cerby | Ponemon INSTITUTE

The Hidden Cybersecurity Threat: Disconnected Apps

New 2026 research on the security, compliance, and operational cost of disconnected apps

Independent research conducted by Ponemon Institute, sponsored by Cerby

cerby

Table of Contents

cerby

Executive summary

Enterprise identity programs have made real progress over the past decade. Single sign-on (SSO), multi-factor authentication (MFA), and automated lifecycle management are now widely deployed. But those gains apply primarily to applications that support modern identity standards and are integrated with identity systems.

The rest of the application estate tells a different story.

A significant portion of enterprise applications remain disconnected from centralized identity systems. These are business-critical applications that cannot be fully integrated with identity providers and identity governance and administration platforms.

This research shows they are more widespread, more business-critical, and more damaging than most leaders recognize.

Key findings at a glance

30%
of enterprise applications are disconnected from centralized identity systems, on average

40%
of those disconnected apps are business-critical

77%
of organizations experienced at least one cybersecurity incident tied to disconnected apps in the past two years

63%
have failed an internal or external audit at least once due to gaps in securing disconnected apps

46%
can only produce audit evidence through significant manual effort

31.2 hrs
per week spent maintaining automation workarounds for disconnected apps

58%
say the number of disconnected apps increased in the past 12 months

56%
say urgency to address disconnected apps has increased

The implications are straightforward: many organizations appear more mature in identity than they actually are, as their metrics reflect controls across only the applications integrated with their identity stack. In practice, they are managing two parallel realities at once: one where centralized controls work as intended (connected app layer), and another where access is still governed through local credentials, manual processes, and fragile workarounds (disconnected layer).

In 2026, identity maturity can no longer be defined by the former alone. It must be measured by how consistently organizations extend identity controls and automation across their full environment, including the disconnected layer.

cerby

Introduction

Identity programs are built for a world where everything can connect. That world does not exist.

Enterprise identity programs are built around the goal of centrally managing as many identities and applications as possible. That goal has long been supported by the assumption that identity standards would make integration straightforward and widely achievable. In theory, most applications should be able to integrate with centralized identity systems using standards such as **SAML**, **OIDC**, and **SCIM**.

That assumption holds true for many applications. But not for all of them.

A meaningful portion of the enterprise application environment still falls outside those standards, either because the applications do not support them or because the integrations were never implemented.

This report examines the consequences of that gap.

DEFINITION — DISCONNECTED APPLICATIONS

For the purposes of this research, **disconnected applications** are business applications that are not fully integrated with an organization's identity systems. These systems may include identity providers (IdP), identity governance and administration platforms (IGA), privileged access management systems (PAM), enterprise password managers (EPM), and related identity tools.

Applications can become disconnected for many reasons. Some lack support for federated authentication (via SAML or OIDC) or automated provisioning and governance controls (via SCIM or user management APIs). Others technically support these capabilities but remain disconnected due to implementation effort, lack of visibility into application usage (for example, shadow IT), cost considerations such as "SSO tax" licensing models, staffing constraints, or competing IT priorities.

When applications remain disconnected, they create two compounding gaps:

A CONTROL GAP

Identity systems cannot enforce authentication, MFA, lifecycle management, or governance controls on these applications.

AN AUTOMATION GAP

Identity workflows cannot be automated, leaving administrators and end users to manage access manually through tickets, direct application logins, spreadsheets, and ad hoc credential handling.

cerby

The day-to-day operational consequences are familiar to most IAM teams:

- users neglect to manage passwords securely
- administrators coordinate access through tickets and email
- administrators log into applications individually to provision or update accounts
- offboarding steps are missed or delayed
- access reviews are conducted through spreadsheets and exported data

These are not edge cases. They are standard operating procedure for a large portion of most enterprise application estates.

This research connects those operational realities to measurable outcomes across four areas:

- identity coverage and maturity
- operational workload and automation
- security incidents and exposure
- audit readiness and compliance performance

What this research shows is not just that disconnected applications exist, but that they systematically limit identity coverage. Across organizations, they introduce gaps in security controls, increase operational workload, and make it harder to demonstrate compliance. As a result, identity automation maturity is often overstated, reflecting only the portion of the environment that can be centrally managed.

The study was designed to measure how common disconnected applications are, understand the risks and operational burden they create, examine how organizations currently manage them, and identify the trends making the problem more urgent.

The findings are based on an independent Ponemon Institute survey of 614 IT and security leaders at organizations with more than 500 employees, including a large share from enterprises with more than 10,000 employees.

> **This research makes one point clear: disconnected applications are not a minor exception. They are a defining constraint on identity automation coverage.**

cerby

— FINDING 01

Confidence in identity programs is high, but coverage tells another story

Most organizations think about identity through the lens of the applications they have already connected. In those environments, SSO works, MFA can be enforced centrally, lifecycle changes can be automated, and audits are easier to support.

That visibility creates confidence. Respondents rate their confidence in their identity program's ability to provide consistent security controls across all applications, including disconnected apps, at an average of **6.3 out of 10**, and **57%** rate their confidence between 7 and 10.

But that confidence only reflects part of the application environment.

On average, respondents report:

69.7
applications not configured for SSO

88.5
applications not protected by centrally managed MFA

60.2
applications that require administrators to log in manually to change access

These numbers point to a structural disconnect between perceived maturity and actual identity control coverage. Many organizations have done a strong job securing the connected layer, but they still operate a large parallel layer of applications where identity is managed manually through tickets, local credentials, spreadsheets, manual provisioning, and workarounds.

> **That is why the central finding of this research is not simply that disconnected apps exist. It is that they are more widespread, more business-critical, and more operationally damaging than most leaders realize.**

cerby

— FINDING 02

Disconnected apps are widespread and business-critical

There is a common assumption that disconnected applications are low-stakes: consumer or convenience apps that do not support critical operations or handle sensitive data, and therefore carry minimal risk. The data contradicts this directly.

Respondents report that **40%** of their disconnected applications are business-critical. These are not peripheral tools.
They support core workflows, house sensitive data, grant privileged access, and keep day-to-day operations running.
Yet access to them is routinely managed through the same manual workarounds that lifecycle automation was designed to eliminate: tickets, direct admin logins, and spreadsheet-based access reviews.

30% of enterprise applications sit outside centralized identity systems on average. At an average estate of 284 applications, that means most organizations are running more than 80 applications outside their identity control plane. Among those, roughly 32 are business-critical.

80+

apps outside the identity control plane at an average organization — roughly 32 of them business-critical

KEY INSIGHT

Organizations tend to assign the lowest operational priority to the very applications that create outsized risk when left unmanaged. A business-critical application with no SSO, no centrally managed MFA, and no automated provisioning is not a minor gap in an otherwise strong program. It is a significant exposure hiding in plain sight.

This is the structural problem. Identity programs are often measured by how well they cover the connected layer, while the disconnected layer, including applications that matter most to the business, remains largely invisible to those same metrics.

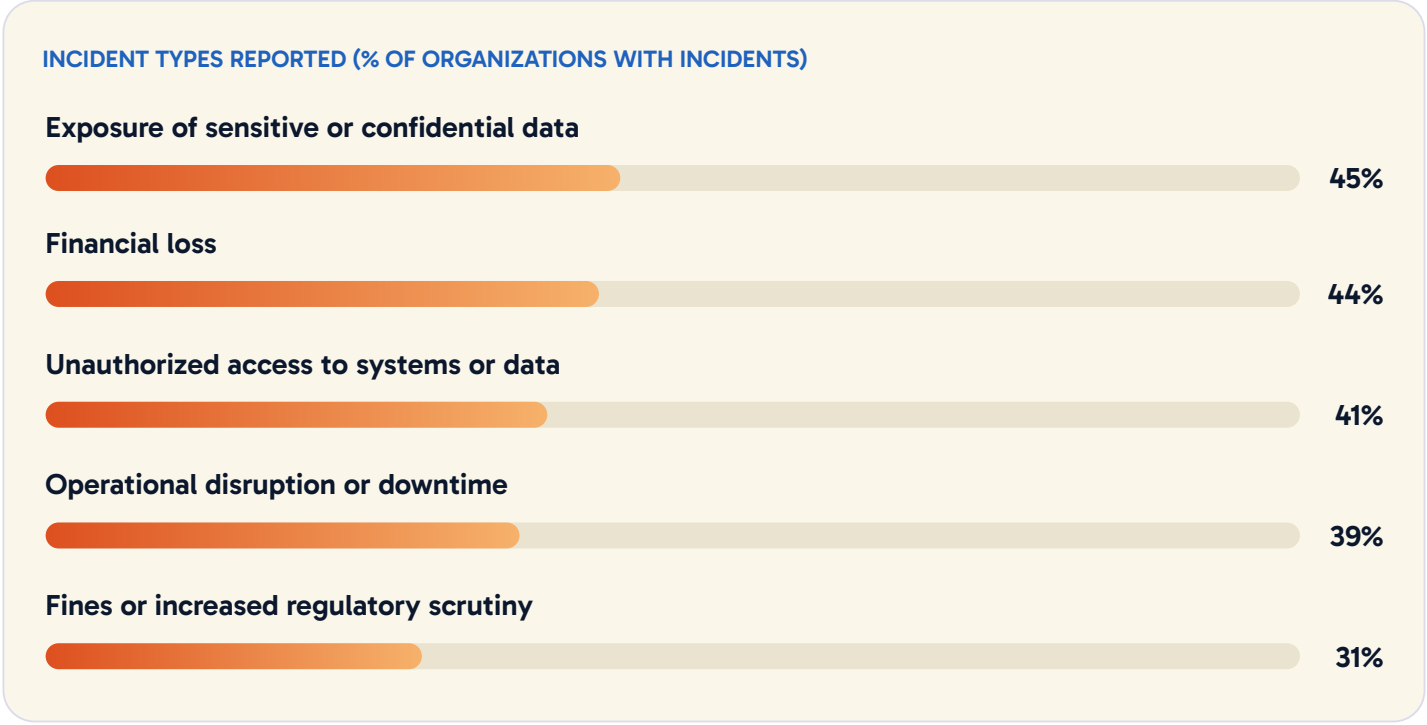
cerby

— FINDING 03

The security consequences are already visible

Disconnected applications do not just create theoretical risk. They are actively contributing to security incidents at a rate that should concern any IAM or security leader.

77% of organizations experienced at least one cybersecurity incident in the past two years caused by the inability to secure disconnected applications. Among those that reported incidents:



The authentication posture underlying these incidents is not a surprise. **55% of organizations** rely on password-only authentication for disconnected applications, with no MFA. Add to that the most commonly cited risks in disconnected environments: excessive privileges (**54%**), users retaining access they no longer need (**49%**), lack of MFA (**41%**), weak or easily guessed credentials (**37%**), and orphaned or dormant accounts (**36%**). This is a predictable failure pattern.

The incident response problem compounds the exposure. When an account in a disconnected application is compromised, the standard response playbook breaks down. Confidence in the ability to contain and recover from incidents involving disconnected apps is low and uneven: **20% of respondents rate their confidence at 1 or 2 out of 10**, while only **18% rate it between 9 and 10.** Disabling accounts, resetting credentials, and validating the scope of access are all slower when those accounts are not centrally managed. The investigation itself is harder when logging and visibility are limited.

This is no longer a theoretical identity gap. It is an active source of exposure, with consequences that are showing up in incident logs, financial statements, and regulatory correspondence.

SOCIAL MEDIA AS A DISCONNECTED APP RISK VECTOR

34% of respondents said incidents involving disconnected applications included social media platforms such as X (formerly Twitter), Meta, LinkedIn, or Instagram. These platforms typically do not support enterprise identity standards, are often managed outside IT, and carry significant reputational and legal exposure if compromised. They are a useful example of the category of application that looks low-risk until it is not.

— FINDING 04

Audit readiness breaks down where identity coverage stops

If the security consequences are significant, the compliance consequences are just as serious and in some ways more immediately felt.

63% of organizations report failing an internal or external audit at least once due to gaps in securing disconnected applications. Of those, **36% failed more than once**. Another **18%** passed the audit but were told significant gaps remained. Only **19%** report no audit findings related to disconnected applications.

The core problem is evidence, not just controls. Auditors do not just ask whether controls exist. They ask for proof. And for disconnected applications, that proof is difficult to produce.

34%

of organizations say they can consistently produce complete and accurate access records for disconnected applications

16%

say they cannot produce audit evidence for disconnected applications at all

46%

report that producing audit evidence requires significant manual effort and is often incomplete

When access is managed outside centralized identity systems, compliance documentation depends on screenshots, manually assembled spreadsheets, exported data files, and after-the-fact reconstruction. This is not just a time problem. It is a credibility problem. Manually assembled evidence is harder to defend as a demonstration of consistent control.

cerby

THE BOTTOM LINE FOR COMPLIANCE TEAMS

An identity program that cannot produce clean, continuous access records for a meaningful portion of the application estate is not audit-ready. It is audit-exposed.

The downstream consequences are already materializing. **31% of organizations** report fines or increased regulatory scrutiny following incidents involving disconnected applications. For organizations subject to SOC 2, ISO 27001, HIPAA, PCI DSS, or similar frameworks, disconnected applications are not just a security concern. They are a material compliance risk.

— FINDING 05

Disconnected apps create an ongoing, hidden operational tax

When centralized identity systems do not reach an application, the work does not disappear.

It shifts to people.

Provisioning and deprovisioning often rely on manual coordination. **51%** use tickets or email, and **43%** provision accounts by logging directly into applications. Organizations try to bridge the gap using custom scripts, workflow platforms, scheduled imports and exports, and robotic process automation.

These workarounds may reduce some manual effort, but they introduce a new burden: maintenance. The systems built to replace manual work often require ongoing manual effort to keep them running.

52% of organizations say they use automation workarounds to manage disconnected apps. Among those organizations, teams spend an average of **31.2 staff hours per week** maintaining or fixing those tools when they break due to application updates or interface changes.

The broader operational cost is significant:

68%
report delayed or incomplete access removal after employee termination

39%
more time on average is spent conducting access reviews for disconnected applications than for connected apps

24%
estimate that between 31% and 50% of licenses for disconnected apps are unused due to lack of automated provisioning

This is the hidden tax of disconnected apps: more manual work, slower operations, higher maintenance overhead, and avoidable waste.

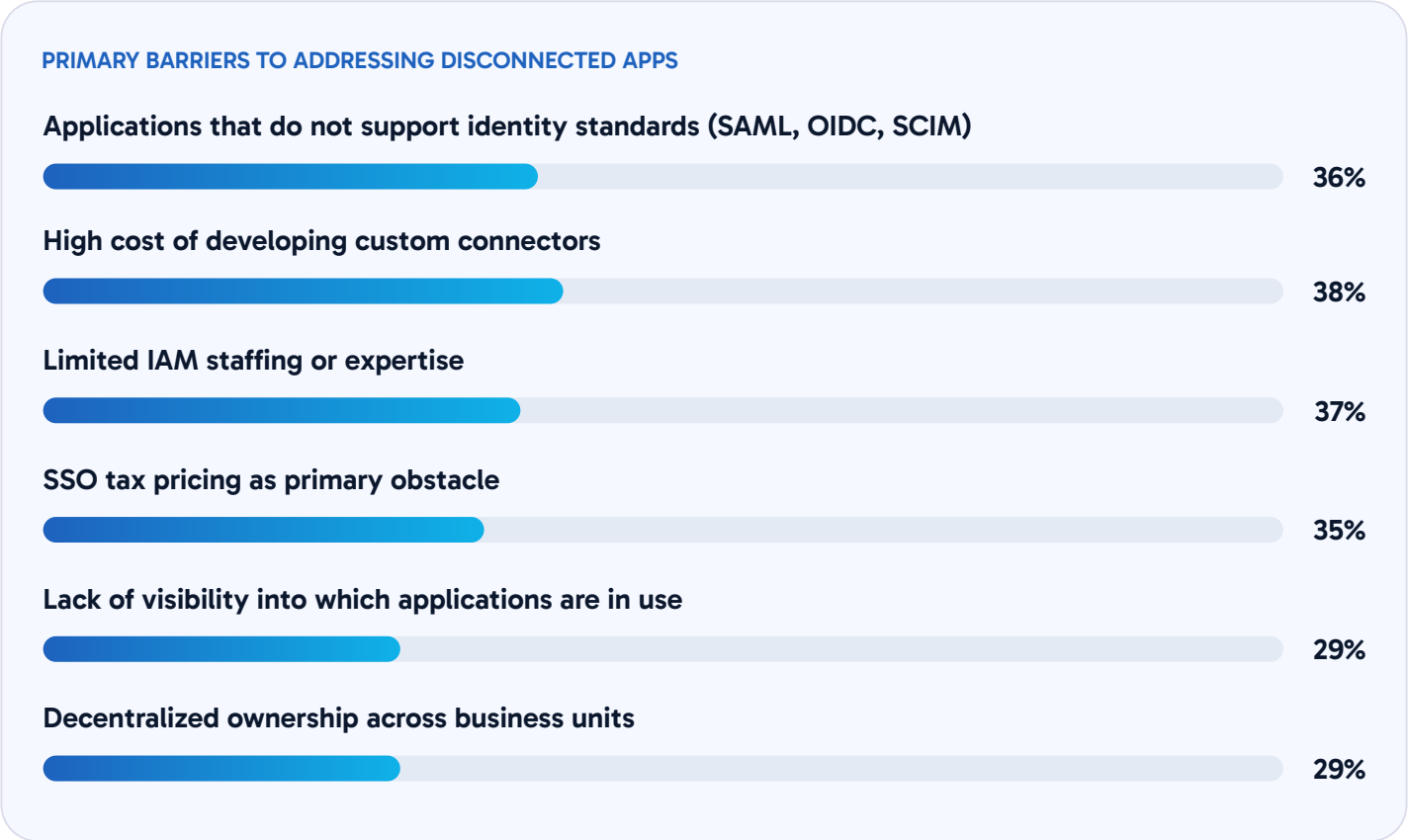
cerby

— FINDING 06

Why the problem persists

The persistence of disconnected applications is not a result of indifference. Identity leaders are aware of the problem. 62% report a significant increase in awareness of disconnected app risks over the past two years, and 63% agree or strongly agree that disconnected applications represent one of the largest remaining gaps in their IAM program.

The barriers are structural.



Applications that do not support identity standards remain the most fundamental constraint. **36%** cite lack of SAML, OIDC, or SCIM support as a primary barrier. The assumption that this problem would fade as SaaS vendors modernized has not held. Many vendors, particularly in specialized verticals, do not face enough enterprise pressure to prioritize identity standards support. Others implement it only behind premium licensing tiers.

Cost and implementation friction are the next most common barriers. **38%** cite the high cost of developing custom connectors, **37%** cite limited IAM staffing or expertise, and **35%** cite SSO tax pricing as primary obstacles. Integrations get prioritized where they are easiest, most urgent, or already funded. The rest accumulate as exceptions.

cerby

Decentralized application ownership compounds the challenge. When business units adopt applications independently, IT and security teams often do not know what is in use until after the fact. **29%** of respondents cite lack of visibility into which applications are in use, and another **29%** cite decentralized ownership across business units as primary barriers.

Over time, these conditions do not resolve themselves. They compound. Each new application adopted without an identity integration adds to the disconnected layer.

— FINDING 07

The gap is getting larger, not smaller

If the disconnected layer were stable, the challenge would be significant but bounded. It is not stable.

58% of organizations report that the number of disconnected applications increased over the past 12 months. **27%** describe the increase as significant.

A widely cited reason is AI. **87%** of respondents say their organization has adopted AI or GenAI in some capacity. And **55%** rate the increase in AI-created or AI-powered applications adopted by employees without IT or security involvement as high, with **25%** of those rating it as extreme.

The compounding problem: most of these AI-powered applications do not support enterprise identity standards. Among organizations that have adopted AI tools:

- **26%** report 51 to 100 AI-created or AI-powered applications that lack SAML, OIDC, or SCIM support
- **24%** report more than 100 such applications
- Only **6%** report none

Application adoption is accelerating faster than identity standards adoption. Without a scalable way to extend controls to applications that cannot federate, every new AI tool an employee adopts expands the unmanaged identity surface.

THE AI WILDCARD

AI-powered applications are being adopted at a rate that outpaces identity standards support. They arrive in the environment without integration planning, often without IT knowledge, and typically without the SAML, OIDC, or SCIM support that would allow them to be brought under centralized identity control. The identity surface is expanding faster than the identity program can follow it using traditional approaches.

cerby

— FINDING 08

The pressure on identity leaders is increasing

For years, disconnected applications were treated as backlog items: acknowledged, deprioritized, and deferred. That calculus is shifting.

56% of respondents say the urgency to address disconnected applications has increased. The reasons they cite go well beyond abstract risk awareness:

- **53%** cite the growth of non-human identities managed outside IAM systems
- **50%** cite the inability to enforce consistent authentication or MFA
- **49%** cite security incidents involving disconnected applications
- **45%** cite audit and compliance challenges
- **38%** cite identity or Zero Trust initiatives stalled by disconnected apps

That last point is worth emphasizing. Zero Trust architecture and broader identity modernization initiatives are increasingly bottlenecked by the disconnected layer. You cannot enforce least privilege access to an application your identity system cannot reach. You cannot automate access reviews for an application that has no API. Zero Trust is not a destination reachable by only securing the connected layer.

> **Securing disconnected or non-federated applications** is tied for the top IAM priority over the next two years at **57%**, alongside strengthening access governance and certifications. Managing non-human identities follows at **49%**. These are program-level priorities, not backlog items.

cerby

— FRAMEWORK

A more useful way to think about identity automation maturity

Traditional measures of identity maturity focus on how well organizations secure connected applications. That is still important, but it is no longer enough.

Disconnected applications introduce two fundamental gaps:

- A **control gap,** where identity systems cannot enforce authentication, MFA, lifecycle management, or governance
- An **automation gap**, where identity workflows cannot be automated and must be handled manually

A more useful way to think about identity maturity is to look at how far these gaps extend across the application environment and how effectively they are reduced over time.

Based on the survey findings, most organizations today operate between Level 1 and Level 2 of the following model. Reaching Level 3 requires solutions capable of extending automation to applications outside traditional identity standards.

LEVEL 1

Connected-only maturity

Identity controls and automation are mature for connected applications. Disconnected applications sit entirely outside centralized control. Access is password-based, provisioning is manual or inconsistent, application ownership is unclear, and many organizations do not have a complete inventory of what is in use.

This is where most organizations start and many remain.

Survey data: 55% rely on password-only auth for disconnected apps | 77% experienced a related security incident in the past two years

LEVEL 2

Visibility and partial controls

Organizations recognize disconnected applications as part of the identity problem. Teams begin identifying and inventorying these applications. Basic controls are introduced: password policies, manual rotation schedules, credential hygiene reminders. Some credential management practices are in place.

However, key identity capabilities are still missing. Provisioning and deprovisioning are not automated or tied to systems like the IdP, IGA, or HR platform. MFA is not consistently enforced at scale across disconnected apps. Awareness has improved, but control and consistency have not yet scaled.

Survey data: 52% have taken steps to discover disconnected apps | 41% actively manage credentials for disconnected apps

LEVEL 3

Controls and automation extended to disconnected apps

Security controls and lifecycle automation begin operating across both connected and disconnected applications. Identity systems such as IdPs or IGA platforms can trigger access changes across the full estate. Centralized credential management replaces ad hoc password handling. MFA can be enforced on disconnected apps.

Coverage expands meaningfully beyond the connected layer. This is the critical inflection point.

Survey data: When evaluating solutions for this problem, respondents prioritize integration with existing IAM and IGA platforms (49%), ability to secure applications that do not support identity standards (45%), and MFA with an SSO-like experience for disconnected apps (41%).

LEVEL 4

Full coverage, automation, and governance

Identity controls operate consistently across the entire application environment. Authentication, lifecycle management, and governance processes are applied uniformly. Provisioning, deprovisioning, access reviews, and audit evidence generation are automated and continuous, not manual and periodic. The disconnected layer no longer behaves differently from the rest of the environment.

The target state for mature programs.

Survey data: Only 34% can reliably produce audit evidence for disconnected apps today. 46% say evidence gathering requires significant manual effort.

cerby

— ACTION FRAMEWORK

What identity and security leaders should do now

The organizations that make meaningful progress on identity automation maturity over the next 12 months will be those that stop treating the disconnected layer as a permanent exception and start treating it as a solvable problem. The survey data points to five concrete priorities.

PRIORITY 01

Redefine identity scope to include the disconnected layer

Identity automation scope should not be defined by what your IdP can integrate with today. It should be defined by the risk profile of the application. Any application that handles sensitive data or supports critical workflows belongs inside your identity program, regardless of whether it supports SAML or SCIM. On average, **30%** of enterprise applications, **40%** of which are business-critical, currently sit outside that program entirely.

PRIORITY 02

Build a complete picture of disconnected apps before expanding coverage

You cannot govern what you have not found. Only **52%** of organizations have taken active steps to discover their disconnected applications. Common discovery approaches include endpoint detection tools (**45%**), CASB (**39%**), business unit self-reporting (**40%**), expense and procurement system reviews (**37%**), and email or browser-based discovery tools (**33%**). Once identified, prioritize by business criticality and risk to create a foundation for targeted action.

PRIORITY 03

Extend automated credential security where federation is not possible

For applications that cannot support federated SSO, authentication defaults to passwords. **55%** of organizations are in this position for significant portions of their estate. Centralized credential management and vaulting, automated rotation, policy enforcement, and MFA enforced directly in the application, delivers real security controls for apps where SAML and OIDC are not available. This is not a workaround. It is the appropriate control model for this category of apps.

PRIORITY 04

Close the joiner-mover-leaver gap for disconnected apps

Joiner, mover, and leaver (JML) processes are among the most automated workflows in mature identity programs, but only for connected applications. For disconnected apps, **68%** of organizations report delayed or incomplete access removal after termination, and **18%** say more than half of all terminations result in incomplete removal. Lifecycle automation has to cover every application that matters, not just the ones the IdP already manages.

PRIORITY 05

Make audit evidence a continuous output, not a manual sprint

46% of organizations say producing access evidence for disconnected apps requires significant manual effort. **63%** have failed an audit at least once because of this gap. At high identity automation maturity, audit evidence is a continuous byproduct of how access is managed, not something assembled under pressure when auditors arrive. Solutions that collect identity and access data from disconnected apps without requiring SCIM or API integration are key.

cerby

Closing perspective

Disconnected applications have long been framed as a technical limitation: applications that simply cannot be integrated, and therefore must be managed manually. That framing has allowed the problem to persist as a category of accepted exceptions.

The research does not support that framing. It shows that disconnected applications are widespread, business-critical, and actively contributing to security incidents, audit failures, and operational burden. They are not peripheral to the identity program. They are a defining constraint on what that program can achieve.

Most organizations have already made substantial progress securing the applications that were easiest to connect. That work mattered. But the next frontier of identity maturity runs directly through the disconnected layer, where critical applications still operate with weaker controls, more manual work, and more audit friction than any other part of the environment.

Identity maturity in 2026 is not measured by how well connected apps are secured. It is measured by how consistently organizations can extend identity controls, automation, and governance across the full application estate, including the parts that do not yet support SAML, OIDC, or SCIM.

That gap is solvable. The organizations that solve it will not just reduce risk. They will operate more efficiently, demonstrate compliance more credibly, and build an identity program that reflects how modern enterprises actually work.

About Cerby

Cerby is the identity automation platform purpose-built to extend identity controls to disconnected applications, including those that do not support standards such as SAML, OIDC, or SCIM. It enables organizations to enforce credential management, MFA, provisioning, and governance across applications that traditional identity systems cannot reach, while integrating with existing IdP and IGA platforms.

By closing gaps in identity coverage and automation, Cerby helps organizations reduce manual access management, strengthen security controls, and improve audit readiness across their entire application environment.

This research was conducted independently by Ponemon Institute. Cerby sponsored the study but had no influence over survey design, data collection, or analysis. All statistics cited in this report are sourced from the 2026 Ponemon survey of 614 IT and security leaders at organizations with 500 or more employees.

cerby

Methodology

The findings in this report are based on an independent survey conducted by Ponemon Institute of 614 IT and security leaders at organizations with more than 500 employees in the United States. A significant portion of respondents represent enterprises with more than 10,000 employees.

Participants were drawn from a broader sampling frame of 17,808 IT and security practitioners involved in their organization's identity and access management strategy.

This research was conducted independently by Ponemon Institute. Cerby sponsored the study but had no influence over the survey design, data collection, or analysis. All statistics cited in this report are sourced from the 2026 Ponemon survey.

Respondents span a range of industries, including financial services (18%), industrial and manufacturing (12%), services (11%), technology and software (10%), retail (10%), energy and utilities (9%), health and pharmaceutical (9%), and other sectors. More than 80% of respondents are at or above the supervisory level.

Download the complete dataset used to create this report, including detailed methodology, study caveats, survey questions, and full results.

www.cerby.com/content-hub/ponemon-report-2026-data