FRONTLINE FRICTION
The State of Authentication for Frontline Workers

A Research Report by Imprivata and the FIDO Alliance

imprivata®

fido™ ALLIANCE

Executive Summary

For organizations with frontline workers, authentication friction is leading to major real-world consequences, such as delaying vital patient care, work production and delivery of tasks. In a typical month, organizations estimate that **more than a third** of their frontline workers are hit by authentication issues when logging into their systems or applications. The impact of this is substantial, with each affected worker losing around **2.5 hours each month** to repeated interruptions, and the average organization surveyed losing **32,400 working hours a year**. This is on top of the time spent on routine sign-ins that succeed but may still slow the work down.

This friction can come from many different places such as account lockouts, password resets and repeated MFA prompts. Additionally, those surveyed expressed slow switching between users and devices, connectivity failures, and logging in while wearing protective equipment as common issues. Organizations cite each of these at similar rates, with **no single barrier, issue, or cause standing out**.

Nearly all organizations **(95%)** have observed frontline workers using workarounds like staying logged in, sharing credentials and bypassing controls. That adds risk to environments that are already complex by design, in fact **six in ten decision-makers** cite confirmed or suspected attempts to misuse account resets and social-engineer service desks.

Executive Summary

Encouragingly, organizations already using passwordless methods of authentication report gains in speed, user switching and productivity. For organizations using passkeys without a password, the most-reported gains are faster access **(38%)**, improved productivity **(36%)**, and better visibility into who is accessing systems **(33%)**, with phishing resistance built in. Many other passwordless methods – such as SMS one-time codes, authenticator app codes and push approvals – are used but **remain phishable**, and organizations that rely on them report more authentication friction and more reported attacks than average.

Most organizations are still early in the transition away from passwords. This is evident as nearly half of those **(45%)** organizations that have modernized with passkeys are still using them alongside a weaker and friction-causing password. With concern about AI-enabled impersonation already matching concern about conventional social engineering, **phishing resistance should be as much of a priority as minimizing friction itself**.

There is no silver bullet. But by addressing authentication holistically, across every device, handover, application, and recovery process, and by adopting phishing-resistant authentication that brings the speed their workforce needs, frontline organizations can reduce friction and security risk together.

Research Methodology

The survey was conducted by Sapio Research in August 2026 among 700 IT and security decision-makers (manager level and above) responsible for authentication, identity security or access-management decisions for frontline workers.

Respondents worked at organizations with 500+ employees and at least one frontline worker, across the US, UK, France and Germany, in healthcare, manufacturing and other frontline-intensive industries. 58% of respondents are final or primary decision-makers, and 76% of their organizations employ 500 or more frontline workers.

Findings reflect decision-makers' perceptions and organizational estimates, rather than direct reporting from frontline workers. Interruption and time-lost figures are estimates derived from the midpoints of banded responses; the organization-level figure applies the per-affected-worker estimate to the 37% of frontline workers affected in a typical month, across an average frontline workforce of around 2,800.

Market	
United States	250
United Kingdom	150
France	150
Germany	150

Industry	
Healthcare	325
Manufacturing	184
Other Industries	191

Organization Size	
500–999 employees	208
1,000–4,999 employees	270
5,000–9,999 employees	108
10,000+ employees	114

Key Findings

01 Authentication Friction Is Delaying Frontline Work

02 The Delays Are Significant, Widespread and Recurring

03 Friction Is Coming From Many Directions at Once

04 Frontline Environments Carry Inherent Complexity

05 Workarounds Turn That Complexity Into Risk

06 High Levels of Identity-Based Attacks Are Being Reported, and Concern Over AI Has Caught Up

07 Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition

Key finding | 01

Authentication Friction Is Delaying Frontline Work

Key finding

01

Authentication Friction Is Delaying Frontline Work

34% of organizations say authentication difficulties delay frontline work.

The impact reaches:

- PATIENT CARE
- PRODUCTION
- DELIVERY

authentication friction

noun

1. Anything that slows or blocks a frontline worker's access—from outright failures such as lockouts, forgotten credentials, and resets to the everyday drag of repeated logins, re-authentication, and MFA prompts.

Key finding

01

Authentication Friction Is Delaying Frontline Work

On the frontline, that is not just an IT ticket. It is a delayed medication round, a stalled production line, a damaged customer experience, or a late delivery. The consequences reach every part of the operation, and **only 5% of organizations report no significant impact.**

37% **of organizations report increased IT and service desk workload,** 30% lost frontline productivity, and 26% increased downtime

29% **report increased security workarounds,** 27% increased exposure to security incidents, and 27% a reduced ability to track user activity

27% **cite difficulty authenticating while wearing gloves or protective equipment as a top challenge.** This is one of three joint most-cited challenges, alongside delays switching between devices and between users on shared devices (27% each)

27% **have observed workers avoiding or delaying system use because of authentication difficulties**

Frontline authentication must fit the realities of the job: gloved hands, masks and constant movement between tasks, devices and workers.

Key finding

01

Authentication Friction Is Delaying Frontline Work

Regional breakdown

	Delays to frontline work	Increased IT/service desk workload	Lost frontline productivity
US	37%	42%	29%
UK	38%	41%	31%
France	31%	31%	35%
Germany	30%	32%	28%

The US and UK report the highest rates of delay to frontline work. In France, lost productivity is the most-cited effect (35%), while in the UK, increased security workarounds make the top three (37%). Security exposure is more prominent in the US (33%).

Industry breakdown

	Delays to frontline work
Healthcare	40%
Manufacturing	34%
Other industries	26%

Healthcare feels the impact most directly: four in ten healthcare organizations say authentication difficulties have delayed patient care or other frontline work.

Key finding | 02

The Delays Are Significant, Widespread and Recurring

Key finding

02

The Delays Are Significant, Widespread and Recurring

32,400 working hours a year lost to authentication interruptions

by the average organization surveyed

2.5 hours a month

lost to authentication interruptions for every affected frontline worker

37%

nearly 2 in 5

of frontline workers experience an authentication issue in a typical month, organizations estimate on average

Key finding

02

The Delays Are Significant, Widespread and Recurring

M T W T F

~20 **interruptions a month for affected workers where issues affect half or more of the frontline workforce,** or roughly once every working day

30 hours/year

Those affected are interrupted 11 times a month on average, losing around 2.5 hours a month in total, or 30 hours a year

56% **of organizations estimate at least a quarter of their frontline workers are affected monthly;** 31% say at least half

74% **say an incident costs six minutes or more;** an estimated 14 minutes on average

55% **say the typical affected worker is interrupted at least weekly;** nearly one in five (18%) say at least once per shift

This counts only disruptive incidents, not the time spent on routine sign-ins that succeed but still slow the work down, **so the true cost is likely higher.**

Key finding

02

The Delays Are Significant, Widespread and Recurring

Regional breakdown

	Average share of frontline workers affected monthly	Organizations estimating 25%+ affected
US	40%	62%
UK	34%	55%
France	32%	48%
Germany	38%	55%

The US sees the widest impact, with organizations estimating 40% of frontline workers affected each month on average, and 62% saying at least a quarter are affected, compared with 48% in France.

Industry breakdown

	Average share of frontline workers affected monthly	Estimated interruptions per affected worker, per month
Healthcare	37%	10
Manufacturing	37%	12
Other industries	36%	11

The problem is strikingly consistent across sectors: healthcare, manufacturing and other industries all estimate that more than a third of their frontline workers are affected each month.

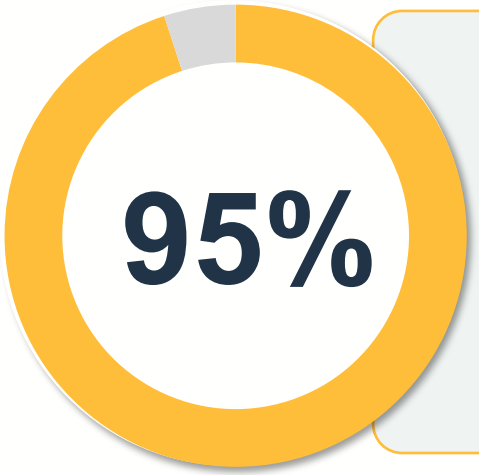
Key finding | 03

Friction Is Coming From Many Directions at Once

Key finding

03

Friction Is Coming From Many Directions at Once



of organizations report their frontline workers face at least one authentication challenge, with the top nine challenges all within six percentage points of each other.

Frontline authentication friction is not driven by any single challenge, so addressing one issue alone will not solve the broader problem.

Instead, an approach is required that can:

- Ensure access is fast and consistent on every device and application
- Work at every handover
- Tie each action to an individual
- Hold up during recovery
- Resist phishing

Key finding

03

Friction Is Coming From Many Directions at Once

27% **The most-cited challenges are delays switching between devices or workstations, delays switching between users on shared devices and difficulty authenticating with gloves or PPE**

They are closely followed by:

- **26%** Password resets or lockouts
- **25%** Connectivity failures
- **23%** Frequent re-authentication
- **23%** Repeated MFA prompts
- **22%** Forgotten credentials
- **21%** And slow logins

Asked for the single improvement with the greatest impact, organizations split almost evenly across five options:

- **15%** Consistency across devices and applications
- **15%** Secure shared-device access
- **15%** Phishing protection
- **14%** Visibility into who accessed what
- **14%** Stronger recovery verification

The same spread appears in:

Reasons unique credentials aren't used
top four within four points

Shared-device challenges
top three within four points

Barriers to passwordless
top eight within five points

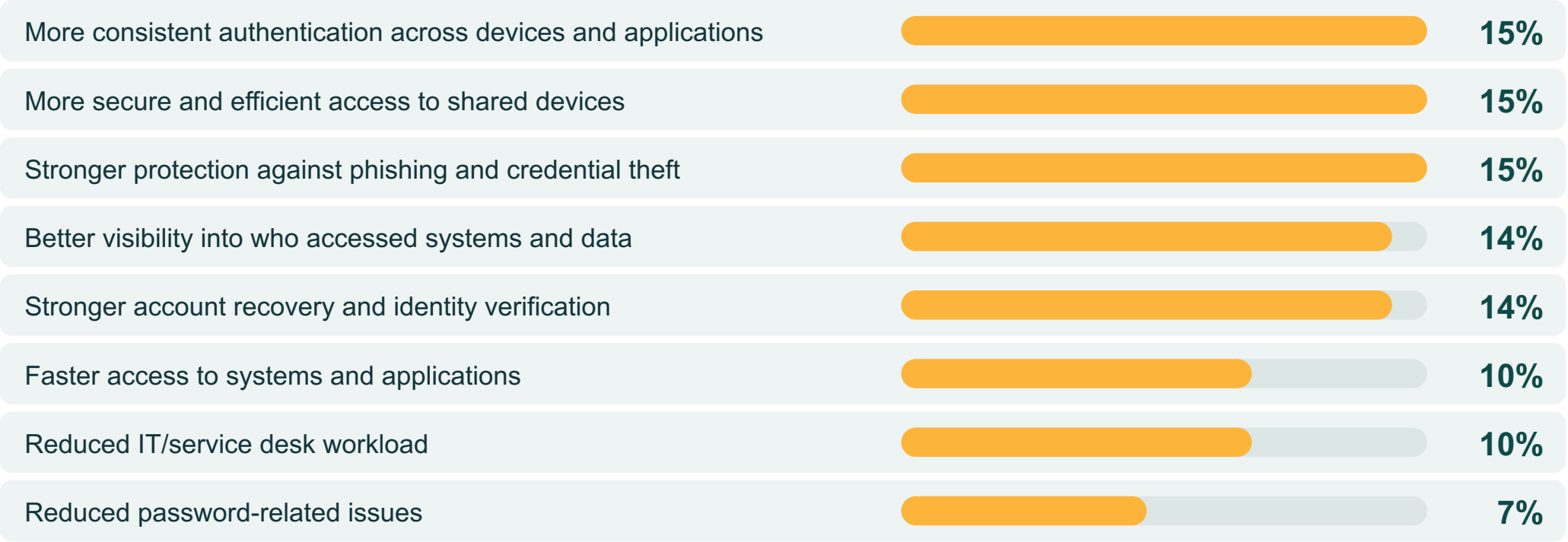
Planned investments
top seven within six points

Key finding

03

Friction Is Coming From Many Directions at Once

Single improvement with the greatest positive impact



Regional and industry notes

Password resets and account lockouts are the single most-cited challenge in France (27%) and in manufacturing (28%). Organizations with a mix of password-based and passwordless methods are the most likely to choose secure shared-device access as their top improvement (23% vs 13% of password-based or inconsistent and 9% of passwordless-led organizations).

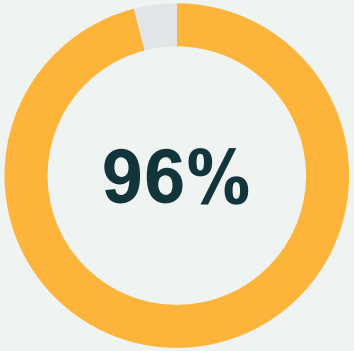
Key finding | 04

Frontline Environments Carry Inherent Complexity

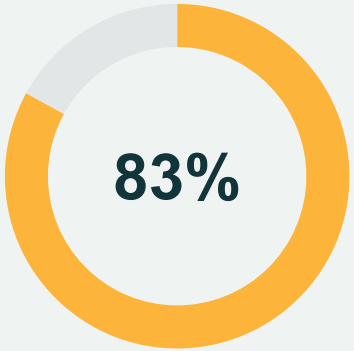
Key finding

04

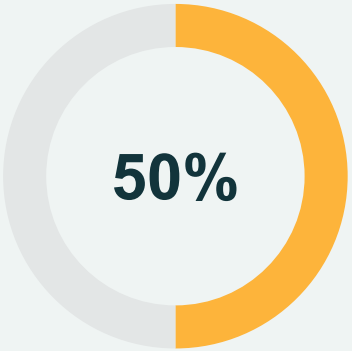
Frontline Environments Carry Inherent Complexity



of shared-device organizations report authentication challenges



of organizations use shared workstations or devices for frontline work



Among organizations using shared devices, 50% say most or nearly all frontline workers use them

Key finding

04

Frontline Environments Carry Inherent Complexity

Frontline workers regularly access (% of organizations):

60%	safety and compliance systems
52%	communication tools
51%	timekeeping
49%	inventory or supply-chain systems

38% **say all or nearly all frontline workers use their own unique credentials**

Where unique credentials aren't used consistently, the reasons are practical:

39%	frequent user switching
38%	wider workflow barriers
38%	devices shared by many users
35%	endpoints or applications that don't support suitable methods

The biggest challenges:

47%	maintaining accurate records of who accessed what
45%	consistent authentication across device and system types
43%	fast, secure switching between users

61% **still use shared or generic accounts to some extent**

35% vs 51%

Organizations using shared devices are less likely to achieve near-universal unique credentials

Given that shared devices are required in many frontline environments, authentication must be designed for the way shared devices are actually used by supporting fast, secure, individual handovers.

Key finding

04

Frontline Environments Carry Inherent Complexity

Regional breakdown

	Use shared devices	Most or nearly all frontline workers use shared devices
US	81%	47%
UK	85%	61%
France	75%	44%
Germany	91%	48%

Shared devices are most widespread in Germany (91%), while reach is deepest in the UK, where 61% of shared-device organizations say most or nearly all frontline workers use them, compared with 50% overall.

Industry breakdown

	Most or nearly all frontline workers use shared devices	Endpoints or apps don't support suitable methods*
Healthcare	54%	31%
Manufacturing	42%	41%

*Among organizations where unique credentials are not used consistently.

Shared-device use runs deepest in healthcare, while manufacturing faces greater technical constraints from legacy endpoints and applications, making modernization part of the frontline access challenge.

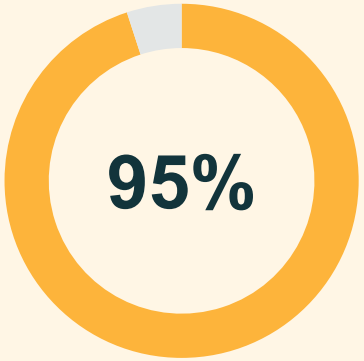
Key finding | 05

Workarounds Turn That Complexity Into Risk

Key finding

05

Workarounds Turn That Complexity Into Risk



of organizations have observed frontline workers using workarounds because of authentication difficulties in the past 12 months

Organizations most often report workers:

40%	staying logged in to avoid re-authentication
36%	attempting to bypass MFA or other controls
33%	sharing credentials

Organizations also widely reported:

32%	password reuse
32%	sharing badges or tokens
29%	using another employee's session
26%	written or posted passwords

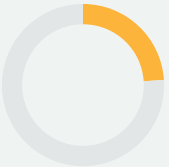
Key finding

05

Workarounds Turn That Complexity Into Risk

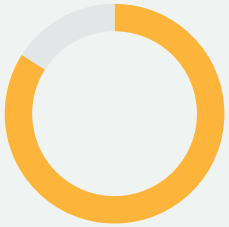
The same behaviors top organizations' identity security concerns:

34% shared credentials or accounts



24% and session hijacking or unattended active sessions

Organizations' confidence level:



84% of organizations are confident frontline access can be attributed to the correct, individually verified employee

40% are very confident

Among those not very confident, the leading reasons are shared devices or incomplete sign-out between users (43%), workers sharing credentials (37%) and shared or generic accounts (31%)

Key finding

05

Workarounds Turn That Complexity Into Risk

Regional breakdown:

	Very confident access can be attributed to the correct individual
US	54%
UK	38%
France	27%
Germany	34%

US organizations are twice as likely as French organizations to be very confident in attribution, yet the US also reports the highest share of frontline workers affected by authentication issues (40%). In the UK, increased security workarounds are among the top three effects of authentication difficulties (37%).

Industry breakdown:

	Very confident in attribution	Credential sharing observed
Healthcare	36%	32%
Manufacturing	39%	38%
Other industries	50%	30%

Healthcare and manufacturing organizations are notably less likely than other industries to be very confident in attribution, and manufacturing reports the highest rate of credential sharing.

Breakdown by authentication maturity:

	Mixed password and passwordless	Passwordless-led
Credential sharing observed	44%	22%
Using another employee's session observed	36%	15%

Organizations part-way through the move to passwordless report twice the rate of credential sharing, and more than twice the rate of session borrowing, seen in passwordless-led organizations. Running two approaches side by side can leave workers juggling both at every handover.

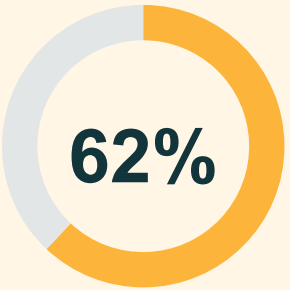
Key finding | 06

High Levels of Identity-Based Attacks Are Being Reported, and Concern Over AI Has Caught Up

Key finding

06

High Levels of Identity-Based Attacks Are Being Reported, and Concern Over AI Has Caught Up



of organizations report a confirmed or suspected unauthorized account-recovery, password-reset or unlock attempt in the past 12 months

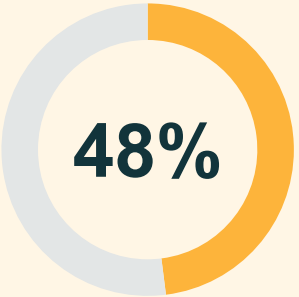
Organizations report:

28%	have confirmed an unauthorized account-recovery, reset or unlock attempt
60%	report a confirmed or suspected social-engineering attempt targeting the service desk (26% confirmed)
57%	report confirmed or suspected AI-assisted or deepfake employee impersonation (23% confirmed)
56%	report confirmed or suspected abuse of MFA-reset or new-device enrollment (21% confirmed)

Key finding

06

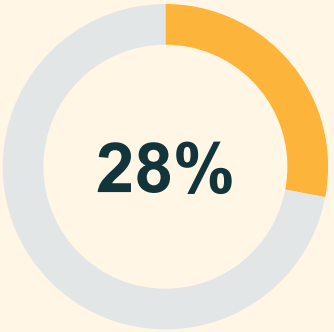
High Levels of Identity-Based Attacks Are Being Reported, and Concern Over AI Has Caught Up



are very or extremely concerned about AI-enabled impersonation, level with conventional social engineering (48%)

Recovery verification is fragmented, with no method used by a majority:

41%	Employee ID or badge
40%	Email
34%	SMS
33%	Biometrics
32%	Manager approval



are prioritizing stronger service desk identity verification in the next 24 months

Key finding

06

High Levels of Identity-Based Attacks Are Being Reported, and Concern Over AI Has Caught Up

Regional breakdown

	Very/extremely concerned: conventional social engineering	Very/extremely concerned: AI-enabled impersonation	Badge verification used in recovery
US	53%	57%	46%
UK	56%	49%	53%
France	46%	43%	33%
Germany	32%	38%	29%

Concern about AI-enabled impersonation is highest in the US (57%), where it now exceeds concern about conventional social engineering. Germany reports the lowest concern on both measures. Badge-based recovery verification is most common in the UK (53%) and least common in Germany (29%).

Industry breakdown

	Very/extremely concerned: conventional social engineering	Very/extremely concerned: AI-enabled impersonation
Healthcare	43%	41%
Manufacturing	48%	51%
Other industries	55%	57%

Healthcare reports the lowest concern about both threats, despite being the sector where authentication failures most directly affect patient care.

Key finding | 07

Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition

Key finding

07

Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition

of organizations using passwordless methods for frontline workers report a benefit

Organizations using passwordless methods report:

35%	Faster access
30%	Fewer resets and recovery requests
31%	Faster switching between users or devices
26%	Better worker experience
30%	Improved productivity
26%	And reduced service desk workload

Faster access is a top-three benefit in every market.

Key finding

07

Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition

Organizations using passkeys without a password

report productivity gains alongside phishing resistance

38%	Faster access
36%	Improved productivity
33%	Improved visibility into individual user access
33%	Fewer resets and recovery requests

Organizations using phishable methods

passwordless methods such as one-time codes, authenticator app codes and push approvals (n=261)

44% **of frontline workers affected by authentication issues each month**

Phishable methods	**44%**
All organizations	**37%**

37% **report confirmed unauthorized account-recovery, reset or unlock attempts**

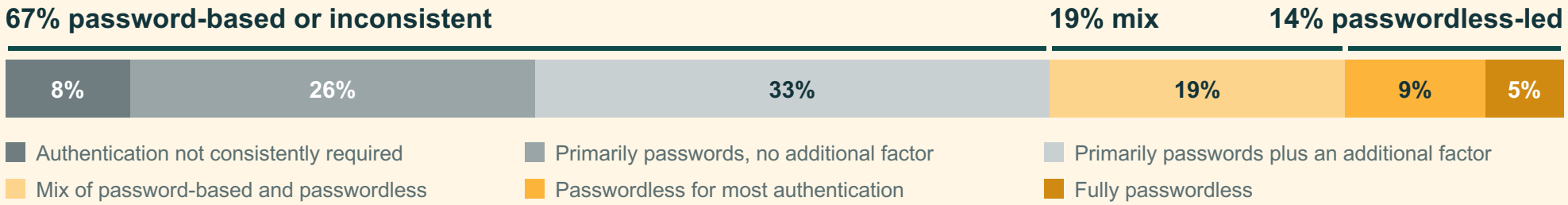
Phishable methods	**37%**
All organizations	**28%**

Not all passwordless is equal: phishing resistance should be as much of a priority as minimizing friction itself.

Key finding

07

Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition



28% **use passkeys or FIDO credentials;** nearly half of them (45%) still keep a password alongside

15% **use them without a traditional password;** the same gap appears for every non-password method

Barriers are spread:

26%	competing priorities
25%	shared-device environments
23%	cost
22%	legacy systems

Investment priorities for frontline workers over the next 24 months include:

32%	biometrics	**30%**	legacy modernization
28%	passkeys/FIDO	**28%**	smart badges
28%	stronger helpdesk verification		

Only 1% have no identity security investment planned

Key finding

07

Passwordless Authentication Is Delivering Benefits, but Most Organizations Are Still in Transition

Regional breakdown

	Use passkeys today	Prioritizing passkeys in next 24 months	Top passwordless benefit
US	32%	33%	Faster access (34%)
UK	31%	33%	Faster access (41%)
France	19%	24%	Faster access (32%)
Germany	27%	19%	Improved productivity (39%)

The US and UK lead on both current passkey use and planned investment, and faster access is the top reported passwordless benefit in every market except Germany, where productivity leads. Germany is the least likely to be prioritizing passkeys over the next 24 months (19%), and France has the lowest passkey use today (19%) despite naming reduced phishing risk as a top-two benefit (29%)

Industry breakdown

	Use passkeys today	Prioritizing passkeys in next 24 months	Top passwordless benefit
Healthcare	27%	26%	Faster access (39%)
Manufacturing	29%	28%	Faster switching (34%)
Other industries	28%	32%	Faster access (32%)

Passkey use is consistent across sectors. Healthcare sees the strongest speed gains from passwordless methods, while manufacturing values faster switching between users and devices most.

Breakdown by authentication maturity

	Mixed password and passwordless	Comparison group
Fast, secure user switching is a challenge*	57%	39% (password-based or inconsistent)
Shared devices a barrier to passwordless	37%	22% (password-based or inconsistent)
Legacy systems a barrier to passwordless	32%	15% (passwordless-led)

*Among organizations using shared devices.

Conclusion

The findings in this report describe a problem that is significant, recurring, and consistent across markets and sectors. Authentication friction delays frontline work, costing affected workers an estimated 2.5 hours a month, and pushes people toward workarounds that weaken both security and accountability. At the same time, attackers are targeting the recovery and service desk processes behind the login, and AI-enabled impersonation is already as concerning as conventional social engineering.

There is no quick fix to the frontline friction problem, and the data shows why. Challenges, barriers and priorities are spread almost evenly across many options, so solving one symptom at a time will not work. To solve frontline friction, authentication must be addressed holistically across the whole environment: every device, every handover between users, every application, and the account-recovery and service-desk processes that attackers are already targeting. It must also take frontline workers' unique environments and workflows into consideration, particularly where equipment like gloves and face masks is required.

The path forward is already visible. Organizations using passwordless methods report faster access, faster switching, and higher productivity; almost all plan to invest in frontline identity security over the next two years. What remains is to complete the transition: moving from methods layered on top of passwords to phishing-resistant authentication such as passkeys, deployed everywhere frontline work happens.

Every frontline organization can start with a careful, holistic assessment of its unique authentication workflows, and by adopting phishing-resistant authentication that brings the speed and usability its workforce needs.

About Imprivata

Imprivata delivers Zero-Friction Security for high-stakes organizations where every second matters and work never stops. Its interoperable identity, access, and privileged access security platform secures every identity from human to AI, and across shared and dedicated devices, complex workflows, and modern and legacy environments. Serving healthcare, manufacturing, public safety, and other regulated industries, Imprivata helps organizations embed intelligent, context-aware access into the flow of work, protecting against threats, reducing operational complexity, and improving productivity and cost efficiency.

www.imprivata.com

About the FIDO Alliance

The FIDO Alliance (www.fidoalliance.org) enables identity technologies that put trust and simplicity at the center of interactions among people, services, and devices. The Alliance publishes open technical specifications, certifies secure and interoperable products, and operates global market enablement programs.

www.fidoalliance.org