

# Extend the identity perimeter to your disconnected apps for enhanced security and governance

As organizations rely on an ever-growing tech ecosystem to run their businesses, security gaps caused by disconnected apps have become a major challenge. While standards like SAML and SCIM are widely recognized, [the reality is that 30-80% of apps are disconnected](#), meaning they do not support these protocols. These apps slip through the cracks of your secure identity perimeter, leaving organizations exposed to risks and driving up costs with manual management.

This is where Cerby steps in to seamlessly integrate with Okta, extending identity security to every corner of your application ecosystem—whether it's SaaS, legacy, on-prem, or a homegrown app. With Cerby, your IT team can easily deploy SSO, MFA, and lifecycle management to all those tricky apps, boosting security, visibility, and control.

## The challenges with disconnected apps

- ✘ **Security blind spots**  
Apps outside the reach of your identity provider create security vulnerabilities that can be exploited by attackers.
- ✘ **Inefficient processes**  
IT spends valuable hours manually managing access controls, diverting resources from strategic work.
- ✘ **Lack of visibility**  
IT has a fragmented view of users and their apps, making it challenging to monitor access and ensure compliance

## The Cerby + Okta Solution

### Seamless, secure access for disconnected apps

- Enable users to log in with SSO and FastPass, even to apps that don't natively support standards
- Enforce the strongest form of MFA supported by each app automatically

### Automated identity management for apps without APIs and SCIM

- Streamline user provisioning and deprovisioning, driven by Okta roles and groups, ensuring changes in access rights are immediately reflected across all apps
- Enable one-click access termination across all supported apps, improving security operations and incident response processes

### Enhanced security for shared privileged accounts

- Automatically enforce MFA for shared administrator accounts to prevent unauthorized access
- Instantly revoke privileged access by auto-rotating passwords when users are deactivated in Okta
- Monitor shared account access at an individual user level for improved accountability

### Complete visibility and control over your app ecosystem

- Centralize oversight of previously disconnected apps, bringing them into full view for greater security and control
- Turn previously dark signals into actionable intelligence, feeding crucial identity data directly into your SIEM

“Using Okta and Cerby, we have eliminated our risk exposure and it’s given us an easy way to govern our accounts.”

— Alexander Schuchman  
CISO



## The benefits



### Strengthened security

Extend modern identity protection to every app, closing security gaps.



### Enhanced IT efficiency

Automate identity and security workflows, freeing IT for strategic initiatives.



### Reduced costs

Cut the “SSO tax” by centralizing access management, lowering manual efforts and extra licensing fees.

## Getting started with Cerby and Okta is easy

- Configure SAML and SCIM with your Okta tenant using the Cerby app available in the Okta Integration Network (OIN).
- Set up your security policies in Cerby.
- Leverage Cerby’s catalog of pre-built integrations to connect any non standards-based app—no custom connectors required.
- Provide your workforce with seamless access through the Cerby app within their existing Okta dashboard, with both web and mobile clients.
- Enable IT to centrally manage access, achieving full visibility and control over your entire app ecosystem.

### About Cerby

Cerby offers IT and Security teams the only identity and access management platform tailored for disconnected applications. Seamlessly integrating with your existing identity provider, Cerby extends SSO, MFA, and lifecycle management to any application, even those without APIs or support for standard protocols. With Cerby’s patent-pending identity automation, IT teams can streamline manual processes like deprovisioning and MFA enrollment, gaining unmatched efficiency and full visibility and control over applications that fall outside traditional identity systems. Cerby empowers identity teams to extend access controls, mitigate risk, and reduce costs.

