cerby

Top 4 Best Practices for Securing Every App in Your Ecosystem

Disconnected applications create significant security vulnerabilities by leaving critical gaps in your organization's defenses. Without visibility or centralized management through your identity provider (IdP), these applications expose your ecosystem to increased risk.

01

Audit your applications

02

Close access gaps

03

Streamline lifecycle management with automations

04

Educate and iterate

cerby

1. Audit your applications

Lack of visibility

Disconnected applications are not easily monitored and secured by IT and security teams

What to do

Comprehensively map your application landscape and identify all currently used apps. Evaluate and rank applications based on their operational criticality and data sensitivity and identify applications that lack secure authentication protocols to effectively prioritize actions.

cerby

2. Close access gaps

SSO tax

Many vendors charge extra licensing fees to unlock identity management functionality, such as Single Sign On (SSO), discouraging organizations from implementing it across all applications.

What to do

Consolidate authentication through an IdP integration and implement SSO for all compatible applications to enforce consistent security policies. For applications that lack APIs or support for standards such as SAML or SCIM, deploy Cerby to extend SSO and lifecycle management capabilities. This ensures all applications are secured under a unified identity perimeter.

cerby

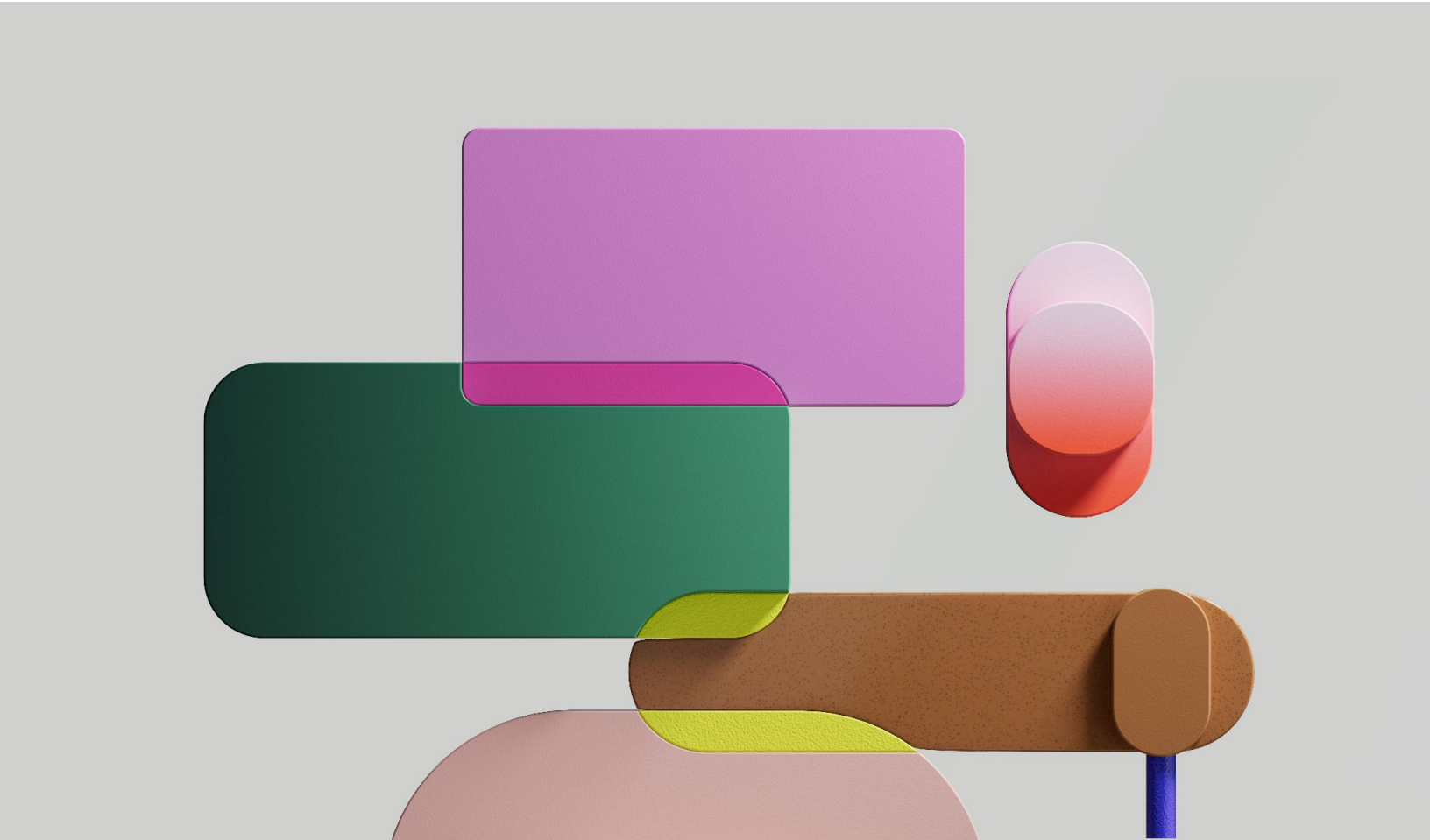
3. Streamline lifecycle management with automations

Manual management

Business users are left to manage security, increasing the risk of human error.

What to do

Streamline user lifecycle management with Cerby's provisioning capabilities and ensure coverage for all apps. Automate role-based access controls to apply appropriate permissions across the organization and ensure that deprovisioning is handled immediately and without error when user roles change.



cerby

4. Educate and iterate

Security blind spots

Without continuous education and process reviews, employees may overlook security risks in disconnected apps, potentially leaving systems vulnerable and unmonitored.

What to do

Regularly review application security processes and user access permissions to identify areas for improvement. Keep employees informed about risks related to disconnected apps, emphasize secure practices, and encourage reporting of potential security threats.

cerby

> “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

Trusted by leading brands worldwide

MATTEL · COLGATE-PALMOLIVE · L'ORÉAL · News Corp · ClickUp · Productiv™ · e.l.f.

About Cerby

Cerby is the only identity security platform designed to seamlessly manage 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.