2026 EDITION

THALES
CYBERSECURITY

DIGITAL TRUST INDEX

The most comprehensive study for IT Security Leaders on how Digital Experiences affect Trust across Consumers, Partners and Employees

#2026TRUSTINDEX

Leadership in the Digital Age

We are living in a very different reality than we were just a year ago. While a significant part of our digital life remains interacting with humans, every click or tap still triggers questions in your mind – am I interacting with a human or AI; is this interaction safe; is the data that I'm sharing going to be private; and above all, can I really trust this digital interaction?

Digital Trust, as defined by the World Economic Forum, is "The expectation by individuals that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values."

The Digital Trust Index aims to address some of these expectations – providing guidance to leaders and their teams on building long-lasting relationships with their different user constituencies and helping them build a more trust-worthy brand.

How an organization's brand is perceived is a combination of multiple expectations of it. Your customers expect better user experience, personalized to their individual needs. After all, they are paying you for it. Employees, too, demand better user experience but often for a different reason – they want to be more productive in their work. Not surprisingly, your business partners and suppliers are no different – they need a frictionless user experience to ensure they can better collaborate with your organization.

User experience is just a part of the bigger equation. From an execution point of view, digital trust rests on three core pillars:

- **User Experience:** Ease of use, enjoyable across all channels
- **Security:** Visible security controls like multifactor authentication (MFA) and encryption build user confidence
- **Privacy:** Users want the assurance that the organization they are interacting with is keeping their private and sensitive data secure

With the changing technology landscape, especially due to advancements in Artificial Intelligence, technology and security leaders need to stay on top of their users' expectations, perceptions and regulatory mandates. Leaders face a tough balance: more security often means more friction. But is there a middle ground that builds confidence? The Digital Trust Index guides technology and security decision makers in making the right choices for their users – the choices that help them build the right mix of controls for enabling digital trust with their users.

Contents

Key Findings

ACCESS FRICTION IS ERODING CONSUMER TRUST, BUT VISIBLE SECURITY STILL EARNS IT

57%

Banking remains the most trusted sector for consumers when it comes to sharing their information

ONLY 16%

say they have a thorough understanding of how companies collect, use, and protect personal information online

Consumers reward familiar protections:

69%

would trust a company more if it used multi-factor authentication

68%

would trust a company more if it used passkeys

57%

The majority of consumers have experienced issues when accessing a website or app in the last 12 months.

68% abandoned or switched from a company online due to a website or app issue

77%

are worried about AI "helpers" that would act on their behalf online

FRICTION AT THE ACCESS LAYER IS DRIVING DELAY, DISTRUST AND CREDENTIAL SHARING

ONLY 22%

say access/log-in details are provided immediately when starting with a new external partner, and only 30% say they always get the full permissions they need first time

92%

experienced access issues with an external partner system in the last 12 months, and almost as many (89%) abandoned or delayed work due to a website or app issue

70%

say they are often asked for information that does not feel necessary when requesting access

66%

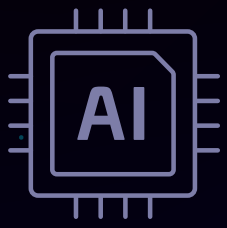
have shared or borrowed access credentials in the last 12 months

HOST ORGANIZATION INTENT IS CLEAR, BUT DELIVERY GAPS ARE WEAKENING TRUST

87% of IT and security leaders say offering passkeys to their organization's consumer customers is important – and yet only 49% currently offer them

ONLY 44% of IT and security leaders say that partner users can see their own permissions

AI ADOPTION IS ACCELERATING, BUT TRUST IS NOT KEEPING PACE



93% of IT and security leaders say that their organization is using, rolling out, or planning GenAI

ONLY 23% of consumers trust a company that uses AI to handle data

81% of partner users would trust an organization more if it used AI to strengthen security

Consumer research findings

For consumers, trust is earned at the access layer

Consumer trust starts to be built in the moments where people try to sign up, log in, share data, and change settings – the core touchpoints of an organization's Customer Identity and Access Management (CIAM) strategy. Those are the moments when consumers decide whether a company feels competent and safe; and, ultimately, whether they are worth committing to.

This year's research findings reinforce a simple point: in most sectors, organizations cannot rely on reputation alone. They start from a trust deficit and must earn confidence through what consumers experience first-hand, especially when it comes to onboarding and authentication. The access layer is therefore where trust becomes measurable, and where revenue outcomes are won or lost.

Banking is the outlier; most sectors still operate in a trust deficit

The 2026 Global Trust Index shows that the gap between the most trusted sector and other sectors has widened. Banking is now a clear outlier: 57% of consumers say they are most comfortable sharing personal information with banks (up from 44% in 2025). It is the only sector where more than two in five consumers express top-level comfort, sitting well ahead of every other sector.

Government (40%) and healthcare (35%) again round out the top 3, but still fall short of a majority and have softened year-on-year. Beyond the top three, the drop off is stark: most sectors sit in low double digits or single digits. This gap reinforces the split between highly regulated sectors (where security and resilience expectations are clearer and protections are more visible) and the wider market, where trust is harder to earn and easier to lose.

Many organizations are still struggling to convince consumers that their data will be handled responsibly. For most, trust must be earned through the quality of day-to-day digital interactions.

> **[They] made it mandatory to setup multi factor authentication as part of the sign-up process. There was no option to opt out. This filled me with a lot of confidence."**
>
> **Consumer, 29-44 years old, USA**

Which of the following types of companies do you trust the most when it comes to online (website or app) interactions?

> When using a government website, I was asked to log in using my digital ID, which increased the security of the service."

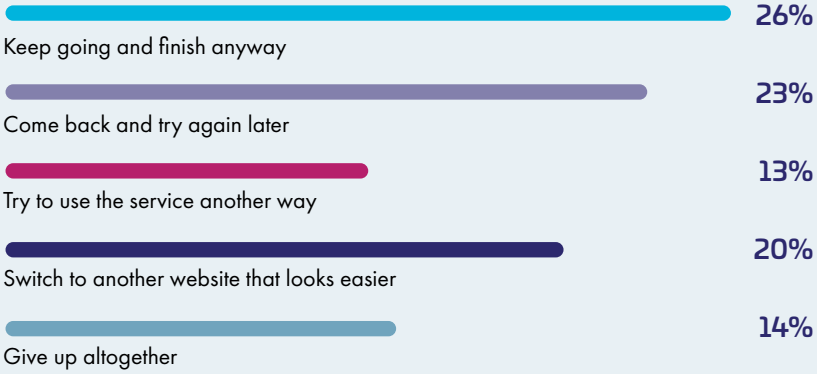
Consumer, 29-44 years old, UAE

Designing for Trust and Preference

The impact is that many organizations begin consumer relationships with a lot of work to do in the early stages to build confidence. Digital trust is then shaped by a combination of user experience, security and privacy (and the trade-offs organizations make between these elements).

Consumers' first digital interactions are critical in earning trust, with sign-up, login and account settings the moments when consumers decide whether an organization feels safe, competent and worth continuing with. And yet **68%** have experienced website and app issues in the last 12 months (such as slow speed, downtime, long sign-up process, etc.), that have forced them to abandon the website and app or switch to another. The result goes beyond brand damage to immediate revenue loss – and potential revenue loss for the future.

When confronted with long or complicated sign-ups, **36%** either come back and try again later or try to use the service another way (for example, in-store or by phone) - resulting in delayed revenue. Most concerningly, **33%** say that they would either switch to another website or app that looks easier or give up altogether. Here the revenue loss is immediate and lasting.



Both of these scenarios (the **36%** delaying, and **33%** switching – nearly seven in ten in total) have an immediate and future impact on revenue. The access journey acts as a gatekeeper for trust: long or unreliable processes increase abandonment, increase channel switching, and reduce user willingness to persist when friction appears later. Reliability and simplicity are preconditions required for trust to be earned at the earliest point of interaction.

However, consumers are not demanding speed at all costs. When asked what they care about more during account creation, **45%** prefer stronger security checks even if sign-up is slower, compared to **22%** who prefer speed even if checks are lighter. Consumers accept friction when it feels protective; but reject friction when it feels excessive or unexplained.

It is also worth noting that the experience gap is not limited to customers. Among the employed consumers in our research, **37%** say accessing their work account remotely is too arduous, and more than half (**57%**) get frustrated every time they have to create a new work password. Digital experience is therefore directly linked to workforce performance as well as customer retention.

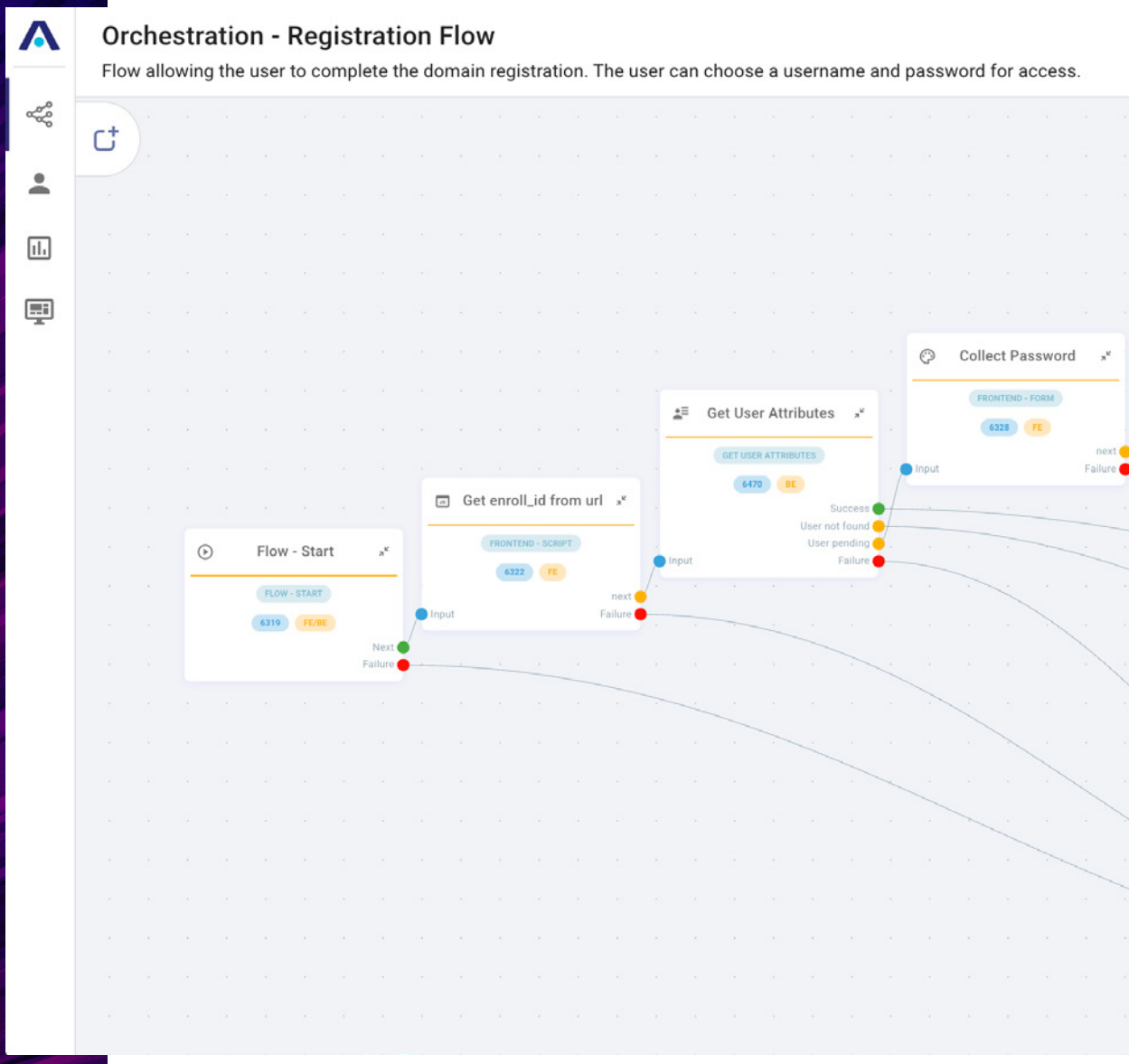
Security and identity checks should scale with risk and be communicated clearly, so that protection does not become a conversion penalty.

> **[It took] too long for the sign up or verification process."**
>
> **Consumer, 29-44 years old, USA**

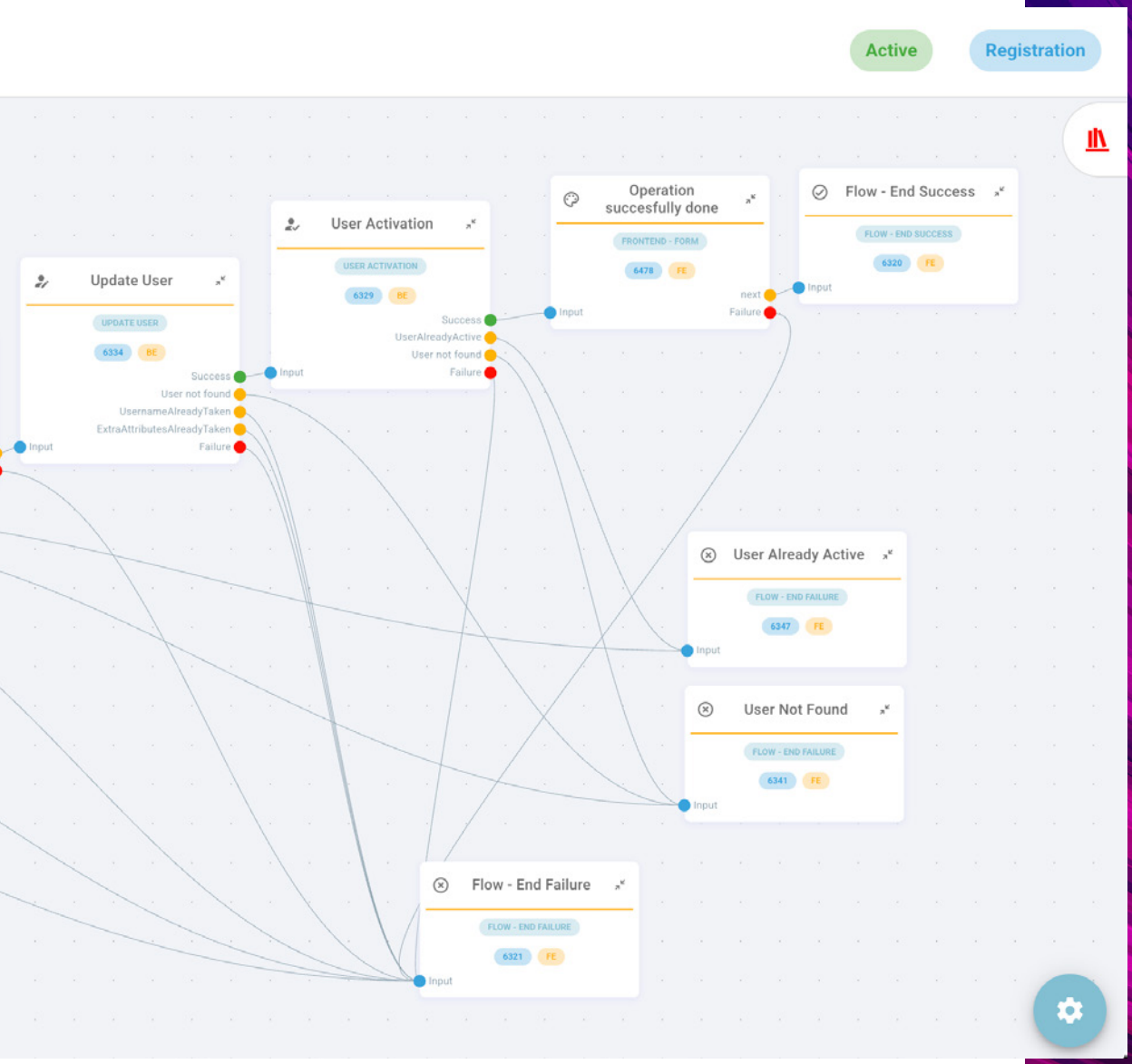
> **The website asked for too much personal information and I did not sign up."**
>
> **Consumer, 45-60 years old, Canada**

Identity Orchestration

With enterprises dealing with a host of different platforms and vendor solutions, has become critical to streamlining your Identity Security Strategy. It unifies different IAM systems across your infrastructure working with multiple applications, enabling organizations to manage user access and security from one central control point.



The Thales OneWelcome Identity Orchestrator (IO) is a next-gen Visual Orchestration tool that acts as the central engine of an Identity Fabric, moving organizations away from siloed, product-centric deployments toward a more connected, risk-aware system of systems that can compute dynamic decisions based on all available contextual signals. As a cloud-based component, IO provides a visual interface and execution engine to manage complex interactions across B2C, B2B, and gig worker markets.



Trust-eroding interruptions

Beyond specific initial sign up requirements, users' digital experiences face notable challenges. These include everyday experiences that shape perceptions of reliability and competence.

In the past 12 months, on at least one occasion:

- Nearly a third (**31%**) of consumers experienced downtime or slow service on a website or app they were using
- More than a quarter (**27%**) saw prices change while trying to buy something
- Nearly one in five (**19%**) were confused about how to use a website or app or access a service

In addition, consumers cite frustrations with low-value, flow-breaking steps such as advertising pop-ups (**38%**), CAPTCHA tests (**30%**) and data entry requests that force the user to re-enter information already provided (**28%**).

Individually, these may seem like minor irritations, and even then, are only reported by a minority in each case. But collectively, they signal inefficiency and indifference to user time, again potentially impacting revenue and customer loyalty. And trust is rewarded when such minor irritations are removed.

When a website/app is simple and easy to navigate, **58%** of consumers say it increases their trust in a company holding their personal information, and when pages load quickly and do not crash or freeze, trust rises for **60%**.

Most notably, when information is written in clear, easy-to-understand language, trust increases for **68%** of consumers, making it the most common trust booster of user experience.

Clear, easy-to-understand language is a visible signal of competence and transparency for an organization. The words on the website or app are part of the security and trust experience: they shape how confidently users can act, how well they understand what is happening, and whether they believe the company is in control. It is critical that website or app copy is expertly crafted, consistent, and written to remove ambiguity at the moments users are most likely to hesitate.

One other potential route for organizations to consider is value exchange:

- Over half (**53%**) would be willing to share more personal information in return for better protection against fraud and scams
- **42%** would exchange more data for lower prices or exclusive discounts
- **40%** would do so for faster and easier log-ins

This shows that consumers are prepared to share their data – but again, only when the benefit is tangible and clearly communicated.

> **"When a company starts asking you for various pieces of your personal information, that's a red flag for me. Why do they want all that information?"**
>
> **Consumer, 18-28 years old, Mexico**

Explain the ask: justification protects conversion and trust

The research shows that consumer willingness to share data is conditional, and it shifts materially when purpose is explained.

Comfort varies sharply by information type:

- Only **7%** are comfortable providing a National ID, while **67%** are not comfortable
- For phone number, only **19%** are comfortable and **32%** are not comfortable
- For email, **33%** are comfortable and **12%** are not comfortable

What changes behavior is justification: when the reason for sharing is clear, willingness rises substantially:

- **24%** would share National ID if the reason is clear
- **48%** would share phone number if the reason is clear
- **54%** would share email if the reason is clear

Transparency then can be regarded as a conversion tool. When organizations clearly justify why data is needed at the point of collection, they encourage sign-up completion that might otherwise be lost to uncertainty or suspicion. If the argument is made well, consumers are open to sharing more information about themselves: only **19%** say that they would be unwilling to share more personal information in order to get better protection against fraud and scams. This makes a strong case for progressive profiling: delay sensitive requests until they are genuinely needed, and pair each step with a clear explanation of what it protects.

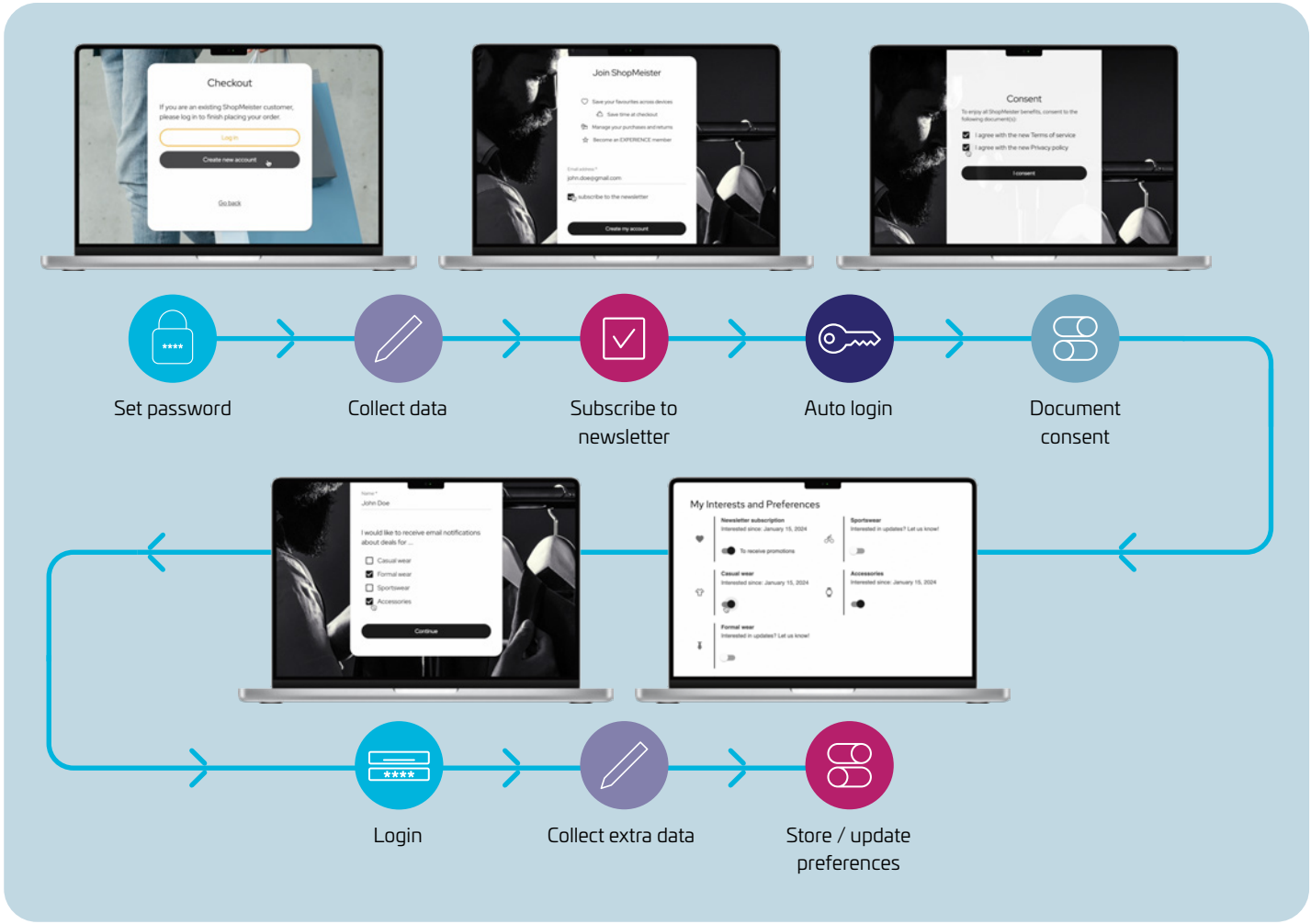
There are also some notable variations by country, although the exact percentages vary by information type:

- Consumers from South Africa (**48%**), UAE (**46%**) and France (**44%**) are most likely to be completely happy to share their name even if it is not made clear why it is needed. Least likely are consumers from Japan (just **11%**)
- Data of birth is information that consumers are more cautious about sharing: those from the UAE (**49%**) and France (**42%**) are most likely to be completely happy to share these details even if it is not made clear why it is needed. Consumers from Japan and the Netherlands are least likely (both **16%**). Respondents from the Netherlands however are most likely to be willing to share if the reason is made clear (**61%**)
- When it comes to bank details, consumers are naturally far less likely to be willing to share: consumers from the USA, UAE, Mexico and Brazil are most likely to be completely happy to share these details even if it is not made clear why it is needed (all **6%**). Consumers from Japan, the Netherlands and Canada are least likely (all **1%**). Respondents from Mexico however are most likely to be willing to share if the reason is made clear (**34%**), with Canada at the other end of the scale (**12%**)

This demonstrates how certain types of personal data may be regarded very differently across countries depending upon local culture and customs. There is delicate balance for organizations to strike when it comes to access processes and permissions globally if revenue is to be maximized everywhere.

Progressive Profiling

As a solution, some brands opt for progressive profiling – a concept in which data is collected gradually and transparently to avoid overwhelming the user. It uses shorter forms or surveys during multiple interactions to create detailed user profiles over time.



Trust deficit: expectations are high, but control is low

Consumers expect transparency (**67%** expect to be informed that data is being collected), but few feel informed or empowered:

- Only **16%** say they have a thorough understanding of how companies collect, use, and protect personal information online
- Only **8%** say it is very easy to exercise privacy rights with companies they use online
- **56%** say companies place too much responsibility on customers to protect their data
- **66%** trust companies more if it is easy to see and change privacy/security settings

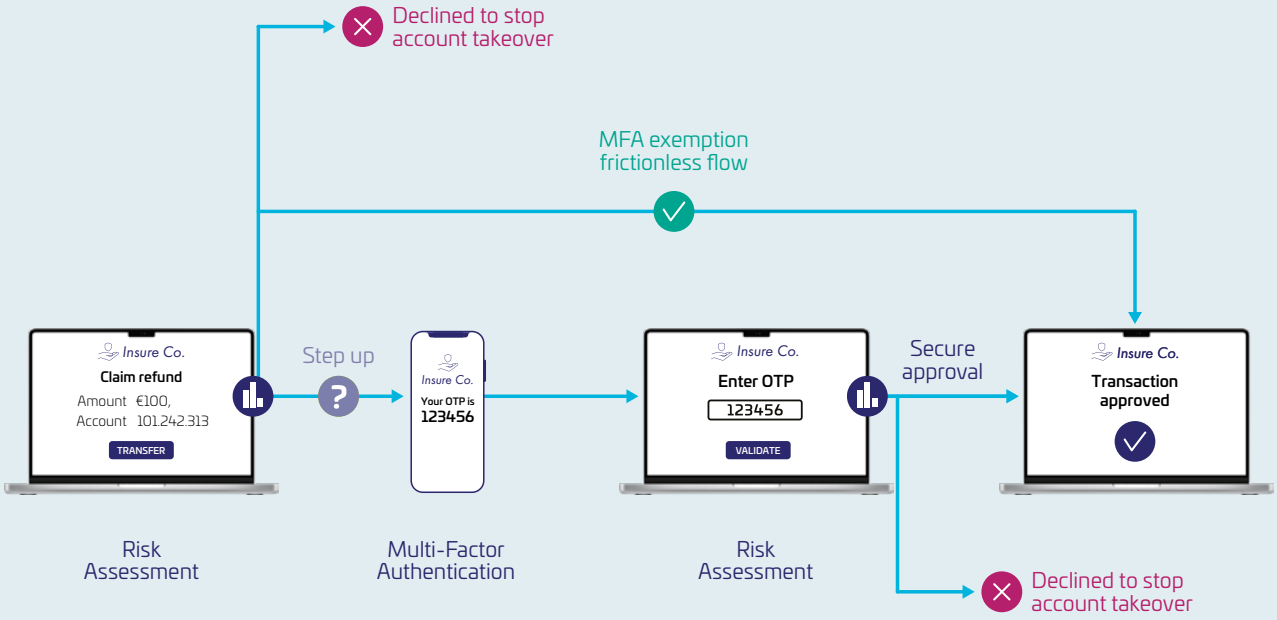
This shows why consumers can lose confidence quickly when journeys are opaque or unreliable: people feel exposed, and they cannot easily correct what is happening. With **66%** saying they trust companies more when it is easy to see and change privacy and security settings, better consent management (clear choices, easy-to-find controls, and simple ways to update preferences) becomes a tool for retention that reduces friction caused by distrust.

> **Easy to read and understand my rights in terms of check out and how my data was being used made me feel more happy and increased my trust because it made me think they were more transparent with customers."**
>
> **Consumer, 18-28 years old, UK**

Did you know?

Risk-Based Authentication (RBA)

Risk-Based Authentication (RBA) is a type of authentication that varies based on certain behaviors and characteristics. It automatically undertakes a risk assessment of a customer and determines threat risk based on those characteristics – including a user's IP address, physical location, browser history, device and their behavior. RBA checks each transaction and user on a case-by-case basis, unlike traditional systems. For consumers it offers the highest level of security, with the least interruption or disruption to their day-to-day user experience.



1 User initiates transaction

Risk assessment passively done to determine flow – exempt, step up, or decline

2 Exempt & approve

If initial Risk assessment checks pass, transaction is allowed to go through frictionless to approval

3 Step up & approve

MFA flow initiated; customer is asked to authenticate through another factor

4 Decline at Initiation

Initial Risk assessment decides to decline transaction upfront

5 Decline after MFA

Further Risk Assessment determines transaction may be account takeover attempt & declines

This simple RBA example depicts how authentication can be made more frictionless and more secure. RBA runs in the background, evaluating when and if, "stepping up" to a stronger form of authentication is necessary.

Trust increases come from recognizable security signals and clear policies

To earn trust, security must be both strong and legible. Our research shows that the biggest trust increases come from familiar signals and clarity:

- MFA: **69%** trust more (only **7%** trust less)
- Passkeys: **68%** say they would trust a company more (only **9%** trust less)
- Clear, transparent policies on data collection and use: **69%** trust more (only **7%** trust less)

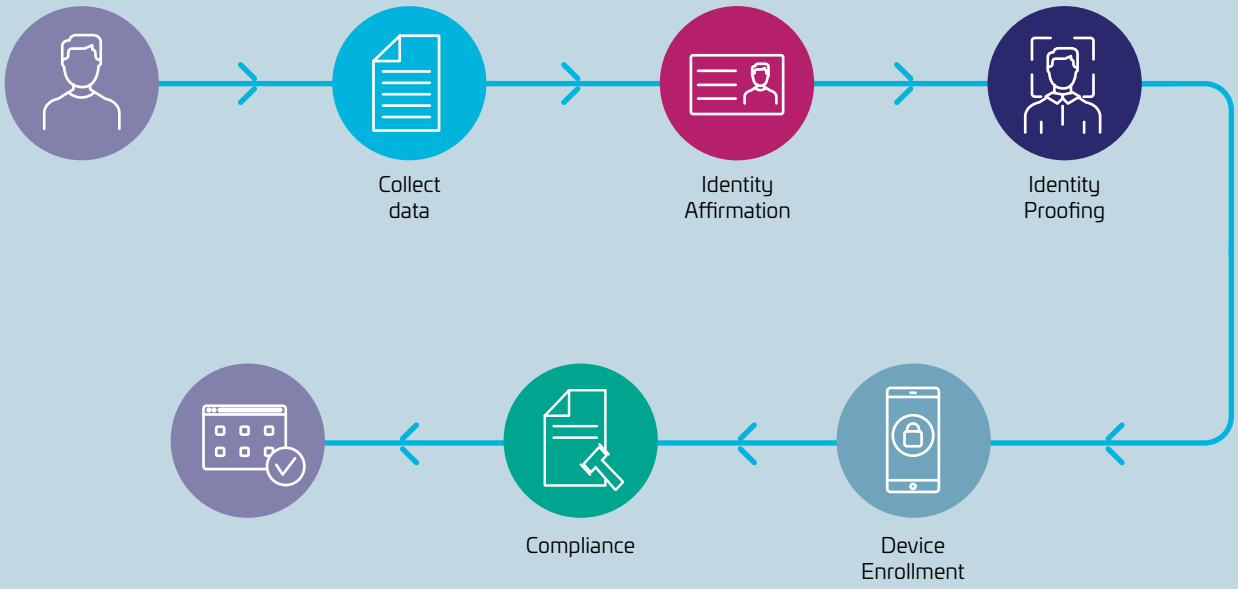
These results show that when protection is recognizable and clearly framed it reassures users, which in turn is likely to support completion.

However, newer approaches can create backlash when they are not understood. AI is more likely to make users trust an organization less (**38%**) than more (**25%**), and more than three quarters (**77%**) are worried about AI "helpers" acting on their behalf online. It is clear therefore that consumers remain wary of AI. But this does not mean that modernization is wrong; it shows that adoption is as much a communication and journey design challenge as a technology choice. Consumers need plain-language explanation of what is changing and why it is safer. Consumer views on AI, and what this means for websites that they access, is explored more in section 4.

> **Trust really increased when a company was transparent and proactive with security settings, like clearly explaining why permissions were needed and offering easy-to-find options for two-factor authentication and login alerts. On the flip side, trust dropped when security controls were hard to find or when the site pushed weak defaults (like no 2FA by default) without clearly explaining the risks."**
>
> **Consumer, 29-44 years old, Australia**

What this means for organizations: the commercial impact is practical and preventable

Across the consumer access journey, the research points to a consistent pattern: trust is fragile, and failure at sign-up and login can drive measurable revenue loss. The route to improvement is therefore to make access reliable; explain why the data is being asked for; use recognizable security signals; and build usable controls into the account experience. This can reduce abandonment and costly channel switching while strengthening security and lowering fraud and remediation costs.



1

New User arrives

and provides information (mobile phone, email etc.)

2

Identity Affirmation

Performs background checks:

- Device Intelligence
- Behavioral Analytics
- Behavioral Biometrics

3

Identity Proofing

- Document Authentication
- Facial Recognition
- Liveness Detection
- Deepfake detection

4

Device Enrollment

- User Authentication
- Email Verification
- Out of Band (OOB) approval

5

Compliance

Backend Checks and any other 3rd party tools such as AML

Partner users research findings

Partner user trust at the point of access

If consumer trust is shaped at sign-up and login, partner user trust is shaped at onboarding, access provisioning, and entitlement management. These journeys may differ, but they are operationally linked. When partners cannot get in, work pauses, quotes stall, deliveries slip, and revenue is delayed, or even lost. The access layer is therefore not just a security control; it is a performance dependency across the value chain.

This section explores where partner user journeys most often break down across onboarding, authentication, authorization and data transparency, and what it takes to make secure access feel reliable, proportionate, and easy to navigate. Partner access is failing at scale. Partner users report delays, visibility gaps, and routine workarounds. The result is slower execution across the value chain and increased identity risk through shared credentials and overexposed access.

> **[I would like to see] Alignment with zero-trust principles while keeping the user experience realistic."**
>
> **Supplier partner user, Pharmaceuticals, Australia**

Trust levels are low: security, privacy and UX all play a role

Only **33%** of partner users (third-party users of external partner systems) say that they would completely trust their industry as a user of its digital services. And when it comes to their organization in particular, this figure barely rises to **41%**. Complete trust is therefore a minority position, even in their own organization's digital services.

When partner users are asked what matters most to trust:

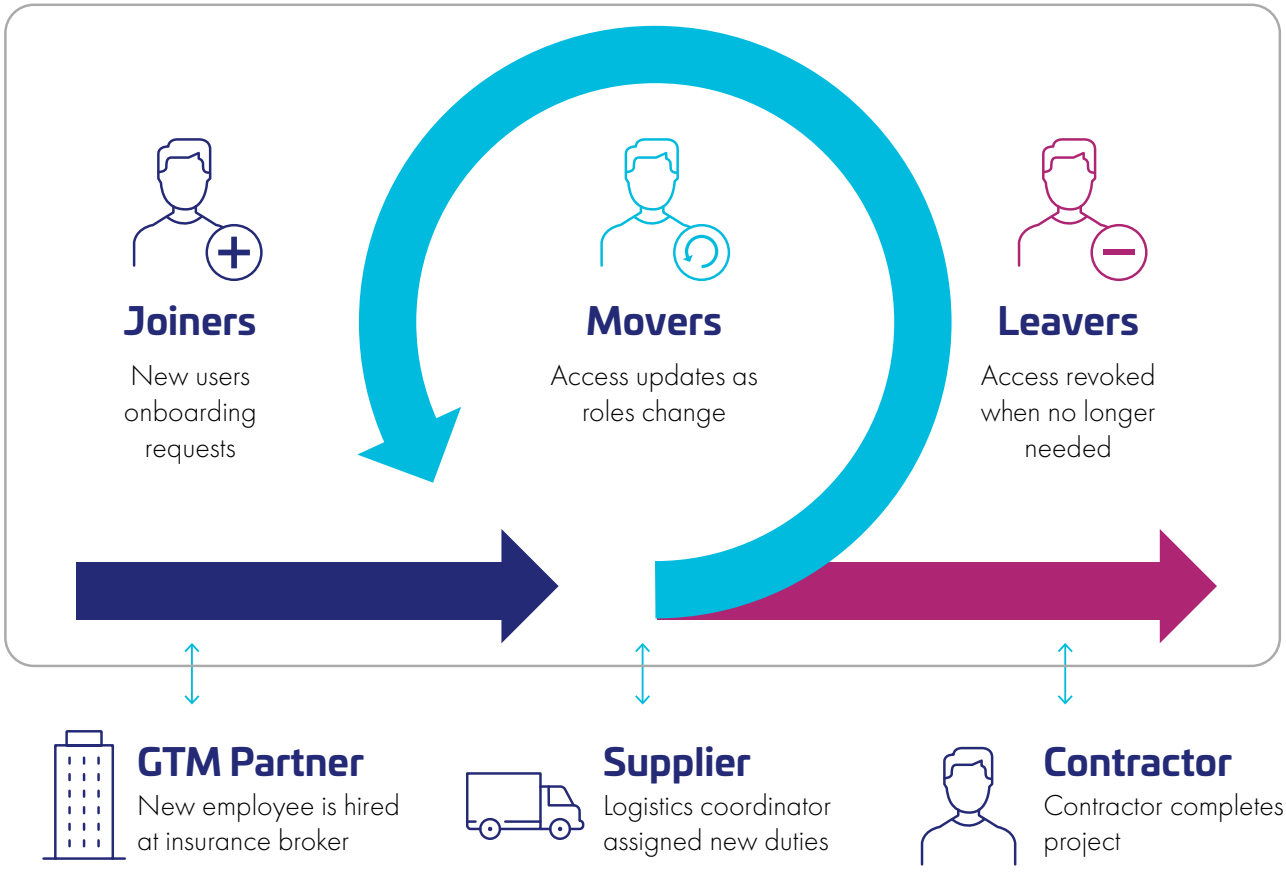
- **82%** say security has an impact on whether they trust an organization's digital interactions
- **81%** say data privacy has an impact
- **75%** cite user experience as having an impact

This shows that trust cannot be won with security claims alone when it comes to partner users: the winners will be the organizations that use Identity Access Management (IAM) to make protection and privacy work visibly and smoothly inside the user journey, turning stronger controls into fewer drop-offs, faster partner productivity, and lower risk.

Mapping the Identity Journey: Joiners, Movers and Leavers

Managing identity and access across the full lifecycle of third-party users is critical to maintaining operational control. External individuals may join, shift responsibilities, or depart unexpectedly. If access rights are not updated immediately, systems remain vulnerable and accountability is compromised. Like workforce identities, third-party identities follow the JML (joiners, movers, and leavers) conceptual framework. This report takes a comprehensive look at identity and access management through the lens of three key user journeys:

- Joiners – New users entering the ecosystem, requiring seamless yet secure onboarding.
- Movers – Those who change roles, role, or entitlements, demanding dynamic, real-time access adjustments.
- Leavers – Users who exit the system, requiring efficient offboarding to prevent lingering access risks.



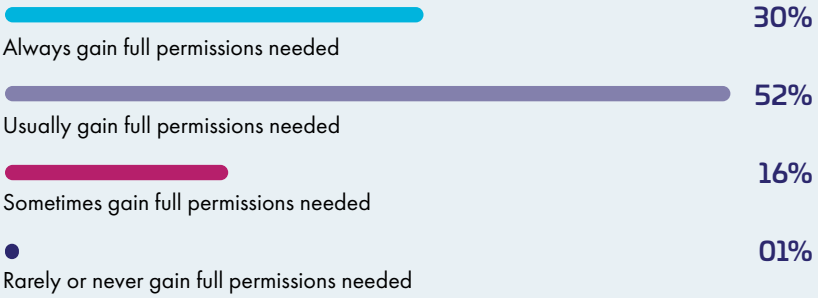
Trust can be earned by reliability and simplicity

Trust is tested earliest and most frequently at the point of access: onboarding, login, and access changes. When these steps work consistently, users experience a process that communicates competence and control. When one or more of these steps fail (through delays, unclear permissions, or unreliable systems) trust can be damaged, even before any service value has been delivered.

Partner users need fast, clear, dependable access to host systems; but that expectations are rarely met. Only **22%** receive log-in details or system access immediately when they first start working with a new external partner. Just **30%** always receive the permissions they need at first access. Many partner engagements therefore start in a holding pattern, with work ready to begin but access gating execution, pointing to weak authorization design and provisioning processes that undermine the experience from day one.

Typically, how quickly do you receive login details or system access when you first start working with a new external partner, once they have been requested?

Do you typically get all the permissions you need when you first gain access to work with a new external partner?



Identity verification itself is usually digital, as reported by **64%** of partners. But ownership is fragmented: while nearly half (**49%**) say that the host organization manages it, the remainder say it is managed either by the other organization or that it is shared. Taken together, partner onboarding is likely to be digitally enabled in most cases, yet operationally inconsistent between organizations.

Once access is granted, change processes often fail to keep pace with working needs: only **19%** say access changes are implemented immediately after responsibilities change. This creates execution delays in live partner work and can directly shift revenue. A reseller unable to access pricing tools may quote a competing vendor, and a distributor unable to retrieve inventory information may lose a sale.

This highlights the need for stronger identity foundations (e.g., SSO) combined with better authorization and provisioning, so that entitlements can be updated quickly as roles change, reducing the risks to projects and revenues.

Impact: knowledge and reliability gaps are common in partner user access journeys

Reliability failures are common in partner access journeys and regularly interrupt day-to-day work. Across partner users, **73%** say that their expectations are not always met when they need to request access or request a change to access. The operational impact is clear: **66%** of partner users say they have experienced problems when accessing or attempting to access external partner systems within the last three months.

These interruptions slow execution and create frustration for partner teams who depend on external systems to complete their work.

Access control issues can cause issues with both productivity and security.

- **66%** of partner users say they frequently lose access to an external partner's system while they still need it to complete their work.
- **71%** are concerned about the security implications of retaining access to external partner systems they no longer need.

Together, these results indicate that access provisioning and access removal are not consistently aligned to real working needs. This points to a lifecycle control problem: access is removed too early for some users, while unnecessary permission persists for others.

Limited visibility into permissions further compounds the issue. Only **30%** of partner users are completely confident that they fully understand what permissions they have on external partners' systems.

When users cannot clearly see what they are authorized to do, they are less confident operating within the system and more likely to perceive the access model as inconsistent or poorly managed. The result is a trust gap: legitimate work is interrupted, while residual access risk accumulates.

Ensure that external partners only receive the minimum permissions necessary to perform their tasks and avoid unnecessary data access."

GTM Partner user, Retail, Germany

A bit more leeway with temporary access for specific projects would save a lot of back-and-forth emails requesting one-off permissions."

Supplier Partner user, Education, Australia

When access fails, partner users find alternative routes

Reliability problems translate directly into aborted interactions and frustration. **92%** of partner users have experienced issues when trying to access an external partner organization's system in the last 12 months. Even if no issues have been experienced, lack of information can be just as damaging, only **22%** receive status updates on access requests very frequently.

When access becomes unpredictable, it forces users to spend time retrying, escalating, or seeking alternatives:

- **89%** of partner users have abandoned or delayed a work task with an external partner in the past 12 months due to a website or app issue

In this situation, controls stop matching real behavior.

In this environment, formal controls stop matching real behavior. **66%** have shared or borrowed credentials; and among those, **53%** cite slow official processes as the cause. This shows how, if the legitimate route cannot meet operational needs, users switch to whatever works – even if this creates risk. These abandonments and delays inevitably not only mean a loss of productivity (and ultimately, of revenue and growth), but also an accumulation of silent security debt: widespread credential sharing and opaque workarounds that increase the likelihood of breaches and compliance exposure. Host organizations therefore need to prioritize the operational fixes (speed, clarity, and responsiveness) that would reduce this risky behavior.

> **Access permissions must be clearly defined to prevent any confusion and ensure optimal use of the system."**
>
> **Supplier Partner user, Manufacturing, UAE**

> **Reduce access granting delays through improved workflow automation."**
>
> **GTM Partner user, Manufacturing and production, Germany**

Self-serve reduces delays and tickets

One effective way to address this is through delegated administration via self-service. Partner users desire self-service elements to be offered to improve access, and most want the ability to reset authentication factors (**54%**) or the ability to see their current entitlements (**52%**). If host organizations can provide self-service options where possible, it can strengthen self-service and visibility. This can reduce repetitive tickets, accelerate resolution, and keep partner journeys moving without costly escalation.

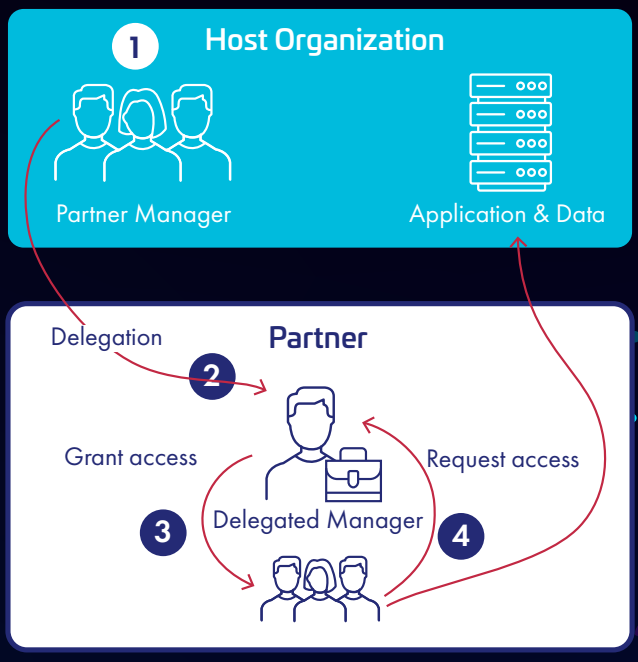
I think they should create a self-service portal where external partners can review and renew their access without so much bureaucracy and waiting time."

Partner user, Pharmaceuticals, Mexico

Delegated User Management: Centralized control, decentralized user administration

Delegated User Management enables organizations to keep control over identity systems while allowing designated business stakeholders—like partner managers or regional leads—to manage third-party users directly within predefined boundaries.

Instead of routing every access request through central IT, user onboarding, updates, and revocations can be handled by those closest to the relationship, improving both speed and accuracy.



1. Host Organization:
The identity and access is managed by the host organization. A Partner Manager configures which access rights and controls can be delegated, while applications and data remain protected under the host's policies.

2. Delegation to the Partner:
The host organization delegates access management privileges to a Delegated Manager within the partner organization. This individual acts as a proxy administrator for their users.

3. Granting Access:
The Delegated Manager can directly grant, update, or revoke access for users within their organization, ensuring that onboarding is fast and aligned with real-world responsibilities.

4. Access Requests:
End users within the partner organization request access through their Delegated Manager, who processes the request in line with the boundaries defined by the host.

Transparency can lead to more secure processes

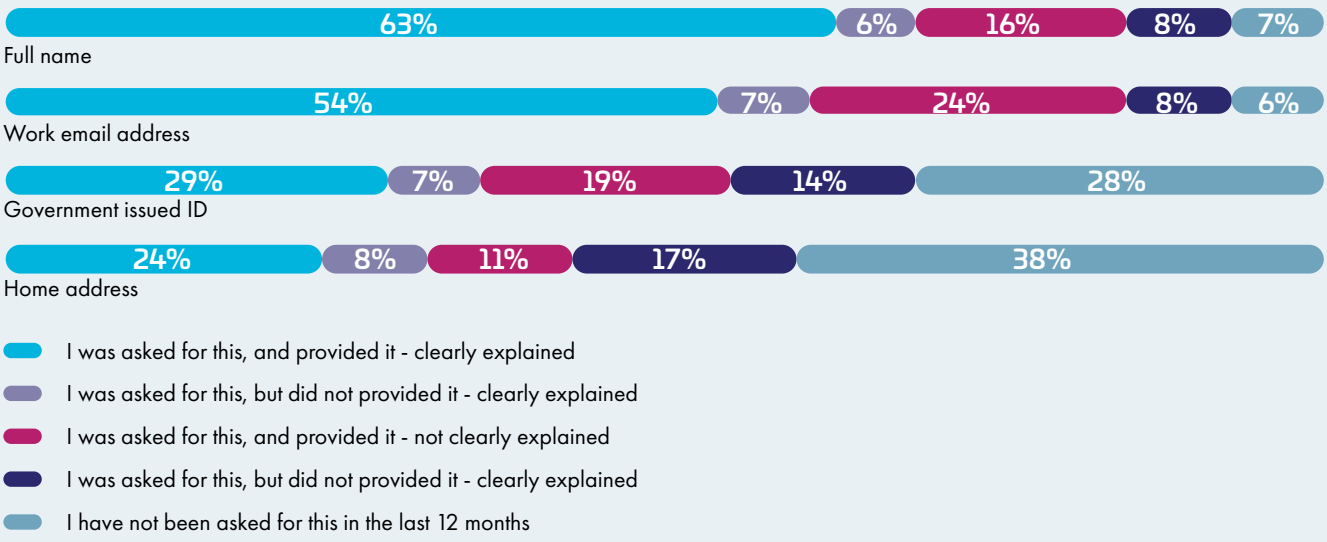
Transparency is one of the main determinants of whether people comply, persist, and trust interaction. When users understand what is being asked of them and why, security checks can feel proportionate and protective. When they do not, the same checks can feel like friction or overreach, which can lead to abandonment, frustration, and workarounds.

The first transparency problem is simple: people feel over-asked. **70%** of partner users say they are often asked for information that does not feel necessary when requesting access to an external partner system.

If a request feels unjustified, users may assume either excessive collection (a privacy risk) or poor process design (an operational risk). These perceptions can reduce willingness to engage and increase resistance at the very point where organizations need users to be accurate, patient, and compliant.

> **[I would like to see] Significantly more explanation, transparency in the process."**
>
> **Supplier Partner user, Logistics/supply chain, Germany**

Across all of the external partners you work with, in the last 12 months, which of the following types of information have you been asked to provide? / Thinking about each type of information you were asked to provide how clearly, if at all, did the organization explain why they needed it?



Clear data policies, risk management and consent management strengthen trust (as well as improve compliance). This is true not only of consumers (**69%** of which say that they trust a company more online if they have clear & transparent data collection & use policies), but of partner users too: **57%** say that they trust an external partner more when it has clear and transparent data collection and use policies. When organizations explain what they collect, why they collect it, and how it is protected, it makes it easy for users to interpret controls as necessary (or at least understandable) safeguards.

Levels of trust do vary by sector:

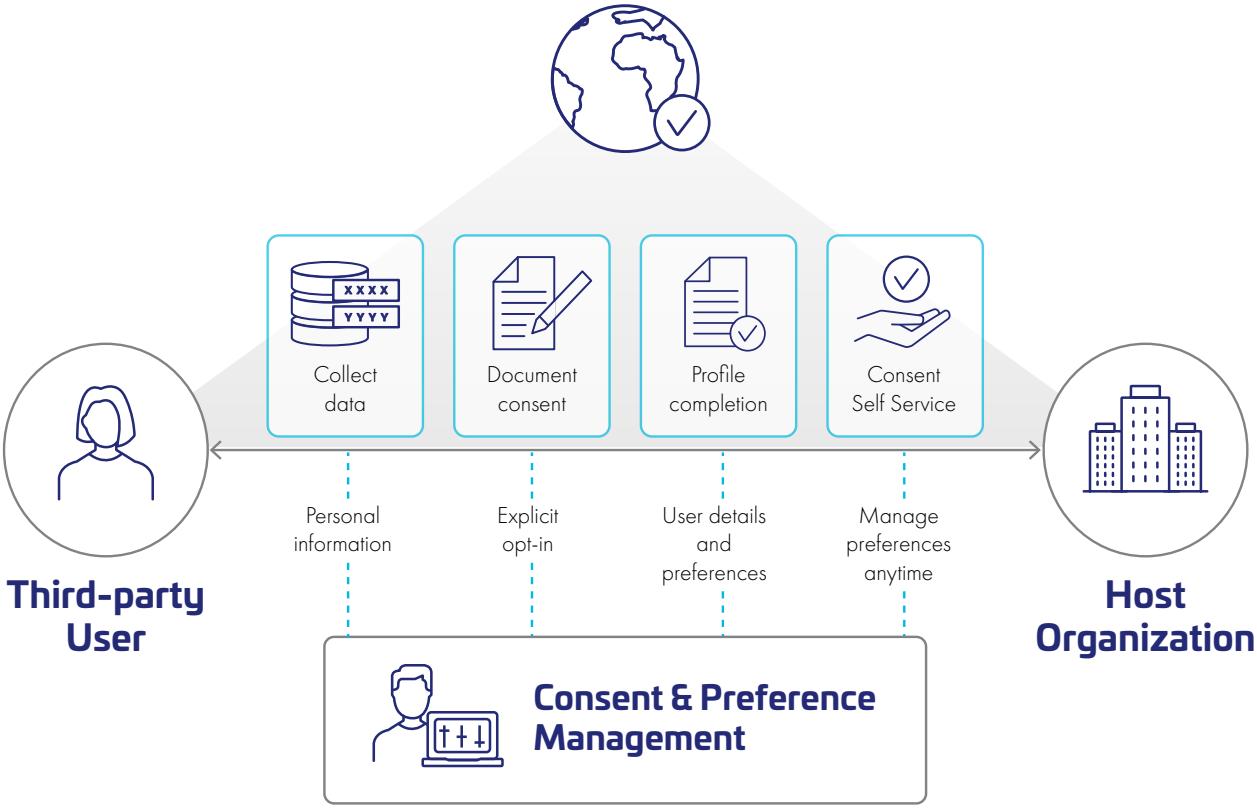
- Those that work in the News media and social media sector, or the Retail sector (**71%** and **70%** respectively) are most likely to be impacted by this. In sectors with higher public scrutiny, misinformation risk, or fraud exposure, respondents are more likely to say transparent data practices would increase trust.
- In contrast, those who work in the Education sector are less likely, although it is nonetheless still nearly half (**45%**) who say that they would be influenced by the presence of clear and transparent data collection and use policies, showing that no sector should be left behind by improvements in this area

Transparency also shows up in what systems accidentally reveal. If controls are misconfigured, users may notice and infer security and privacy weakness as a result. **65%** of partner users say they often encounter information they should not have access to and/or are able to modify information they shouldn't be able to modify when using external partner systems. And this leads to a wider concern: **72%** of partner users do not completely trust that their organization's digital interactions with external partners are secure and will not cause harm.

> **"They should be more careful with the data they request and explain better why they are requesting that data and what they are going to do with it."**
>
> **Supplier Partner user, Manufacturing and production, Mexico**

Consent and Preference Management

Third-party users are not exempt from compliance requirements. Consent and preference management are critical because organizations must ensure that all personal data handling—including that of third-party users—adheres to applicable privacy regulations. Regulations such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other regional laws require explicit consent and management of user preferences for data collection, processing, and sharing. Proper consent management for third-party users is essential to maintain compliance, build trust, and reduce legal risks related to data privacy.



High expectations, low understanding, and weak control create a trust deficit for partner users

Partner users expect transparency: **59%** expect the right to know what data is collected. But these expectations collide with low understanding – **72%** say they do not have a thorough understanding of how external partners collect, use, and protect their personal and work data.

In addition, users may find it difficult to take corrective action when needed. Only **23%** of partner users say it is extremely easy to update, correct, or remove data held by external partners. The result is that partner users are likely to feel that the burden is on them to protect and manage their own data, as illustrated by the fact that **76%** say external partners place too much responsibility on third-party users to navigate complex requirements.

When understanding is low and control is hard, users can feel exposed, as they are being asked to accept a risk that they cannot properly evaluate. This weakens trust in the system and reduces tolerance when anything goes wrong. This can damage working relationships with partners.

Identity security is already a concern for organizations

This feeling of excess responsibility occurs against a threat backdrop where identity compromise is already part of the landscape: **52%** of partner users believe someone else might have accessed an external partner system in the last 12 months pretending to be them. Stronger and better-explained controls reduce both security risks and the operational cost of remediation.

When data requests feel unnecessary, cooperation drops. When understanding and control are low, responsibility shifts onto users and trust declines. On the flip side, when security friction is explained, many users accept it; when it is opaque, it is interpreted as waste. And when official routes are too slow, insecure workarounds become normalized. This minimizes trust and creates barriers to revenue and efficiency. Transparency therefore reduces the conditions that create risky shortcuts.

> **The focus should be on how external partners handle user data, while ensuring privacy and transparency in practices."**
>
> **Supplier Partner user, Pharmaceuticals, UAE**

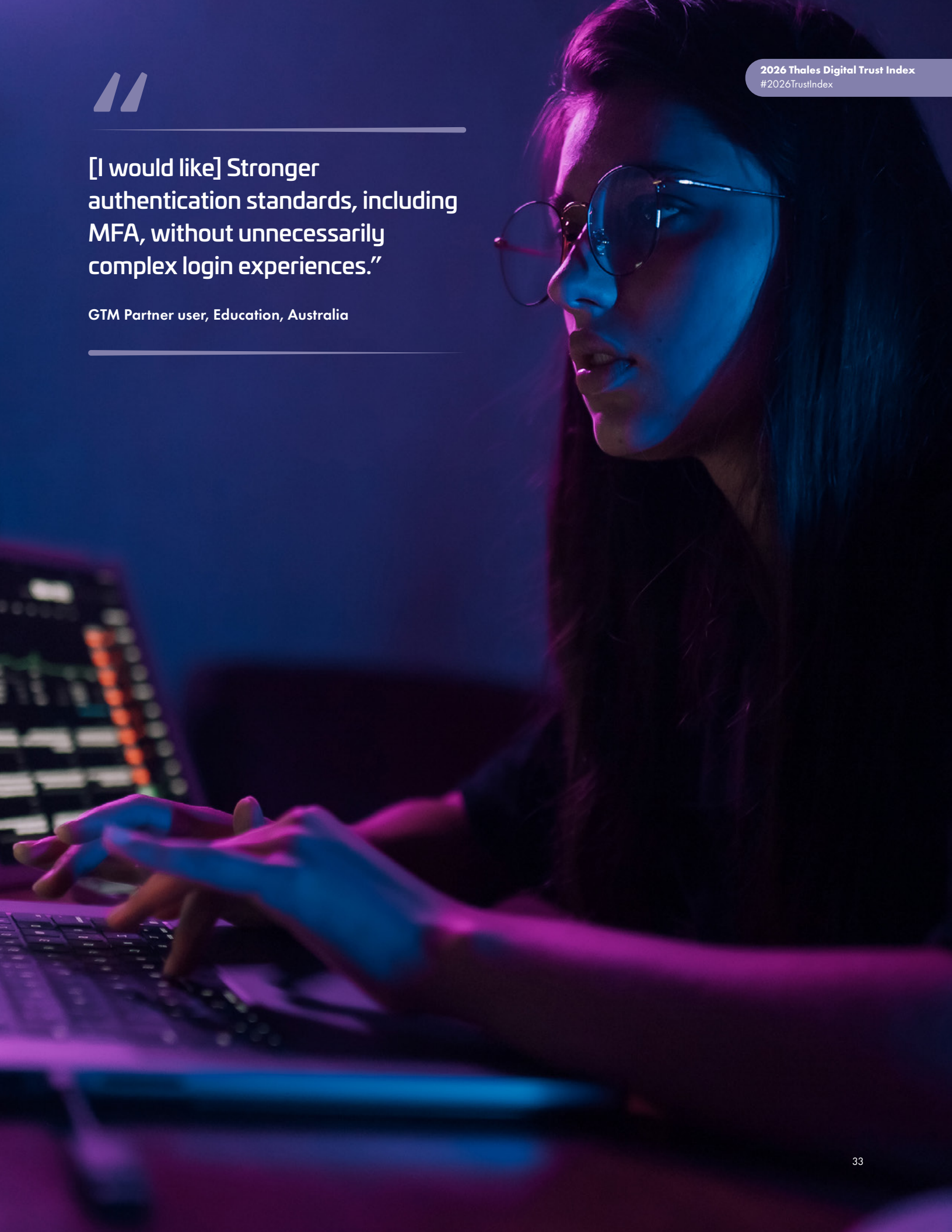
Technology can close the trust gap when deployed appropriately

The technology choices that organizations make as part of their access strategy can have a notable impact, not only in how effective their security is, but in how their organization is perceived by partner users. The majority (**57%**) say that they trust an external partner more when they use multi-factor authentication (MFA) as part of their security practices. **33%** also say that they would trust an external partner a lot more when they use biometrics as an authentication factor.

Deployment of IAM technologies like MFA and biometrics can become a visible signal of competence. They strengthen security while shaping partner users' perceptions at the key moments where trust is earned or lost

Building competitive advantage through better access

Organizations can strengthen partner trust by improving journey orchestration: designing onboarding, authentication, authorization and data consent as one connected flow rather than separate processes. By combining stronger authentication and governance with transparency and self-service, organizations can reduce workarounds, improve data confidence, and deliver a smoother user experience without weakening protection..



> [I would like] Stronger authentication standards, including MFA, without unnecessarily complex login experiences."

GTM Partner user, Education, Australia

IT and security leaders research findings

Consumer perception vs. delivery: where trust (and revenue) leaks in onboarding and login

A clear perception gap between IT and security leaders and consumers emerge around data collection. Only **11%** of IT and security leaders believe that initial data collection is the step most likely to cause abandonment, and yet **28%** of consumers say they have abandoned a company online because it demanded too much personal information. This gap suggests that organizations may be underestimating the commercial impact of excessive or poorly justified data requests. Re-evaluating what data is collected, when it is requested, and how clearly its purpose is explained could directly improve consumer completion rates and protect revenue.

IT and security leaders appear confident that their organizations have a solid baseline of consumer trust: 44% believe customers completely trust their digital interactions with the organization, and a further **50%** believe trust is at a moderate level. But this confidence sits alongside a harsher operational reality: **62%** of organizations have discovered fraudulent consumer accounts using synthetic identities in the past 12 months.

The implication is that organizations are being forced to strengthen identity controls in a high-threat environment while still preserving the seamless, reassuring experiences that trust depends on. If additional checks or data requests are introduced without clear justification and careful journey design, they risk turning necessary security improvements into avoidable friction. This can undermine completion and, over time, the trust IT and security leaders believe their organizations have earned.

There is also a distinct execution gap in authentication strategy.

- **68%** of consumers say that they would trust a company more if it offered passkeys, and **87%** of IT and security leaders agree that providing passkeys is important, but only **49%** of organizations currently offer them
- **51%** allow customers to sign up using preferred identity providers such as Google or Apple, but just **36%** already offer Bring Your Own Identity (BYOI) or social login as a defined capability, with **43%** still only planning or considering this

This shows that intent is frequently outpacing implementation. We have already seen in the previous sections how consumers are looking for stronger, more user-friendly authentication and visible security controls. Organizations that hesitate may find that competitors who implement a passwordless approach, federated identity options, and clear policy transparency, will gain a trust advantage. Closing the gap between strategic awareness and operational delivery can therefore strengthen both security posture and customer confidence simultaneously. This can serve to reduce fraud exposure while protecting revenue growth.

IT and security leaders indicate operational gaps and a growing trust responsibility in host organizations

IT and security leaders occupy an important position in building trust. They design, implement, and manage the identity and access processes that shape consumer and partner experience throughout its lifecycle. Their perspective reveals how organizations that act as a host believe they are performing, and where perception may diverge from user reality. In several areas, IT leaders report higher levels of confidence than users (consumers or partners) report satisfaction. This divergence suggests that governance maturity and journey orchestration may not yet be fully aligned with the lived user experience.

But there are areas where there is broad agreement across the respondent types. IT and security leaders, similarly to partner users, are likely to report that identity and access processes are digitally enabled, but operational inconsistencies remain. While **73%** say identity verification is mostly a digital process, responsibility for managing that verification is fragmented: **48%** say it is handled by the host organization, **24%** say it sits with the partner organization, and others report shared ownership.

> **I hope to introduce a single sign on system to improve access efficiency."**
>
> **IT Manager, Automotive, USA**

This split suggests that while digitization is advanced, governance alignment across ecosystems is less mature. **50%** of IT and security leaders also say their organization often asks for information that feels unnecessary when an external partner requests access to their systems. These findings echo the views of partner users, showing that friction and inconsistency are not just perceived externally but recognized internally. This points to a need for clearer ownership, more proportional data collection, and more joined-up controls across the end-to-end partner access journey.

> **Implementing a centralized Single Sign-On (SSO) system would improve the user experience."**
>
> **C-level DevOps, Insurance, Mexico**

Self-service progress, but weak visibility and a difficult balance

On self-service capabilities, IT and security leaders report partial progress. Fewer than half (**48%**) say their organization provides authentication factor reset capabilities, broadly aligned with partner expectations. And only **44%** say that their organization's partners can see their current entitlements, indicating that visibility into permissions (an important governance control) is also not yet widespread.

This gap may contribute to downstream access confusion and support burden. **62%** are also concerned about external partners retaining access to systems that they no longer need to, and **55%** say that their organization struggles to strike a good balance between security measures and ease of use for external partners.

These points again echo concerns cited by partner users and demonstrate the difficult balance that host organizations are trying to strike between allowing enough permissions and visibility for partner users to carry out their tasks, without allowing so much that it presents an unnecessary security risk.

> **[I would like] More single sign on with 2FA, it's the sweet spot for ease of use and security."**
>
> **IT Manager, Entertainment, UK**

Risk signals: perception gaps, limited confidence, and active threat

Another noticeable difference between IT and security leaders and partner users involves how they view risky actions IT and security leaders. When credential sharing occurs, IT and security leaders are most likely to attribute it to operational preference: **39%** believe account sharing happens because partner organizations prefer a common credential for convenience. Only **17%** attribute credential sharing to slow official access provisioning, in contrast to partner users who are likely to highlight this as the key driver (**53%** reporting this). This suggests IT and security leaders may underestimate the operational friction that drives insecure workarounds. This is also concerning since only 44% of IT and security leaders say that they are completely confident that their organization has full visibility into the permissions external partners currently have within systems.

At the same time, IT and security leaders recognize that identity compromise is a real and present threat. **53%** believe someone may have accessed an external partner system in the past 12 months pretending to be them, and **69%** report discovering fraudulent consumer accounts using synthetic identities in the last year.

These figures are somewhat larger than the consumer (**27%** concerned about someone using stolen personal details or AI-generated fake to open an online account in the respondent's name) and partner user (**52%** have had cause to believe that someone else might access an external partner's system pretending to be the respondent) equivalents. This suggests that, if anything, users may underestimate the true scale of the issue.

IT and security leaders clearly recognize both the scale of identity-related risk and the importance of modernizing access journeys. However, this section shows that awareness does not always translate into alignment, and that friction is often underestimated. Where IT and security leaders see digitally enabled processes, users frequently experience delay, confusion, or excessive data demands. Closing these gaps requires intelligent deployment of new technology. It demands clearer ownership, proportional data collection, stronger entitlement visibility, and faster rollout of user-friendly authentication. This will lead to improved levels of trust, and faster project and revenue delivery.

AI research findings

The AI trust gap is already visible

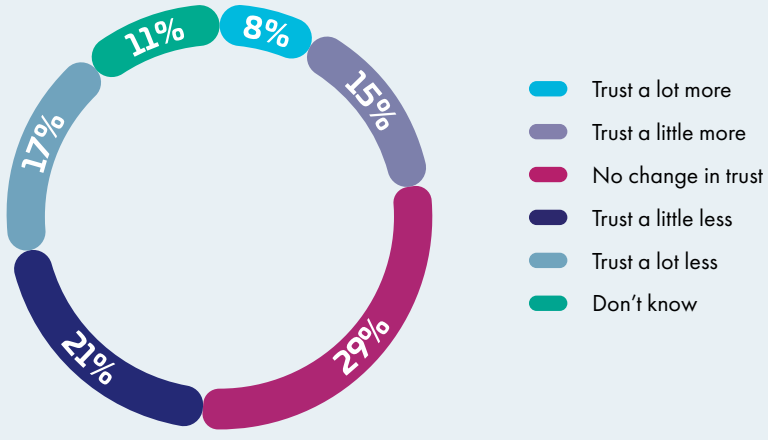
AI represents both an opportunity and a potential weakness in digital trust. While the IT security benefits of AI are numerous, there is a pronounced gap between consumer comfort with AI and business optimism about it.

Consumers are extremely cautious when it comes to AI. **77%** of consumers would not trust a company more if it used generative AI (**37%** would trust an organization less). That is a substantial gap relative to the partner users.

AI, when deployed correctly, can accelerate partner onboarding and reduce access delays (improving time-to-value), but consumer-facing AI without clear safeguards risks suppressing sign-up and increasing churn. ROI therefore depends on where and how AI is deployed.

Generational differences of trust in AI exist between consumers, with younger respondents slightly less likely to report reduced trust, and more likely to say their trust would increase. Trust in GenAI peaks, and distrust in GenAI dips, with those aged 29-44 years – those aged 18-28 years are therefore potentially slightly more cautious, potentially giving organizations a difficult balancing act as this younger cohort ages up.

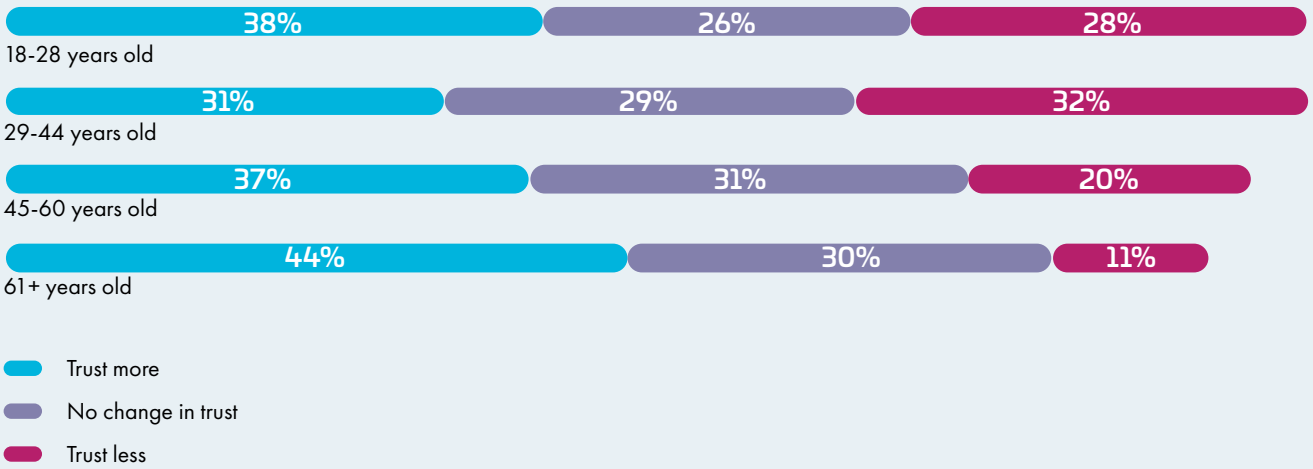
To what extent does your level of trust change in a company that handles your data, if they said that they are using GenAI? (Asked of consumers)



They put AI between me and what I wanted to do. The AI kept getting things wrong and I couldn't get past it to what I actually wanted to do."

Consumer, 45-60 years old, Canada

To what extent does your level of trust change in a company that handles your data, if they say that they are using GenAI?



For partner users however, there is strong belief that AI can improve trust, particularly when AI is positioned as an enabler of better security and access controls. **70%** of partner users say that they would trust an external partner more if it used generative AI to handle data and access management, and the same proportion (**70%**) say they would trust a partner more if it used agentic AI for the same purpose. This shows an appetite for solutions that can improve access processes, especially when current processes are often slow and inconsistent.

This is further demonstrated by the fact that **81%** of partner users say that they would trust an external partner more if it used AI to strengthen security. In other words, partner user trust increases when AI is applied to outcomes they prioritize.

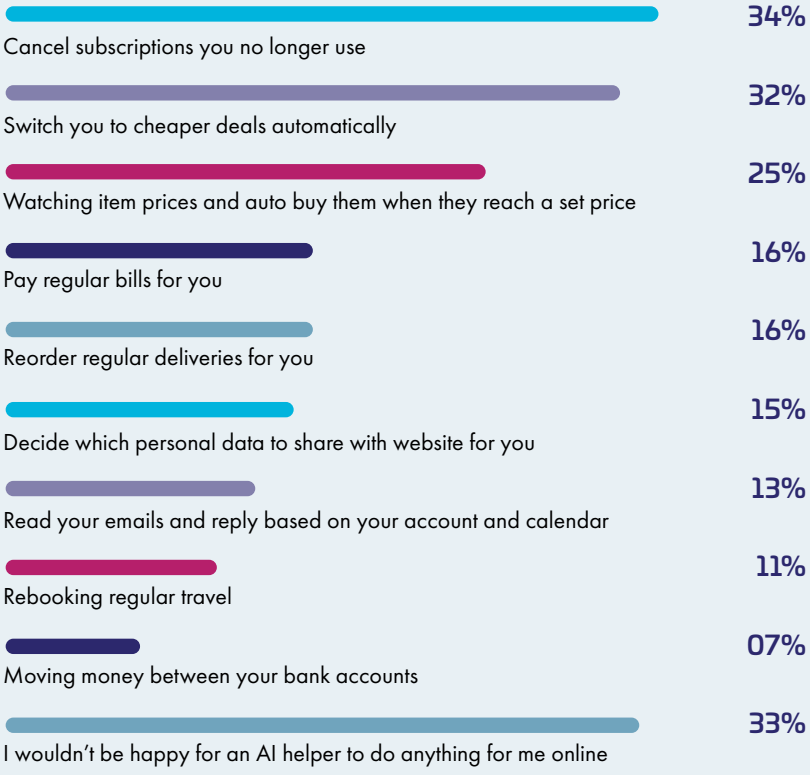
> **Making much greater use of AI would reassure me far more than current methods."**
>
> **Partner user, Hospitality, France**

Consumers will use AI, but only within clear boundaries

However, consumer openness is not uniformly negative; it is more conditional and task dependent. **63%** of consumers say they would be happy for an AI helper to do something online for them. However, there is a clear indication that less critical tasks (such as cancelling subscriptions no longer used) are far more likely to be preferred than significant financial management tasks (such as moving money between bank accounts).

This combination (low trust levels of trust increase, but moderate acceptance into some of the lower risk administrative tasks of day-to-day life) suggests that consumer acceptance may depend on how AI is used, what tasks it performs, and how visible the controls are. AI is not being rejected by consumers, but its use is conditional. Based on this, organizations could consider initially deploying AI in low-risk, high-volume tasks (support, status updates, form assistance) to reduce service costs and abandonment. Then, at a later point, expands to higher-risk steps only when consumer caution abates.

Which of the following tasks, if any, would you be happy for an "AI helper" to do for you online (through a website or app)?



> **They used artificial intelligence to give me the information I requested, and this contributed to increasing my trust in the company."**
>
> **Consumer, 18-28 years old, UAE**

Future trust outcomes are already being shaped as AI is introduced

This matters because organizations are moving quickly. Among IT and security leaders, adoption intent for AI is already high: **93%** say they are using, rolling out, or planning the use of generative AI, and **92%** say the same for agentic AI. The risk is that AI will arrive faster than user trust can adapt, if transparency and safeguards do not keep pace. When only **23%** of consumers say that they trust a company that uses AI to handle data, while deployment intent exists for nine in IT and security leaders, the trust outcome depends on governance and clear communications, not the technology alone. This can impact on service quality and margins, even where the technology is effective.

What this gap points to is a critical trust design challenge: the same AI deployment can be read as either 'protective' or 'intrusive', depending on how users understand what the AI is doing and why. At this point, AI runs the risk of being deployed faster than trust for it is forming. If AI is used to reduce fraud, tighten access control, and improve reliability (with clear explanation and visible user control) it can reinforce the top trust drivers (security and privacy). But if it is introduced without clarity, it risks compounding the transparency problems already evident in data collection and data rights experiences.

Organizations can address this by rolling out AI alongside clear explanations, visible user controls, and practical safeguards. They should make sure people understand what it does, why it is there, and how they can stay in control. Give users visible control and easy opt-outs, and prioritize AI use cases that measurably improve security, privacy and reliability rather than opaque automation.

> **I think we can make greater use of AI to make everything faster and a lot more efficient than what it is now."**
>
> **ITDM, Education, Singapore**

Conclusion

Trust today is no longer determined by reputation alone. It is tested at login, challenged during onboarding, and reinforced every time a user is asked to share their data. This research shows that while organizations are investing heavily in security and AI, users still experience friction, confusion, and limited visibility. The future of digital trust depends on aligning operational reality with user expectation.

Across both consumer and partner ecosystems, trust is fragile and commercially consequential. IT and security leaders often believe they are delivering balanced, secure, digitally enabled journeys, while consumers and partners report friction, confusion, and workaround behavior. This perception gap is itself a trust risk, and closing it requires better measurement, communication, and journey orchestration.

For consumers, sign-up, login and account settings are commercial conversion points. When onboarding is slow, data requests feel excessive, or security is opaque, abandonment rises and loyalty weakens. But the research also shows that consumers will accept friction when they feel protective. Organizations should design CIAM journeys to be fast, but with clear context or explanation when requesting data. Minimizing initial data capture, explaining purpose at key moments, applying risk-based verification, and making privacy controls visible and usable can turn identity into a lever for both trust and revenue protection.

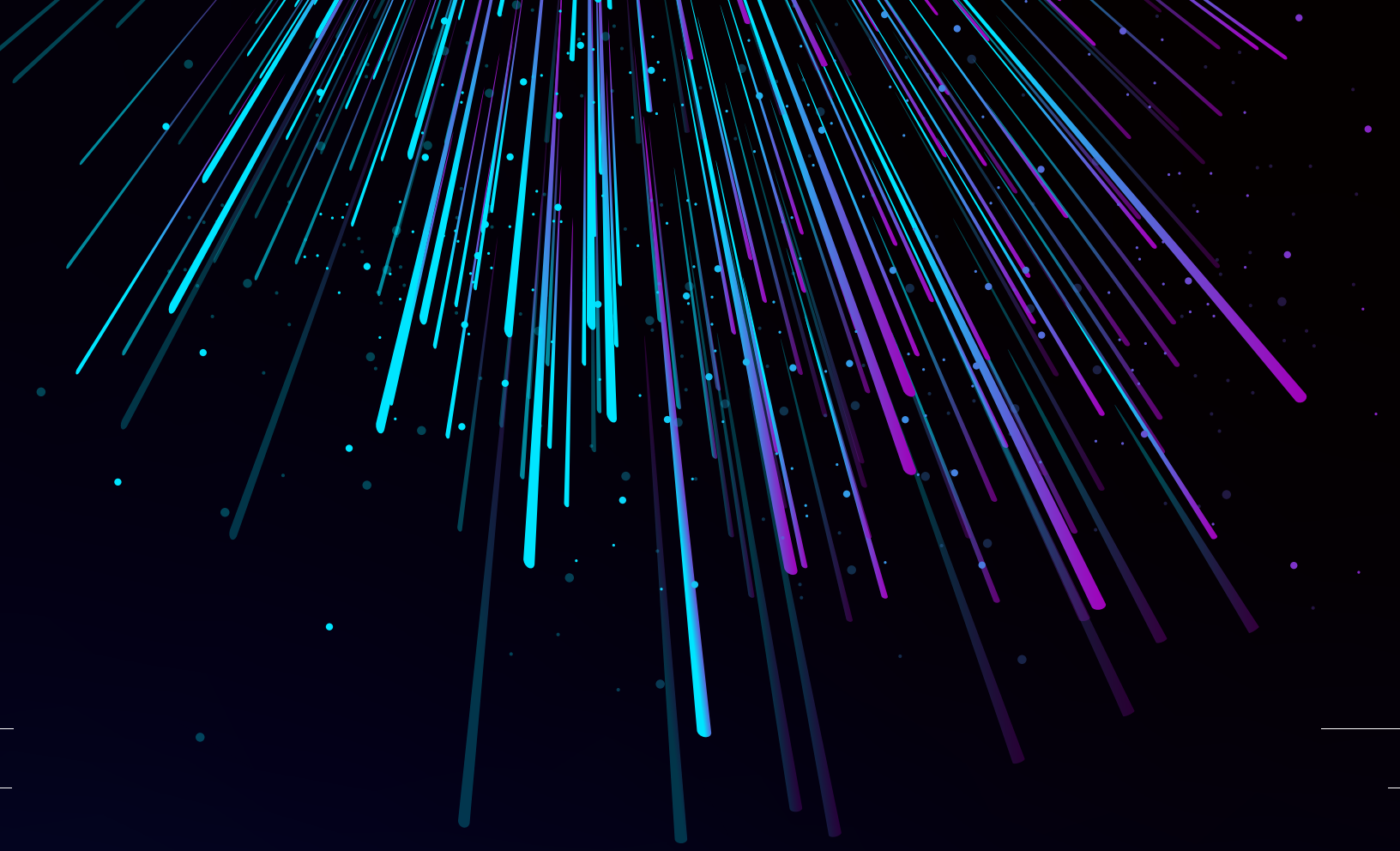
For partner users, the broad themes are similar but operationally diverse. IAM failures delay projects, disrupt billing, and create security debt through workarounds like credential sharing. Slow provisioning, poor entitlement visibility, and unclear ownership reduce confidence before value can be delivered. For the partner user experience, improvement lies in journey orchestration: aligning onboarding, authentication, authorization and offboarding into a coherent flow, supported by self-service and transparent governance.

Artificial intelligence adds both opportunity and risk. Used to accelerate low-risk tasks and strengthen security with clear explanation, it can enhance trust. But deployed without transparency, it can deepen skepticism, and organizations should factor this into their AI deployment strategy and plans.

Digital trust is shaped at specific operational touchpoints: onboarding, login, permission changes, and data transparency. When these moments work reliably and proportionately, trust compounds. When they fail, abandonment, workarounds, and revenue leakage follow. The organizations that design access as a trust-building mechanism will be best positioned to compete. This means improving reliability, balancing friction against risk, explaining data use clearly, modernizing authentication with user-friendly framing, and embedding meaningful control into the account experience. These measures can reduce abandonment and insecure workarounds, lower support and remediation costs, and strengthen trust at the moments that shape long-term value.

Methodology

Findings are based on a survey of 1,300 partner uses (with procurement or GTM remits), 200 IT and security leaders, and 14,300 consumers aged 18+ years, commissioned by Thales and conducted by Vanson Bourne in January-February 2026. Partner and IT and security leader respondents represent organizations across a range of sectors in the USA, Canada, Mexico, Brazil, UK, France, Germany, Netherlands, UAE, South Africa, Singapore, Japan and Australia, with consumer respondents also sourced from across all these countries.



THALES

CYBERSECURITY

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com/digital-trust-index