simplify authentication through some form of single sign-on (SSO).

To make this happen, meaning to authenticate users in a fashion that authorizes their access to all the resources they need, a cumbersome mix of technology has been required. It includes technologies such as password synchronization, Active Directory, identity management with credential caching, and federation.

Cyolo's SSO capability eliminates the need for users to enter credentials every time they want to access an application or resource. Instead, they are transparently authenticated and validated through Cyolo's vault where user information, credentials, and/ or certificates are stored and logically correlated. Every digital asset receives a digital fingerprint, so Cyolo clients can analyze how resources are being used. Live and recorded session monitoring is also supported, so an audit trail for specified transactions can be maintained.

## Last Mile Coverage

And finally, Cyolo's coverage is not limited to modern cloud-based SaaS applications.  Unlike competitive products that are promoted as "optimized" for these environments, as they do not provide legacy coverage, Cyolo is agnostic to where the asset is located or how it is hosted. Therefore, Cyolo is often implemented as the "last mile solution" by organizations that have already implemented previous generation ZTNA solutions.

## Benefits Summary

**“Zero-Trust as-a-Service”**
By eliminating password usage, organizations can control who has access to its systems and reduce the threat of breaches. Passwords pose risks: workers reuse them and do not like to change them. These make passwords easy to crack. Cyolo’s SSO capability overcomes this danger, by eliminating the need for users to remember passwords, and adding appropriate authentication factors.

**Better User Experience**
One of the reasons users reuse passwords is because remembering and re-entering unique passwords is annoying and time-consuming. SSO creates a seamless user experience by enabling users to access applications immediately, with all the authentication heavy lifting taking place in the backend. Furthermore, because Cyolo does not impact quality of service, application performance is not degraded.

**Organizational Governance for Controlled Access**
Properly defining and setting up the governance structure for shared services continues to be a key success factor for the organizations that rely on them, as the underlying control architectures tend to be reactive, if not fluid. For example, Banks, Financial Services organizations, and Insurance companies can centralize their authentication policies and gain control over who can access their assets and whose permissions should be revoked. Onboarding and offboarding independent agents can become an automated process. This not only enables credible governance over how shared services are used but it dramatically improves the organization’s overall security posture, arming it with a clear audit log of who accessed what, when, and where.

**Employee Productivity**
Cyolo saves time by eliminating the friction of authentication and access. The business of authenticating users happens before they are provided access to valuable assets and applications. Every time a user wants to access an application, a token is transparently used to validate their identity. Passwords cannot be used to login and because identities cannot be switched, secure access is ensured. Cyolo provides its own SSO capability (out of the box) and/or can leverage the client’s SSO system if it has already invested in one. Cyolo enables “always on” access providing its customers an incentive to increase services that drive value, instead of constraining them based on security concerns.