


Modern identity security for nonstandard applications

Extend your reach, not your budget


The most significant threats facing organizations today are from the human element, like credential reuse. Applications that can't be connected and managed through your identity provider fall into this category. Verizon's June 2023 Data Breach Investigations report found that "74% of breaches involved the human element, which includes social engineering attacks, errors or misuse." These attacks, as well as the common approach of phishing, target ways to capture user credentials of either privileged or non-privileged users. Even if you've invested significantly in your identity provider, universally leveraging security standards is challenging. Estimates reveal that 30-50% of organizations' applications support SAML or OIDC for user authentication and less than 10% support API endpoints or SCIM for user management.


Cerby detects and remediates the following risks:


- Disabled 2FA
- Unsecured privileged accounts
- Freemium and paid SaaS sprawl
- Password reuse
- Nonstandard app access




Activity Log					
Time	Event	Account	User	Location	Browser
	Request Access		Charlie Levy		Internet Explorer
	Login		Charlie Levy		Google Chrome
	Post		Charlie Levy		Mozilla Firefox
	Share Access		Charlie Levy		Safari
	Rotate Password		Charlie Levy		Opera
	Rev				
	Ter				
	En				
	Re				
	Log				

**Secured accounts**
1,285

**Not fully secure**
12

**Active Users**
12

**Inactive accounts**
4

“

We are impressed by Cerby's approach to facilitating distributed access management for traditionally unmanageable applications, allowing users and IT to complement each other's efforts.

- Lana Farrand

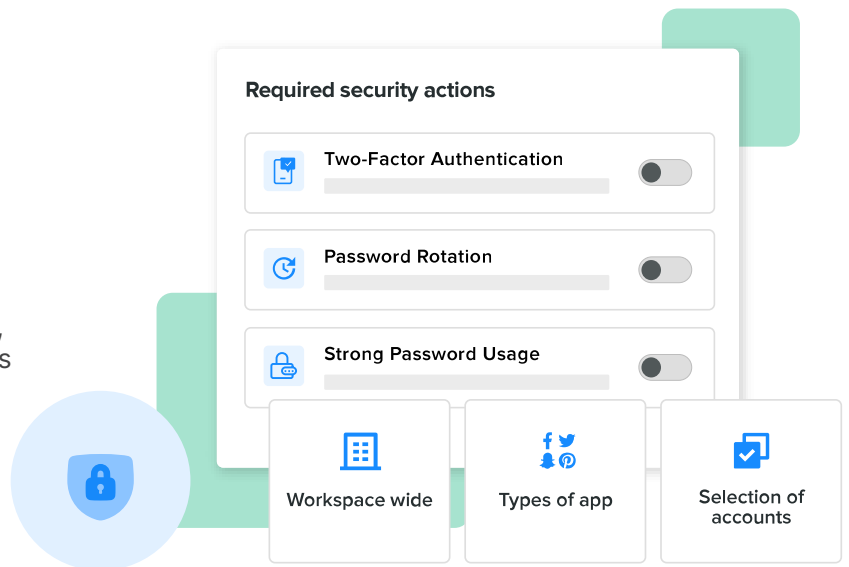
Executive Director, Information Security
Fox Corporation

Extend access

Cerby's access management platform extends single sign-on (SSO) and lifecycle management capabilities to any application, regardless of its support for modern protocols.

Reduce risks

When employees onboard applications into Cerby, it automatically corrects security misconfigurations like weak passwords and disabled 2FA. With Cerby, reliance on manual, employee-driven actions to maintain compliance and security becomes a thing of the past.



Lower costs

Cerby provides a more efficient and cost-effective approach to access management and security, helping companies save money while improving their security posture.

Cerby key capabilities

Automate user onboarding and offboarding

- Link employee creation or removal events in your identity provider to any application. Cerby is the bridge between your identity provider and nonstandard applications.

Passwordless authentication for nonstandard applications

- Employees logged in with their corporate identity can seamlessly access nonstandard applications registered in Cerby without ever needing to know their usernames and passwords.

Automatic password rotation

- Cerby eliminates manual password rotations and can trigger rotations based on policies, SCIM events, or on-demand.



Why Cerby?

- Reduce risk from manual security tasks
- Centrally manage access to any app with your identity provider
- Gain 100% coverage of your app estate
- Achieve passwordless authentication for nonstandard apps
- Automate manual compliance tasks

Trusted by organizations around the world



About Cerby

Cerby provides identity teams with the only comprehensive access management platform for nonstandard applications. Harnessing the power of identity providers, Cerby removes the need for enterprise password managers by extending single sign-on (SSO) and lifecycle management capabilities to any application.