cerby

Benchmark Survey

The State of Disconnected Apps in Identity

Insights from Oktane 2025

Modern identity security programs depend on centralization: one system to control who has access to what. But what happens when more and more apps fall outside that system?

> At **Oktane 2025**, we surveyed IT and security leaders to understand how widespread these “disconnected apps” really are—and what teams are doing about them.

The results show a growing blind spot in enterprise identity security. Most organizations are still managing access manually, struggling with visibility, and exposed to risk they can’t easily detect—let alone control.

This report breaks down what’s driving the disconnect, why it’s growing, and where leading teams are focusing next.

The Identity Coverage Gap Is Real—and Growing

App Access Still Relies on Credentials, not SSO

Only **42%** of IT and security leaders say most of their apps support SSO via Okta. For the rest, it's still login via email and password on a per-app basis.

Without SSO, users log in with standalone credentials—often weak, reused, or shared insecurely—making those apps far more vulnerable to compromise.

Lifecycle Management Is Still Mostly Manual

Only **15.8%** said most of their apps are connected to their IAM or IGA tools for lifecycle management

50% said less than half of their stack is covered

When access isn't automatically updated, users keep permissions they shouldn't. Every new app adds more work—and risk.

IT Can't Keep Up With App Growth

66% of respondents strongly agree: "Business teams adopt new apps faster than IT can secure them."

This isn't just a tooling problem—it's a scale problem. Manual identity management can't match the pace of today's app sprawl.

The SSO Tax Keeps Apps Disconnected

Only **21%** of IT teams say they'll pay the premium to enable SSO or provisioning via SCIM.

The rest? They delay, avoid, or rely on workarounds—leaving SaaS access unmanaged and exposed. Security isn't just limited by technical constraints. It's priced out—one SSO tax at a time.

What's Driving the Disconnect and What to Do About It

Why Traditional IAM Breaks Down

When asked what's blocking identity coverage, three major challenges stood out:

33%

cite lack of identity standards

Many modern apps still don't support protocols like SAML, SCIM, or even basic APIs

⚠

If the app can't connect, your traditional IAM tools can't help.

20%

cite legacy and on-prem apps

Some apps are too critical to retire—but too complex or costly to integrate.

⚠

These systems stay disconnected by default.

16%

cite IT resource constraints

There's simply not enough time to build workflows or manually manage access across dozens of systems.

⚠

Without automation, governance falls through the cracks.

→ These aren't edge cases. They're the everyday reality of most large IT environments.

You Can't Secure What You Can't See

80% of IT & security teams lack visibility into apps used in the org

20% described their visibility as **very low**

→ If you don't know an app exists, you can't enforce access, revoke credentials, or investigate incidents. It all starts with visibility.

Disconnected Apps Drive Real-World Risk

Disconnected apps introduce operational and security risk across the organization. Here's what respondents said they've experienced—or actively worry about most:

01 **Security incidents** tied to unauthorized access and compromised credentials

02 **Audit or compliance findings** due to lack of governance

03 **Added costs** from services and integrations to compensate for missing controls

What Leading Teams Are Prioritizing

Asked what would make the biggest impact in reducing disconnected app risk, here's what IT leaders said:

1 in 2 Say extending automated lifecycle management to disconnected apps

1 in 3 Say securing credential management and extend SSO where possible

Start where the Disconnected App Risk Is Concentrated

When asked which parts of the business app stack pose the greatest identity risk, IT leaders pointed to three departments:

- Marketing
- Engineering
- Finance

These teams adopt apps quickly, often without IT involvement.
That means no SSO, no central provisioning, and no visibility into who has access.
→ **If you're trying to close the identity gap, this is where to start.**

Conclusion

- Disconnected apps aren't just unintegrated—they're unseen, unmanaged, and unsecured. And they're creating a growing identity blind spot that most identity providers and systems weren't built to address.
- IT & security leaders aren't waiting for apps to adopt standards. They're taking control by extending security, automation, and governance to the parts of the stack traditional systems can't reach.
- A solution like Cerby helps IT and security teams close the gap by bringing identity controls and automation to disconnected apps—completing your IAM stack, not replacing it. Because identity-first security isn't about covering what's easy. It's about covering everything your teams use.

Learn more at cerby.com

Methodology

This survey was conducted at Oktane 2025 and includes responses from IT and security professionals across industries including financial services, healthcare, retail, and tech. Respondents included CISOs, CIOs, IT managers, identity architects, and system administrators at companies ranging from 500 to 10,000+ employees.

cerby

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