Plug Your MFA and Okta Gaps
with a Secure and User-Friendly Solution

Multi-factor authentication (MFA) does an excellent job of lessening the risk of credential-based attacks, which have become commonplace. The challenge is that most MFA solutions are limited to supporting modern authentication, or SAML. Yet many organizations have a plethora of applications and systems that users and third parties need to access and which do not support SAML. These applications require things like RADIUS, NTLM, and even good old basic authentication. Just think about Windows and Linux servers, legacy client server applications, privately hosted applications, etc.

What this means is that users need to access and authenticate to different applications in different ways. Unfortunately, we all know what happens when things become too complicated for users – they take shortcuts and/or make mistakes, ultimately leaving your organization vulnerable to malware, ransomware, and data breaches.

Cyolo adds all of your non-SAML based applications and systems to your Okta or other identity provider (IdP) portal. Cyolo also includes back-end single sign-on (SSO) access to these applications. Now, your users can connect to all the applications they need from their Okta or IdP portal with one simple, frictionless way to strongly authenticate. Chief among the many benefits of this approach are happier users and fewer support tickets.

In addition, Cyolo provides all users with zero-trust access, ensuring that application traffic is hidden from the internet. This dramatically reduces the organization's attack surface and gives IT and security teams a single place to quickly provision access and get visibility and control of who has access to what.

Okta and MFA are great out-of-the-box authentication solutions for SaaS and web-based applications. But what happens when you need to access applications and systems that they do not support?

Cyolo integrates seamlessly with your existing application portal. Your users continue using the same system they are accustomed to – only now all applications are accessible in one place.

CYOLO + OKTA/MFA ENSURE:

MFA AND SSO FOR EVERY APP

Cyolo secures your entire organization by extending MFA protection to applications that are not natively supported, like server-based or client-server based apps.

ZERO FRICTION

Cyolo simplifies the user experience by enabling users to access any application from the IdP portal they already know. IT and security teams manage all permissions from a single, intuitive system, enabling them to provision application access in minutes.

## SECURE THIRD-PARTY CONNECTIONS

Cyolo and Okta together secure access for third parties and your supply chain and enforce the principle of least privilege for all users. Cyolo also offers supervised access and session recording capabilities for added security.

CYOLO AUTHORIZATION FROM A USER'S POINT OF VIEW

STEP 1 - LOGIN

Users log in to their existing Okta or other IdP portal.
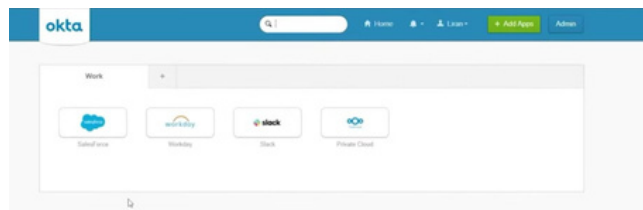
- User experience doesn't change
- No training or onboarding required
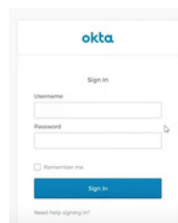
STEP 2 - VIEW ALL APPS

Users will see their SaaS applications as usual, as well as new apps not traditionally available via OKTA courtesy of Cyolo applications.
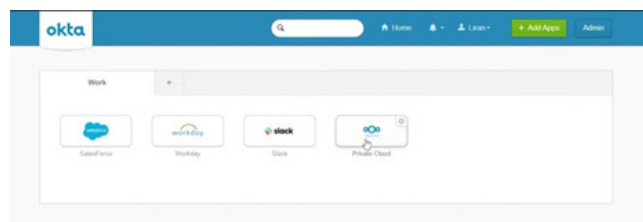
- All organizational apps accessible from a single platform
- Zero friction
- Enhanced security - MFA and SSO to every app

STEP 3 - CHOOSE THE APP

The user simply clicks on the desired app to get access. In the background, Cyolo provides a connectivity and authorization layer.
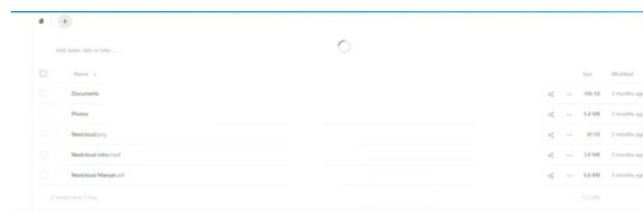
- Simplified access
- No slow, bulky & insecure VPNs
- MFA and advanced authorization for all apps

STEP 4 - GET TO WORK

Users can work on their private applications while Cyolo saves IT and Security teams time with enhanced control and visibility.

- Visibility and control
- Business agility
- No friction
- Compliance

Cyolo brings secure, seamless connectivity to your whole organization.