cerby®

SOLUTION BRIEF

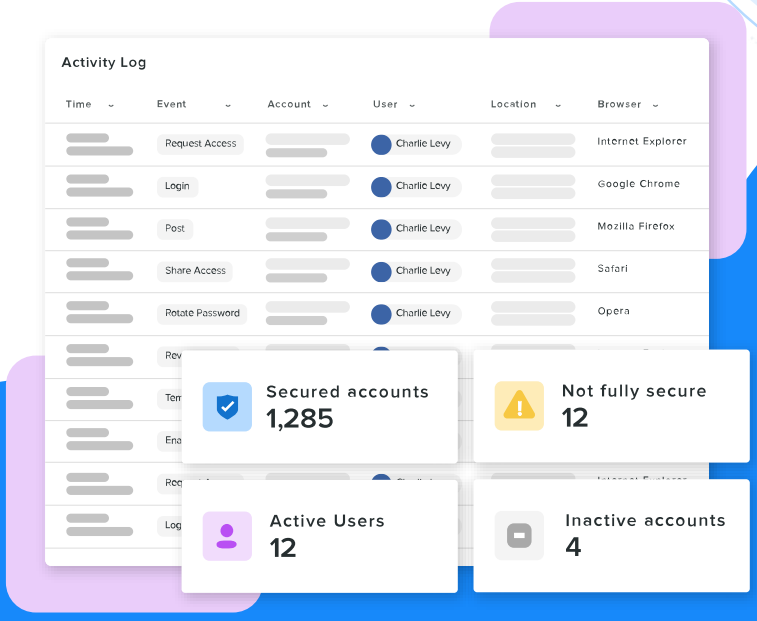
Access management for nonfederated applications

Extend your reach, not your budget

The most significant threats facing organizations today are from the human element, like credential re-use. Applications that can't be connected and managed through your identity provider (nonfederated) fall into this category. Even if you've made significant investments in your identity provider, you are fighting a losing battle. Only one out of three applications supports SAML, and less than one in ten supports SCIM[1]. Time and resources across your organization are wasted on manual security tasks like offboarding, and security and compliance are at risk with the growing number of nonfederated applications.

Cerby detects and remediates the following risks:

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



> 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*

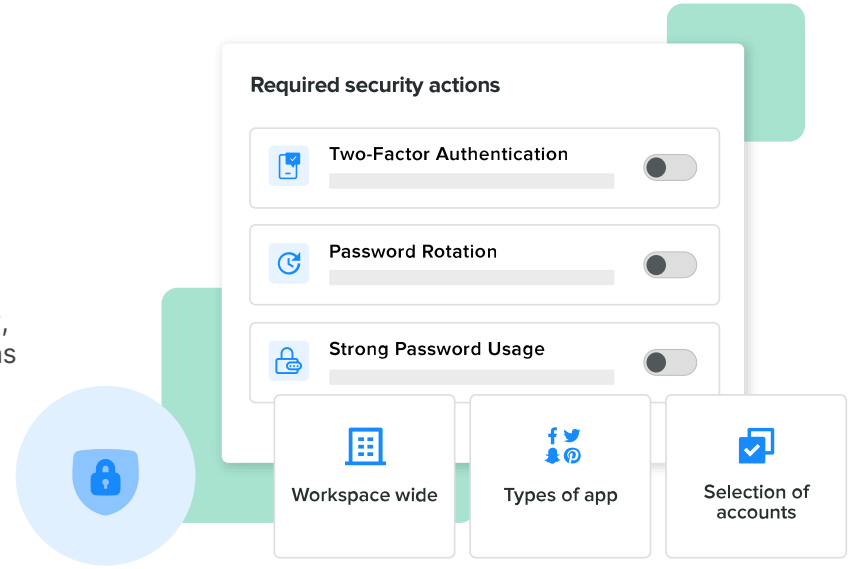
[1] *"Out of the shadows." Cerby, June 2022, https://www.cerby.com/resources/blog/out-of-the-shadows*

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 systems like Okta or Azure AD to any application. Cerby is the bridge between your identity provider and nonfederated applications.

Passwordless authentication for nonfederated apps

- Employees logged in with corporate SSO credentials can easily access nonfederated apps registered in Cerby. No password required.

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 IdP
- Gain 100% coverage of your app estate
- Achieve passwordless authentication for nonfederated apps
- Automate manual compliance tasks

Trusted by organizations around the world

FOX · WIZELINE · COLGATE-PALMOLIVE · Televisa · dentsu · Coppel · crunchyroll

About Cerby

Cerby provides identity teams with the only comprehensive access management platform for nonfederated 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.

cerby®

Experience Cerby. Get a demo at cerby.com/demo