cerby®

SOLUTION BRIEF

Automate user provisioning and protect authentication credentials for decentralized SaaS management

Identity standards should be leveraged for secure authentication and automated user provisioning. However, innovative SaaS technologies tend to delay the support of identity standards like SAML, OIDC, and SCIM because of resource constraints. As a result, to drive business outcomes, many business department leaders may purchase hot new software that require the good ol' username and password to access the application. These applications are also known as "nonstandard applications" and are often managed in a decentralized manner.

Reduce identity fragmentation, enable user provisioning for decentralized SaaS

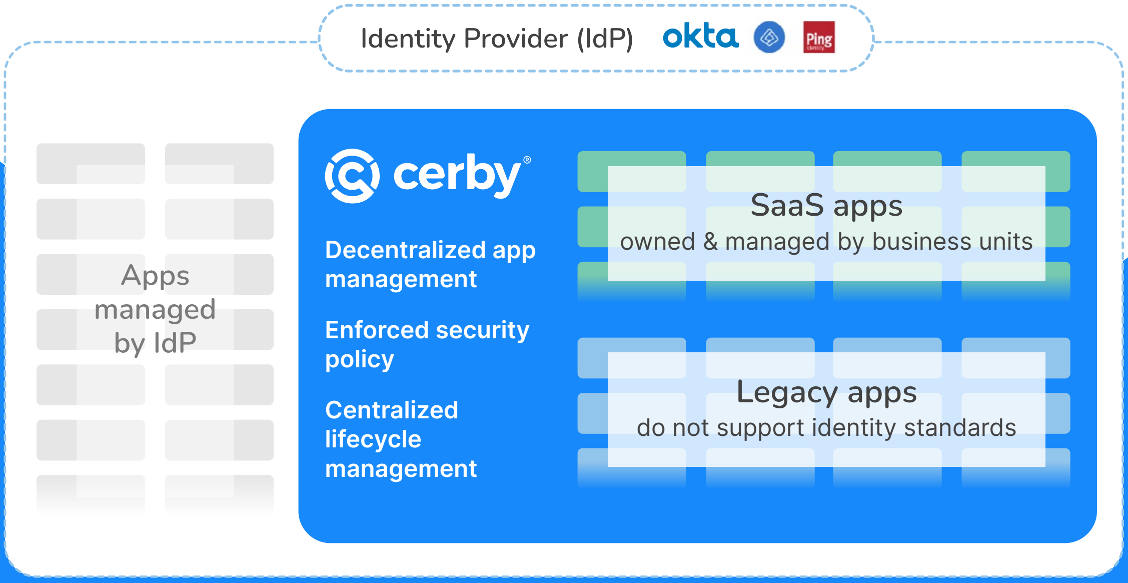
With an identity-first security strategy, IT and security teams need an integrated ecosystem of technology to ensure the right people have the right access at the right time. SaaS purchased by business leaders often sits disconnected from this integrated ecosystem for three common reasons:

1. The software can't integrate with the center of excellence built by identity, IT, and security teams
2. Corporate policy to include IT or security review is ignored because it slows down the purchase
3. The software is low risk or low cost, so it doesn't require additional scrutiny from resource-constrained IT or security teams

According to **Gartner**, 80% of CXOs outside of IT believe digital leadership is part of their job, so they are dedicating as much as 20% of their resources to implementing and maintaining the technology their department purchases.

These department resources are usually wasted on manually provisioning and deprovisioning when employees, contractors, and external agencies join, move, or leave. Why? Because business-owned technology is often disconnected from the centralized automated provisioning process IT and security teams have built.

Cerby connects decentralized SaaS user management with identity-driven provisioning capabilities found in modern identity platforms.


Identity Provider (IdP)
okta
Ping
Apps managed by IdP
cerby®
Decentralized app management
Enforced security policy
Centralized lifecycle management
SaaS apps
owned & managed by business units
Legacy apps
do not support identity standards

Cerby capabilities

Centrally manage user access to shared logins

Time bound user access to shared logins

Reduce friction without sacrificing security for individual and shared logins

Automate security defenses like password rotation and MFA enrollment

Activity log of who used which login credentials

Integrate with secret vaults

Migrate from other EPMs

One place for your end users to store credentials and access nonstandard work apps

Go beyond password vaults that neglect the last mile of security

Every social media platform handles their ad managers Even though password vaults can sit behind an identity perimeter, they still rely on human interaction to execute the last mile of security, like password rotation and MFA enrollment. This is due to the nature of password vaults being a repository of credentials separate from the systems that users authenticate into.

While secure password vaults are better than written passwords in a pocket journal, security leaders still need a better way to enforce the parts of security policy that are currently reliant on human engagement and adoption.

With Cerby, admins can:

- **Enforce password rotations and MFA enrollment** for individual logins to business-owned apps that don't integrate with identity platforms
- **See and manage who uses shared logins.** Whether those shared logins are service accounts or corporate social media logins, admins can now see and manage who gains access using shared logins.
- **Automate the last mile of security** for shared logins. Cerby fully manages password rotations and shared MFA so these shared logins have the added layer of defense without the friction it usually introduces for the end-user.

Customers choose Cerby

> "We chose Cerby because we needed a secure and centralized place to manage access to our paid social accounts. Additionally, the automated access removal of employees who have left the company provides a level of security we did not previously have."

- Nina Donnard, AVP Paid Social at L'Oréal L'ORÉAL

> "This solution allows us to treat social media platforms like corporate applications, subject to the same security rules, including multi-factor authentication and password complexity."

- Alex Schuchman, CISO at Colgate-Palmolive COLGATE-PALMOLIVE

About Cerby

Cerby puts identity security into the hands of the business and technology workforce, enabling them to secure their applications, while working faster and more efficiently. By providing robust and dependable last mile connectivity to all applications, including centralized, cloud and nonstandard applications, Cerby ensures that identity security is everywhere your organization works. Cerby is trusted by large enterprises like L'Oréal, Colgate-Palmolive, Fox, and Dentsu, and backed by Two Sigma Ventures, Outpost Ventures, Okta Ventures, Salesforce Ventures, and more.

> "Cerby automatically logs us in using our corporate credentials and handles 2FA. No more password or 2FA code sharing. No more calls to the account holder in Japan, Australia, or the UK in the middle of the night."

- Siobhan Sullivan, Director of Global Community Marketing at Crunchyroll

crunchyroll

cerby®

Book a demo to explore how Cerby could work for you: **www.cerby.com/demo**