descope

State of Customer Identity

[2025 Report]

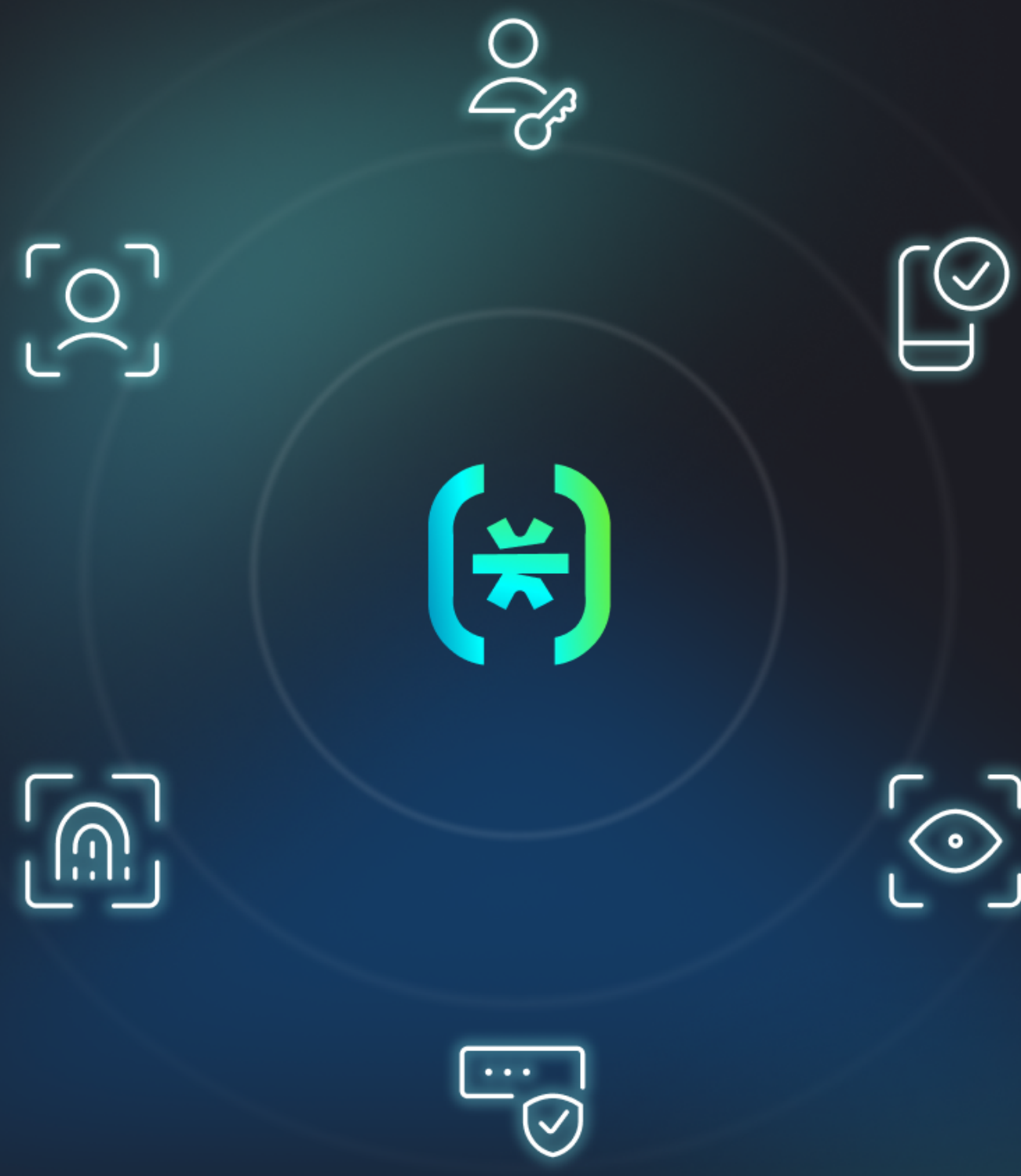


Table of Contents

descope

State of Customer Identity 2025

Executive Summary

Authentication should be easy and effective. But in practice, especially for the teams that manage it every day, it's often the complete opposite.

We commissioned a survey of over four hundred CIAM (Customer Identity and Access Management) decision-makers across industries, from engineering leaders to security experts. Our goal was to understand how organizations handle customer authentication today: their challenges, motivations, and burning desires.

While these sorts of studies often boil down to predictable "bad thing is bad" conclusions, the responses we gathered surprised us—and they'll probably offer you a few lightbulb moments, too. You might deeply identify with the struggles our respondents face, or perhaps see a previously hidden path in your own auth journey.

In either case, the following report reveals a marketplace wrestling with fundamental contradictions and searching for better ways forward.

Identity crisis is the status quo

Organizations deploy authentication strategies they already know don't deliver. Username/password authentication appears in 87% of companies' customer-facing applications, yet only 2% of respondents believe it effectively balances security and user experience. The near-universal use of passwords isn't a revelation, but the dismal sentiment for them speaks volumes.

The lack of password alternatives could be because more than half (53%) of respondents currently repurpose their workforce IAM for customer authentication. It's a square-peg-into-round-hole approach that a mere 8% would choose if they started fresh today.

Why the disconnect? Teams know better options exist, and they see passwordless and purpose-built CIAM succeeding elsewhere. But when you're barely keeping the lights on with legacy systems, the path from status quo to the best auth available feels like an uphill battle.

Pay the invisible auth tax

Authentication misfires rarely stay contained, and they often directly affect an organization's growth. Our data shows that 82% of organizations suffered tangible business impacts from CIAM issues, with a wide variety of root causes.

As expected, security incidents from weak or missing multi-factor authentication (MFA) affected a significant portion (39%) of respondents. But identity issues also played havoc with product roadmaps: 37% of organizations delayed projects to address authentication gaps, while 46% postponed CIAM updates to deal with other pressures.

Companies know they can't defer authentication improvements indefinitely, but many feel torn between competing priorities. Respondents were acutely aware of moments when their marching orders should have been to upgrade CIAM tools, but other projects took precedence.

In these scenarios, organizations end up paying an unseen "auth tax" when they least expect it: in the form of long-term tech debt, as an obstacle to moving upmarket, or even from a damaging breach.

Security vs. user experience vs. both

CIAM decision-makers have been locked in a debate since before the days of dialup: lock it down or open it up? Our respondents split into three groups: 39% emphasize security, 26% favor user experience, and 34% aim for a balance between them. Yet, 73% admit their organizations struggle to find equilibrium, regardless of which side they favor.

The consequences of overcorrection can carve a chunk out of a company's bottom line, with over a quarter (27%) of organizations reporting lost revenue after implementing stricter authentication controls.

And, as we noted above, more than a third (39%) of companies that attempted low-security strategies experienced a harmful incident as a direct result.

Company size heavily influences these sentiments. Among enterprises with more than 20,000 employees, 48% put security first. This seems to indicate that scale and risk exposure push organizations toward more constrained, restrictive approaches.

However, the practical outcomes seem to defy this sentiment, with large organizations that enforce stricter policies reporting a much higher rate of customer pushback compared to their smaller counterparts.

Devs do everything (while equipped with less)

Over half (51%) of the organizations we surveyed have developers with minimal authentication experience building customer-facing identity systems prone to vulnerabilities. Meanwhile, the time they spend on developing authentication is a point of contention. The majority (64%) of respondents say devs spend too little time on authentication (creating security risks), while 36% say they spend too much time (delaying core features).

The most inexperienced devs in this bunch—who are admirably willing to learn on the job—aren't really responsible for the gap in expertise. This technical gulf is about specialization, not potential.

For example, if we drill down into companies who use in-house, DIY authentication (36% of all respondents), only 27% have full-time CIAM developers. That's a shockingly low number, and it points to two core issues: developers who work on authentication are asked to do more with time (time, training, and resources); and organizations tend to make auth decisions based on short-term thinking (meeting immediate needs rather than planning long-term).

Modern authentication requires deep knowledge of security best practices that simply won't occur to a novice. Asking product developers to master this highly focused domain while shipping features is a recipe for neither goal being met.

Some dev work is well-suited to a learn-as-you-go approach, but not authentication and identity management.

AI attitudes and adoption blues

As organizations embrace AI at a seemingly breakneck pace, identity management often lags behind. While 88% of our respondents are using or planning to use AI agents, only 37% have actually progressed beyond small pilot programs. The identity considerations? Mostly uncharted territory.

A nearly unanimous 95% of respondents recognize that authentication is critical for AI security. Yet, the trust dynamics in human versus non-human identities (NHIs) appears to be in flux. Organizations just starting with AI see humans as the bigger data breach risk (70% vs. 30%). But among those with wider AI deployments, that gap narrows by 33% (60% vs. 40%). In other words, the longer companies spend working with AI agents, the less likely they are to trust them with sensitive information.

What's inside this report and how to navigate

This report unpacks the nuanced responses we gathered from a market in the midst of a paradigm shift. We've analyzed the data to provide actionable insights for every CIAM stakeholder:

- **For engineering leaders:** Deep dives into the true cost of build-versus-buy decisions and how other organizations are modernizing authentication to create a competitive advantage
- **For security decision-makers:** Data on peer organization (not end-user) sentiment regarding various auth methods, perceptions around security objectives, and biggest challenges
- **For product managers:** User experience impressions from leading organizations, including reflections on security-versus-UX tension and shifting product priorities
- **For executives:** Tangible impacts and real-world outcomes from business decision-makers dealing with familiar CIAM challenges, drawing from dozens of different industries

Most importantly, this report will show you that you're not alone. Every challenge your team faces, from developer bandwidth to security/UX tradeoffs, appears throughout these pages. We hope our analysis will guide you to make better decisions and light the way forward.

The state of customer identity in 2025 is far from perfect. But this report offers a clear picture of where we are and where we need to go. Let's start that journey right now by exploring the data together.

Business impact of CIAM: Why does It matter?

Authentication is the only feature every customer is guaranteed to see. Because of this unique position in the product experience, it's simultaneously critical to everyone—and partially owned by all.

Perspectives compete and CIAM stagnates

Just think about the ways CIAM touches each part of an organization:

- Marketing needs clean identity data for outreach campaigns
- Sales wants to know if that demo request is legitimate or a bot
- Product teams balance friction against user experience and conversions
- Security demands strong protection and fraud prevention
- Support and customer success bear the cost of confused users

Each team has metrics, motivations, and priorities. Every one of them might have some say in how CIAM works, yet none are its "true" owner. This inevitably leads to competing pressures in how authentication should be implemented: the resources it receives, the teams who have to maintain it, and a laundry list of other obligations.

The result? Everyone wants CIAM to work toward their team's goals, but virtually no one has the time and resources to improve it. Inevitably, this leads to broken authentication processes.

84%

Agree that authentication is critically important, but the needs are not unique to their business

Impact of broken authentication

This fragmentation of CIAM, whether by coincidence or design, shows up frequently in our data. When we asked if authentication is important to their business, **84% of respondents agreed it's critical, but not unique to their business.**

In other words, authentication is both widely viewed as essential yet seen as undifferentiated. It's the digital equivalent of a door handle: utterly necessary for operating your business, but no one's first pick when it comes to improving the bottom line.

But remember how 46% of our respondents had delayed CIAM improvements to deal with other projects on their roadmap? Authentication gets de-emphasized often because it isn't seen as a top-line revenue source. Yet, this is a common misconception about CIAM's ability to keep and convert customers versus the competition.

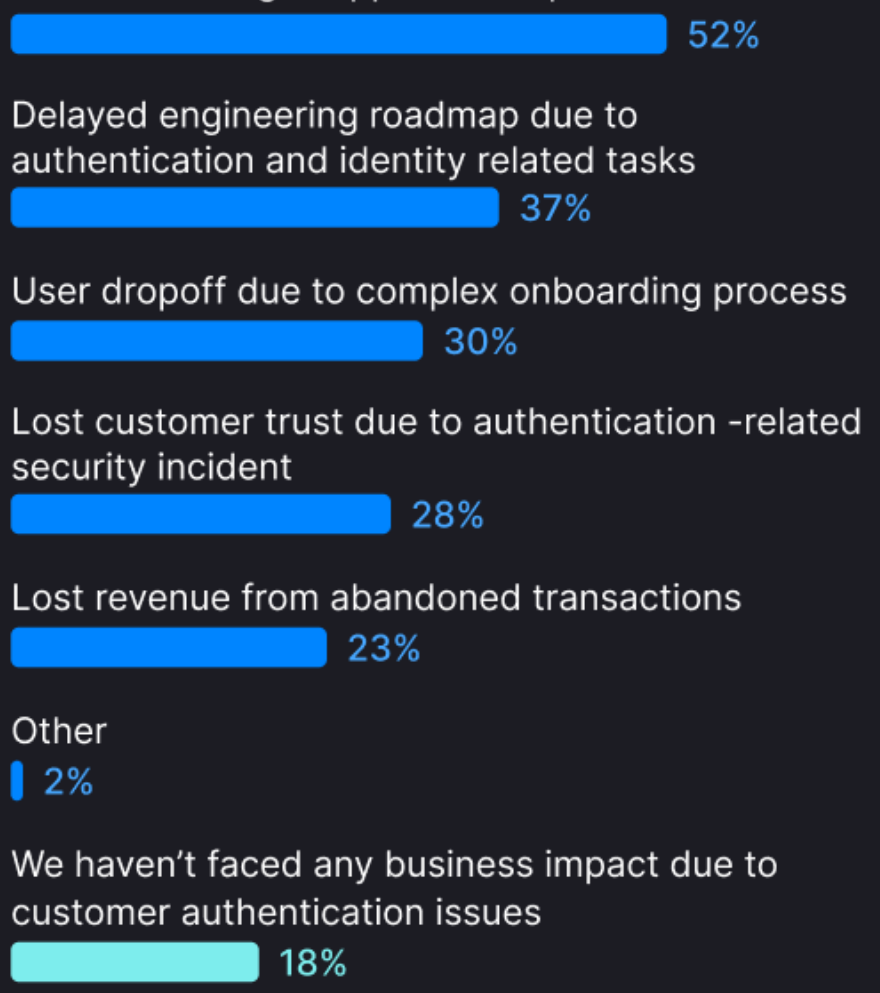
The disconnect becomes unavoidable when we compare it to data regarding authentication friction:

82%

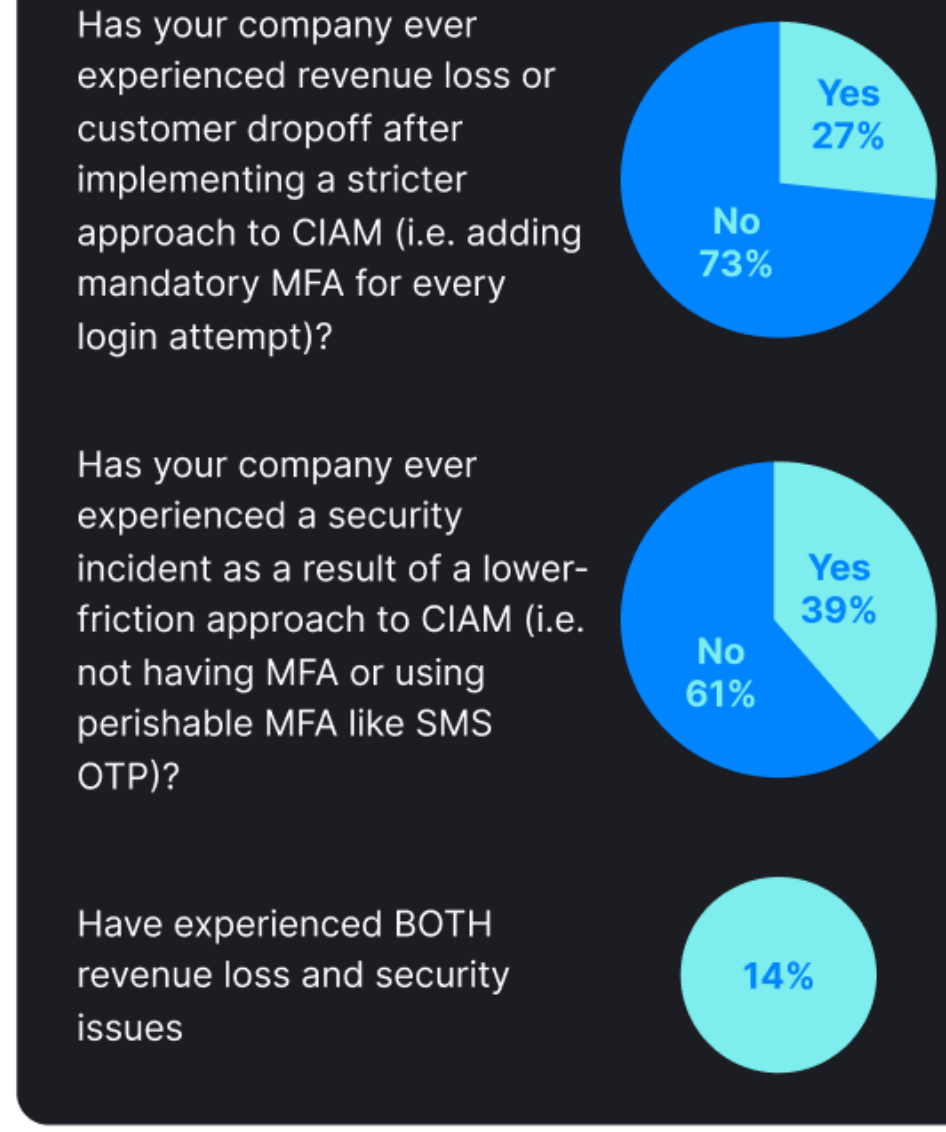
Have experienced business impact as a result of customer authentication issues

- A staggering 82% of respondents indicated they'd suffered negative business impacts as a result of customer authentication issues.
- Support teams report the highest direct cost, with 52% seeing increased ticket volumes due to poor authentication
- Nearly a third (30%) reported user drop-off because of complex onboarding processes
- Another 28% admitted customer trust fell due to an authentication-related security incident
- A quarter (23%) saw direct revenue impact as frustrated customers abandoned transactions

What negative business impacts has your company experienced because customers faced authentication issues?



CIAM decisions can result in direct business impact for some companies



Why endless auth cycles keep happening

The issues above result from what we've dubbed the "authentication doom spiral": auth problems pile up, but fixes are perpetually deprioritized because no one really owns it. In this never-ending cycle, improving authentication ends up as a side project relegated to product dev backlogs, issues they'll *hopefully* find time to tackle... ideally before a security incident or loss of revenue occurs.

Fragmentation is just part of the equation, though. Much of the reluctance to quickly address authentication issues stems from a fear of the negative outcomes:

- Over a quarter (27%) of organizations report losing revenue or customers after implementing stricter security measures
- And on the flip side, 39% experienced security incidents from enacting a lower-friction auth strategy (like no MFA or using phishable methods like SMS OTP)

The build-versus-buy dilemma directly amplifies these risks. Organizations using open-source CIAM solutions see dramatically worse outcomes:

- 50% report revenue loss from stricter authentication (compared to 26% for commercial solutions)
- 51% suffer security incidents from lax controls (versus 39% for commercial)

Our data indicates that the DIY approach, often chosen to maintain control over the implementation or to reduce costs, doubles down on the very problems it aims to solve.

Authentication can be a competitive advantage

Let's contrast this data with the CIAM experience of Cequence Security. As an API security organization, they needed ironclad authentication to protect customers on their cloud platform. Cequence faced two key challenges:

- Their existing solution required workarounds, meaning product developers spent precious time building complex fixes
- Onboarding new customers as SSO tenants required significant support from their team

After switching to a modern CIAM platform, their UX designers were able to take the reins of creating seamless authentication flows. Product devs no longer spent cycles resolving identity issues, and customer SSO onboarding became a self-service process that cut support time by 90%.

AI-driven access governance platform BalkanID originally chose open-source Ory Kratos to serve their customer identity needs. However, as they scaled to serve enterprise customers, authentication maintenance became an obstacle to refining their core offering. Hours per week were diverted from the product roadmap to deal with authentication edge cases, SSO onboarding, and auth feature additions.

Migrating to a commercial CIAM platform recouped precious time for their lean development team:

- Customers self-configure SSO, restoring time spent by infrastructure devs guiding them through the process
- Support for multiple login ID linking and aliases saves up to 2 days a month
- Countless hours reclaimed previously spent exporting login logs, troubleshooting lockouts, and cleaning up employee identities

Branch Insurance faced a different set of challenges, but ones that similarly affected support overhead. Operating in the highly regulated insurance industry, Branch served over 12,000 independent agents who generated mountains of auth-related support tickets. Their implementation of passkeys with a modern CIAM solution cut these support requests in half, but more importantly, reduced the negative impact of broken authentication on their bottom line.

In the scenarios involving Cequence Security, BalkanID, and Branch Insurance, authentication proved to be a powerful enabler for business processes. Authentication didn't generate top-line revenue, but it had a tangible impact by:

- Reducing potential losses due to customer drop-offs
- Eliminating costly support tickets
- Refocusing development time on the core product

The bottom line is that decision-makers who view authentication as necessary but unimportant miss its strategic value. In a marketplace where every customer interaction starts with identity, authentication is the actual foundation for meaningful digital transformation.

The impacts of authentication run deep, both good and bad. Broken auth hurts business, and better identity can be a powerful enabler—a digital doorknob, maybe, but not a simple checkbox to tick.

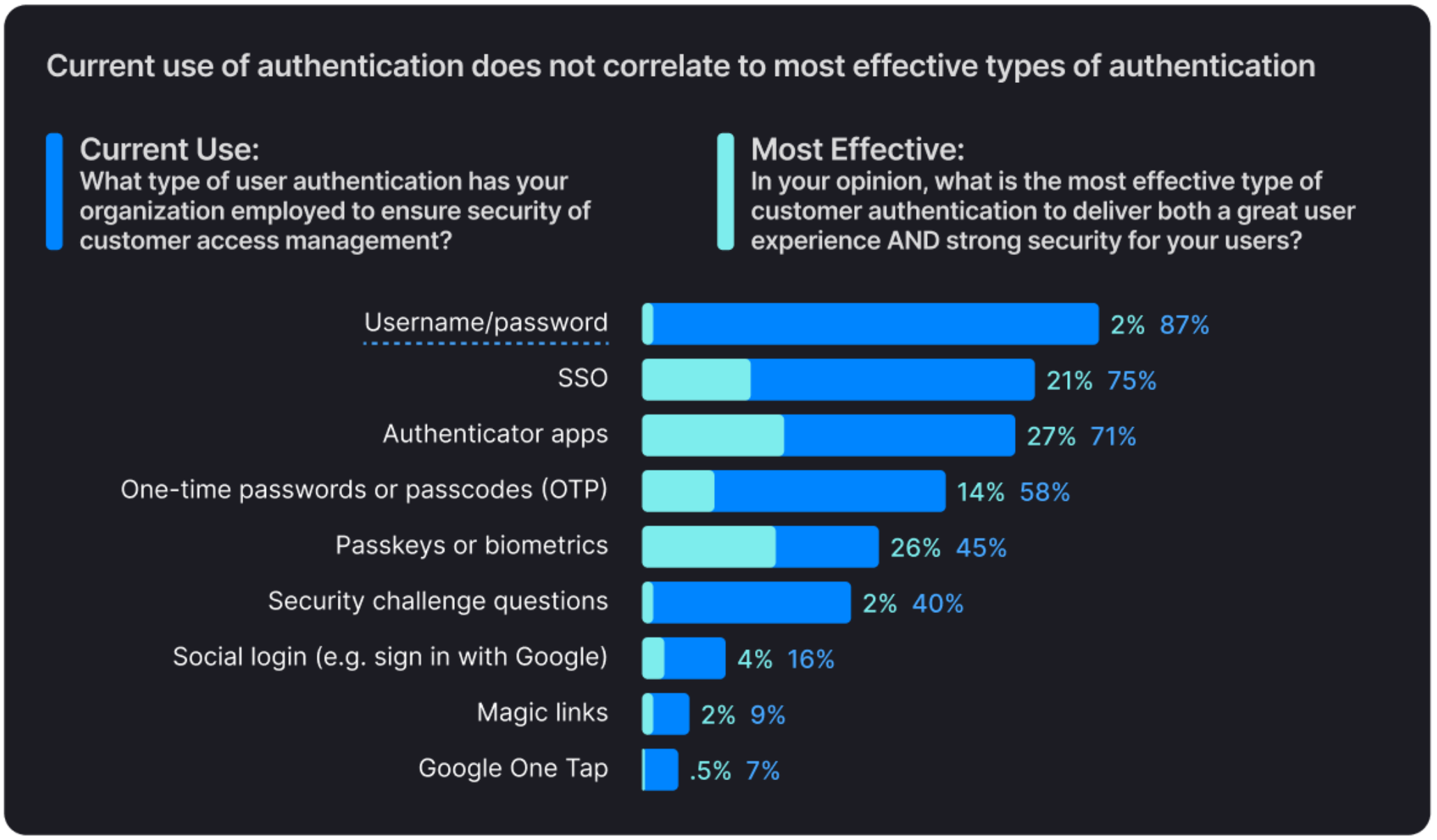
Authentication stagnation and the password paradox

Why is everyone using methods that nobody wants?

Organizations in 2025 are feeling insecure about their relationship with passwords. They know passwords are inherently destructive to their security posture and user experience, but they're hesitant to change.

Passwords are bad for CX, but...

We clocked a massive disconnect between what decision-makers know and what they deploy to customers: 87% still rely on username/password-based authentication, but only 2% believe it effectively balances security and user experience.



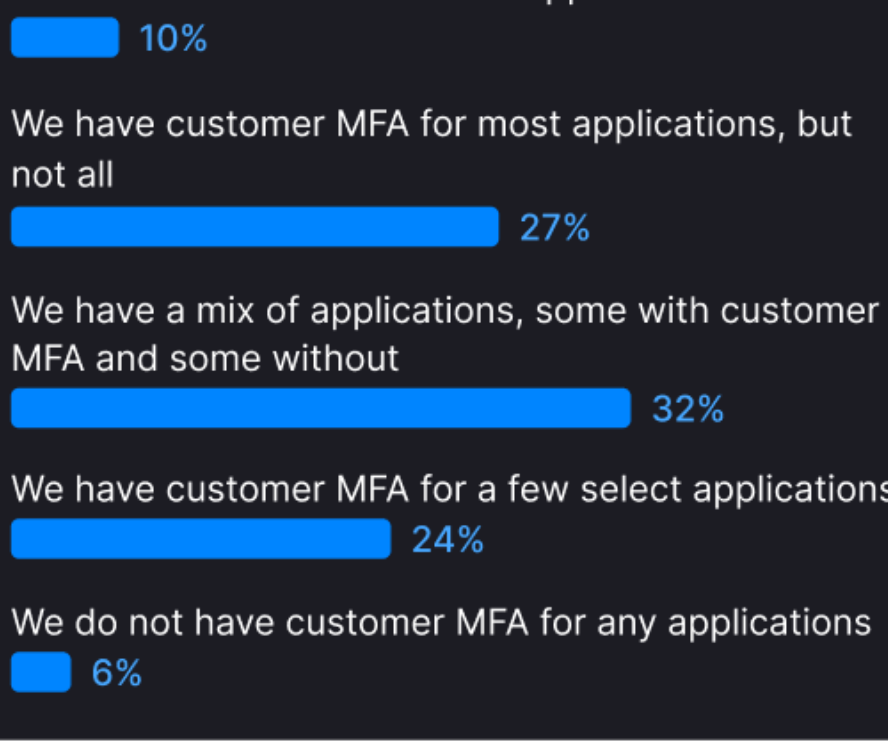
Of course, passwords aren't going it alone: SSO adoption sits at 75%, authenticator apps at 71%, and one-time passwords (OTPs) at 58%. These three methods are rarely used as a complete password alternative (with OTPs and auth apps more often a second factor), so this tells us that most companies know MFA is necessary for passwords to be sustainable.

87% of survey respondent organizations use passwords but only **2%** believe it's the most effective authentication method for UX and security

Yet, even MFA coverage is patchwork. While 94% have some form of MFA, only 10% give customers the option to enable it across all their apps. The majority (59%) have a mix of MFA-enabled and unprotected apps, while a quarter (24%) provide MFA on just a handful of applications.

MFA is a work in progress: 94% have MFA, but only 10% have it across all applications

Which of the following statements best describes your company's current implementation of customer multi-factor authentication (MFA)?



In short, we're seeing an authentication landscape dominated by passwords, which desperately need MFA to meet modern security standards. However, MFA adoption is piecemeal: an app here, a portal there, but rarely the whole customer-facing product suite. We're likely seeing the result of competing pressures, where MFA adoption remains half-finished likely because another roadmap item took priority over modernizing authentication.

Passkeys show disconnect between knowledge and practice

The story gets even more nuanced when we look at the sentiment toward modern methods like passkeys and biometrics.

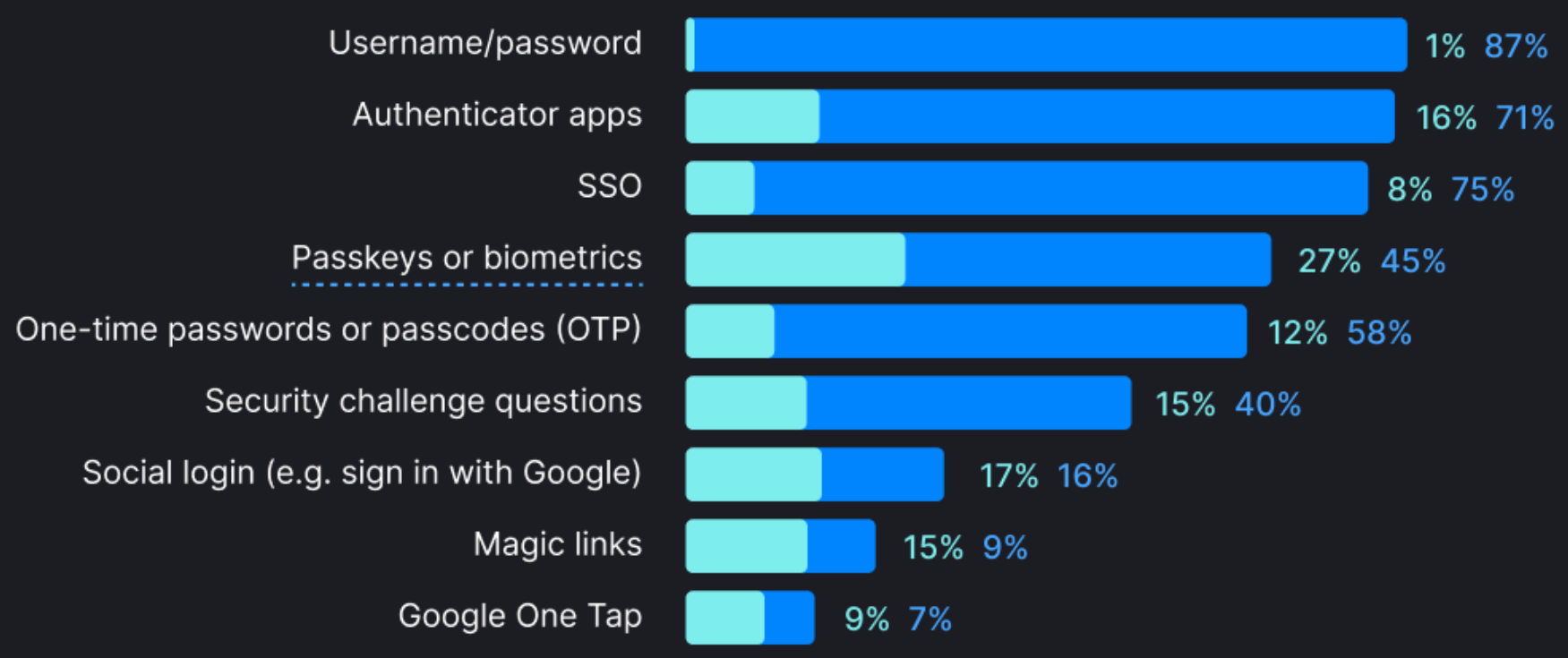
Currently, 45% of organizations have deployed passkeys or biometrics. Surprisingly, these are methods that only 26% of respondents identify as most effective for balancing security and UX. Our participants believed authenticator apps using TOTPs were more effective (27%), despite passkeys being widely regarded as one of the most user-friendly and secure authentication methods available.

This assessment of biometrics and passkeys doesn't match up with our participants' next moves, however: more than a quarter (27%) plan to implement passkeys over the next two years. Combining that number with those who already use passkeys (72%) makes it the third-most favored authentication method, only slightly trailing behind single sign-on (SSO).

Passkey/biometrics expected to have the highest rate of growth in next two years

Existing:
What types of user authentication has your organization employed to ensure security of customer access management?

Additional:
Does your company have plans to offer ADDITIONAL types of user authentication to customers within the next two years?



72%

of survey respondent organizations have already adopted passkeys for CIAM or plan to do so in the next 2 years

It's worth noting that a considerable percentage (21%) of respondents pointed to SSO—a method typically that offloads the primary burden of identity security to another organization—as the most balanced. Some of the most popular choices for B2B SSO, like Microsoft's Entra ID, allow users to sign in with passkeys. While we won't count this as tacit approval of passkeys, it does point to a frustrating reality for identity decision-makers. Authentication methods often overlap, and understanding which ones are working or not can be a challenge without proper observability baked in.

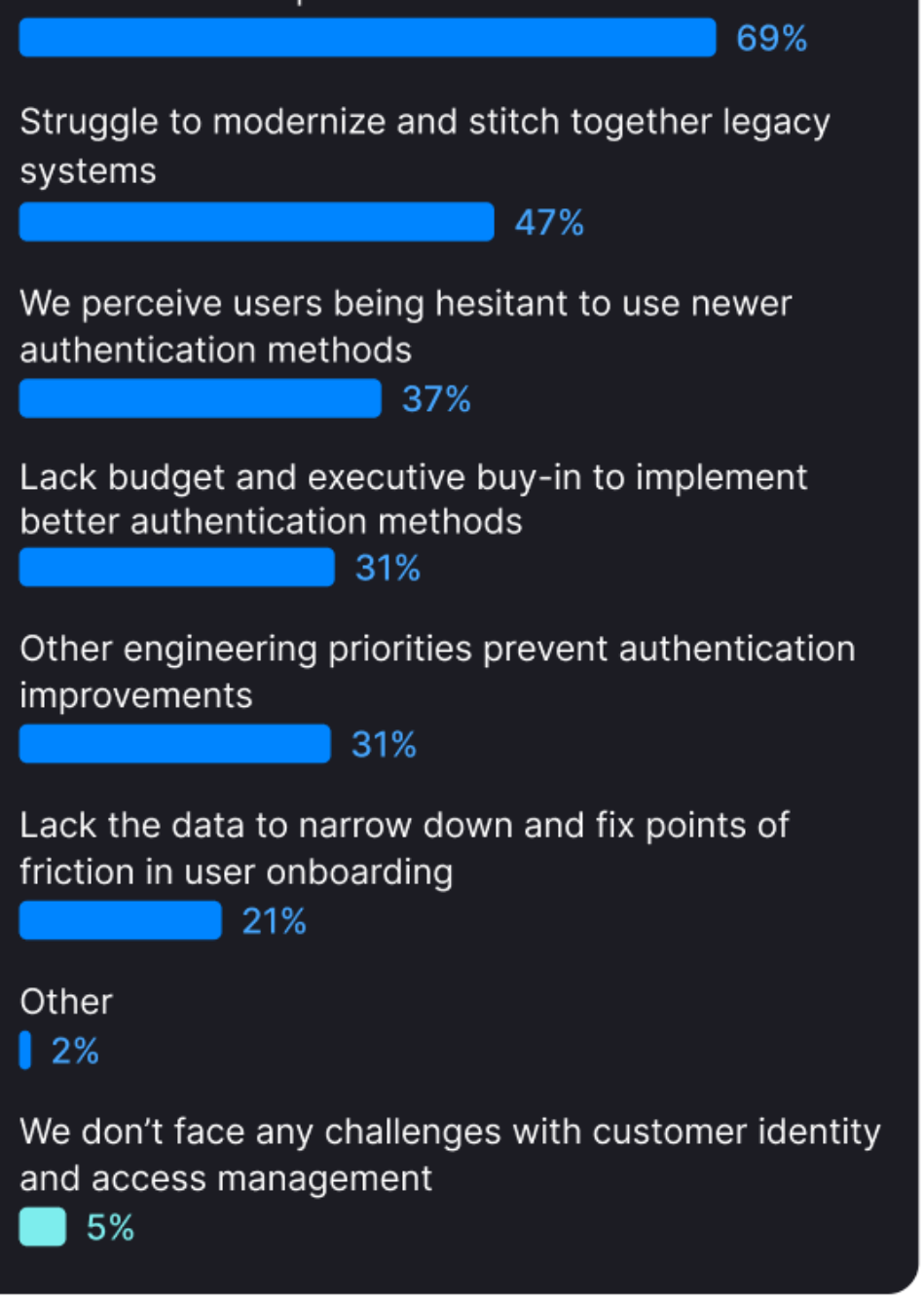
With these gaps in sentiment, we're witnessing a fundamental disparity between how CIAM needs are identified, prioritized, and resolved. When we dig into why organizations maintain a status quo that no one likes, we see that institutional barriers run deep:

- **User adoption fears:** 37% believe their users are hesitant to adopt newer authentication methods. This is a perception that becomes self-fulfilling when organizations delay change.
- **Budget constraints:** 31% lack the budget and executive buy-in to implement better authentication methods, reflecting how CIAM struggles for priority in spending decisions.
- **Engineering bandwidth:** Another 31% say other engineering priorities prevent authentication improvements, while 46% report CIAM projects are delayed by other roadmap items.
- **Difficulty modernizing legacy systems:** Half of organizations (47%) report struggling to modernize and stitch together legacy infrastructure, making it the biggest technical challenge.

These fears lead to hesitation in upgrading authentication, creating a vicious cycle where technical debt mounts while solutions get pushed to next quarter, next year, or never.

95% report that they find CIAM challenging; balance between CX and security tops the list

What challenges does your company face with implementing, maintaining, and evolving your customer identity and access management?



The "what if" of authentication

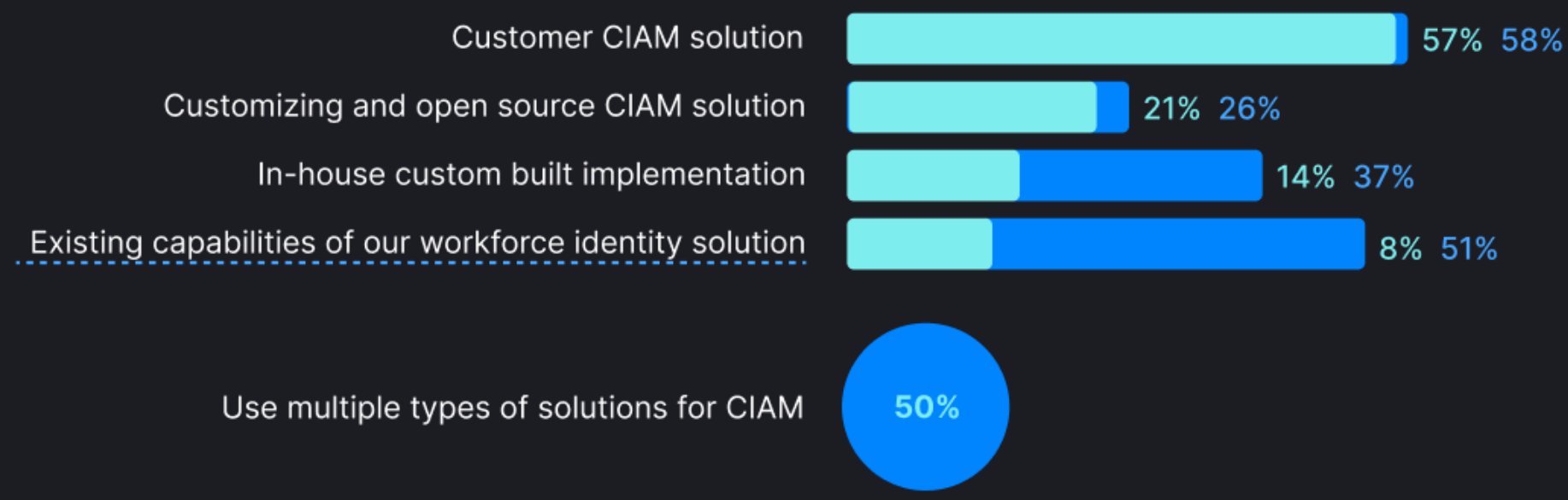
Perhaps the most telling discovery is what organizations wish they could do differently, were they to begin again from square one.

51% of respondents currently use workforce IAM for customer authentication. But when asked about starting from scratch, only 8% would actually choose to continue doing so. Similarly, 56% would prefer commercial CIAM solutions if given a clean slate, compared to the messy reality where 50% currently use multiple solutions cobbled together.

Half (51%) are using the existing capabilities of workforce identity, but only 8% report it's their preference

Existing:
What type of solutions does your company currently use for customer identity and access management (CIAM)?

New:
What type of customer identity and access management (CIAM) would your team prefer if you were starting from scratch in a new environment?



The gap between the current status quo and the desired "what if" scenario reveals the true nature of authentication stagnation. With over half of organizations using employee identity tools for external identities—knowing full well it's the wrong approach—they feel trapped by decisions made early and hastily.

51%
of survey respondent organizations use workforce solutions for CIAM but only
8%
would choose the same path if starting from scratch

But why do companies settle for methods they actively dislike (passwords) and solutions they'd prefer not to use (workforce IAM)? The data indicates customer experience and modernization regularly take a back seat to other pressures. When asked about their organization's top priorities in choosing an identity solution, the top three choices as ranked by respondents were:

- Security and compliance (64%)
- Total cost of ownership (51%)
- Reliability, scalability, and uptime (43%)

Respondents placed a solution's ability to adapt to customer needs fifth (32%), and interoperability with other tools—a critical component of modern CIAM—in sixth position (31%). These priorities may explain why companies readily repurpose their workforce IAM for customers, but gradually regret that choice when it proves unwieldy. Internal IAM may meet the basic functions of security and uptime paired with lower costs, but they lack the flexibility and connectivity to meet changing market expectations.

Nine out of ten CIAM decision-makers agree

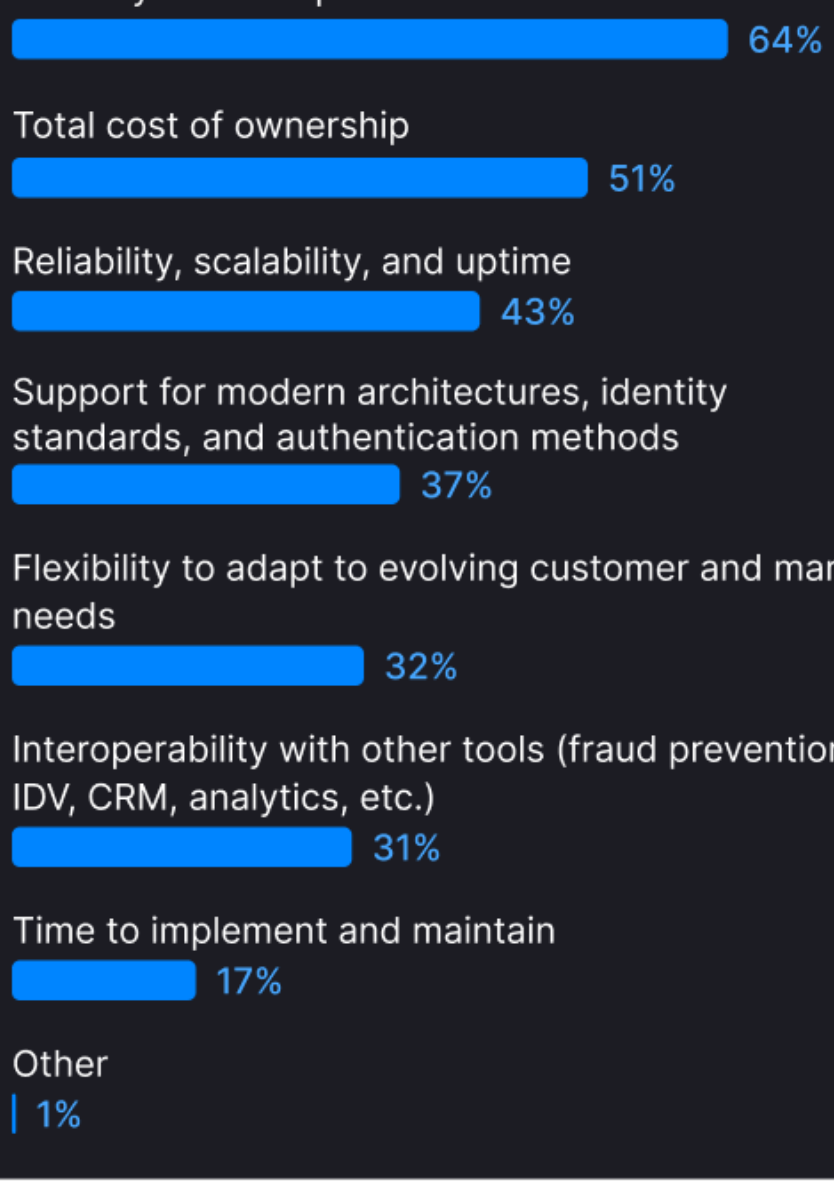
Imagine a room with ten CIAM decision-makers sitting in a circle. You could start with one, rotate clockwise to face each in turn, and come nearly 360° before you were looking at someone who doesn't use passwords at their organization. Now think about what they might say if you asked those nine people why they still use passwords despite all the issues they pose:

- Using workforce IAM for budgetary reasons (and passwords are the easiest or only option)
- Limited dev cycles compounded by competing priorities
- Lack of executive buy-in to implement better auth methods
- No in-house expertise with modernizing authentication
- Doubt that users will adopt expensive new auth upgrades

Ultimately, the “password paradox”—that is, the practice of using methods no one actually wants—reveals a deeper organizational paralysis around seemingly disparate goals. Companies know what good CIAM looks like, and our survey shows a remarkable consensus that passwords are the least-favored option. But between that knowledge and action lies a chasm of competing priorities wrestling to come out on top: budget constraints, developer bandwidth, unwieldy legacy systems, and fear of user pushback.

Security/compliance and TCO top lists of solution selection priorities

What are your company’s top priorities when choosing an in-house, open-source, or commercial solution for CIAM?



The takeaway here is simple: Authentication stagnation isn’t really a technical problem. It’s a strategic one, borne out of the psychology that “what works for us will work for customers.” Unfortunately, for many long-suffering companies, the pain of staying the same hasn’t yet exceeded the perceived pain of change.

The developer (in)experience

Developer experience with CIAM looks a bit like a game of Hot Potato: nobody wants to hold the responsibility of authentication when the music stops, so everyone keeps passing it along. Yet, everyone still plays, expressing sentiments (and disappointments) when things aren't done how they'd like.

So much to do, so little time

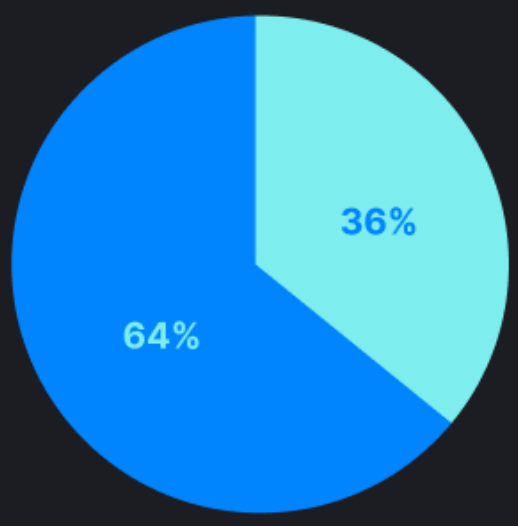
Our data reveals a fundamental disconnect between CIAM development and stakeholders (who, as we've previously noted, are virtually everyone at an organization).

CIAM decision makers are almost twice as likely to think developers don't spent enough time on authentication

Which of the following statements best characterizes your opinion about the amount of developer time spent implementing and maintaining customer authentication for your company's applications?

Not enough time:
Developers don't spend enough time on authentication, creating security risks

Too much time:
Developers spend too much time on authentication, which distracts them from core product priorities



The majority (64%) of CIAM decision-makers believe developers don't spend enough time on authentication, creating potential security risks. The rest (36%) think they're spending too much time on authentication, drawing their limited bandwidth away from core product responsibilities. In either case, developers are often juggling countless authentication responsibilities alongside their "real" work.

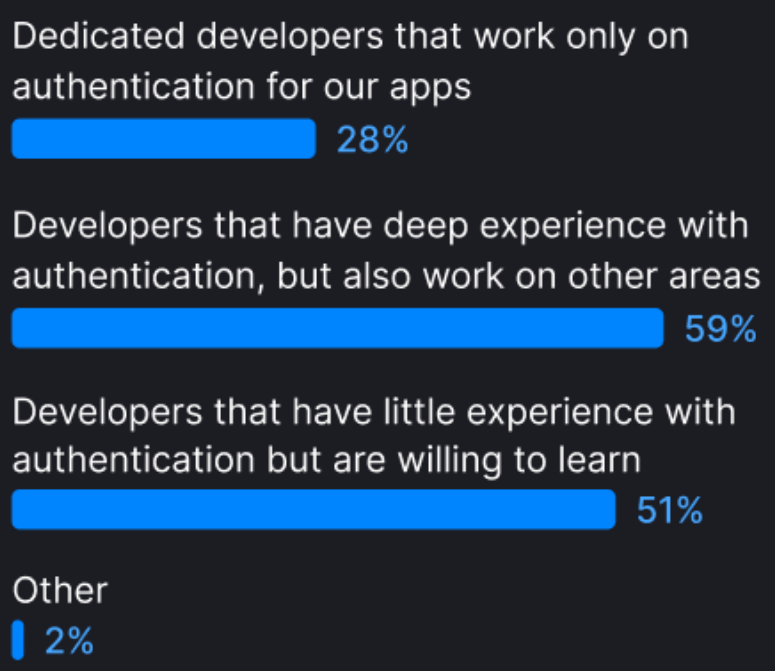
The expertise gap may explain some of this uncertainty:

- Half (51%) of all organizations task developers possessing minimal authentication experience with building these critical systems.
- Only 28% of all organizations report having dedicated CIAM engineers.
- Among companies who use in-house, custom-made authentication (36% of all respondents), only 27% have full-time CIAM developers.

Let that last number sink in for a moment. The very organizations that went with "build" over "buy" are the least likely to invest in specialized expertise—with 54% of them reporting that developers having little to no experience are responsible for their home-brewed authentication.

Half (51%) have developers without experience working on authentication

What types of developers implement and maintain customer authentication for your company's applications?



Pair that with the fact that most companies trust their customer identity infrastructure to devs who are learning on the job, and you've got a recipe for authentication disasters. It's like asking a car mechanic to fix an airplane: There's lots of overlap between the two disciplines, sure, but it's not a scenario where mistakes are acceptable. You want to be beyond certain the plane will fly without a hitch. And mistakes in production made by authentication amateurs, no matter how willing they are to learn, can be costly.

51%

of survey respondent organizations task developers with minimal authentication experience to build and manage CIAM systems

The quiet cost of context switching

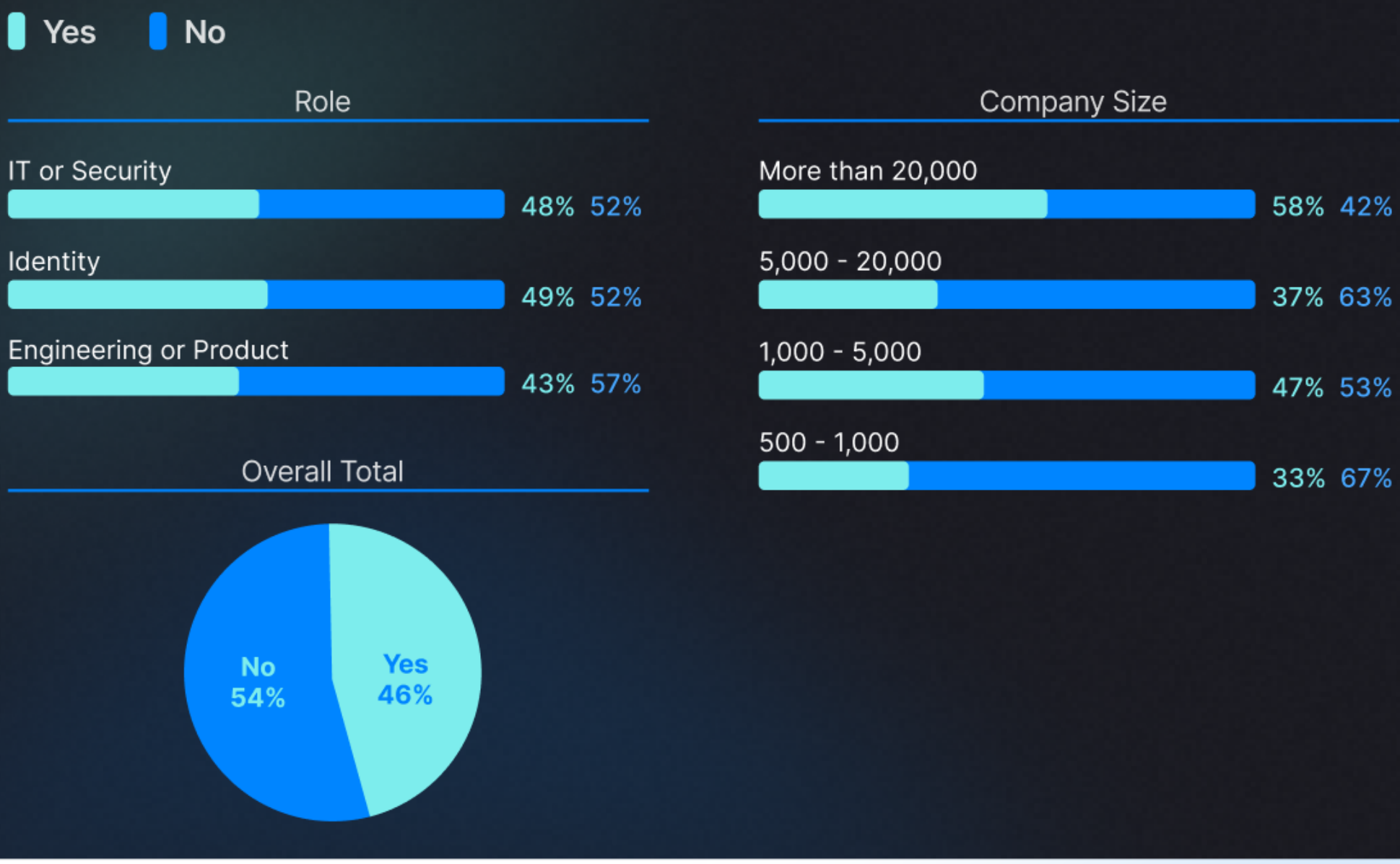
Dig deeper into the relationship between company size and CIAM impacts, and subtle patterns emerge. Organizations with 20,000+ employees show the most acute problems with 58% reporting CIAM projects were delayed by other priorities (versus 33% for smaller companies). And despite having more developers at their disposal, authentication is rarely anyone's full-time job even at these large enterprises: 64% say the developers who work on authentication are tasked with other priorities.

Organizations with homegrown solutions and companies using open-source frameworks face perhaps the steepest challenges:

- Both experienced revenue losses, with 30% of those using in-house CIAM and a staggering 50% of those with open-source solutions seeing financial impact
- 51% of those using open-source solutions reported security incidents from poor authentication

Almost half (46%) report that CIAM projects have been impacted because of other requirements

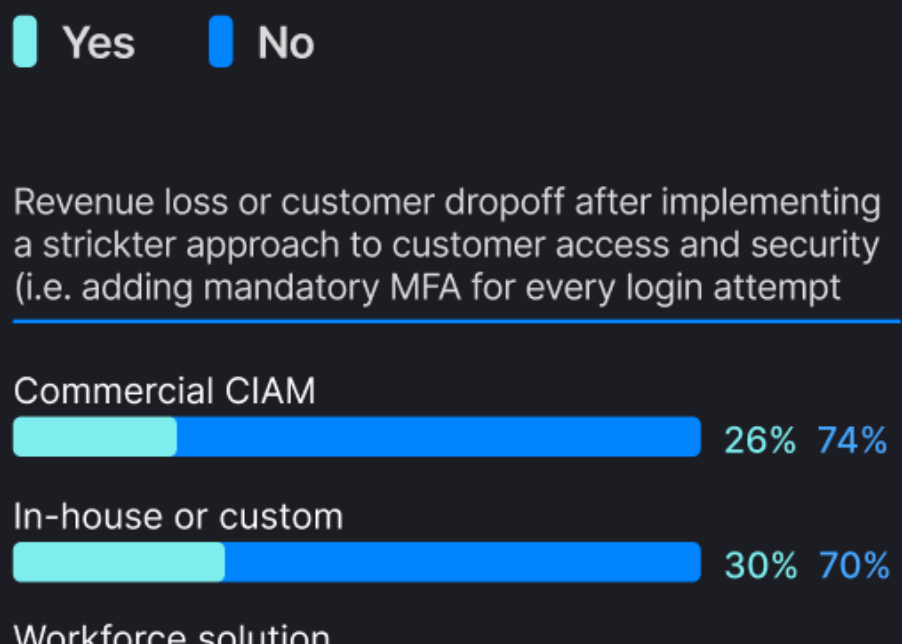
To the best of your knowledge, has your company ever cancelled or delayed a customer identity or authentication initiative because other product requirements took priority?



- Both groups had some of the least comprehensive MFA coverage, with 41% of open-source solutions only offering customer MFA on a handful of apps
- 55% of open-source solutions have canceled or delayed CIAM upgrades due to competing priorities

Companies using open-source CIAM are far more likely to report both revenue loss and security incidents.

To the best of your knowledge, has your company ever experienced:



These companies chose control, but their developers—only 27% of whom are CIAM specialists, in the case of homegrown—are unable to fully focus on authentication.

The result? Authentication improvements happen in fleeting, stolen segments between "real" feature work.

Opinions on improving developer experience

Respondents felt strongly about where developers needed the most help in implementing effective CIAM. When asked what capabilities would benefit their development teams, 99% identified at least one area that was missing or needed a boost:

- 57% want comprehensive support for identity standards (OAuth, SAML, FIDO2)
- 52% need self-service SSO and SCIM setup
- 51% want unified authentication across multiple apps
- 49% need adaptive, phishing-resistant MFA

46%

of survey respondent organizations say that CIAM projects have been delayed due to competing product requirements

What developers actually need

The solution to these push-and-pull pressures isn't more developers or more time. It's less developer commitment. The 39% asking for abstraction layers have the right idea: Modern CIAM, our digital doorknob, should be like a part of the furniture. It's critical infrastructure that just works. And based on our data, those with a strong sense of how modern CIAM works know it should be maintained by specialists, simplified for non-specialists, and invisible to everyone else.

The tools developers actually want look like this:

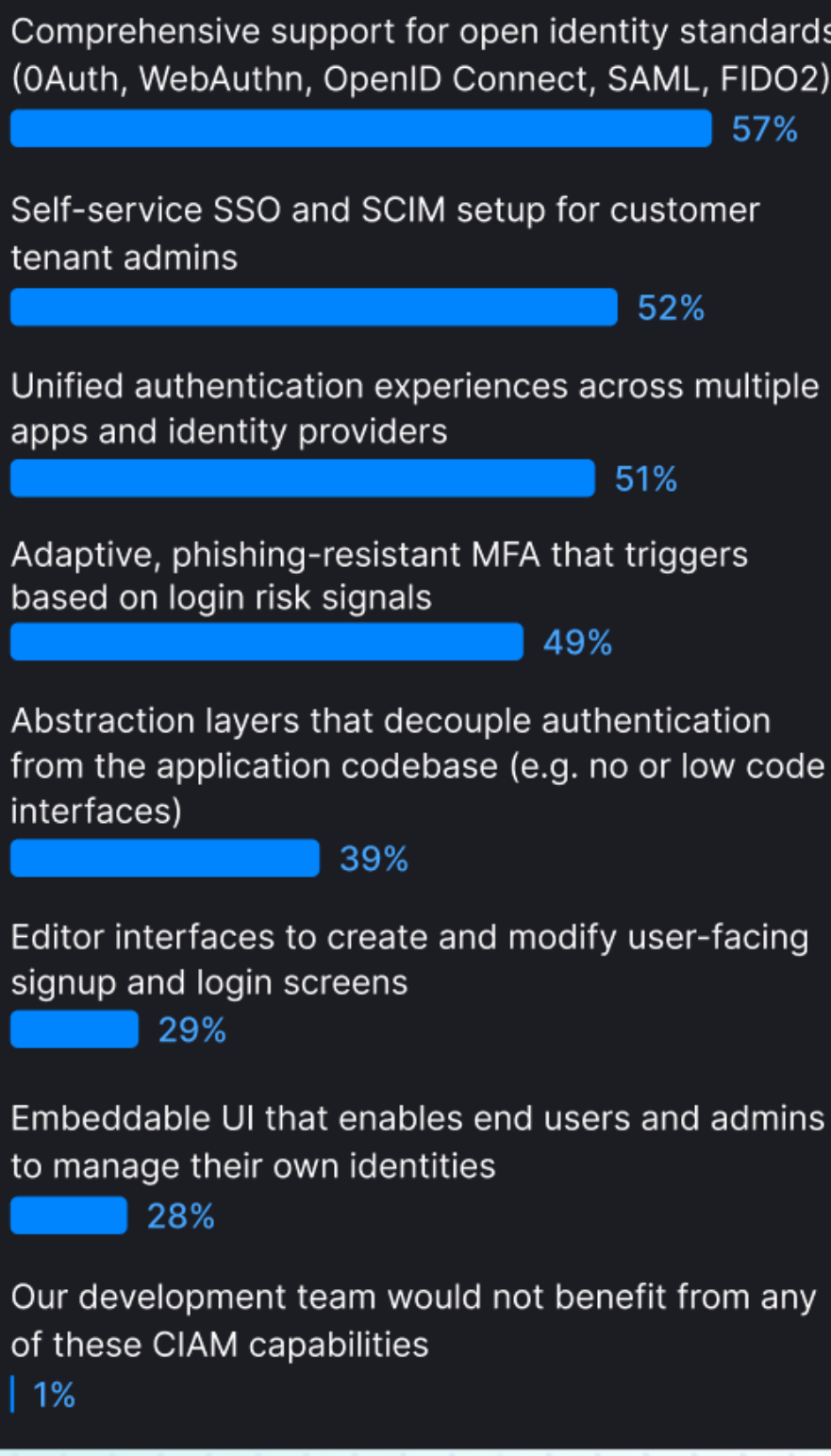
- **Visual workflows:** Let security and product teams modify authentication flows without touching sensitive code
- **Prebuilt integrations:** Stop reinventing the wheel with from-scratch connections to third-party systems
- **Managed infrastructure:** Handle scaling, uptime, security updates, and compliance automatically
- **Clear documentation:** When devs actually need to wade into technical waters, they've got a guide for every scenario

Looking back at our findings, we see that the developer "inexperience" problem isn't a skill issue at all. It's a specialization and bandwidth dilemma. Asking devs who came aboard to build your product to do on-the-job auth training is not only unfair, it winds up hurting revenue. True, sometimes developers will have to roll up their sleeves and do something not in their "job description." But we're seeing that square-peg-round-role approach come back to kick a lot of companies while they're down.

Organizations that recognize authentication as highly specialized, constantly evolving infrastructure (not feature work or product capabilities) can free their developers to build what actually matters to them. The key characteristics that differentiate the product from the competition. The reason these engineers answered the job offer. It's either that, or continuing to pass the Hot Potato until someone gets burned.

52% say their CIAM development teams would benefit from self-service SSO and SCIM setup

Which of the following capabilities would be beneficial to the developers at your company?



The security-CX balancing act (and why everyone's tired of it)

Three-quarters (73%) of organizations say finding the right balance between security and customer experience is genuinely hard. But it's easy to see why so many respondents feel this way: Even within the same company, departments can't agree.

Teams pull in different directions

We asked our participants whether they emphasize security, customer experience, or aim to balance both. Unsurprisingly, the results were split:

- 39% lean toward security
- 26% favor customer experience
- 34% aim for equal emphasis on both

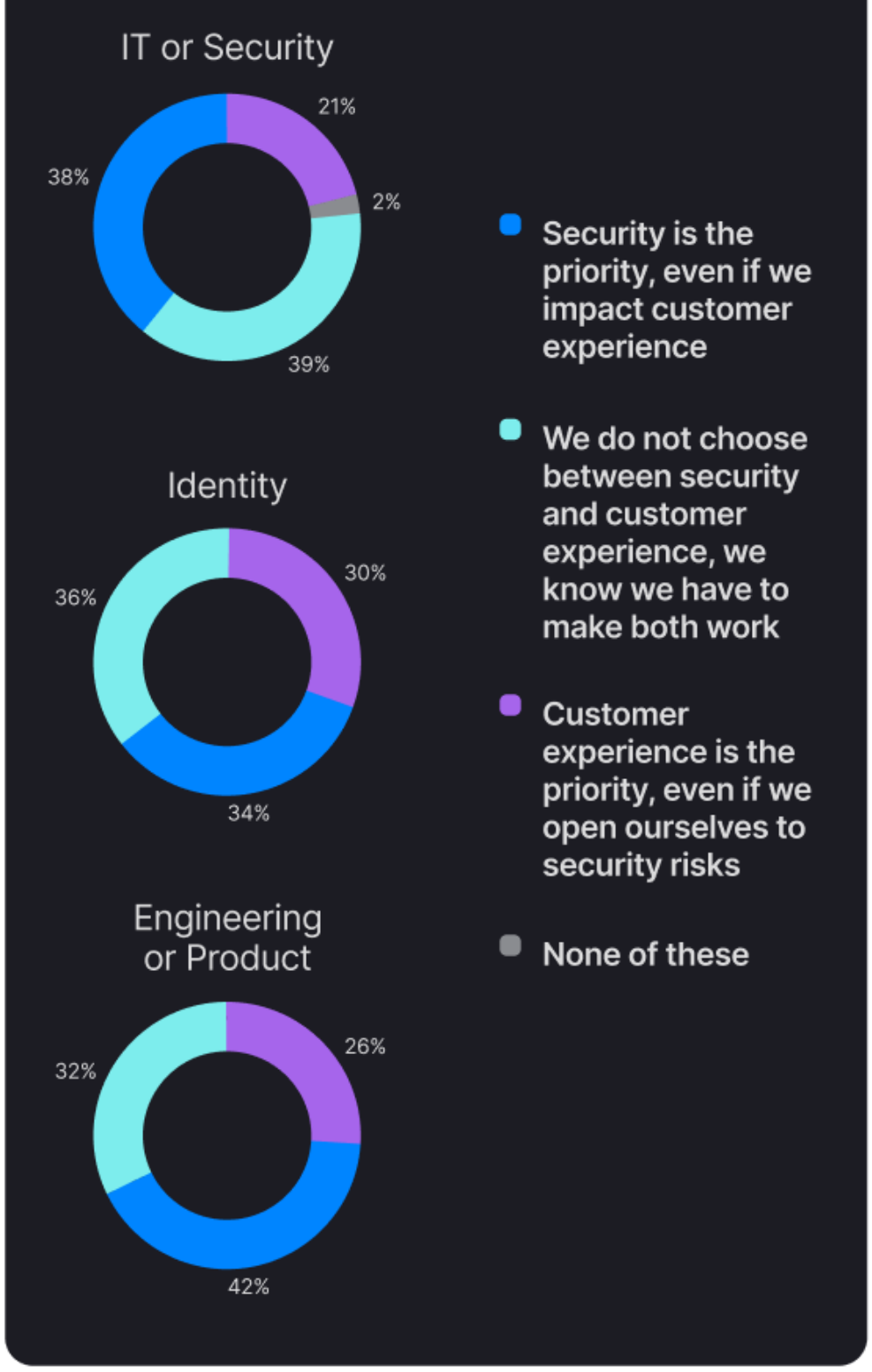
No consistency on how CIAM decision makers balance security and CX demands

Which of the following statements best describes your company's approach to balancing security requirements with customer experience needs?

This is the natural result of different teams pulling in different directions based on their lived experience. Engineering teams (who favored security the most at 42%) have seen what happens to their hard work when risky authentication takes over. Identity teams (who favored CX the most at 30%) see users drop off from friction daily. Security decision-makers leaned toward lockdown less than engineering, coming in at 38%, perhaps demonstrating a disconnect in confidence.

All roles struggle with priorities, although identity is slightly more likely to prioritize CX and dev to prioritize security

Which of the following statements best describes your company's approach to balancing security requirements with customer experience needs?



Even though everyone prefers security over CX to varying degrees, there's considerable gaps in priorities between teams. This internal misalignment explains why balance is a struggle; everyone feels like their approach is right from where they're sitting, which makes finding common ground that much harder.

Business consequences of getting auth wrong

Favoring security tracks neatly with the size of an organization: the larger the company, the more willing they are to add friction. The biggest companies in our survey showed the strongest bias toward security, with a 27-point gap compared to favoring CX.

Now, take a look at how security favoritism drops as company size shrinks:

- **Large enterprises (20,000+ employees):** 48% prioritize security over CX
- **Medium enterprises (5,000-20,000):** 39% emphasize security
- **Small enterprises (1,000-5,000):** 34% favor security

These numbers suggest the largest enterprises (20,000+ employees) can afford to be security-heavy—or so they believe. But 29% saw negative impacts from implementing a too-strict security policy, which is ten points higher than organizations with 5,000-20,000 employees (19%). Our take? Despite a winning market position, even household names can't convince impatient customers to stomach extra auth friction.

Let's put these CX vs. security preferences into perspective by examining which types of organizations lost revenue when pushing stricter controls:

- Overall, 27% lost revenue after implementing overzealous authentication
- Open-source organizations: 50% (nearly double the average)
- Workforce IAM: 33%
- In-house at 30%
- Commercial CIAM is the best by far with only 26% reporting losses

On the reverse side, when security gets deemphasized too much with weak or phishable MFA:

- Overall, 39% experienced security incidents
- 28% of all participants say they lost customer trust as a result
- Open-source orgs: 51% suffered security incidents

Largest companies more likely to prioritize security of customer experience

Which of the following statements best describes your company's approach to balancing security requirements with customer experience needs?

- Security is the priority, even if we impact customer experience
- Customer experience is the priority, even if we open ourselves to security risks
- We do not choose between security and customer experience, we know we have to make both work
- None of these

- Workforce IAM: 41% saw breaches
- Commercial CIAM (39%) and in-house builders (36%) were the lowest for security issues

Meanwhile, the 14% who experienced both revenue loss and security incidents? They've learned (perhaps the hard way) that oscillating between extremes isn't the same as achieving balance.

50%

of organizations using open-source CIAM lost revenue after implementing stricter approaches to user auth

51%

of organizations using open-source CIAM experienced a security incident after implementing lower-friction auth approaches

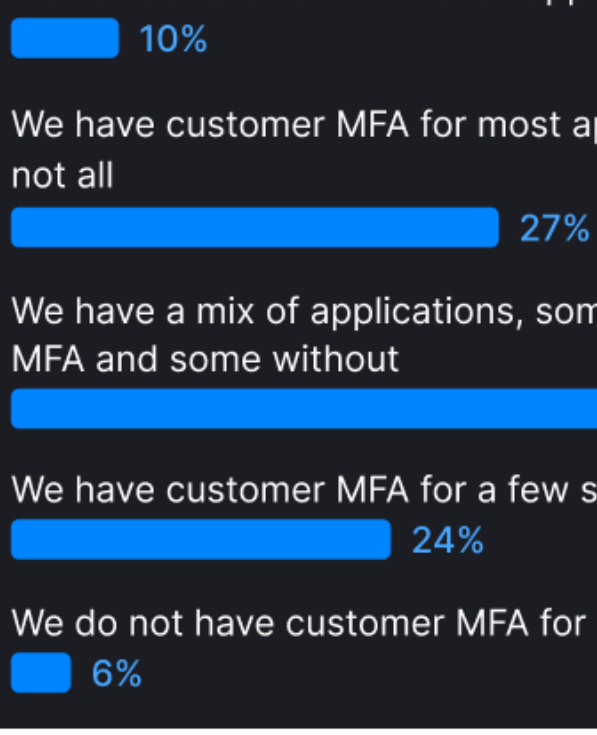
MFA coverage shows a lack of commitment

MFA is an incomplete solution for an imperfect ecosystem, but it's the best we've got until passwords are finally in the rearview mirror. Our MFA numbers tell a story of good intentions undermined by inconsistent execution.

Yes, as previously mentioned, 94% of organizations have some form of customer MFA. That sounds impressive until you realize only 10% have MFA across all their applications. The majority (32%) live in a messy middle, mixing protected and unprotected apps, while the rest (27%) have MFA on "most" (but not all) applications.

MFA is a work in progress: 94% have MFA, but only 10% have it across all applications

Which of the following statements best describes your company's current implementation of customer multi-factor authentication (MFA)?



Here's our take: This is no accident. The half-hearted implementation of MFA is a result of competing fears, pressures, and organizational attitudes. Companies they're also apprehensive about customer friction. With 37% perceiving users as hesitant to adopt new authentication methods, and 27% already having lost revenue from stricter security, every MFA decision feels like picking the lesser of two evils.

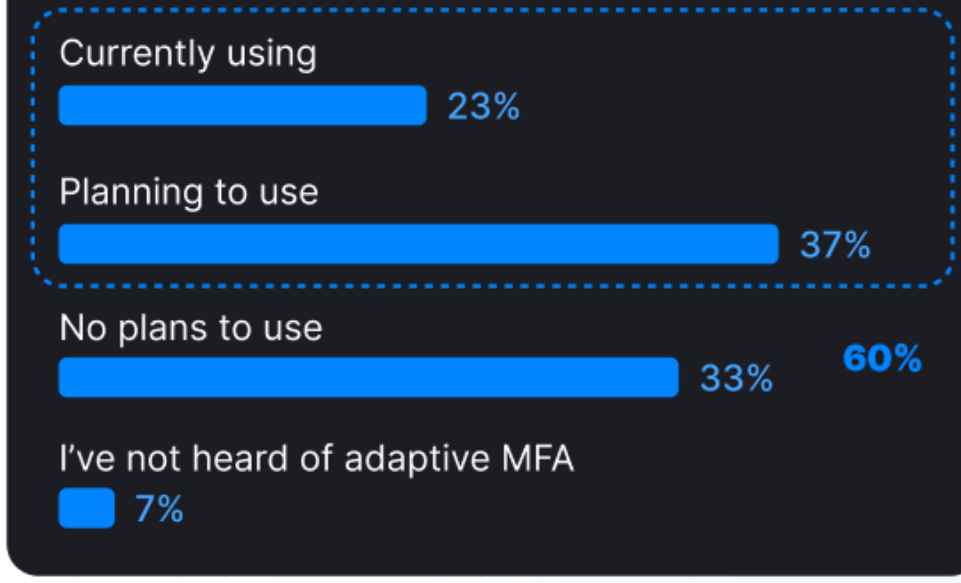
Because of this dichotomy, organizations compromise... sort of. They protect critical apps but not others, enacting security theater that causes always-on friction for legitimate users while leaving some doors unlocked for attackers. It's really the worst of both worlds, based on the assumption that MFA is an optional luxury for some applications.

Adapting to modern customer expectations

Here is where the story turns into a bit of a rollercoaster. Adaptive, risk-based MFA exists specifically to solve the dilemma above: adding friction only when something looks suspicious, disappearing when legitimate users go about their business. Only 23% currently use it.

60% are using or planning to use adaptive MFA

Is your company using or planning to use adaptive or risk-based MFA (i.e. only enforcing MFA for risky logins, not enforcing MFA for legitimate repeat users)?



Here's the upside: A reassuring 37% plan to adopt adaptive MFA, which (eventually) puts our tally at 60%. We were surprised that these combined numbers were greater than half our participants, and it provides a hopeful outlook for customer friction.

As organizations realize adaptive MFA provides an equally strong alternative to mandatory MFA for every login, we hope they'll be tempted to implement the method across all their apps.

And now for the final descent on our adaptive MFA rollercoaster: A full third of respondents (33%) simply aren't considering adaptive MFA at all. This begs the question, "Why not?" After all, this approach to MFA elegantly balances CX and security.

But the holdouts to adoption are to be expected, especially when you consider:

- 51% of organizations rely on developers with little to no authentication experience
- 31% cite other engineering priorities as barriers
- 64% of respondents said their devs don't spend enough time working on authentication

It's possible that the 33% who aren't even considering adaptive authentication are struggling to find the bandwidth, personnel, and expertise to begin. These organizations are already buried under tech debt, making authentication modernization a luxury they can't afford. That's unfortunate, because gracefully balanced auth friction can be a competitive advantage because today's customers easily become frustrated (and drop off) when faced with always-on MFA.

Only **10%**

of organizations have implemented MFA across all customer-facing applications

The promise (and puzzle) of passkeys

The passkey adoption numbers tell an encouraging story:

- 45% currently use passkeys/biometrics
- Another 27% plan to add passkeys in the next 2 years

That's 72% of the market bought in or buying in soon, which is a remarkable curve for technology that's relatively fresh compared to its peers. This organizational momentum tracks neatly with consumer awareness and acceptance, according to FIDO Alliance survey data.

In their 2025 "World Passkey Day" research, FIDO revealed that 75% of global consumers are now aware of passkeys, and critically, 38% of those who report using passkeys enable them everywhere possible. Infrastructure is catching up, too, says FIDO: Nearly half (48%) of the world's top 100 websites now support passkeys, which paves the way for an ecosystem without passwords—and where customers increasingly expect this option.

Yet, despite the signs of significant buy-in, something curious emerges in our data: only 26% of respondents identified passkeys as the best balance between UX and security. Authenticator apps edge them out at 27%, while SSO trails in third at 21%. It's an unexpected twist for TOTPs to out rank the intrinsic MFA of passkeys, or for SSO to even come close behind. Our take? It's misplaced skepticism because passkeys haven't earned their stripes among the old guard (yet).

Information gaps and real-world passkey outcomes

Microsoft successfully onboarded a cool one billion users to passkeys, documenting some truly impressive metrics:

- Passkeys are fast: Passkey users log in three times faster than password users
- Passkeys are effective: Passkeys result in a login success rate three times that of passwords (98% vs. 32%)
- Passkeys speed up MFA: Passkey sign-ins are eight times faster than a password with traditional MFA

These are truly transformative improvements in user experience. Microsoft also points out the inherent security advantages of passkeys compared to passwords, noting they "block 7,000 attacks on passwords per second—almost double from a year ago." Passkeys are much more resilient and face none of the automated threats aimed at knowledge-based credentials.

Thus, when we combine these outcomes to the perception of passkeys among our survey participants, we see a disconnect. We think organizations may be projecting their own hesitation toward the new breed of auth methods onto customers. Remember how 37% of respondents worry customers won't adopt new authentication methods?

Well, Microsoft discovered something surprising when they actually asked users to give passkeys a test drive: About 25% of users who saw a passkey nudge engaged with it. That may not sound like a lot, but it was five times Microsoft's pre-launch predictions.

The point we're driving at is that organizations deploying passkeys (that's 76%) but don't prompt users to actually turn them on are going to create a self-fulfilling prophecy.

Why can't organizations find the perfect balance?

The 73% struggling to balance security and CX are not failing, at least, not at the decision-maker level. Our participants are reporting the very real difficulty of navigating complex organization dynamics while keeping the lights on. Looking at the data, we can see where their pains originate:

Misaligned teams with competing priorities. Remember how much of our engineering crowd favors security (42%), how many identity specialists prefer CX (30%), and how no one really owns the complete picture. Every authentication decision becomes a negotiation between departments measuring success differently.

Resource constraints complicate CIAM improvements. With 51% relying on developers with minimal authentication expertise, 31% citing competing engineering priorities, and 47% fighting legacy system limitations, even knowing the right answer doesn't mean you can implement it.

The paradox of choice without conviction. Organizations deploy multiple authentication methods (45% use passkeys, but only 26% believe they're the best UX/security balancer), use MFA (but only 10% have total coverage), and perform security theater that frustrates users while still leaving gaps. They know passwords aren't the answer (only 2% believe passwords balance UX and security well), but 87% still use them.

Real talk: The security and CX push-pull relationship is a good problem to have. It drives innovation, pushes companies to deliver better experiences, and creates opportunities to outdo the competition.
We think it's time for companies to realize these two objectives are not mutually exclusive. Are they in tension? Absolutely! But this is not a zero-sum game. We're not bound by technology limitations anymore: methods that are CX-friendly and secure are here, they're superior, and they're well-established. Modern authentication (passkeys, adaptive MFA, magic links) proves you can have both, but it requires investment, expertise and organizational alignment.

The agentic AI future compounds identity challenges

Organizations are rushing headlong into AI adoptions with authentication infrastructure that's already stretched unbearably thin. While 88% of respondents are using or planning to use AI agents, only 37% have progressed beyond pilot programs. The identity implications are mostly in uncharted territory.

Everyone is betting on AI, but nobody's ready

The numbers from our research paint a picture of widespread AI enthusiasm colliding with operational realities:

- 95% believe authentication will be critical for secure AI agent adoption
- 88% are currently using or plan to use AI agents / chatbots
- Only 37% have moved beyond early pilots to meaningful deployment
- Just 12% aren't considering AI adoption (mostly smaller companies)

This gap between AI aspirations and actual implementation outcomes makes perfect sense. Gartner predicts 30% of all AI projects will be abandoned by the end of 2025, citing "inadequate risk controls" and unclear goals among the key reasons. An MIT study from 2025 revealed that 95% of custom enterprise GenAI pilots fail to enter production.

Meanwhile, five of the OWASP Top Ten for LLM and GenAI have authorization and authentication-related mitigations. Simply put, organizations are being asked to secure tomorrow's technology with today's already strained resources.

88%

of respondents are using or planning to use AI agents, but only

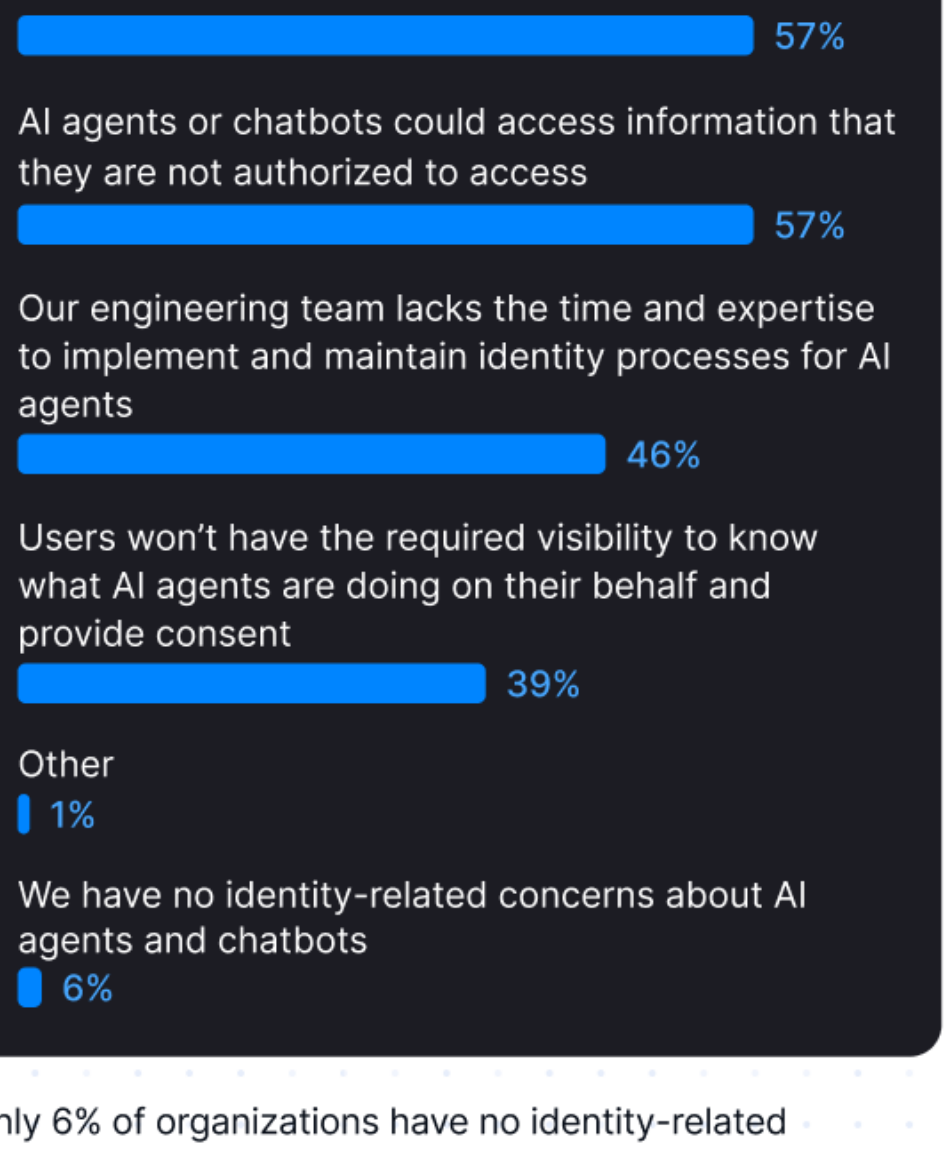
37%

have progressed beyond pilot programs

The concerns are universal and justified

94% have concerns about identities and chatbots

What identity-related concerns does your organization have about AI agents and chatbots?



Only 6% of organizations have no identity-related concerns about AI agents, meaning 94% are worried about something. Their top fears underscore the challenges ahead:

- **Unauthorized data sharing (57%):** AI agents potentially sharing data with users who shouldn't see it
- **Unauthorized access (57%):** Agents accessing data beyond their scope
- **Resource constraints (46%):** Engineering teams lacking time and expertise for AI identity processes
- **Consent and visibility (39%):** Users not knowing what agents are doing on their behalf

These are genuine, practical concerns from teams who understand that AI agents multiply the attack surface while their organizations lack the frameworks to secure them. The 46% citing lack of engineering time and bandwidth are being refreshingly honest: They know what needs to be done but don't have the wherewithal to do it.

Too many cooks in the robo-kitchen

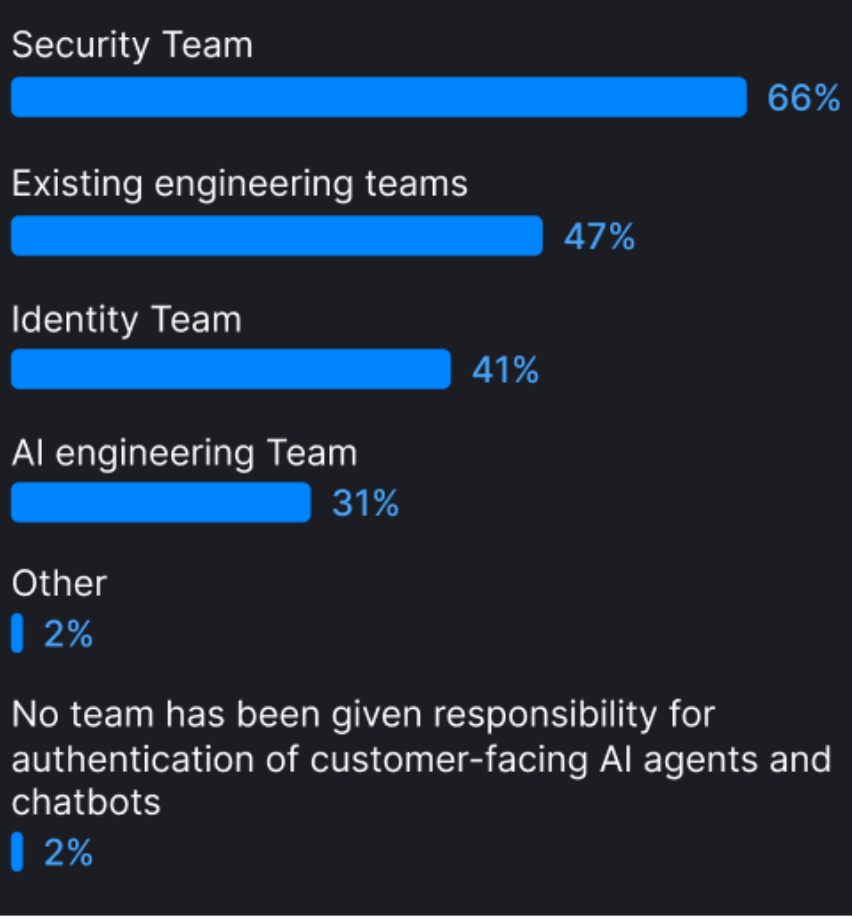
Agent identities introduce unprecedented complexity, and as you might expect, no single team owns it:

- **Security teams:** 66%
- **Existing engineering teams:** 47%
- **Identity teams:** 41%
- **AI engineering teams:** 31%

The fragmented ownership reflects the same organizational realities we've been seeing throughout this study. Teams are doing their best to adapt existing structures to nascent challenges, but AI is moving faster than legacy orgs can.

Many teams will have responsibility for authentication of AI agents

What team of your company has responsibility for authentication, access control, and identity management for customer-facing AI agents and chatbots?



Our take: Authentication for AI agents is another shared responsibility, often split between teams who each tackle part of the challenge (but have their own goals in mind).

Once again, we're seeing that identity touches many parts of an organization, with only a small portion of organizations building AI-specific teams—which trends along organizational resources and size.

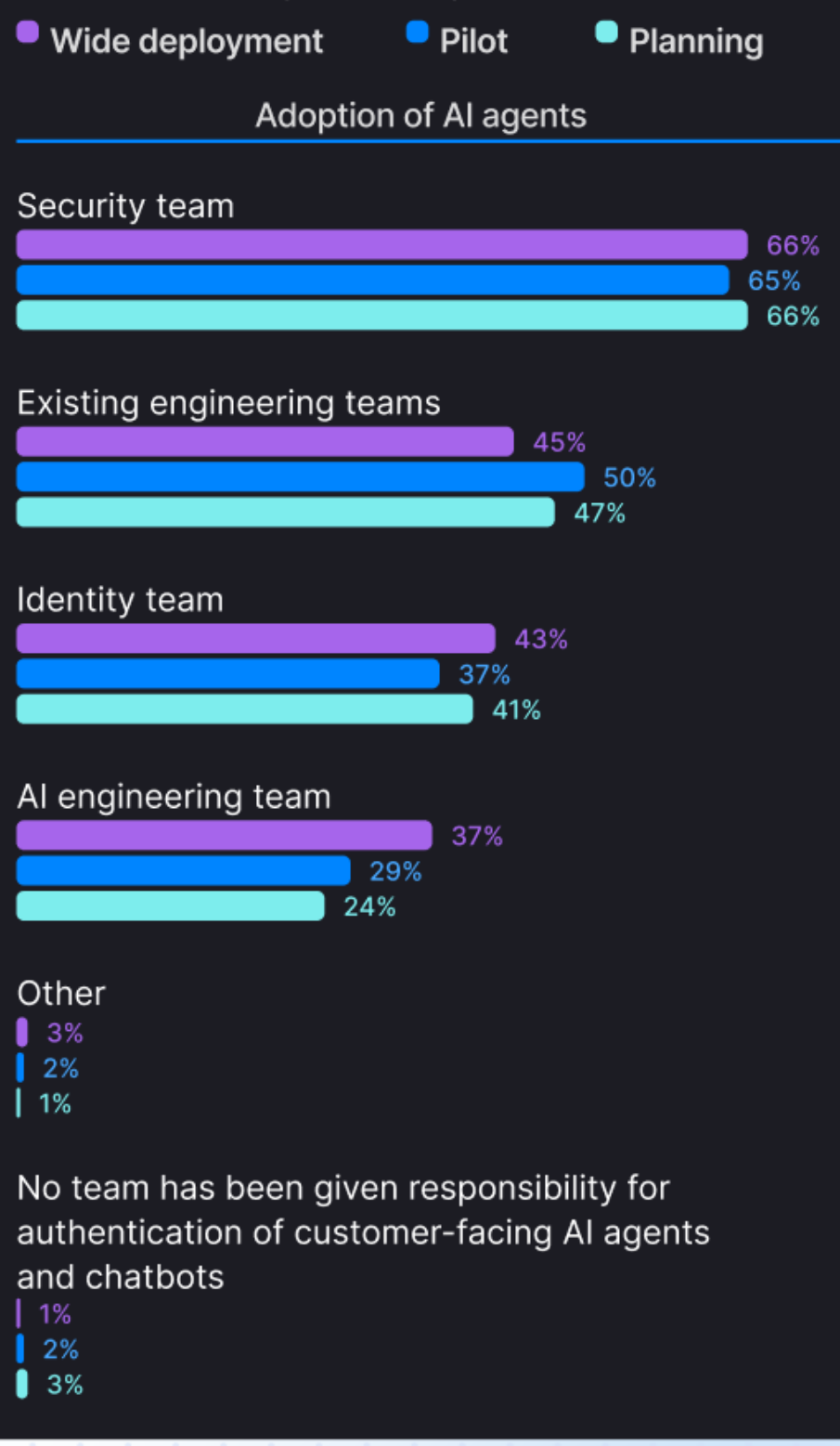
To specialize in AI, or not?

Of respondents with wide AI agent deployment, 37% have AI-focused teams. This is higher than our average (31%), but still underscores the fact that existing security and engineering teams are expected to address AI challenges in addition to their regular tasks. This isn't because companies don't care about AI security though; it's simply the only option for organizations of a certain size.

AI engineering more likely to have responsibility for authentication in mature organizations

What team of your company has responsibility for authentication, access control, and identity management for customer-facing AI agents and chatbots?

88% are considering or adopting AI chatbots



In 2024, McKinsey's survey on the state of AI reported 52% of organizations with over $500 million in revenue had established dedicated teams to drive AI adoption. Smaller organizations were less likely to follow suit, with only 23% installing AI-specific working groups, but there's solid representation regardless.

Our numbers are consistent with McKinsey's report. As company size increases, so does the presence of dedicated GenAI teams.

- **The smallest organizations (500-1000 employees)**: 23%
- **Small companies (1,000-5,000 employees):** 28%
- **Medium companies (5,000-20,000):** 31%
- **Large enterprises (20,000+):** 38%

The logical conclusion here is that the more resources you have, the more likely you are to dedicate a team to an emerging technology.

The knowledge gap (that's completely understandable)

One of our more nuanced results was that only 26% of CIAM decision-makers consider themselves knowledgeable about the Model Context Protocol (MCP), a critical component for standardizing how LLMs interact with external systems. It's also an important part of securing these remote calls, since its authorization specification invokes the latest OAuth 2.1 standards.

There are a couple of reasonable explanations for this. First, of the organizations that have adopted MCP, the majority (60%) are deploying local servers only. That means the authorization challenges are much different, and far more contained—so the CIAM decision-maker respondents we spoke with wouldn't need to be MCP experts.

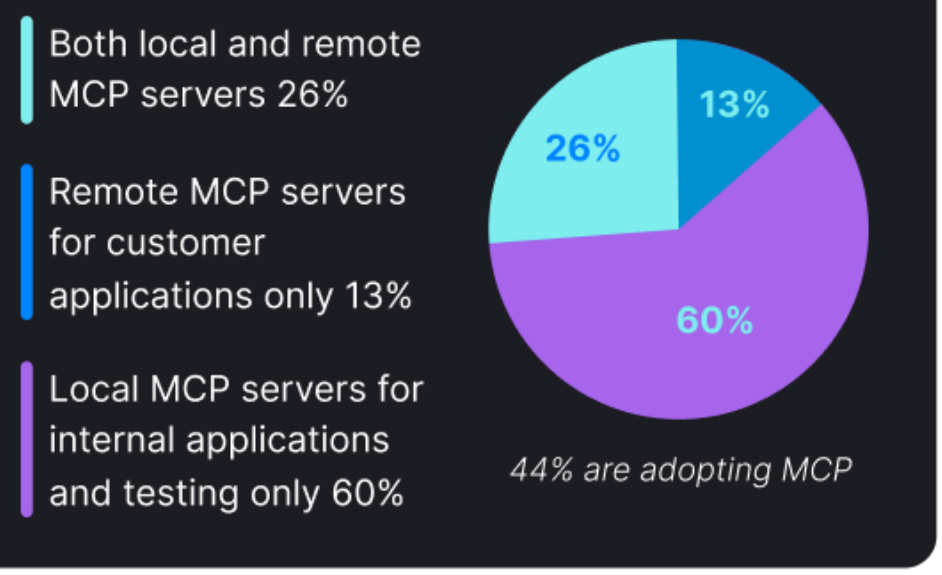
The second reason could simply be that MCP isn't a part of their AI deployment: MCP is primarily intended for standardizing how external data sources and tools are called or contextualized, and the 56% who aren't adopting it are getting by with other approaches.

We've drilled down into the MCP number for a specific purpose: demonstrating that AI knowledge isn't an all-or-nothing affair. When we see organizations diving into AI adoption with tough auth challenges still piled up, we know it's because companies want to remain competitive.

Our insight into why they mostly choose local-only deployments? They know there are security risks, and keeping their AI agent in a vacuum is an easy solution (that doesn't drain dev cycles).

Current MCP plans are focused on local servers

What types of environments has your company adopted the Model Complex Protocol (MCP) for agentic AI systems?



Trust in AI erodes with experience

Speaking of understanding security risks, we see an interesting pattern as organizations spend more time integrating AI. They often start out quite optimistic about AI security, but more interactions lead to healthy caution.

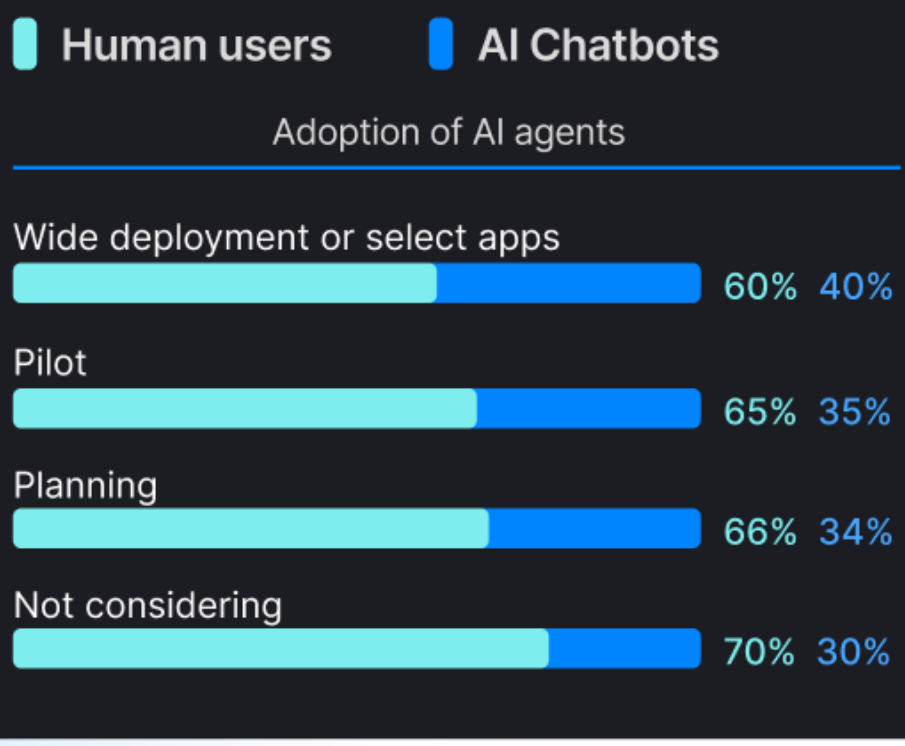
This reflects a pattern already present among the general public, according to a 2025 study published in the Journal of Marketing. The research notes, "[P]eople with lower AI literacy are typically more receptive to AI" and that "those who are more clued in to how the tech works are less likely to use it."

In our own study, when we asked whether human users or AI agents pose a greater risk to security, 65% say humans are riskier (more likely to share unauthorized information) than AI agents (36%). But watch what happens as a respondent's experience grows:

- **Organizations not considering at all:** 70% say humans are riskier
- **Planning AI:** 66% say humans
- **Pilot phase:** 65% say humans
- **Wide deployment:** 60% say humans

CIAM decision makers become more likely to say chatbots are riskier as their experience with AI agents increase

In your opinion, which of these creates a greater risk for sharing unauthorized data with customers?



If this pattern continues, it's possible that another category labeled "Long-term AI integration across all apps" would show a much more cautious outlook toward NHIs. A 50/50 split or lower wouldn't be out of question.

In a similar vein, those with wide deployment were also the group most concerned that "Users won't have the required visibility to know what AI agents are doing on their behalf and provide consent" (44%). Perhaps, the more you deploy AI, the more you learn to distrust it.

The reality of agentic IAM

The data we've seen here tells a story of caution and shows a marketplace in flux. Organizations are deploying AI agents into environments where essential authentication capabilities remain just out of reach. With 94% expressing security concerns over AI, standards like MCP remaining unknown or underutilized, and trust in AI declining with experience, we're seeing companies learn as they go in real time.

We aren't calling these patterns reckless, though. These are the inevitable outcomes when a huge technological paradigm shift occurs, and it outpaces organizational agility. The same teams who are struggling to balance security and CX for human users, fighting legacy tech debt, and spinning plates for different projects—well, now they're responsible for agentic identities, too.

No wonder 46% openly admit they lack the time and expertise to implement proper AI identity processes. The respondents in our research aren't failing at their responsibilities, but they are facing a difficult, uphill battle. And as AI adoption accelerates from pilot to production (whether or not it lasts), these challenges will only compound—unless organizations fundamentally rethink their approach to customer and agentic IAM.

A wakeup call for companies with stagnant auth projects

The state of customer identity in 2025 reveals a marketplace in the middle of transformation. Today, organizations are wrestling with a painful paradox: Everyone agrees authentication matters, yet it stays on the back burner. It remains the critical project that's first in line to lose priority.

Organizations know their infrastructure is risky and in need of a fix. They've looked into solutions. But the cracks in customer identity splinter outward over time. Quarter after quarter, they adapt to tiptoeing around the problem areas because broken authentication that still "works" feels less urgent than everything else demanding their attention. Until one day it causes a catastrophe.

Yet, we're still optimistic about the future. Here's what makes us hopeful:

- Organizations are no longer satisfied with antiquated security methods and authentication bandaids
- Teams are increasingly aware of authentication's shared (or fragmented) ownership, even if they're not agreeing yet
- The scramble to secure AI is forcing authentication conversations that might never have happened
- Companies are embracing modern methods like passkeys and adaptive MFA

The gaps in priority between security and engineering teams? The IAM-as-CIAM companies who wish they could start over? The frustrating knowledge that passwords are past their expiration? These are all signs that the marketplace is waking up to what needs fixing.

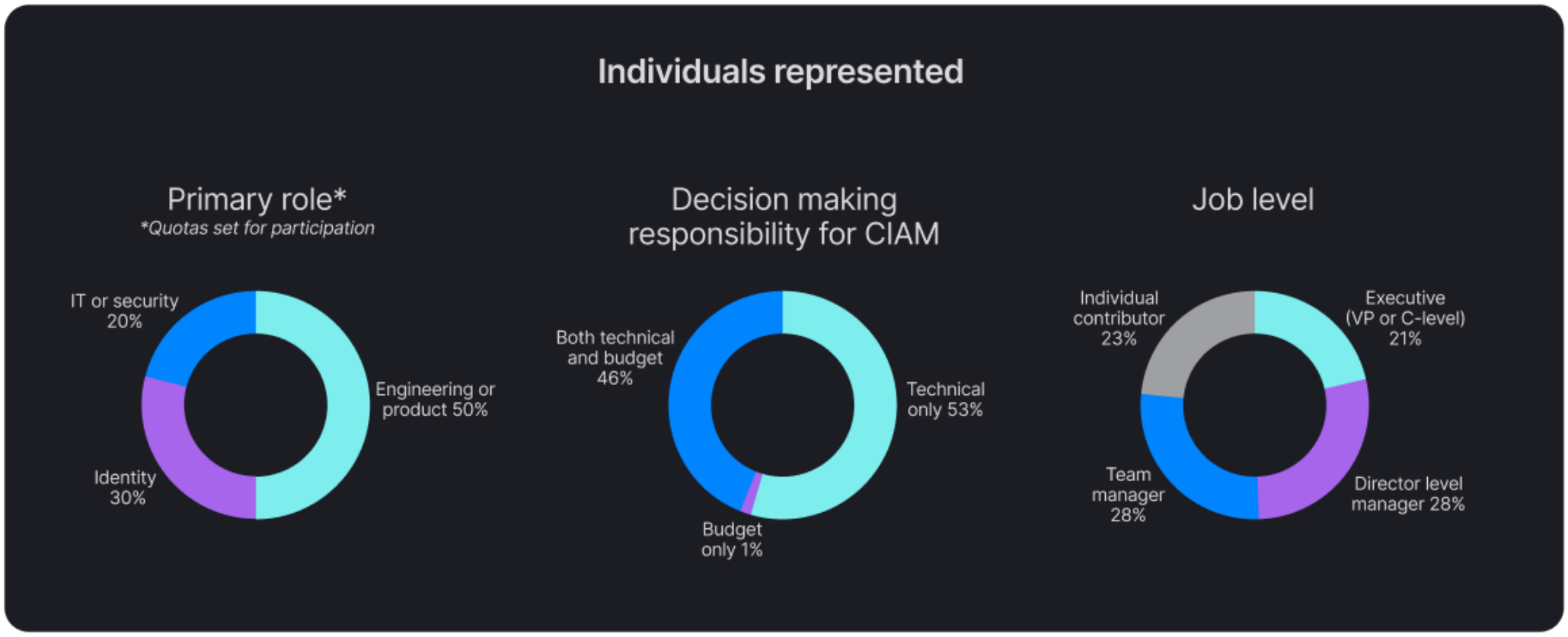
Ultimately, we're confident that more and more organizations will stop seeing customer identity as a burden—and recognize it as a key business enabler.

Methodology

Research approach

The primary research goal of this survey was to uncover key trends, challenges, and innovations shaping customer identity and access management (CIAM), while highlighting how organizations are managing authentication, privacy, and user experience in an evolving digital landscape.

Independent sources of technology stakeholders were invited to participate in an online survey in mid-2025. The survey was fielded in English and included a variety of questions on current approaches and experiences with customer identities and authentication.



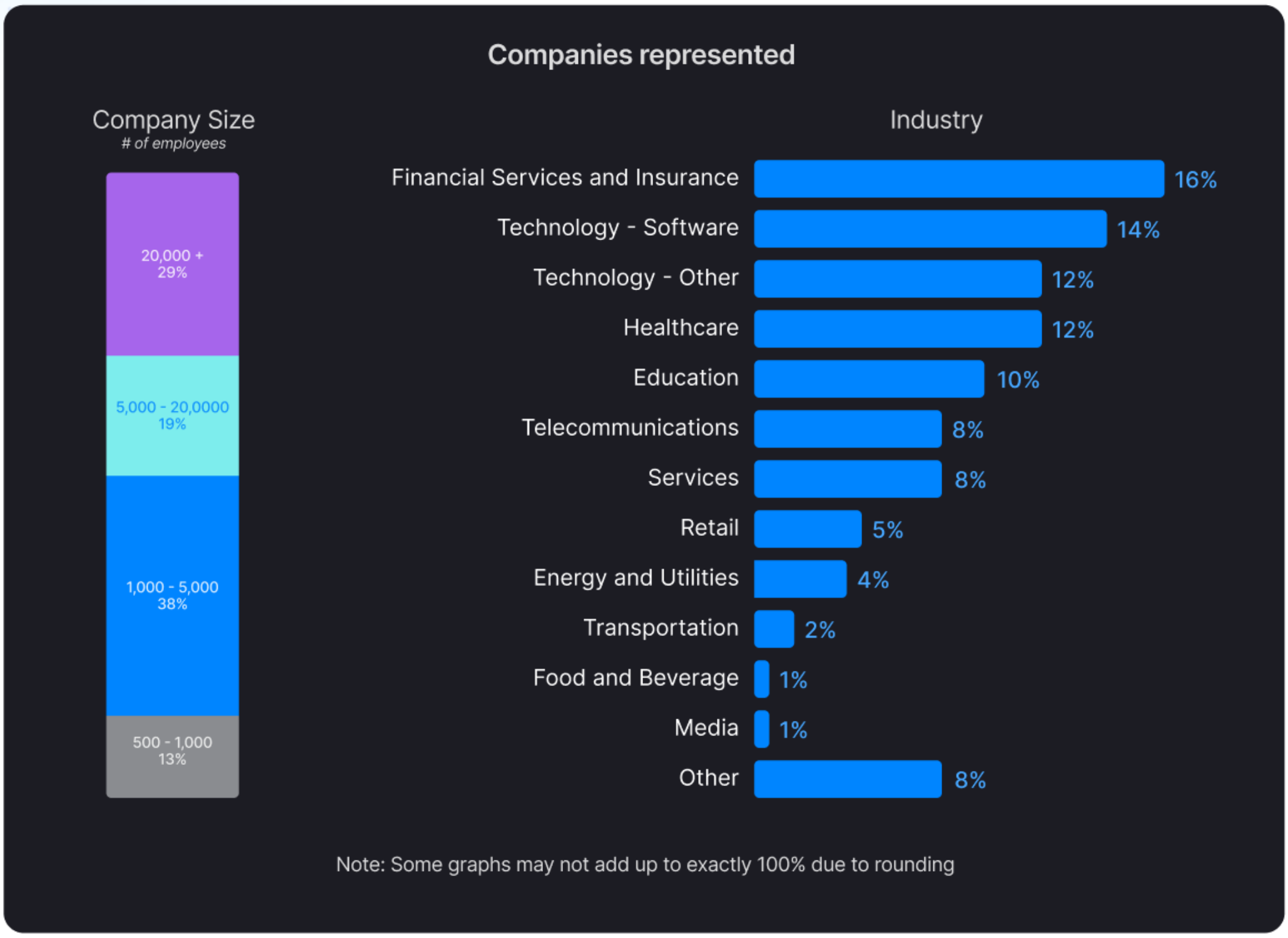
Who we surveyed

A total of 416 qualified individuals completed the survey. All participants had decision-making responsibility (technical and/or budget) for Customer Identity and Access Management solutions at companies with more than 500 employees.

The respondent pool was carefully balanced across roles and seniority levels. This mix ensured viewpoints from both technical implementers and business decision-makers to capture the full range of CIAM challenges:

Organizational representation

The 416 respondents in this survey represented companies across diverse industries and sizes. This distribution was thoughtfully planned to provide an accurate cross-section of the real-world CIAM scenarios modern organizations face:



About Dimensional Research

Dimensional Research® provides practical market research for technology companies. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. Our researchers are experts in the applications, devices, and infrastructure used by modern businesses and their customers.

For more information, visit www.dimensionalresearch.com.

descope

State of Customer Identity

[2025 Report]

About Descope

Descope is a drag & drop platform to help organizations manage all their external identities. Our no / low code external IAM solution helps organizations create, modify, and secure authentication and authorization journeys for customers, partners, AI agents, and MCP servers. Over a thousand organizations use Descope to improve customer experience, prevent account takeover, and securely adopt agentic AI and MCP. Learn more at https://www.descope.com