

# Cloudflare and Okta

Simplify access controls and protect applications against threats



## Securing Remote Access Creates Friction

Remote and hybrid workers need seamless access to enterprise applications to maintain productivity. However, the authentication process must also be robust to prevent unauthorized access. Zero Trust security can protect applications and networks while maintaining a simple single-sign-on (SSO) experience that reduces friction.

## Adopt Seamless Zero Trust Access

Okta identity and access management combined with Cloudflare's Zero Trust network security makes it easy for employees to access internal applications from anywhere. The integration provides consistent, easy-to-manage controls across identity, device, and network security while enabling access on a per-user basis. Web-based applications don't require modification, and onboarding typically takes less than ten minutes.

## Share Risk Scores and Take Action Automatically

Configure Okta to use Cloudflare risk scores and automatically enforce policies based on user risk. This lets organizations adapt to evolving threats faster with less manual effort.

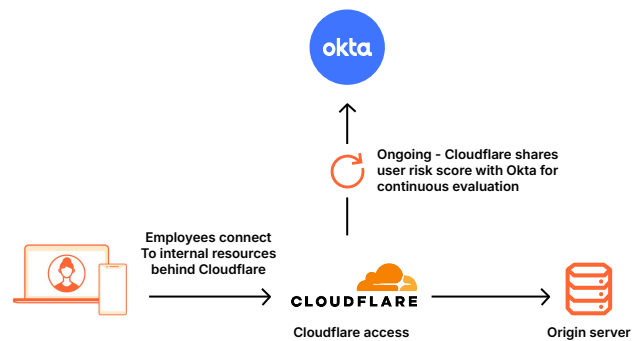


Figure 1: Cloudflare/Okta Integration

Employees connect to Cloudflare using Okta authentication before accessing internal applications.

## Unified Dashboard and SIEM Support

Monitor and search user access or change logs in real time via the Cloudflare dashboard or integrate with third-party SIEMs. With Okta and Cloudflare, your remote workforce stays connected to the apps they need without delays or disruptions



### Accelerate Deployments

Onboard new applications and communities in minutes with centralized application access controls.



### Block Identity Threats

Authenticate with Okta before providing access to internal resources. This prevents data breaches and keeps you protected.



### Anywhere, Any Device

Every individual network request is authenticated, with access granted only to compliant and validated devices.