CUSTOMER IDENTITY TRENDS REPORT 2026

auth0

Identity is the new revenue growth engine



Contents



1 **Executive Summary**

3 **AI investment is up. Consumer trust hasn't caught up.**
- Leaders see AI as an innovate-or-die race
- 80% of orgs are behind schedule—and split on why
- Consumers want AI help, not AI autonomy

9 **The agentic era puts identity center stage**
- Trust requires security, convenience, and control
- Security friction is already costing revenue—AI raises the stakes
- Agentic workflows expand the attack surface

17 **Your CIAM platform can make or break your AI ambitions**
- External CIAM delivers the experience consumers demand
- External-only CIAM orgs are winning the AI race

23 **Building customer journeys for today and tomorrow**

24 **Methodology**

Executive Summary

The rapid maturation of autonomous systems and other AI-powered capabilities has kicked off a “must-win” race as brands redefine digital customer journeys for the AI era.

Facing an innovate-or-die competitive market, nearly 60% of organizations have already introduced at least one action-taking or API-calling agent into their customer journeys or are on track to do so. And yet, despite the high stakes, 80% of transformation initiatives are behind schedule. Senior leaders cite governance (and related) issues; developers largely agree, but many point to identity and authentication infrastructure that “can’t support agent access patterns” as the prime culprit for delays.

At the same time, only 38% of consumers are currently willing to delegate decisions to AI agents, and the vast majority of those are only willing to do so in low-value, low-risk scenarios. More than any other internal or market force, this “trust gap” has the potential to derail AI initiatives—or, at the very least, to artificially limit the returns they deliver.

Crucially, control can bridge this gap. Willingness to delegate to an AI agent becomes the majority position when consumers are kept in the loop to approve actions and have the option to undo them.

But although integrating AI into experiences introduces new considerations, it doesn’t change the fundamentals. Just as in traditional customer journeys, consumers still expect a seamless combination of convenience and security, in which friction is proportional to their perception of utility and risk. To protect revenue, brands must take care in how they address AI’s authentication and authorization requirements. Too much friction, at the wrong moments, may drive customers away—but just the right amount, at the right time, will build trust without disrupting the journey.

In addition to safeguarding against the usual identity threats (e.g., fraudulent accounts, brute force login attacks, etc.), brands must also manage new cybersecurity and data risks, as AI agents, autonomous systems, and the APIs they use can serve as conduits to personal and sensitive data.

Executive Summary cont.

Preventing common failure modes—including overpermissioning, a large blast radius, lack of behavioral context for agents, and credential sprawl—requires an evolved approach to identity, not a repurposing of controls designed for human users.

For too many organizations, the pilot-to-production pipeline is slowed by customer identity that just can't meet the needs of agentic customer experiences.

However, development doesn't have to grind to a halt when customer identity and AI intersect. Organizations that rely on only an external customer identity platform are more likely to report:

- Employing security measures—including frictionless authentication—that safeguard interactions while protecting revenue
- Building transformative AI or agentic capabilities
- Having AI or agentic features fully embedded in production already
- Being on schedule with their AI rollouts

Consumers are clear that they value convenience, security, and control—whether within a traditional customer journey or an AI-assisted one. To manage this tension, brands need to:

1. **Reject the zero-sum "convenient OR secure" mindset,** which is a relic of outdated identity solutions
2. **Build an identity model that manages human customers and the AI agents working on their behalf differently**, with AI agents treated as first-class identities in their own right
3. **Recognize and respect the trust gap, then take steps to close** it by keeping users in the loop to approve or undo AI-driven actions

By taking these steps, brands can transform digital customer experiences while maintaining the security, convenience, and control needed to build trust in an increasingly agentic era.

Brands are investing in AI-assisted customer experiences, but consumer surveys point to a trust gap

Key takeaways:

Agents and autonomous systems are already part of the customer experience: 52% of senior leaders regard AI as “a must-win” capability (with another 31.1% seeing it as “important”), and more than 75% of organizations have introduced or will soon introduce customer-facing AI agents or autonomous systems

The success of AI initiatives hinges on overcoming a trust gap: Although 59% of organizations already have at least one action-taking or API-calling agent in production or in development, only 38% of consumers are currently willing to delegate decisions to them

Unnecessary friction multiplies the risk of lost revenue: Organizations cannot bridge this trust gap if their front door is broken. Unresolved authentication friction and clunky account creation drain conversion today, and these impacts could compound when AI agents enter the journey

In a memorable scene in Lewis Carroll’s *Through the Looking Glass*, the Red Queen explains to Alice that “*Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!*”

We have a similar situation today: leaders are racing to introduce AI-assisted customer experiences to keep pace with competitors who are doing the same. Yet, in the rush to innovate, many overlook the foundational layer where growth actually succeeds or fails: customer identity. If basic login and registration flows frustrate users today, adding autonomous agents will only magnify that friction and erode consumer trust.

Senior leaders regard AI capabilities as an innovate-or-die ‘Red Queen’ race

When asked what represented *“The single biggest threat to their business right now,”* nearly a quarter (23.2%) of senior leaders selected “competitive disruption from AI-native competitors,” *second only to “cybersecurity and data risk”* (31.4%).

Moreover, more than two-thirds (67.2%) of senior leaders responded that their business would be at least moderately threatened if a competitor launched *“a meaningfully better AI-driven customer experience.”*

These competitive pressures are evidently strong motivators.

Practically every developer and senior leader polled (96%) reported that their organization intends to integrate AI into customer journeys—and more than three-quarters (75.2%) either already have such features fully embedded in production today or are actively building them.

All told, 59% of organizations already have at least one agent that takes actions on a user’s behalf, or that autonomously calls external APIs or third-party services, either in production today or in the pipeline.

Fast Fact

More than half (52%) of senior leaders reported that AI is a *“must-win capability” for their organization’s “ability to compete and grow over the next two to three years.”*



80% of organizations are moving slower than planned; developers and senior leaders disagree on why

In a Red Queen race, all your competitors are already moving fast—and your success relies upon moving even faster.

However, only about a fifth of developers and senior leaders polled (20.3%) report that they're moving/shipping at the target pace. What factors are holding back the other ~80%?

The survey reveals some differences of opinion.

For example, 59% of senior leaders consider compliance, security review, or governance to be the single biggest reason for delays—far and away their most popular choice. In contrast, while this set of requirements was also the top choice among the developer group, a much smaller percentage (34.6%) pointed to it as the primary culprit.

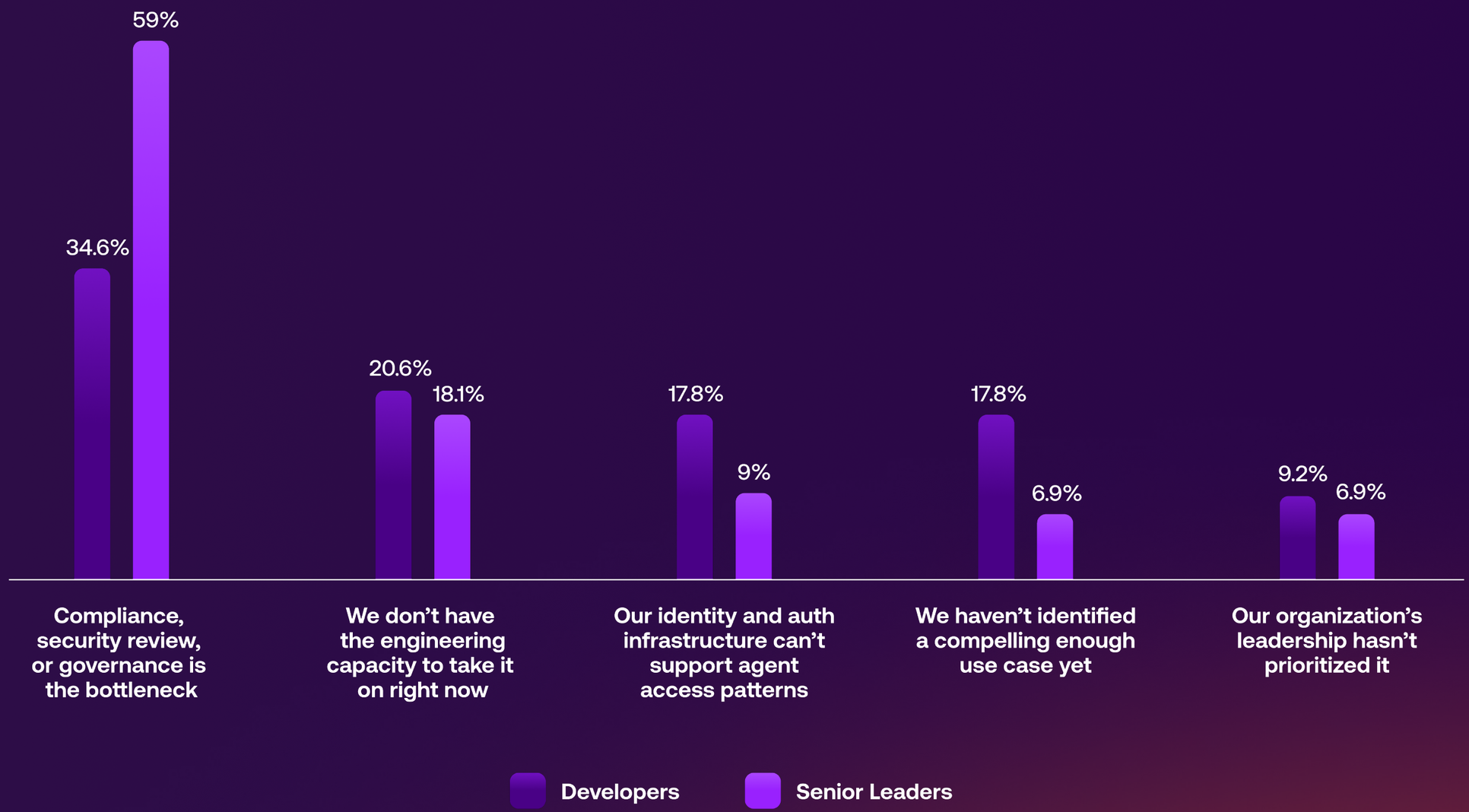
Instead, developers were nearly twice as likely as senior leaders (17.8% to 9.0%) to say that their identity and authentication infrastructure *"can't support agent access patterns."*

Identity & AI

The safest approach for managing agent authentication and authorization is to have a unique agent identity with tightly scoped, time-limited credentials.

And yet, only 22.4% of respondents from organizations that are actively building AI and agentic capabilities report that this is what they do. The remainder rely on dangerous approaches including shared service accounts or long-lived API keys (17.4%), inheriting the user's token or credentials (11.5%), or even hardcoded or embedded credentials (6.4%).

IF YOU'RE NOT MOVING AS FAST AS YOU'D LIKE ON AI OR AGENTIC FEATURES, WHAT'S THE SINGLE BIGGEST REASON?



N:910

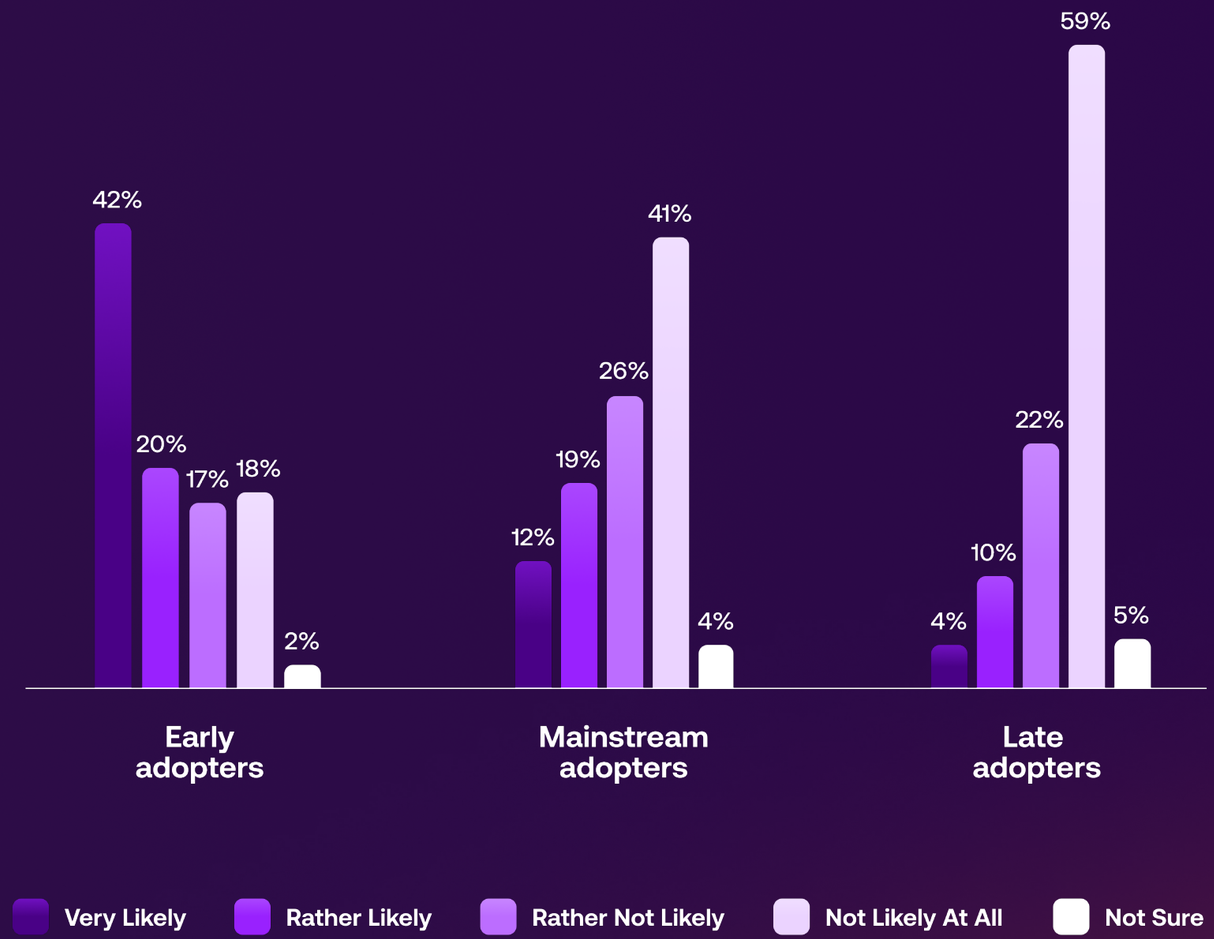
Consumers are open to AI-assisted experiences, but they place clear limits on autonomy

While organizations are racing to embed AI and autonomous capabilities within their apps and services, product owners would be mistaken to assume that the customer base as a *whole* is ready to embrace these new technologies.

For example, 52% of consumers overall say the pace at which AI capabilities are evolving in apps and websites is *"moving too fast,"* while only 35% report that it's *"moving at about the right pace."*

This doesn't necessarily mean that consumers want less AI, but it does indicate that many aren't entirely comfortable with its pervasiveness and the powers it has been granted.

HOW LIKELY ARE YOU TO LET AN AI TOOL COMPLETE A PURCHASE OR BOOKING ON YOUR BEHALF WITHOUT REVIEWING IT BEFOREHAND?



N:5250

In particular, consumers draw the line when AI acts without their oversight. While 38% would be comfortable giving AI some decision-making authority in the next two years, only 6% want AI to make final decisions and take actions on their behalf completely autonomously.

It's also clear that comfort levels vary enormously within the overall consumer population. Younger cohorts and self-professed early adopters are primed to embrace AI, whereas comparatively older cohorts, mainstream adopters, and late adopters are hesitant to fully delegate decisions and actions.

Identity & AI

Trust requires control: As AI takes on more actions, identity and authorization help ensure it operates within the boundaries people and organizations set.



The agentic era puts customer identity, consumer control, and security in the spotlight

Key takeaways:

Convenience, security, and control can bridge the trust gap: Consumers are open to AI-assisted experiences, but are hesitant to fully delegate consequential decisions and actions. Brands can accelerate mainstream adoption by ensuring consumers retain control over what AI does on their behalf and understand how their data is used

Preserving convenience remains essential for protecting revenue: AI introduces new authentication and authorization requirements, but—just as in traditional customer journeys—friction must be proportional to the consumer's perception of utility and risk

Customer-facing AI systems introduce new cybersecurity and data risks: AI agents, autonomous systems, and the APIs they use can serve as conduits to personal and sensitive data; preventing common failure modes requires an evolved approach to identity

Even in its early stages, the agentic era is changing how consumers interact with brands and pursue their objectives. As AI assistants evolve from providing information to taking action, mainstream consumer adoption hinges on a combination of convenience, security, and control.

Finding the right balance is a familiar challenge, and one that becomes more difficult due to new security requirements and data risks introduced by AI systems in general, and by agents and autonomous systems in particular.

Consumers trust secure and convenient experiences that they can control

For the vast majority of consumers (93%), trust is an outcome of an app/website providing *"strong security without making access difficult."*

These dual attributes are implicit in the convenience features that consumers report valuing in the apps and websites that they regularly use, including continuity across sessions (85%) and devices (80%), and faster checkout through saved information (84%).

But while convenience is necessary to bridge the trust gap, it's insufficient on its own: 89% of consumers value having clear control over their data and being able to see how it is used.

To better understand how organizations can increase trust, we presented consumers with eight different features/measures and asked which would make them feel more comfortable with an app/website using AI to take actions on their behalf.

Looking at the responses as a whole, two things stand out.

First, no single measure addresses the concerns of the majority of the population, which suggests that a range of options will be necessary to cater to individual consumer tastes.

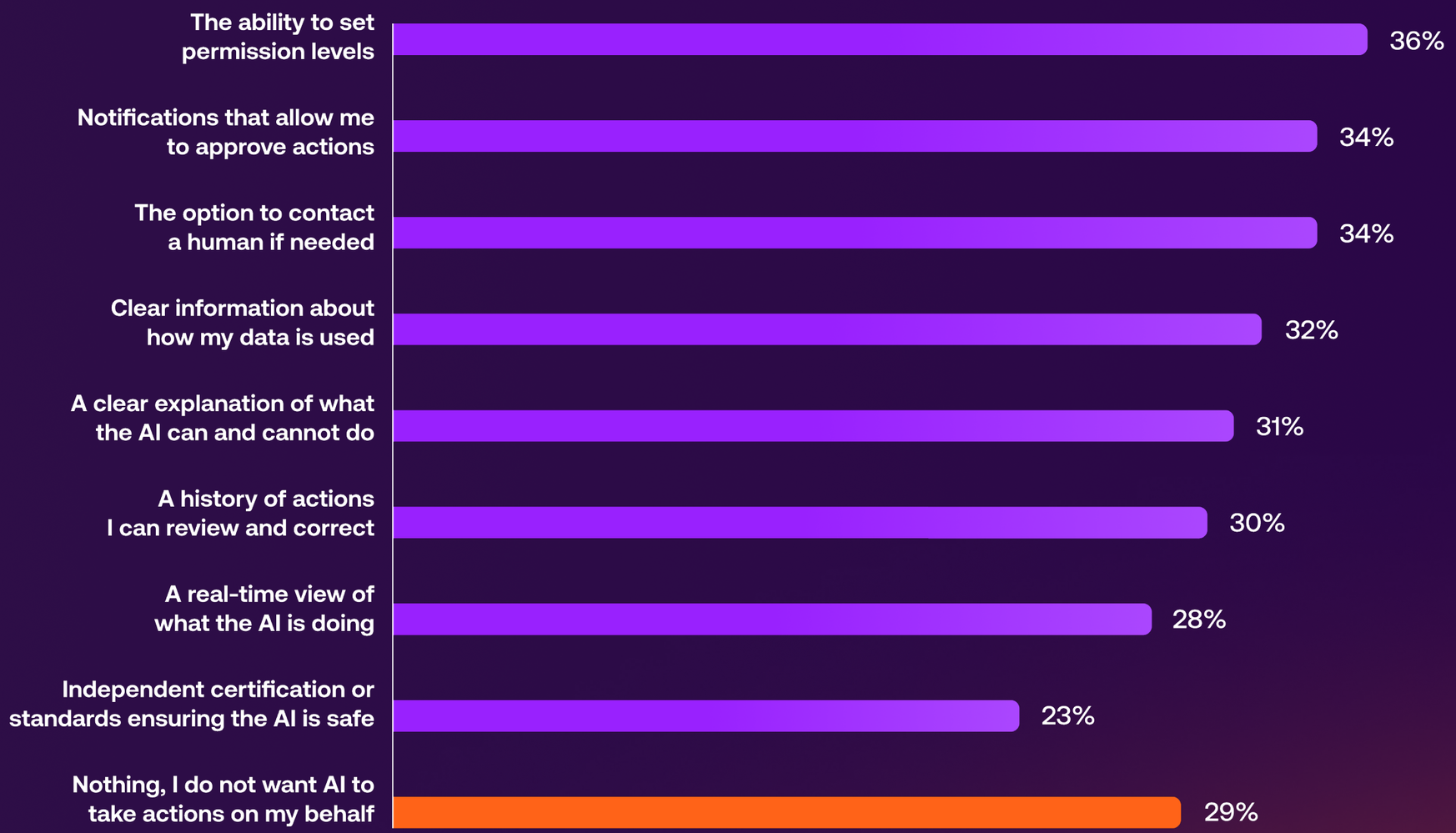
Second, the strongest-performing measures center on transparency, control and choice, suggesting that consumers need multiple ways to build confidence in AI-powered experiences.

Identity & AI

There's ample evidence that what works to address one person's concerns about AI might not work for another.

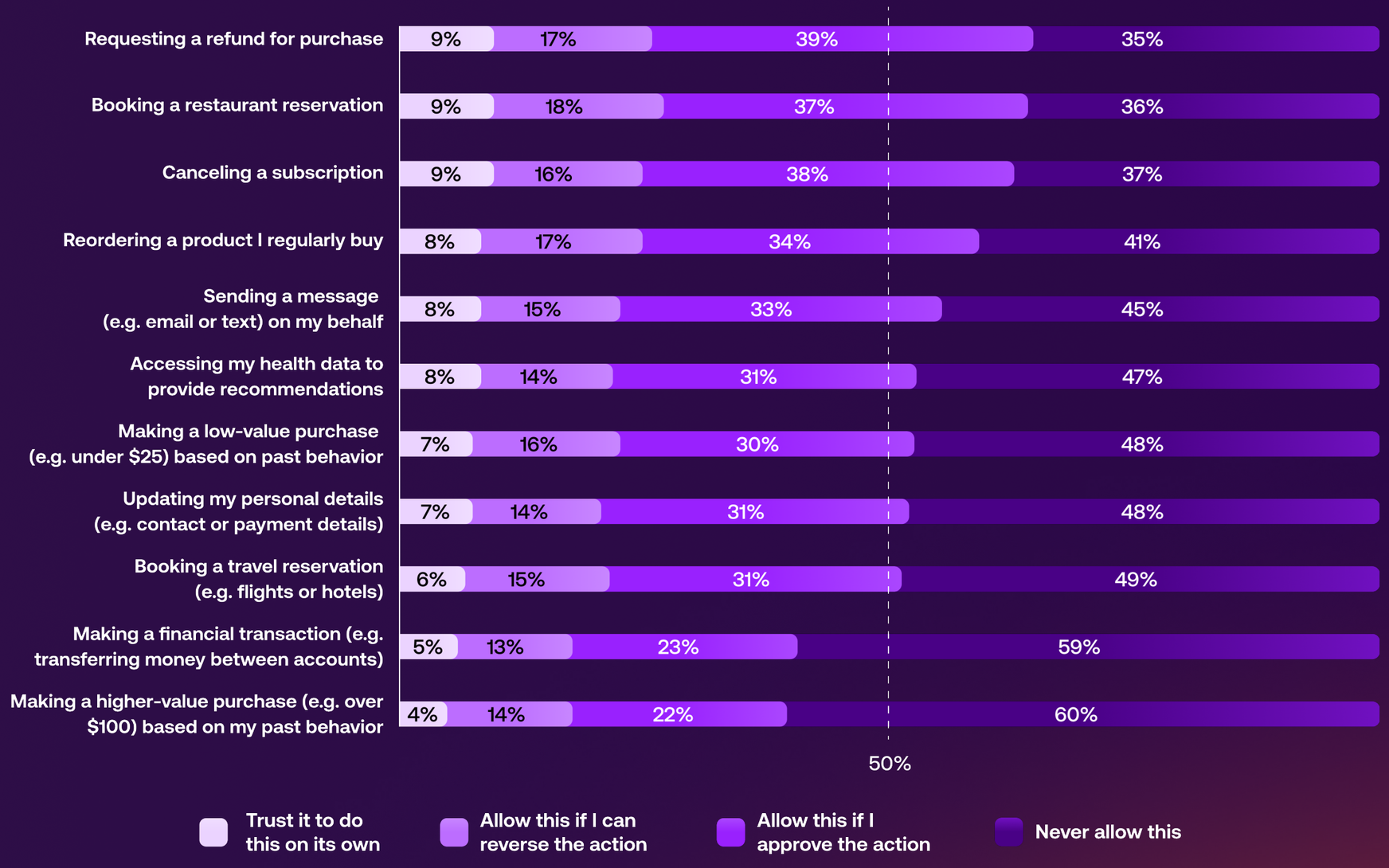
This is a simple but important insight, because it points to the need for identity platforms engineered to meet the authentication, authorization, and audit needs of AI agents and autonomous systems—both in general and in support of individual customer preferences.

WHICH OF THE FOLLOWING WOULD MAKE YOU MORE COMFORTABLE WITH AN APP/WEBSITE USING AI TO TAKE ACTIONS ON YOUR BEHALF?



N:5250

HOW WILLING WOULD YOU BE TO ALLOW AN AI TOOL TO TAKE THE FOLLOWING ACTIONS ON YOUR BEHALF?



Now, while there may not be a single feature that bridges the trust gap for all consumers, a small number of controls can have a meaningful impact.

In fact, for use cases where the potential financial or personal consequences of an error are limited, the majority of consumers are willing to allow AI to act on their behalf so long as they approve the action first, or have the option to reverse it.

N:5250

Security measures already contribute to revenue leakage, and AI introduces new complexities

Organizations invest heavily in acquisition marketing, spending significant portions of their budgets to drive qualified prospects to the digital front door.

Yet identity-related friction can still cause users to abandon these journeys, particularly when they are asked to create an account before they can access what they need.

Nearly three-quarters of consumers (74%) reported that being asked to create an account *"before seeing key information (e.g., prices, reviews)"* would cause them to definitely or probably stop what they're doing when using apps or websites.

Still, the research suggests that consumer sensitivity to friction varies by context. Fewer consumers (59%) said they would stop what they're doing when asked to create an account *"before completing a purchase,"* and we also see comparatively higher tolerance for familiar security measures like MFA and CAPTCHAs.

These findings have direct implications for brands rolling out AI-powered services: security measures should be proportional to the utility and risk of the task the user or AI agent is performing.

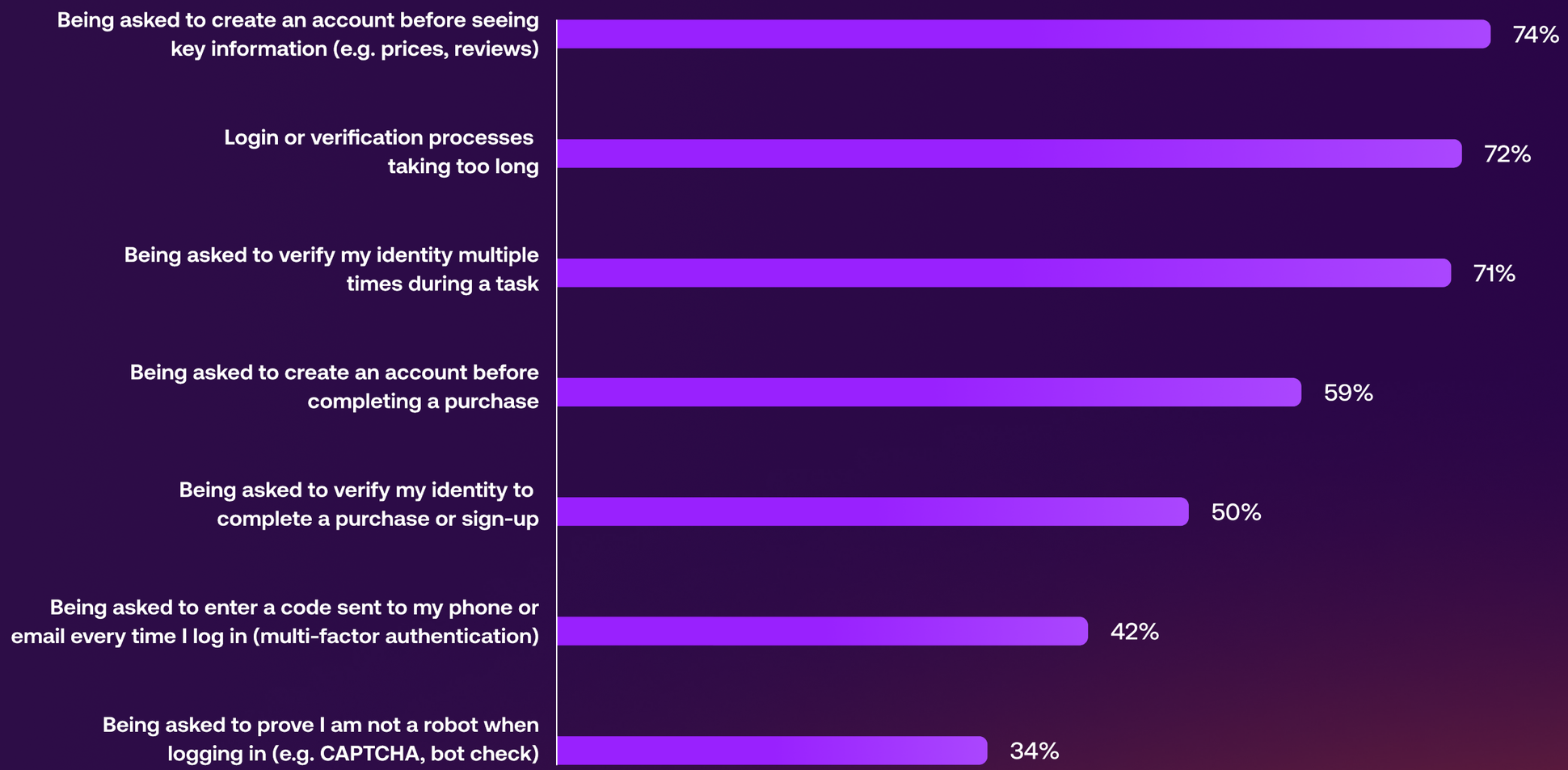
For instance, an agent accessing a brand's public information to perform basic research may require little or no additional verification. However, when an agent executes a meaningful task or accesses private data, stronger authentication is appropriate, but it should still be fast and frictionless to maintain convenience and trust.

Fast Fact

Account creation is a major point of disagreement between brands and their potential customers: brands want consumers to create new accounts; consumers are reluctant to do so.

But if they absolutely had to sign up to use a new app or service, then the preferred approach (by far) for consumers is the most convenient and familiar one: social login/sign-up using an existing account (e.g., Google, Apple, Facebook, etc.).

WOULD THE FOLLOWING SITUATIONS BE A REASON FOR YOU TO STOP OR ABANDON WHAT YOU ARE DOING (E.G. RESEARCHING, PURCHASING, OR SIGNING UP) WHEN USING APPS OR WEBSITES? (SUM OF “DEFINITELY YES” AND “PROBABLY YES”)



N:5250

Agentic workflows can expand the attack surface, increase data risk and create new security requirements

There's a very good reason why brands need strong authentication, even if security measures can add friction to customer journeys: identity systems are under constant attack.

Nearly 9 out of every 10 developers and senior leaders polled (88.8%) reported that their organization is actively dealing with at least one of seven different identity-related security or fraud challenges, with each challenge cited by between 30% and 40% of respondents.

Unfortunately, there's every expectation that the situation will only get worse.

For one thing, AI technologies are easily weaponized, making it possible for anyone—regardless of technical acumen or financial resources—to plan and execute large-scale attack campaigns.

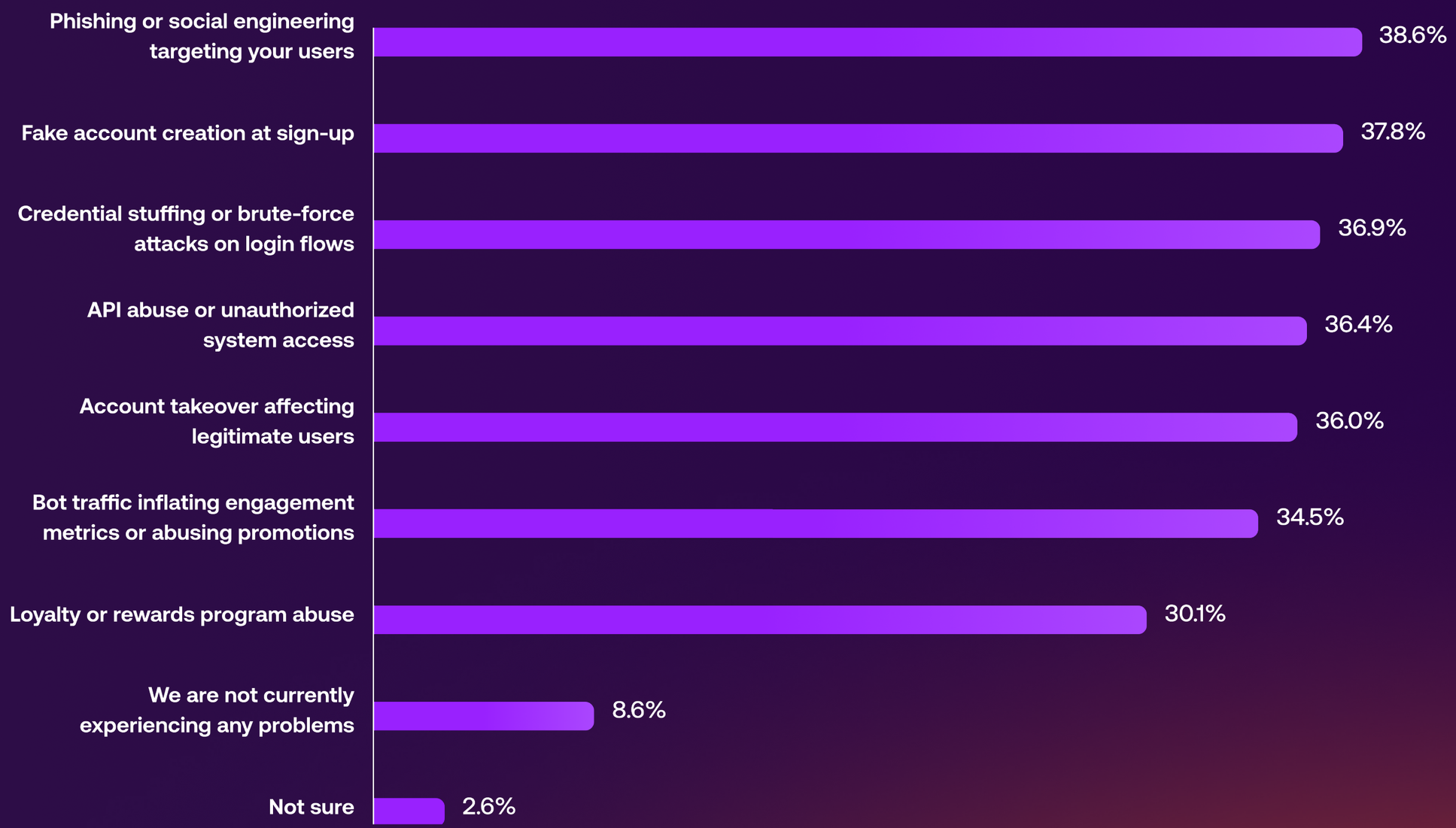
At the same time, AI agents, autonomous systems, and the APIs they use introduce new cybersecurity and data risks, as threat actors can exploit them to access personal and sensitive data. These risks can be amplified as agent usage scales, if an implementation suffers from one or more of four common failure modes:

- **Over-permissioning:** The credential carries broader authority than the agent needs for the task in front of it
- **Blast radius:** A compromise of the agent process, its memory, or its logs exposes a credential that grants standing access to production systems
- **Lack of behavioral context:** The identity layer cannot distinguish between different actions when they present the same broadly scoped credential
- **Credential sprawl:** Every new tool the agent integrates with means another credential to provision, store, rotate, and audit

Identity & AI

Protecting AI agents, autonomous systems, and the APIs they use requires an evolved approach to identity—one that links agents to individual customers and uses tightly scoped, time-limited credentials to control what they can access and do.

WHICH OF THE FOLLOWING, IF ANY, SECURITY OR FRAUD CHALLENGES IS YOUR ORGANIZATION ACTIVELY DEALING WITH RIGHT NOW?



N:910

Your customer identity platform can make or break your AI ambitions

Key takeaways:

Convenience and security aren't mutually exclusive: Modern, external customer identity platforms allow organizations to safeguard customer journeys without disproportionately harming the customer experience

Seamless security protects revenue: An external customer identity platform empowers organizations to easily leverage frictionless authentication technologies, resulting in significantly less revenue leakage

Organizations using only an external identity platform report stronger AI outcomes: They are more likely to report building or planning to build transformative AI or agentic capabilities, having AI or agentic features fully embedded in production already, and being on schedule with their AI rollouts

Customer identity is complicated enough, and agentic systems introduce an entirely new layer of complexity.

For many organizations, as AI ambitions grow, the pilot-to-production pipeline is slowed by a seemingly never-ending stream of technical hurdles, security surprises, and integration considerations.

But development doesn't have to grind to a halt when customer identity and AI intersect. A modern identity layer can centralize authorization, establish clear permissions for agents, and provide the controls needed to scale AI securely and efficiently.

External customer identity platforms can deliver the smooth and secure experiences consumers demand

Many brands struggle to craft customer journeys that are both convenient and secure. But is this tension an unavoidable operational reality, or is it a false choice?

As it happens, there's considerable evidence that an external identity platform allows organizations to largely avoid the convenient-or-secure conundrum.

For example, when we asked developers how their approach to security affects the customer experience, those using only an external identity provider were the most likely to report that *"This isn't a problem for us yet."*

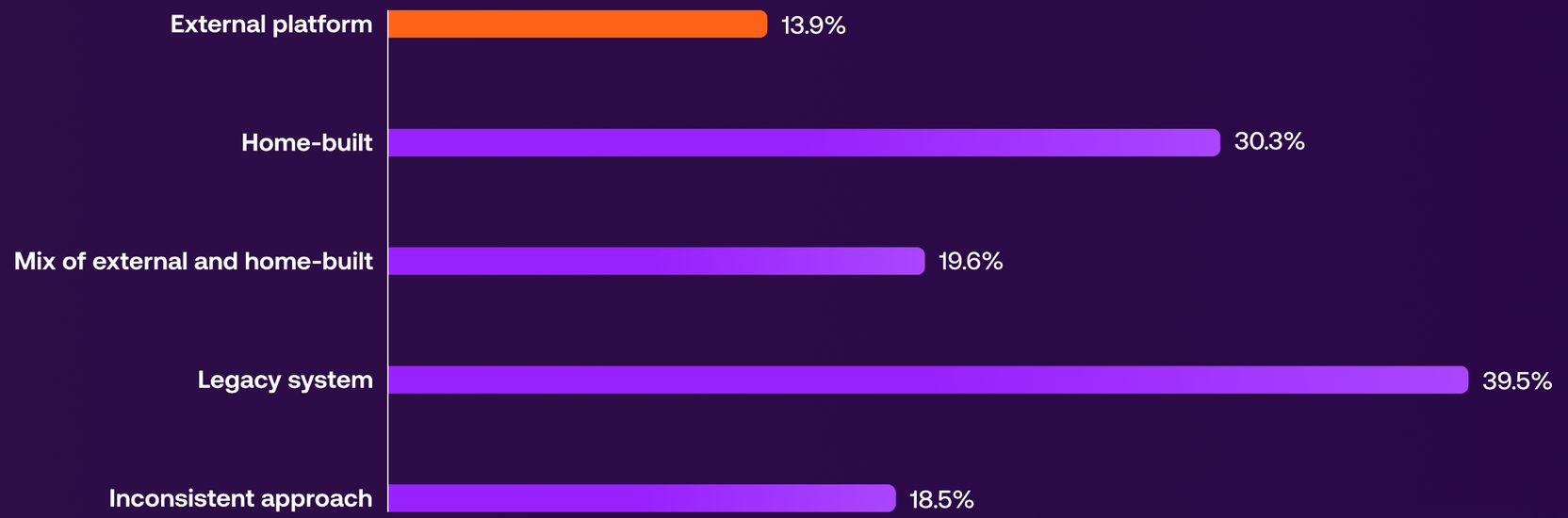
What's more, the developers using only an external customer identity platform were also:

- The most likely to report that they've invested in frictionless security, allowing them to stop fraud without hurting conversion
- The least likely to report that they're losing customers because security friction is too high
- The least likely to report not having the visibility needed to knowledgeably answer the question

Fast Fact

Developers who use only an external identity platform are the most likely to report that their organization has *"solved"* identity to the degree that it's *"a competitive advantage, not a burden."*

TO WHAT EXTENT DOES FRICTION IN AUTHENTICATION OR ACCOUNT ACCESS AFFECT HOW OFTEN CUSTOMERS USE YOUR PRODUCT? (“MAJOR” IMPACT)



***Note**: Respondents with legacy systems were ~2.5 to 4.5 times more likely than the other groups to report that they “haven’t measured it directly, but suspect it matters”*

N:556

These findings indicate that an external customer identity platform meets customer expectations for security and convenience, allowing organizations to build trust at critical moments through proportional authentication measures.

As more evidence of the benefits of external identity platforms, we see that organizations using only these platforms are the least likely to report that their authentication experience:

- Has a “major” negative impact on customer retention
- Has a “major” negative impact on how often customers use their product

And when we asked retailers in particular about their experiences, those using only an external identity platform were the least likely to report that their authentication experience:

- Negatively impacts average order value per customer
- Negatively impacts purchase frequency

These differences become clearer when we contrast how different identity approaches shape specific customer experiences. Greater visibility into those experiences can also help brands identify and manage friction, measure the impact of identity-related changes, and support compliance requirements.

Customer Experience Stage	Legacy Identity	Customer-Centric Identity
Account Creation	Long, multi-field registration forms requiring email verification before site access	Frictionless, one-click passwordless, passkey, or social sign-up
Returning Login	Manual password entry with frequent reset prompts and forgotten credential loops	Biometric authentication (e.g., passkeys, TouchID) or single-click magic links
Data Collection & Privacy	Front-loaded data requests asking for personal details before delivering value	Progressive profiling that gradually gathers context over time, capturing high-value, voluntarily shared (zero-party) data in a consent-forward way
Security Verification	Static, mandatory MFA prompts applied equally to every user session	Context-aware, adaptive MFA that triggers step-up authentication only when risk signals spike

Organizations that use only an external customer identity platform are winning the AI race

In addition to enabling secure and convenient customer experiences, evidence is mounting that an external platform provides the best foundation for AI initiatives.

First, developers whose organization uses only an external identity platform are the most likely to report that they are already building or are planning to build each of the AI or agentic capabilities shown in the chart on the following page.

Second, more than a third (34.4%) of organizations that use only an external identity platform already have AI or agentic features fully embedded in production today, compared to 22.3% of organizations using an alternative approach.

And third, although barely 20% of developers and senior leaders reported that their AI initiatives are progressing at the desired pace, the figure rises to 28.3% at organizations that use only an external identity platform—a much higher success rate than the organizations that take an alternative approach to managing customer identity (18.1%).

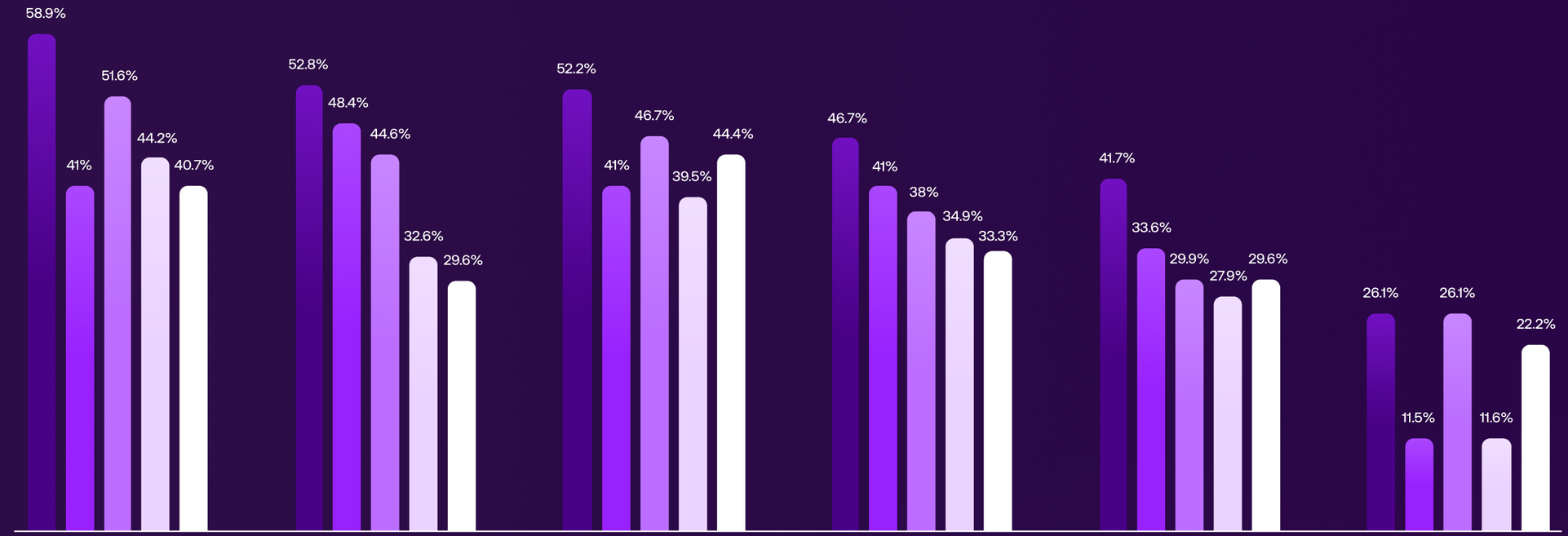
Taken together, these findings point to a clear pattern: organizations using an external identity platform are further along in adopting and scaling AI and agentic capabilities.

Identity & AI

As agents get deployed more widely, the authentication and authorization work around them grows quickly. An external customer identity platform allows builders to:

- Standardize identity in one place, removing repetitive work
- Define AI agent permissions once and apply them across multiple systems
- Scale without rework or rearchitecting

WHAT KINDS OF AI OR AGENTIC CAPABILITIES ARE YOU BUILDING OR PLANNING TO BUILD INTO YOUR PRODUCT?



N:445

Where ambition meets reality: Building customer journeys for today and tomorrow

As the saying goes, *"The more things change, the more they stay the same."* Within larger digital transformation initiatives, businesses have ambitious plans for AI agents and autonomous systems. At the same time, consumers are clear that they value convenience, security, and control—whether within a traditional customer journey or an AI-assisted one.

Here are three steps to help manage this tension:

1. **Reject the zero-sum "convenient OR secure" mindset**
   Transitioning to a modern, external identity platform helps brands balance security and convenience, building consumer trust while reducing avoidable revenue leakage.
2. **Build an identity model that manages human customers and the AI agents working on their behalf differently**
   AI agents need to be treated as first-class identities in their own right, distinct from human users and from traditional machine identities. A modern identity platform provides the authentication, authorization, and governance capabilities needed to manage them at scale in a more secure manner.
3. **Recognize and respect the trust gap, then take steps to close it**
   Consumers are not uniformly ready to embrace AI. While some are eager to use it, others remain cautious, with many falling somewhere in between. Brands can help close this gap by combining strong security with convenience, transparency and control, including keeping users in the loop to approve actions when appropriate.

By taking these steps, brands can transform digital customer experiences while maintaining the security, convenience, and control needed to build trust in an increasingly agentic era.

Methodology

To construct a representative view of both the demand and supply side of the customer experience landscape, Okta commissioned two surveys:

- Statista GmbH conducted an online survey of 5,250 consumers exploring their values, perceptions, experiences, and usage habits regarding customer journeys and the emerging role of AI within them. The survey included 750 respondents in each of seven countries: the US, Canada, UK, Germany, Japan, Australia, and New Zealand. Respondents were not informed that Okta had commissioned the survey. Fieldwork took place in July and August 2026.
- Rep Data recruited 556 developers and 354 senior leaders to take an online double-blinded survey exploring their and their respective organizations' experiences with customer identity and access management (CIAM) and digital transformation—especially with respect to agentic and autonomous systems. Respondents were recruited from the US (22.3%), Canada (16.5%), UK (22.2%), Germany (16.8%), Japan (11.0%), and Australia and New Zealand (11.2%) and across four key industries: Healthcare, Financial Services, Retail, and Telecom. Rep Data recruited the panel and fielded the survey in July and August 2026.



auth0