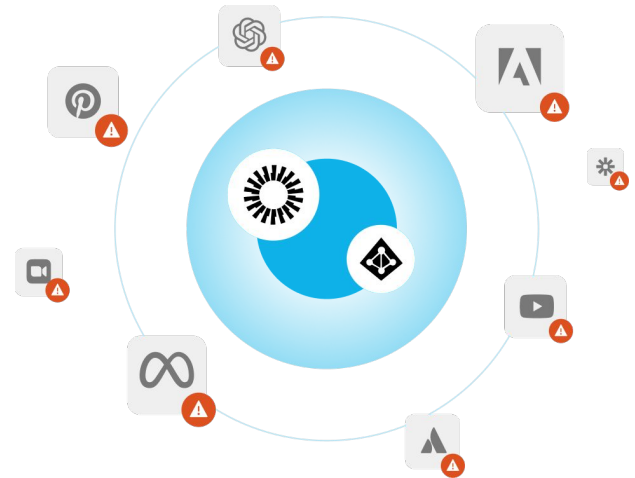


Extend identity security to your disconnected applications

As business apps proliferate—large companies now use over 300 SaaS apps on average—IT and security teams face a growing challenge: managing secure access to every app, particularly those beyond the reach of central identity providers (IdPs). These "disconnected" apps lack APIs and don't support standards such as SAML, SCIM, or OIDC, making it extremely challenging to enforce a secure identity perimeter.



The problem?

Each app outside these systems creates a visibility and control gap, leaving critical security tasks like password management and user lifecycle to manual oversight. This manual approach isn't just inefficient; it's risky. Inconsistent access controls open exploitable gaps, putting sensitive data and compliance at risk.

 **1.5-2.6x**

annual growth in attack surfaces as security tools struggle to keep up with rapid app adoption

—Censys

 **58%**

of orgs say their current security solutions cover **less than half** of their app ecosystem

—CSA

Challenges for IT and security leaders

✗ Manual security processes

Without automation, security relies on end users, leading to inconsistent practices and higher risks.

✗ Visibility and compliance gaps

Disconnected apps create blind spots, limiting IT oversight and increasing compliance risks with untracked access and lack of audit trails.

✗ The costly SSO tax

Many apps charge a premium for SSO or SCIM, forcing teams to either pay extra or rely on error-prone, manual processes that increase the risk of breaches.

Cerby automates the last mile of identity security across your app ecosystem

Cerby addresses these challenges by bringing all apps under one secure platform—no standards, APIs, or SSO tax required—and automating key security processes across apps that typically fall outside identity provider reach.

Key capabilities with Cerby



Unified access management for disconnected apps

- Centralize access management, reducing manual workload and improving IT efficiency
- Sync with identity or HR systems to manage user access and permissions based on roles — even for non-SCIM apps
- Extend SSO to any app, enhancing security and the employee experience



Advanced security automations

- Automate password rotations, user deprovisioning, and numerous critical tasks
- Enforce MFA enrollment on shared administrator accounts automatically, adding an extra layer of security for privileged users
- Reduce manual work and user dependency to strengthen enterprise security posture



Complete visibility and compliance oversight

- Detect app sprawl instantly and suggest IT-approved apps to control costs and limit proliferation
- Centralize visibility into the entire app ecosystem — even disconnected ones
- Integrate with SIEMs to transform hidden data into actionable insights, giving IT real-time intelligence on risks

The Cerby difference

No APIs or SCIM? No Problem.

Cerby secures access to all apps—no APIs or standards needed—bringing your entire app ecosystem under one secure, unified platform.

Automated Security, Zero User Reliance

Automates critical security processes, removing the weakest link—manual end-user steps—while guiding users toward security best practices and enforcing hygiene with ease.

Seamless IdP Integration

Integrates seamlessly with Okta, Microsoft, Ping, and any provider you use, extending identity security to every disconnected app and closing critical gaps in your security perimeter.

AI-Driven, Self-Healing Technology

Uses AI to detect and resolve login drift and interface changes automatically, maintaining uninterrupted integrations and cutting manual work for IT and Dev teams.

Trusted by leading brands worldwide

FOX



L'ORÉAL

News Corp

ClickUp

Productiv

elf

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](https://twitter.com/CerbyHQ).

