cerby

Privileged Access Management

Secure privileged accounts in disconnected applications

Disconnected apps leave privileged accounts exposed and at risk. Without native integrations, IT can't apply standard identity controls, leaving shared credentials, standing access, and unmanaged admin sessions without proper monitoring or auditing. These gaps create serious security and compliance risks.

Cerby eliminates these risks by delivering just-in-time access with zero standing privileges, automatically granting admin rights only when needed, then revoking them immediately after. Credentials are rotated behind the scenes, access permissions update in real time as roles change, and every session is attributed to the individual who used it, even in shared account environments.

With Cerby, security teams eliminate manual credential processes, gain complete visibility over privileged access, and bring disconnected apps under PAM governance, without custom integrations or workflow workarounds.

> When dealing with privileged service accounts and apps outside of SSO coverage, we needed better security, visibility, and auditability", "Cerby delivered on all three.
>
> William Levie
> Sr. Manager, IT & Facilities Operations
>
> Productiv™

The Cerby Solution

Full Control Over Privileged Accounts

Bring disconnected apps into PAM

Apply PAM policies to disconnected SaaS, cloud, and admin apps that are accessed with privileged, shared accounts. Cerby enforces privileged access controls with backup to your PAM vault.

Replace standing privileges with just-in-time access

Automatically grant and revoke privileged access based on identity and policy—no permanently shared credentials or standing admin rights.

Eliminate manual privileged account workflows

Automate access provisioning, revocation, credential rotation, and policy enforcement, freeing teams from tickets and reducing risk.

Capture complete audit trail for shared accounts

Attribute every privileged session to a specific user, even for shared logins, supporting audits and closing compliance gaps.

cerby

Cerby Features & Capabilities

Just-In-Time Access Controls

Grant time-limited privileged access based on need, removing persistent credentials and risk.

Automated Deprovisioning & Credential Rotation

Revoke access and rotate passwords automatically as roles change, no manual intervention required.

Zero-Knowledge Access Enforcement

Allow secure credential checkout without ever exposing passwords.

Audit Logs

Capture logs for every privileged access event, even for shared accounts, for full accountability & compliance.

Disconnected Privileged Account Coverage

Extend privileged access governance to SaaS, cloud, and administrative apps.

Automated MFA Sharing

Route MFA codes directly to authorized users via Cerby-managed channels.

> Cerby is one of the few companies addressing the challenge of managing disconnected apps," "Most solutions ignore this issue entirely. But by combining Cerby with Okta, we now have comprehensive access controls and governance across our entire app ecosystem, without gaps.

Josh Mullis
VP of IT & InfoSec
Productiv™

COLGATE-PALMOLIVE FOX WIZELINE L'ORÉAL dentsu

About Cerby

Cerby is the only identity security platform built for disconnected applications, providing IT and Security teams with comprehensive control over apps that lack APIs or support for protocols like SAML or SCIM. Seamlessly integrating with existing identity providers (Okta, Azure AD, etc.), Cerby extends critical security automations—such as single sign-on, multi-factor authentication, and lifecycle management—to any application without incurring the costly "SSO tax." Cerby automates essential tasks like user deprovisioning and password rotations, reducing manual work while closing security gaps. With Cerby, teams gain full control over their app ecosystem, strengthen security, and reduce costs.

Visit us at Cerby.com and follow us on social at @CerbyHQ.