Our Passwordless Future: a New Era of Security

JUNE 2022

PingIdentity®

yubico

Introduction

Passwords have become increasingly cumbersome for users, and the burden is adding up to more than an inconvenience: passwords also create serious security concerns. As a result, IT leaders are sounding the alarm and advocating for a passwordless future to become a reality.

To better understand the drawbacks of passwords and how to move beyond them, Wakefield Research conducted a survey of 600 IT leaders across five markets on behalf of Ping Identity and Yubico, garnering results that show how reliance on this outmoded tech can't sustain in the current business environment. IT leaders estimate employees enter a password an average of 12 times a day. In fact, 25% estimate they input a password 20 times or more. **Most troublingly, an overwhelming 94% of IT leaders are concerned about passwords, including 50% who worry they are too weak for security purposes.**

In addition, IT departments are experiencing a 30% rise in password-related incidents. And their employees are also suffering from lost productivity, wasting minutes or even hours a week entering and re-entering passwords. With new and advanced security options available, IT leaders recognize the best password security might be one with no password at all.

Key Global Findings

91% are very or somewhat worried about passwords being stolen at their organization.

33% of IT leaders say employees at their organization make minimal changes to passwords or—worse—reuse an old one; this might be why 50% rank passwords' lack of security strength as a primary concern.

33% of IT department's tickets are related to passwords, on average. For over a fifth (21%), half or more of their tickets are password related.

99% have not yet adopted passwordless authentication, but all (100%) IT leaders see the benefits of it. Over half see opportunities such as reduced security costs (52%) and enhanced security (52%), and nearly as many say it'll lead to a reduced need for support (48%).

28 minutes a day: that's the average amount of time employees could save if they switched to passwordless authentication—that's over 2 hours each week, or nearly 120 hours per year! Nearly a third of IT leaders (32%) estimate employees would save more than 30 minutes a day.

65% say their organization is completely or very likely to adopt passwordless authentication in the near future, 19% who have plans to do so.

91% agree that password security is a cultural issue that business leaders, not users, need to take responsibility for.

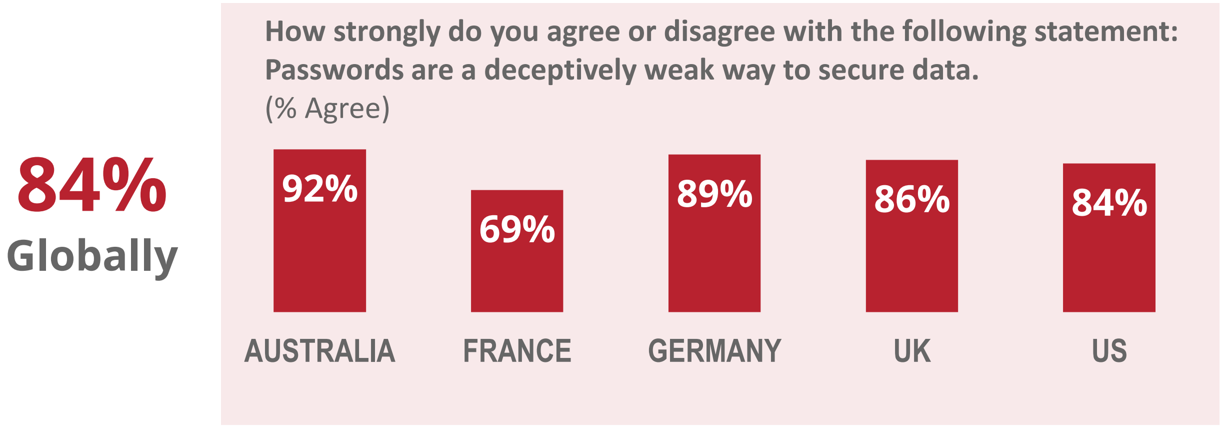
83% of those with no plans for passwordless authentication admit their organization is unsure how to implement this.

96% recognize that passwordless authentication would create an easier user experience for employees, and nearly as many at organizations with customer logins (95%) say it would create an easier user experience for their clients.

Finding #1: IT Leaders Say Passwords Are Deceptively Weak

With 94% of IT leaders expressing concerns about passwords, nearly universal recognition of passwords' dire limitations and risks include 50% admitting they are too weak for security purposes. **In fact, 84% say passwords are deceptively weak, made even more clear by the 91% who are very or somewhat worried about passwords at their organization being stolen**. The thought that passwords are deceptively weak is highest among Australian IT leaders (92%), compared to a still sizable 69% of French IT leaders. This widespread realization that passwords are not the vanguard they once were points to a need for a new cybersecurity stance.

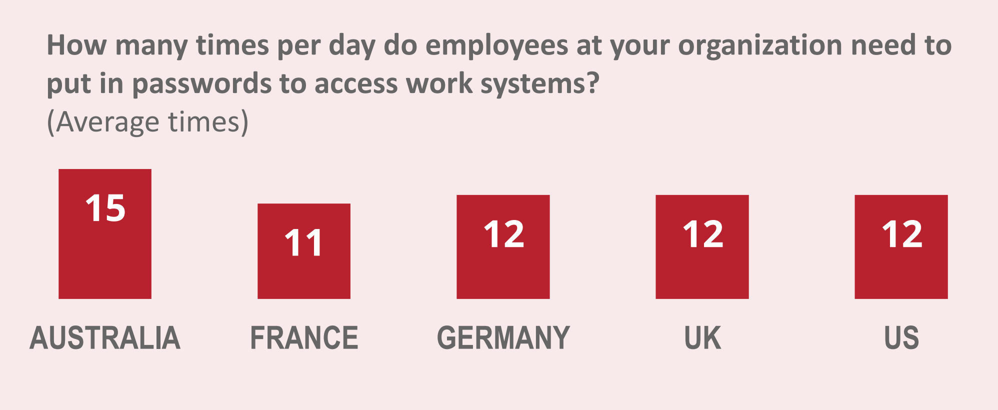
An overwhelming majority of IT leaders (84%) say passwords are a deceptively weak way to secure data.



It's not just cybersecurity: 40% of IT leaders cite concerns over passwords being simply inconvenient for users and employees alike. On average, IT leaders estimate their employees are stuck entering passwords 12 times a day, including 25% who estimate they need to do so 20+ times a day—and the passwords don't always work. **In the past month, employees have been locked out of accounts or devices due to forgotten passwords 78 times on average; this jumps to 92 times among organizations with customer logins.** The time and energy wasted on passwords, multiplied across the millions of workers and customers trying to log in every day, makes the sheer scope of this problem shockingly clear.

Across all markets, employees input passwords 12 times a day on average.

12 times Globally

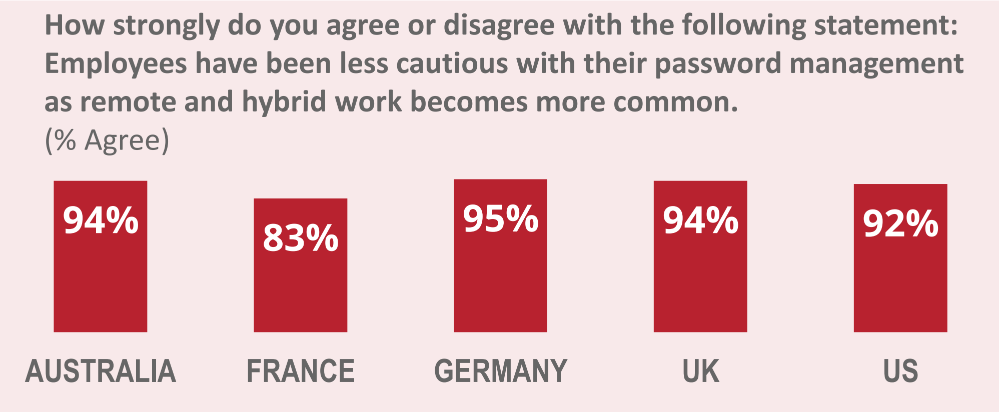


How many times per day do employees at your organization need to put in passwords to access work systems?
(Average times)

Irritation with passwords add up not only to time and money wasted, but the depreciation of passwords' altogether: 33% of IT leaders admit employees at their organization make minimal changes or—worse—reuse an old one when changing their passwords. While 56% say employees use password management software, they also acknowledge riskier methods, including phones or mobile devices (45%) and even notepads on their desk (41%). This is a problem getting worse in our work-from-anywhere world: **92% of IT leaders believe employees have been less cautious with password management as remote and hybrid work become more common.** The problem persists among employees and customers alike, as 71% of IT leaders are less than completely confident that their customers are maintaining proper password security.

Hybrid work has caused employees in all markets to be less cautious with their password management.

92% Globally

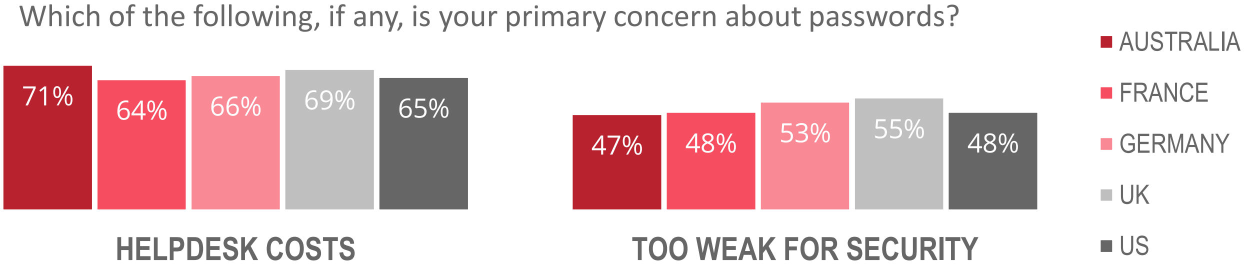


How strongly do you agree or disagree with the following statement: Employees have been less cautious with their password management as remote and hybrid work becomes more common.
(% Agree)

Time wasted on passwords also means money wasted organizationally, which is why IT leaders' top concern for passwords is the helpdesk costs associated with them (67%), made clear by the estimated 33% of department's tickets which are related to passwords, including 21% who estimate half or more. **This is a crisis on the rise, with leaders citing an average increase of 30% in password related-incidents.** These tickets take up time better spent elsewhere—especially given that these costly passwords still remain vulnerable.

Globally, helpdesk costs are the top concern for passwords, followed by security concerns.

Which of the following, if any, is your primary concern about passwords?



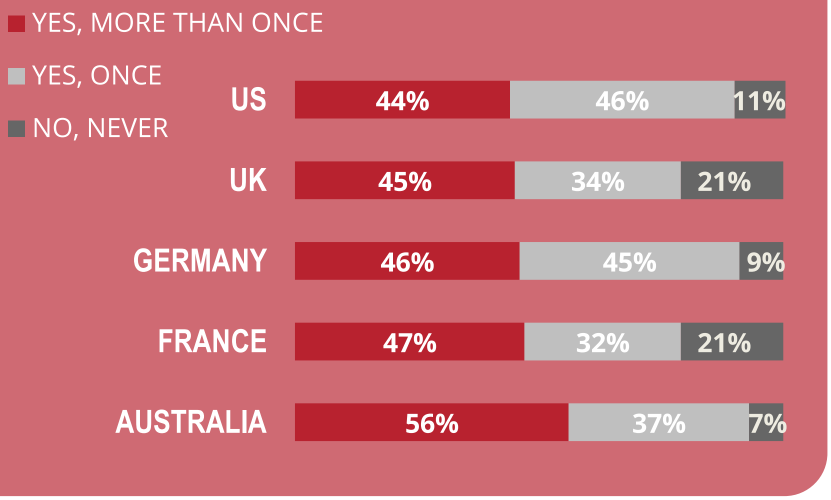
67%
Globally

50%
Globally

Spotlight: Follow the Leader
Customers and employees might be annoyed by insecure passwords, but a solution needs to come from the top: **91% of IT leaders say password security is a cultural issue that business leaders, not users, need to take responsibility for.** But too many IT leaders see business leaders' unwillingness to do so. **A shocking 87% of IT leaders have felt unfair pressure to relax password rules for executives or organization leaders, including 47% who say this has happened more than once.**

IT leaders in Australia, Germany and the US have felt more pressure to relax password rules for leadership.

Have you ever, even once, felt unfair pressure to relax password rules for executives or organization leaders?



Finding #2: Many Look to Passwordless Authentication as the Solution

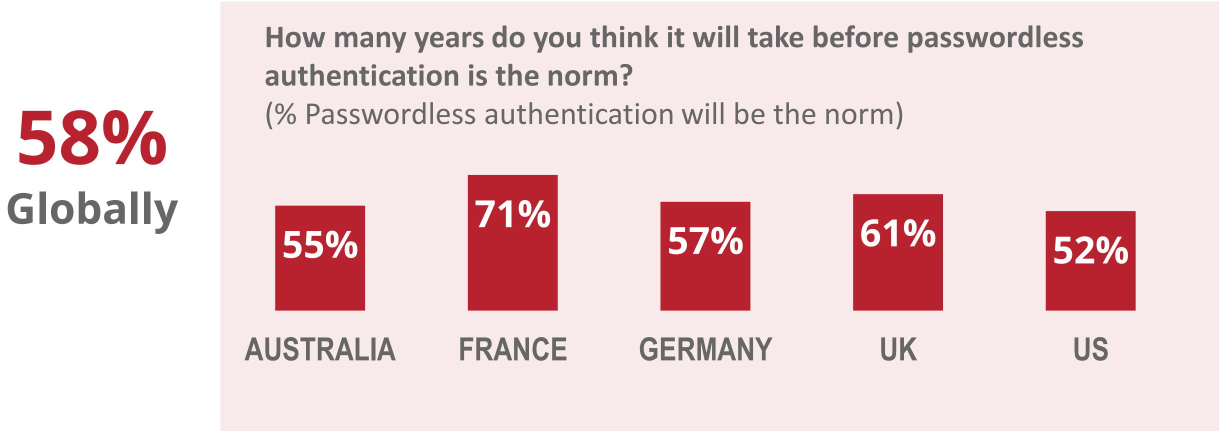
Securing passwords and mitigating their risks is quickly becoming the security solution of the past: IT leaders instead predict that passwordless verification is the reality of their industry—one with immediate solutions and long-term benefits. The fix is the adoption of passwordless authentication, verifying users with methods that do not require a password, such as PINs, hardware security keys or biometric factors. This solution offers benefits for security, productivity, and beyond.

With 91% of IT leaders very or somewhat concerned about passwords being stolen, 65% say their company is completely or very likely to implement passwordless authentication, pointing to a strong willingness to make this change. While passwordless authentication is not yet common, as 99% have not adopted it, IT leaders' plans reflect the future of their industry.

This change would have an immediate and massive effect. **IT leaders estimate employees at their organization would save 28 minutes a day with passwordless authentication.** That's over 2 hours each week, or nearly 120 hours a year! In other words, companies implementing passwordless security would give each employee back three weeks of productivity per year.

As a result of benefits like these, nearly 3 in 5 (58%) say passwordless authentication will eventually be the model. French IT leaders (71%) are the most likely to say passwordless authentication will be the norm, part of a global cohort who estimates it will take just 7 years on average. Even German IT leaders believe this will take 9 years on average, the highest among all markets surveyed—but a change within a decade, nevertheless.

French IT leaders are the most likely to say passwordless authentication will become the norm



Fully 100% of IT leaders recognize the advantages of passwordless authentication. **A majority cite reduced security costs (52%) and enhanced security (52%), and 48% cite a reduced need for support.** Considering how much of IT's time is taken up by password-related incidents, the impact of passwordless authentication on IT costs—and organizations' bottom lines—could be truly staggering.

Spotlight: The State of Passwordless Protection

Progress has been made among organizations that have adopted or plan to use passwordless authentication, with the most common methods being biometrics (67%), PIN (48%) and hardware security keys (38%). **These popular approaches align with what all IT leaders see as the best forms of passwordless authentication: biometrics (58%), PIN (51%) and hardware security keys (40%) top their list.**

IT leaders' preferred passwordless authentication methods

Which of the following forms of passwordless authentication has your organization adopted or plans to adopt? (Top 3 responses)

	Global	Australia	France	Germany	UK	US
Biometrics	67%	61%	47%	67%	64%	80%
PIN	48%	39%	47%	33%	50%	56%
Hardware security keys	38%	29%	40%	42%	45%	38%

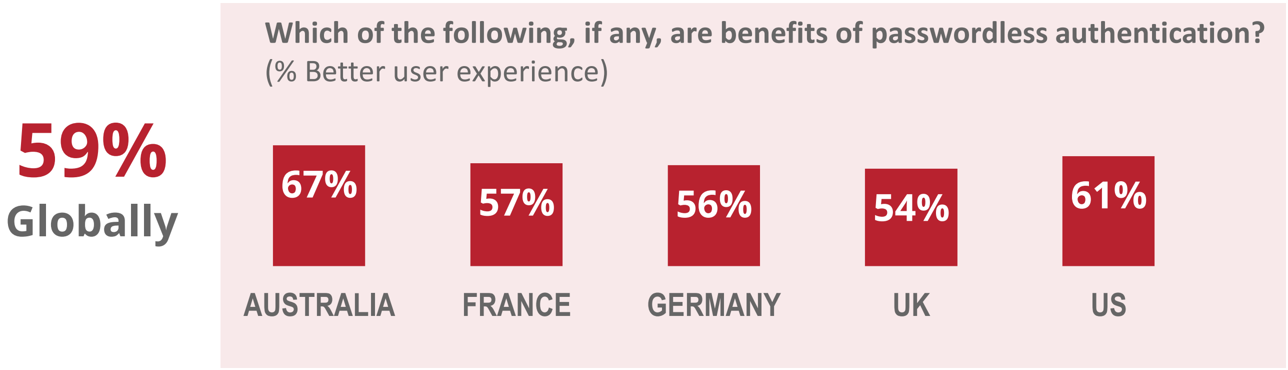
Finding #3: The Benefits of Passwordless Outweigh the Barriers

Passwordless authentication may be the future, but implementation means inevitable roadblocks: 97% of those without passwordless authentication predict barriers. But with the right partners, IT leaders can build a better, more secure future.

Many of these roadblocks are not technological, but cultural. **The top barrier for implementing passwordless authentication is a lack of urgency from IT or business leaders (46%), even more than the 45% of IT leaders who cite the technological limitations of the applications.** Another third (33%) say lack of expertise is a barrier, highlighting the need for intelligent help to navigate pushback. **An overwhelming 88% of those without passwordless authentication believe their organization would be somewhat or very resistant to adopting it; 35% say this is a key barrier.**

Another huge barrier could be a lack of knowhow: 83% of those with no plans to execute passwordless authentication admit they are unsure how to implement it—signaling the need for outside expertise. This partnership is especially important for the 59% of IT leaders who say a better user experience is a benefit of passwordless authentication.

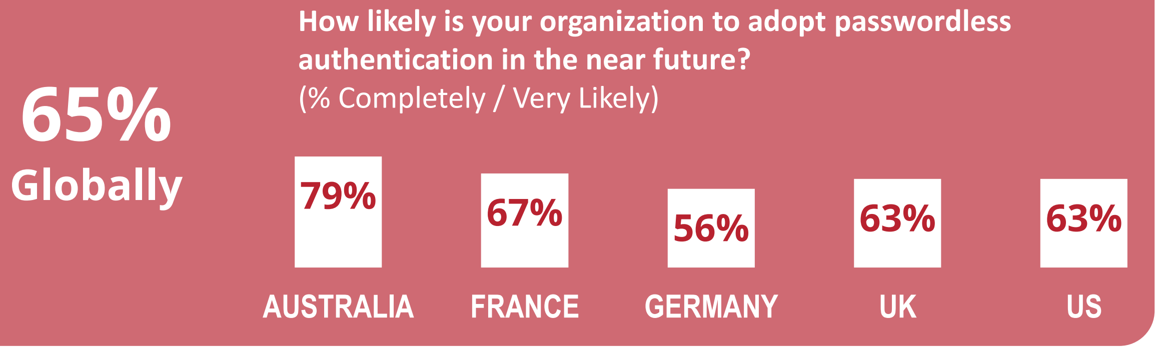
Improving the user experience is a key benefit of passwordless authentication across all markets


Which of the following, if any, are benefits of passwordless authentication?
(% Better user experience)

Indeed, nearly all (96%) say passwordless authentication would create an easier user experience for employees at their organization, and nearly as many with customer logins (95%) say it would create an easier user experience for their clients.

Spotlight: A World Without Passwords
A vast majority of IT leaders across all markets (93%) say their organization is at least somewhat likely to adopt passwordless authentication, including 65% who are very or completely likely. Most enthusiastic are Australian IT pros, 79% of whom say they're very or completely likely to institute it.

Australian IT leaders lead the way in likelihood to adopt passwordless authentication.


How likely is your organization to adopt passwordless authentication in the near future?
(% Completely / Very Likely)

Conclusion

IT pros have made it clear that the future of their industry is one in which passwords are phased out in favor of passwordless authentication that provides a more secure, frictionless user experience. While this transition will require skill and insight to manage correctly, with the right partners, the future of cybersecurity can unlock certainty and convenience for everyone involved. To thrive in a passwordless future, companies must:

- Take stock of the cost of passwords, including users' and customers' time, as well as helpdesk resources—and evaluate how those stack up against passwords' lack of security.
- Consider the many passwordless options available: biometrics, PINs, hardware security keys, and more.
- Move to passwordless authentication, not only to secure their data, but to provide their users, employees and customers alike, with access to the benefits of this improved experience.
- Partner with experts on passwordless authentication to make the most of their passwordless future.

ABOUT WAKEFIELD RESEARCH

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world's most prominent brands and agencies, including 50 of the Fortune 100, in 90 countries. Our work is regularly featured in media.

To learn more, visit: https://www.wakefieldresearch.com/

STUDY METHODOLOGY

The Ping Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 600 IT leaders / Decision-makers, defined as senior IT staff with a director-level position or higher from large organizations, defined as companies with 10,000+ employees in the following markets: 200 US respondents, 100 per market for: UK, Australia, France, Germany, between April 6th and April 19th, 2022, using an email invitation and an online survey.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.0 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

WAKEFIELDRESEARCH.COM