Research report

The 2025 Identity Automation Gap

How manual identity tasks are undermining enterprise security.

Identity security stacks have evolved. Most organizations now deploy password managers, Multi-Factor Authentication (MFA) solutions, centralized directories, and advanced governance tools. But the foundation of identity security—execution—still relies on something far less reliable: people.

Despite years of investment, critical workflows are still handled manually in most enterprises. As disconnected applications—those that don't integrate with existing identity stacks—become more deeply embedded across every organization, the cracks in identity execution are widening.

Cerby's 2025 Identity Automation Gap Report set out to quantify this automation gap—how wide it is, how much risk it introduces, and what forward -looking organizations are doing to close it. The findings are clear: Manual execution is still the default. Automation is the exception. And the last mile of identity—the handoff from policy to practice—still runs on human error.

01

Introduction: a false sense of control

The modern identity stack looks mature. Today's enterprises have no shortage of tools: enterprise password managers, identity orchestration and governance platforms, privileged access controls, and more. Many have centralized their identity providers, mapped roles to entitlements, and rolled out MFA across core systems.

But beneath that surface, a deeper problem persists. Traditional tools were never built to cover the heterogeneity of modern environments. From SaaS to mobile to legacy on-prem, many critical applications remain disconnected—unable to integrate with core identity platforms. They don't support standard identity protocols like SAML or SCIM, and they can't be governed through centralized policy.

These disconnected apps are used across every function—from marketing to legal and finance—and often contain sensitive data. Yet they sit outside central control and visibility, managed manually or not at all. This is where identity security breaks down.

Cerby's 2025 Identity Automation Gap Report, based on input from more than 500 IT and security leaders, reveals the magnitude of the problem.

> Fewer than **4%** of respondents say they've fully automated core identity tasks.

In many organizations, the most critical controls are still dependent on end-user action.

This isn't just operational debt—it's critical risk exposure. The automation gap is now one of the most overlooked risks in enterprise security. And it's one organizations can no longer afford to ignore.

02

The reality: what the data tells us

Cerby's 2025 Identity Automation Gap Report, based on responses from over 500 IT and security professionals at mid-to-large companies in the U.S., reveals a clear disconnect between identity strategy and execution.

The core workflows of identity automation are severely limited

> Less than **4%** of respondents said their organizations have fully automated core identity workflows. For the remaining **96%**, execution still depends on human-centric workflows—difficult to scale, error-prone, and risky.

41%

of organizations handle credential sharing and password rotation manually, often through spreadsheets, emails, or chat tools.

89%

of organizations do not enforce MFA or passkeys automatically. Instead, they rely on end users to enroll themselves, leaving this critical layer of protection optional and inconsistent.

59%

still perform user access provisioning, offboarding, or both manually—through ticketing systems, ad hoc requests, or follow-up emails.

72%

distribute user entitlement data—records of what each user can access—manually or through flat-files like Excel or CSVs, limiting visibility into who has access to what, and when.

Why it matters

These aren't edge cases. This is the current state of identity execution in most enterprises. Policies are written. Tools are deployed. But execution still depends on people—at scale.

Visibility and control are fragmented

Identity security enforcement and execution isn't just manual—it's also fragmented across teams, tools, and systems. Visibility is limited, and ownership is often unclear.

58%

of organizations say their identity approach is fragmented or highly fragmented —relying on a mix of disconnected tools, inconsistent workflows, and limited oversight.

21%

say business units manage access to their tools without IT or security involvement. This approach leaves access decisions unmonitored and unenforced at the departmental level.

Why it matters

Fragmentation doesn't just slow things down—it introduces blind spots. Without centralized control, oversight fades and risk multiplies in places no one is watching.

03

Why the automation gap exists

Disconnected applications are at the heart of the problem—and they're not going away.

Today's enterprise application environments are increasingly heterogeneous and complex, spanning SaaS, mobile, cloud-native, and legacy on-premise systems. Identity platforms, while highly effective for standards-compliant apps, were never built to integrate with the long tail of disconnected applications—those that don't support common protocols such as SAML, SCIM, or OIDC. And there are more of them than most teams realize.

In theory, custom integrations can close these gaps. In practice, they rarely scale. Maintaining these integrations demands constant upkeep; even small interface changes can cause breakage.

Instead, most organizations fall back on brittle methods: spreadsheets, ticketing systems, and ad hoc fixes. These approaches might suffice in the short term, but they are no match for the pace or complexity of modern identity risk.

To move faster, many teams are exploring AI agents as a way to accelerate integrations and automate identity workflows more securely. But trust remains a barrier.

> In the survey, **78%** of security professionals said they do not trust AI agents to autonomously perform core identity tasks. Still, **45%** are open to a collaborative, human-in-the-loop approach—signaling that the future of identity automation may lie in dependable, not fully autonomous, execution.

04

The cost of doing nothing

The risks tied to manual identity workflows are no longer theoretical—they're showing up in audits, operations, and security incidents.

46%

of security and IT leaders say their organization has already experienced a security, compliance, or operational issue directly caused by manual workflow execution.

34%

haven't yet experienced a known incident, but say they've identified manual execution as a clear and present risk. In other words, 4 in 5 organizations either have encountered problems—or know they're vulnerable.

One of the most persistent and dangerous gaps is deprovisioning.

58%

of teams say former employees have retained access to systems after leaving the organization.

23%

aren't sure—acknowledging the possibility, but lacking the visibility to confirm. In both cases, the outcome is the same: unauthorized access and risk exposure with no clear perimeter.

And despite this, action still lags

49%

of respondents said the single most important step they would take to reduce identity risk is extending automation across more applications and workflows. Yet for many, that work remains unfinished.

Why it matters

Every day that identity workflows remain manual is another day risk stays embedded in the business. Waiting to act is not a strategy—it's an invitation for the next security incident.

05

A way forward: principles for closing the gap

Based on Cerby's research and work with enterprise security teams, five core principles have emerged for reducing identity risk through automation:

1 Map your full application landscape

Go beyond what IT manages directly. Capture every SaaS, on-prem, mobile, and third-party app used across departments. Business units often run their own tools—and that sprawl is only growing. Most organizations underestimate how many apps fall outside centralized identity coverage until they take inventory.

2 Assess where enforcement depends on humans-in-the-loop

Find the apps that don't support SSO, MFA, or federation with your existing platforms. Then examine how key processes are executed. If your team still relies on ticketing systems or spreadsheets, those gaps aren't just manual—they're high risk.

3 Centralize IT policy and enforcement—without slowing other teams down

Effective identity management and governance means IT defines the rules and maintains oversight, while business units manage access within secure boundaries. This model—central policy with decentralized execution—lets organizations move fast without losing control.

4 Choose security vendors that extend and complete your stack

The goal isn't to replace your existing tools—it's to extend them. Look for platforms that automate workflows across disconnected apps, integrate easily with your current systems, and adapt to your environment without introducing complexity.

5 Leverage AI that fits your framework

The right approach to agentic AI should reflect the complexity of your environment and the maturity of your organization. Whether that means full autonomy or a collaborative approach, AI should match your architecture—not force you to reshape it.

Conclusion

The takeaway is clear: identity automation is still missing where it matters most. Yet it's no longer a nice-to-have. Automation is a foundational requirement for securing the identity layer at scale.

But the answer isn't starting over. It's extending what you already have—beyond dashboards and integrations, into the last mile where execution still relies on people. That's where risk lives—and where the next phase of identity security needs to begin.

Identity automation self-assessment

5 questions to identify your last-mile automation gaps

1. Do you have applications in your environment that do not support SSO?
2. Are employees responsible for manually storing, updating, and sharing passwords?
3. Do you have any apps where IT is unable to enforce MFA automatically?
4. Do you have applications where onboarding and deprovisioning users relies on manual workflows or ticketing systems?
5. Do you have to manually extract identity and entitlement data from applications to prepare for audit or compliance requirements?

Appendix

Methodology and Demographics

This report is based on a survey of 500 U.S.-based IT and security professionals conducted in May 2025. Respondents:

- Represent companies with 500+ employees
- 83% work in IT or security roles
- 80% are directly responsible for managing user access to applications

Respondents span small enterprise to large enterprise segments:

- 36.6% from companies with 501–1,000 employees
- 22.6% from 1,001–2,500
- 10.4% from 2,501–5,000
- 30.4% from organizations with 5,001+ employees