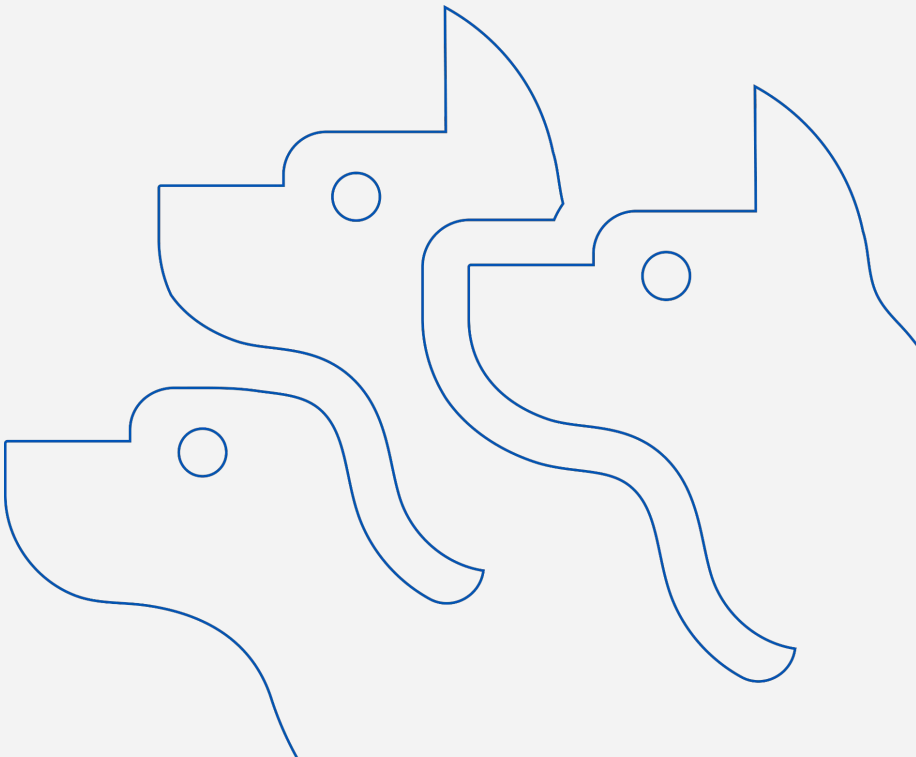
cerby

Comparison Guide

Comparing Different Ways to Secure Disconnected Applications

cerby

Table of Contents



cerby

Introduction

Disconnected applications are one of the biggest blind spots in enterprise security. These are apps that can't easily plug into your organization's identity management systems. They're not just old on-prem tools, either. Many modern SaaS platforms in marketing, finance, and social media fall into this category. And the number keeps growing.

What Are Disconnected Apps?

Disconnected apps are systems that

- Aren't managed by IT or security in an automated, centralized way
- Don't support federated authentication (like SAML or OIDC)
- Use credentials such as usernames, passwords, and sometimes MFA codes for access
- Lack support for SCIM or even APIs for lifecycle automation

For example, marketing teams rely on social media platforms like Meta, X, TikTok, and LinkedIn. Finance teams use banking and payment systems, and operations teams often depend on on-prem data tools. These are just a few examples. Disconnected apps exist in nearly every function and introduce unmanaged risk.

The Four Critical Areas of Disconnected App Risk

Aspect	What's at Stake	Typical Problem in Enterprises
Credential Management	How passwords and secrets are created, stored, and shared	Weak, reused, or shared credentials handled insecurely
Authentication	How users log in and whether MFA is enforced	Users manage their own credentials; MFA is often disabled
Identity Lifecycle Management	How users are provisioned and deprovisioned	Former employees keep access
Logging & Auditability	Whether access is tracked and auditable	No centralized visibility or logs

Disconnected Doesn't Mean Unimportant

These apps are often business-critical. Their lack of integration makes securing them even more urgent.

cerby

How Organizations Typically Respond

1. **Denial or Do Nothing**

   Some IT and security teams insist they only allow apps that support SAML and SCIM. Others let employees use whatever tools they want. In both cases, shadow IT thrives; employees create accounts, manage passwords themselves, and share credentials via chat or email. MFA enforcement? Optional. IT visibility? None.

2. **Manual Effort**

   Other organizations try to manage disconnected apps through ticketing systems, spreadsheets, or coordination via email. It's inefficient, error-prone, and scales poorly.

3. **Automation Attempts That Don't Scale**

   Some use RPA, custom scripts, or iPaaS tools to automate tasks. But these are brittle. When an API or user interface changes, the automation breaks. Maintenance is expensive, and many apps still remain unmanaged.

What This Guide Covers

This guide compares how IT and security teams can secure disconnected apps across four key areas:

Credential Management

Authentication

Identity Lifecycle Management

Logging & Auditability

It also shows how Cerby delivers complete coverage and automation at scale.

cerby

Credential Management

Credential management governs how passwords and secrets are created, stored, shared, rotated, and revoked. For disconnected apps, passwords are often the only authentication method, so this becomes a major security and compliance challenge.

Common Approaches to Credential Management for Disconnected Apps

Approach 1

Do Nothing (Users Self Manage)

In many organizations, employees create and manage credentials on their own. Passwords are often weak, reused, or shared informally across teams. They might be stored in spreadsheets, browsers, or notes apps. When people leave the company, access usually isn't revoked.

- Passwords are reused across multiple apps.
- Shared credentials circulate through unsecured channels.
- No centralized control or tracking.

⚠ Former employees often retain access indefinitely due to lack of enforced credential revocation.

Approach 2

Enterprise Password Managers (EPMs)

Enterprise Password Managers improve security by storing credentials in encrypted vaults and enforcing stronger password policies. They can detect reused passwords, generate complex ones, and reduce credential leaks. However, for disconnected apps, they only solve part of the problem:

- No automated password rotation or revocation.
- No integration with provisioning or deprovisioning workflows.
- Shared accounts might still require manual management, depending on the EPM.

cerby

Cerby's Differentiated Approach

Cerby was purpose-built for disconnected applications. These are apps that can't plug into your identity provider or governance systems. Cerby goes beyond secure credential storage to deliver full governance, automation, and auditability for these apps.

Centralized Control
Admins can define who can view, use, or share credentials —and revoke access instantly.

Automated Rotation and Revocation
Passwords rotate automatically when users leave or roles change.

Orphaned Account Transfer
Orphaned accounts are identified and can be reassigned to reduce security risks.

Policy-Based Access
Enforces least-privilege principles and corporate standards.

Complete Audit Trail
Every credential action is logged for compliance.

Comparing Credential Management Options for Disconnected Apps

Capability	Do Nothing	EPM	Cerby
Secure Storage	✗	✓	✓
Enforced Password Policy	✗	✓	✓
Secure Sharing	✗	⚠	✓
Automatic Rotation	✗	✗	✓
Access Revocation	✗	✗	✓
Admin Visibility	✗	⚠	✓
Audit Logging	✗	⚠	✓

✓ Fully Supported ✗ Not Supported ⚠ Limited Support

Why Rotation Matters
With Cerby, users never have to see or handle a password. When someone leaves, Cerby automatically rotates credentials, eliminating lingering access and the risk of password reuse.

cerby

Authentication

Authentication verifies user identity and controls access. Disconnected applications, which lack support for federated standards like SAML or OIDC, force users to rely on manual logins and personal MFA methods. This creates inconsistent experiences, weak security, and significant exposure across the enterprise.

Common Approaches to Authentication for Disconnected Apps

Approach 1

Do Nothing (User-Controlled)

Users create and manage their own credentials, often using weak or reused passwords stored in browsers, spreadsheets, or even memory. Each login becomes a security risk.

- Credentials are easy to phish, share, or steal.
- MFA is applied inconsistently or disabled entirely.
- IT and Security teams have no visibility into login events, MFA usage, or account access.

⚠ Users who self-manage credentials often create weak or reused passwords, are more vulnerable to phishing, and frequently disable MFA, leaving corporate identities exposed.

Approach 2

Enterprise Password Managers (EPMs)

EPMs improve password hygiene by securely storing credentials and auto filling login fields. They help reduce phishing risk and promote stronger passwords. But they stop short of true authentication control.

- Passwords are protected but still user-managed.
- MFA remains inconsistent and user-dependent.
- Shared accounts create friction during authentication when MFA codes are tied to personal phones or emails.
- Admins can't enforce policies around how or when credentials are used.

cerby

Cerby's Differentiated Approach

Cerby delivers seamless, secure, and policy-driven authentication for disconnected apps. Like an EPM, it retrieves credentials from an encrypted vault and logs users in automatically, but it goes far beyond that. It integrates with identity providers like Okta or Microsoft Entra ID, enabling users to launch disconnected apps directly from their SSO dashboards, creating a true SSO-like experience. Cerby centralizes authentication control under IT governance, bringing disconnected apps into the enterprise identity framework.

Policy-Based Authentication Control

Admins define how credentials are used, shared, and revoked. Permissions can restrict access to login-only mode—users can sign in, but never see or copy passwords.

Automated MFA Enforcement

Cerby enforces MFA automatically across disconnected apps, ensuring no user can disable or bypass it. MFA becomes consistent and centrally managed, not user-dependent.

Integration with Identity Providers

Cerby connects directly with identity platforms like Okta or Microsoft Entra ID, allowing IdP admins to easily incorporate tiles to disconnected apps in users' IdP dashboards.

Seamless SSO-Like Experience

Users simply click a tile on their IdP or Cerby portal. Cerby orchestrates the entire login flow, including MFA, in real time. No passwords, no manual steps, no copy/paste of MFA codes.

Purpose-Built for Shared Accounts and Social Media Platforms

Disconnected apps like social media tools often rely on shared credentials tied to personal accounts. This makes MFA especially messy. Codes get sent to employees' personal devices or emails, creating both security and continuity risks. Cerby solves this by replacing user-owned MFA factors with organization-owned ones—company-managed emails, phone numbers, and authenticator apps.

It automatically retrieves and inputs MFA codes from these shared, enterprise-owned factors, even for complex multi-step logins. That means marketing, comms, and operations teams can access shared social accounts securely without losing productivity or oversight.

cerby

Comparing Authentication Options for Disconnected Apps

Capability	Do Nothing	EPM	Cerby
Automated Login	✗	✓	✓
SSO via IdP Dashboard	✗	✗	✓
MFA Enforcement	✗	⚠	✓
Credential Exposure Limitations	✗	⚠	✓
Shared Account MFA	✗	✗	✓
Admin Visibility	✗	⚠	✓
Audit Readiness	✗	⚠	✓

✓ Fully Supported ✗ Not Supported ⚠ Limited Support

Cerby Eliminates the Human Risk in Authentication

Instead of relying on users to handle credentials, Cerby enforces authentication best practices automatically, ensuring enterprise-grade security every time.

cerby

Identity Lifecycle Management

Overview

Identity lifecycle management governs how users are provisioned, updated, and deprovisioned across apps. Connected apps with SCIM or APIs can be automated; disconnected ones cannot, creating access sprawl and compliance risk.

⚠ Without automated lifecycle management, organizations face serious risk. Former employees may retain access, orphaned accounts become breach points, and compliance requirements remain unmet.

Common Approaches to Lifecycle Management for Disconnected Apps

Approach 1

Do Nothing (User-Driven Account Creation)

End users or business teams independently create accounts with no centralized visibility or enforcement. IT and Security teams cannot track who has access, accounts remain active indefinitely, unneeded subscription licenses drain budgets, and compliance is impossible to maintain.

Approach 2

Manual Provisioning via Tickets or Email Requests

Organizations attempt to control access through ticketing or email workflows. IT or app owners manually log into each app to provision and deprovision users.

- Provisioning is slow and error-prone.
- Deprovisioning is often incomplete or delayed.
- Administrative effort grows unsustainably with scale.

Approach 3

Custom Scripts or RPA

Some teams build scripts or use robotic process automation (RPA) to handle joiner/mover/leaver workflows. Scripts depend on APIs, and RPA can be trained on user interfaces.

- Scripts require ongoing maintenance and are brittle.
- Changes to app UIs or APIs often break automations.
- API keys are frequently stored insecurely.
- When script owners leave, maintenance lapses and workflows break, creating tech debt.

Approach 4

Integration Platform as a Service (iPaaS)

iPaaS tools can automate a variety of workflows by providing connectors built on app APIs or enabling teams to build connectors.

- Focused on general-purpose APIs, not identity.
- High complexity and maintenance cost.
- Requires skilled staff to build and maintain connectors.
- Creates tech debt when internal maintainers leave.

Cerby's Differentiated Approach to Lifecycle Management

Cerby is the only identity automation platform designed specifically for disconnected applications. It closes the governance gap by extending identity lifecycle automation to every application—whether or not it supports SCIM or APIs.

1. Purpose-Built Lifecycle Management for Disconnected Apps

Cerby maintains a catalog of connectors that integrate with disconnected applications through both APIs and patent-pending UI automation. This architecture provides continuous control and reliability, even when app interfaces change. Building on its proven UI drift detection, Cerby is advancing further with a vision-based automation engine that continuously observes application interfaces, detecting and repairing drift before it causes failures. This proactive, AI-driven approach minimizes maintenance effort, eliminates technical debt, and establishes a new benchmark for resilient, long-term automation.

2. Seamless Integration with Existing Identity Solutions

Cerby complements existing IAM and IGA tools by extending automated joiner, mover, and leaver (JML) workflows to disconnected apps. It listens to identity provider events from platforms like Okta or Microsoft Entra ID to trigger provisioning and deprovisioning workflows. Beyond basic account creation, Cerby also manages role assignments, permissions, and group memberships for disconnected apps, ensuring least-privilege access. All activity is logged and auditable.

3. Managing Shared Accounts on Social Media Platforms

Many social media apps require personal profiles to manage business accounts, creating risk when employees depart. Cerby solves this by registering accounts with organization-owned emails, phone numbers, and MFA factors, transferring ownership from individuals to the company. When employees leave, Cerby automatically revokes access, rotates passwords, and maintains operational continuity for remaining users.

Cerby automates provisioning, deprovisioning, access changes, and entitlements for disconnected apps using a combination of APIs, UI automation, and Agentic AI mechanisms.

cerby

Comparing Lifecycle Management Approaches for Disconnected Apps

Capability	Do Nothing	Manual Provisioning	Scripts / RPA	iPaaS	Cerby
Automated Provisioning	✗	✗	⚠ (APIs only)	⚠ (APIs only)	✓
Automated Deprovisioning	✗	✗	⚠ (APIs only)	⚠ (APIs only)	✓
Role & Group Mapping	✗	✗	⚠	⚠	✓
Compliance & Audit Logging	✗	✗	⚠	⚠	✓
Handles Apps Without APIs	✗	✗	✗	✗	✓
AI-Based Drift Detection	✗	✗	✗	✗	✓

✓ Fully Supported ✗ Not Supported ⚠ Limited Support

Cerby extends your identity stack's coverage to 100% of applications. While traditional identity platforms cover only connected apps, Cerby eliminates blind spots by automating lifecycle management for every app in your environment.

cerby

Logging & Auditability

Logging and auditability are essential components of enterprise compliance frameworks such as SOX, PCI DSS, ISO 27001, HIPAA, and GDPR. These standards require detailed records of who accessed sensitive applications, when access occurred, how authentication was performed, and whether access was revoked appropriately.

Disconnected applications create major gaps in audit coverage. Since they lack integration with centralized logging or identity systems, user actions go untracked and unreported, exposing organizations to compliance violations and potential credential misuse.

⚠ If an app is disconnected from identity and logging systems, it's also disconnected from regulatory oversight, creating a material audit finding.

Common Approaches to Logging & Auditability

Approach 1

Do Nothing (No Logging)

Organizations that let end users manage disconnected apps typically have no logging at all. There's no record of access, credential use, or attempted logins.

- No evidence trail for auditors
- No ability to detect unauthorized access
- No data for forensic investigations

Approach 2

Native Application Logs

Some disconnected apps offer limited logging capabilities, but these logs are:

- Inconsistent across applications
- Difficult to parse and not standardized
- Lacking critical identity context (e.g., who used a shared credential)
- Often inaccessible to IT or security teams

Approach 3

Enterprise Password Managers (EPMs)

EPMs can log vault-level events, such as who retrieved a password, but they don't capture application activity or authentication details.

- No session-level visibility
- No MFA enforcement logging
- Limited SIEM integration for real-time monitoring

Approach 4

RPA or Custom Scripts

Scripts may generate basic logs of execution, but these are incomplete, stored locally or insecurely, and lack compliance value.

Cerby's Differentiated Approach to Logging & Auditability

Cerby delivers centralized, enterprise-grade logging for disconnected applications that meets and exceeds compliance requirements. It records every authentication, session, credential use, and access action—regardless of whether an application natively supports logging. This provides organizations with complete visibility into how users interact with disconnected apps, ensuring full compliance and audit readiness.

With Cerby, audit logs are consolidated across all disconnected apps, creating a unified view of access activity. Each event is tied to an individual user, even when shared accounts are used, giving IT and security teams the context needed to understand who did what and when. Cerby also captures detailed MFA enforcement data, including which factors were used and whether authentication was successful, allowing enterprises to confirm MFA compliance.

Cerby maintains a complete record of credential rotations, showing when changes occurred and whether they were user-initiated or system-automated. These insights provide traceability for every access-related event. Additionally, Cerby integrates directly with SIEM tools such as Splunk and Sumo Logic, allowing security and compliance teams to monitor disconnected app activity in real time and correlate events with broader enterprise security data.

cerby

Comparing Logging & Auditability Approaches for Disconnected Apps

Capability	Do Nothing	Native App Logs	EPM	Cerby
Centralized Logging	✗	✗	⚠ (vault access only)	✓
Shared Account Logging	✗	✗	✗	✓
MFA Enforcement Visibility	✗	⚠ (app-dependent)	✗	✓
Credential Rotation Logs	✗	✗	✗	✓
Compliance Audit Readiness	✗	⚠	⚠	✓
SIEM Integration	✗	✗	⚠	✓

✓ Fully Supported ✗ Not Supported ⚠ Limited Support

Cerby Makes the Unmanageable Auditable

Disconnected apps can no longer be dismissed as “out of scope.” Cerby brings them into your compliance framework by delivering full auditability, logging, and integration with enterprise monitoring systems—even for apps without native logging support.

cerby

Conclusion: The Cerby Advantage

Disconnected applications are no longer edge cases. They're integral to modern business operations. Yet many organizations still struggle to manage and secure them effectively. Tools like password managers, scripts, RPA, and iPaaS platforms only address fragments of the challenge, leaving critical gaps in visibility, governance, and compliance.

Cerby closes those gaps. By addressing credential management, authentication, lifecycle management, and auditability in one unified platform, Cerby enables IT and security teams to:

Centralize control of every application

Automate access and deprovisioning securely

Enforce MFA and credential policies consistently

Achieve full compliance and audit readiness

With Cerby, enterprises can extend their identity stack to every corner of their application ecosystem without compromise. The same proven identity workflows used to manage connected apps now apply seamlessly to disconnected applications. Cerby unifies governance, automates secure access, and enforces policy consistency across all applications. The result is stronger control, frictionless user experiences, and complete confidence for IT, security, and compliance teams.

About Cerby

Cerby is the identity automation platform purpose-built to secure disconnected applications—those that fall outside the reach of traditional identity security tools. By integrating with existing IAM, IGA, and PAM systems, Cerby brings centralized access controls, automates manual security tasks, and extends governance across your entire application ecosystem. IT and security teams gain complete visibility and control, reducing risk and operational overhead. Founded in 2020, Cerby is backed by leading investors and trusted by enterprises across the globe.

To learn more, visit www.cerby.com