LastPass

From Passwords to Passwordless

Addressing the password problem as employees work from anywhere.

WHAT'S INSIDE

INTRODUCTION

The problems with passwords are still an ongoing struggle. Undoubtedly, managing passwords is still taking up time that could be spent elsewhere by you and others in your organization. They're causing a lot of headaches and frustrations for your IT department and organization's employees alike. Security issues might be the core of that headache for you and your IT team, but it's the lack of convenience and ease of use that employees care about.

It's clear that change is long overdue.

In a world where work from anywhere is the norm, this change is even more crucial. Speaking with IT and security professionals during a time of radical change for all, one thing is clear: secure identity is important, no matter where you're working.

You need a solution that is twofold, which maintains absolute security and eliminates those irritations for employees all in one.

So, is passwordless authentication a realistic solution that your business can use to address the password problem once and for all?

RESEARCH SCOPE

LastPass by LogMeIn commissioned independent technology market research specialist Vanson Bourne in order to understand the current state of passwords in organizations today, and how these trends are driving passwordless authentication models moving forward.

750 IT and security professionals were interviewed in April and May 2020, ranging from CIOs and CISOs, through to IT managers and analysts. The respondents were from a variety of private and public sectors, across the US, UK, France, Germany, Australia and Singapore, and were from organizations with between 250 and 3,000 employees.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

Where applicable, historical comparisons have been made to data from the "The SMBs Guide to Modern Identity" research report from 2019, for which the research scope was similar. For last year's survey, 700 IT and security professionals were interviewed in April and May 2019. They were based across the US, UK, France, Germany and Australia, and were from organizations with between 250 and 2,999 employees operating across a range of private and public sectors.

Diagnosing the Password Problem

The password headache.

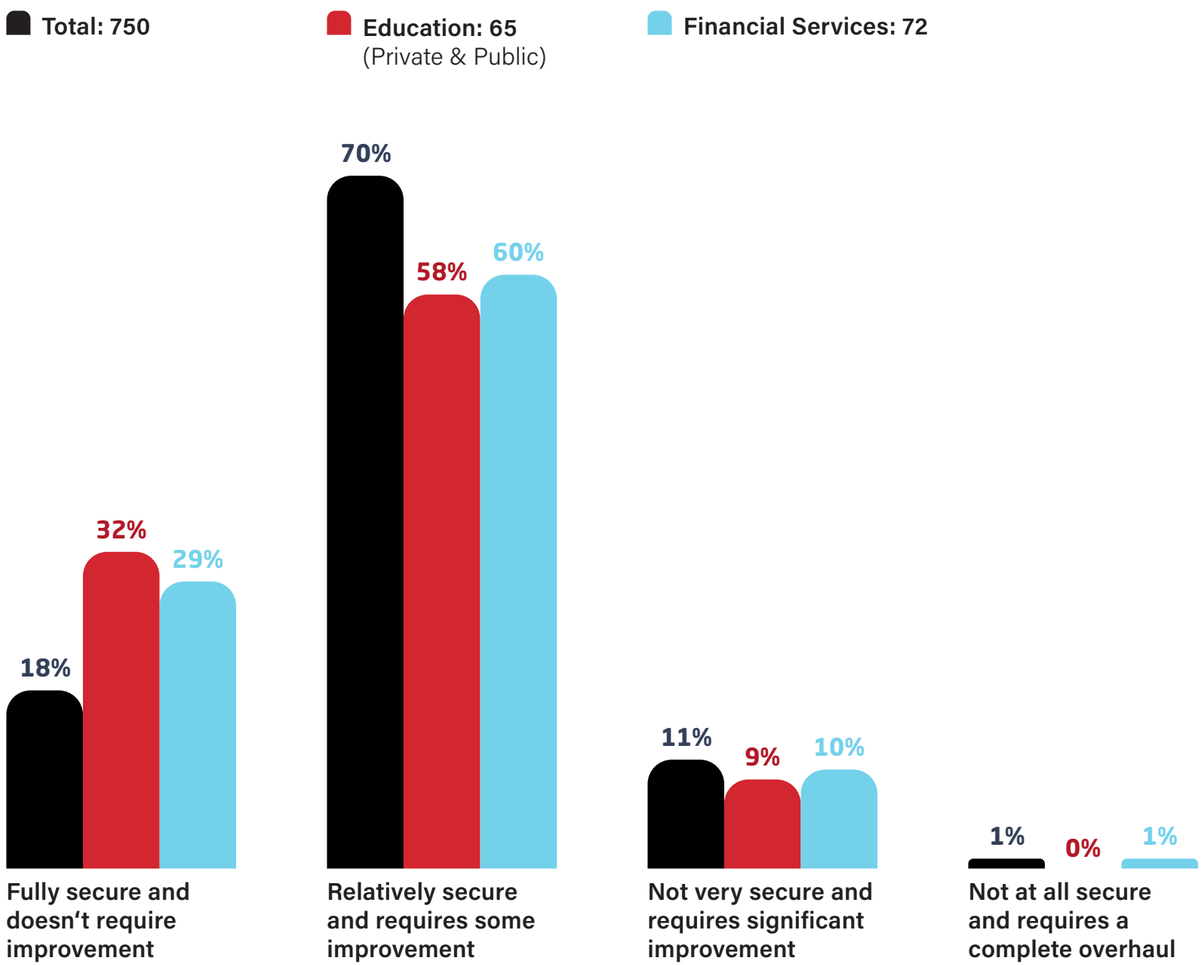
Current identity and access management landscape.

Within the current identity and access management landscape, there's clear room for improvement when it comes to security. Just under a fifth (18%) of IT and security professionals report that their organization's current solution(s) is fully secure and doesn't require improvement, leaving a lot to be desired for the remaining four fifths.

It comes as no surprise, given the highly confidential types of data they deal with, that those in the education (32%) and financial services and insurance (29%) sectors are more likely than most to report that their solutions don't require improvement.

However, even in these sectors, the majority cite the need for improvements. When looking at current identity and access management landscape by region, the UK (25%) and France (25%) rank the highest in noting no improvements needed, whereas Singapore (86%) are most likely to acknowledge security improvements are needed.

Perceived Security of Current Identity and Access Management Solution(s)



Time spent managing passwords each week:

3 HOURS

Singapore

4 HOURS

United Kingdom
France
Australia

5 HOURS

Germany

6 HOURS

United States

Weekly time spent managing users' password and log in information has increased 25% since 2019.

Security isn't the only issue currently being faced. The amount of time that IT and IT security teams spend managing users' password and log in information has increased year on year.

Respondents in the US report the highest average time of 6 hours. That's the majority of a working day. If a solution existed to rid your IT teams of this burden, imagine how that time could be better spent elsewhere.

Using passwords.

There are a lot of concerns around the security of using passwords and the number that are being used. The vast majority (85%) of IT and security professionals agree that their organization should look to reduce the number of passwords that individuals use on a daily basis.

Additionally, nearly half (48%) of all respondents don't believe that passwords are always secure. With this in mind, why are they still used extensively across the business, and why hasn't more been done to implement more secure authentication methods?

Almost all (95%) respondents surveyed say there are risks to using passwords which could contribute to threats in their organization, making the lack of confidence reported in the security of passwords even more alarming.

The most likely causes of potential threats are human behaviors, which is what makes them so dangerous. Passwordless authentication largely eliminates the concerns and risks associated with human behavior, providing a peace of mind that will never be possible when using password-based methods.

Given the aforementioned risks associated with passwords and current global working situation, the need for secure authentication and identity is the greatest it's ever been. The transition to remote working has potentially highlighted new security risks that wouldn't have existed in the traditional office setting. Employees are using less secure home internet connections, or even using their own devices for work purposes, opening them up to the possibility of new risks threatening to harm the business.

Biggest causes of potential threats:

67% Password reuse/using the same password for multiple accounts

65% Password weakness (i.e. not using strong passwords)

51% Leaking company data

43% Social media hacking

36% Not changing default passwords

5% No risks

Frustrations:

Not only does the research uncover fundamental issues for organizations with the use of passwords, it puts a spotlight on the frustrations that are experienced across the business, for both the IT department and employees alike.

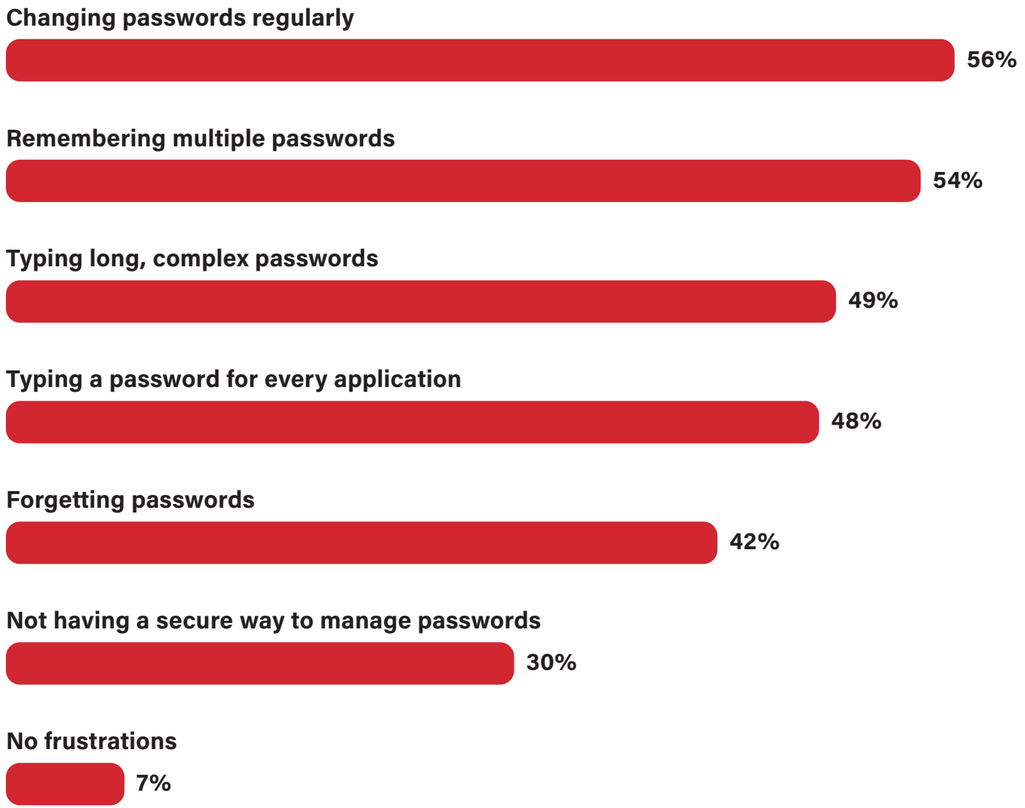
Security is the main source of frustration for the IT department, particularly when security issues are often derived from user behavior.

Top 3 Frustrations:

1. Users using the same passwords across applications
2. Users just forgetting their passwords
3. Time spent on password management

IT Department Password Challenges

Employee Password Challenges



For employees on the other hand, the issues lie with convenience.

Top 3 Frustrations:

1. Changing passwords regularly
2. Remembering multiple passwords
3. Typing long, complex passwords

Identifying a solution

Passwordless authentication.

What is Passwordless?

Passwordless authentication does what it says but, what is it really and is it a realistic possibility for your business or simply a buzz word? Well, passwordless authentication enables users to login to devices and applications without the need to type in a password.

It streamlines the user experience for employees within an organization, while still maintaining a high level of security and complete control for IT and security teams.

As such, it's no surprise that the frustrations and security concerns arising from using passwords are driving organizations to turn to passwordless methods.

To understand more about how passwordless authentication is already being used, and the benefits it provides in being more secure and easier to use, our research focused on three technologies:

Biometric authentication enables employees to securely authenticate and bypass typing in a password by using their face or fingerprint.

Single sign-on (SSO) requires only one set of credentials to access everything, eliminating the need for employees to use multiple passwords.

Federated identity integrates with an existing IT ecosystem and user directory login details, requiring users to only use one password to unlock their work.

The Benefits of Passwordless.

The benefits of deploying a passwordless authentication model are twofold – for the user it largely eradicates the frustrations of using passwords and for the business it increases security. Introducing a model such as this allows IT to overcome the security hurdles that passwords create.

Better security (69%) and eliminating password related risk (58%) are most likely to be believed by respondents to be benefits of deploying a passwordless authentication model for their organization's IT infrastructure. With time (54%) and cost (48%) savings also commonly cited as benefits of passwordless authentication, the case for deployment builds.

Benefits of passwordless authentication for IT infrastructure:

69%
Increasing security

58%
Eliminating risk

54%
Saving time

53%
Gaining more control and visibility

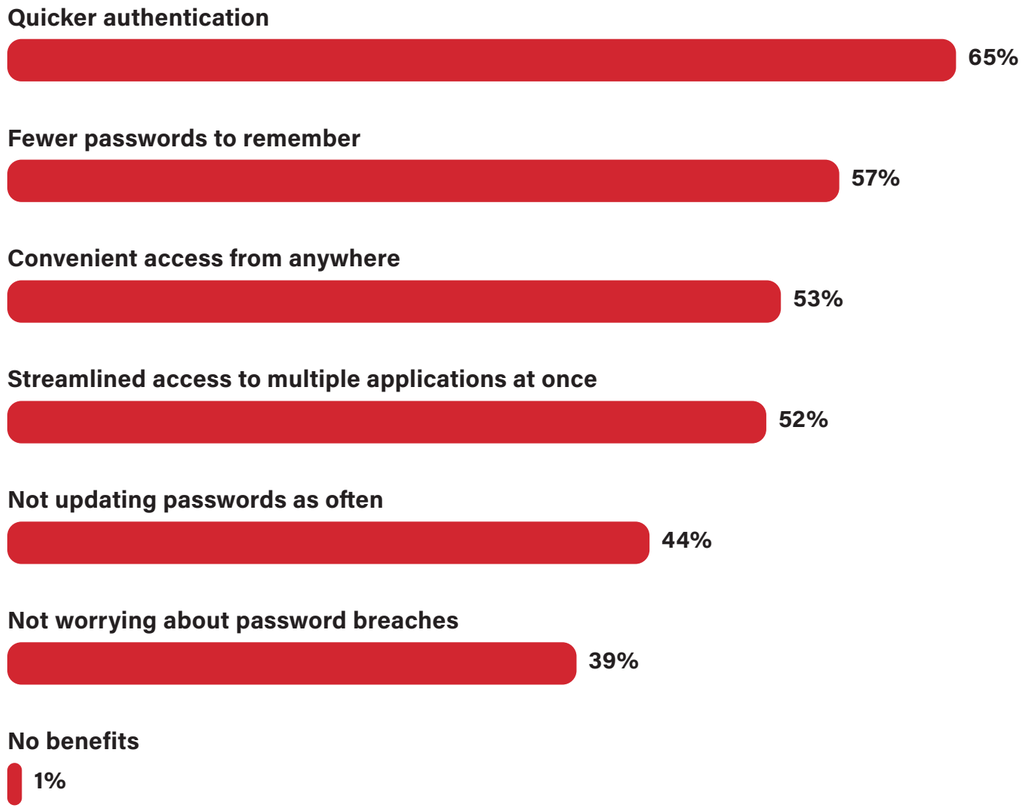
48%
Saving costs

3%
No benefit

Meanwhile, for employees a passwordless authentication model would help to address efficiency concerns.

Out of all regions, the ability to authenticate more quickly is ranked the highest by Singapore (78%) where Australia are most likely to note the benefit of fewer passwords to remember most frequently (67%). Further to this, over half (53%) report that passwordless authentication offers potential to provide convenient access from anywhere; all the more so important now given the shift towards remote working that is likely here to stay.

Benefits of Passwordless Authentication for Employees



The Challenges of Passwordless.

Surveyed IT and security professionals claim to have a relatively good understanding of passwordless authentication, with 49% saying they have a complete understanding, and a further 47% saying they have a good understanding. That level of complete understanding is highest amongst those in the US (60%) and lowest in the UK (39%).

Perhaps this understanding is misinformed though, as not all methods of passwordless are recognized as being so. 71% of respondents identify biometric authentication as a passwordless authentication method, however only 49% identify single sign-on and only 39% identify federated identity as the same.

Secondly, there are challenges in the deployment of a passwordless authentication model. Respondents report the initial financial investment required to migrate to such solutions (43%), the regulations around the storage of the data required (41%) or the initial time required to migrate to new types of methods (40%) as the biggest challenges for their organization to overcome.

France identifies their biggest challenge in adopting a passwordless authentication model to be the initial financial investment (44%), and Germany finds the regulations around the storage of data most challenging for them (49%) – likely due to compliance regulations such as the General Data Protection Regulation.

There are also some concerns around resistance to change too, both from employees (38%) and from the IT department (33%). Indeed, there may be more of an uphill battle when it comes to employees.

74% **Three quarters of IT and security professionals think that end-users in their organization would prefer to continue using passwords, as it's what they're used to.**

It's therefore vital that when implementing and considering passwordless options, IT teams demonstrate the widespread benefits for both the organization and employees to ensure they're on board.

Challenges of Deploying a Passwordless Authentication Model

The Verdict

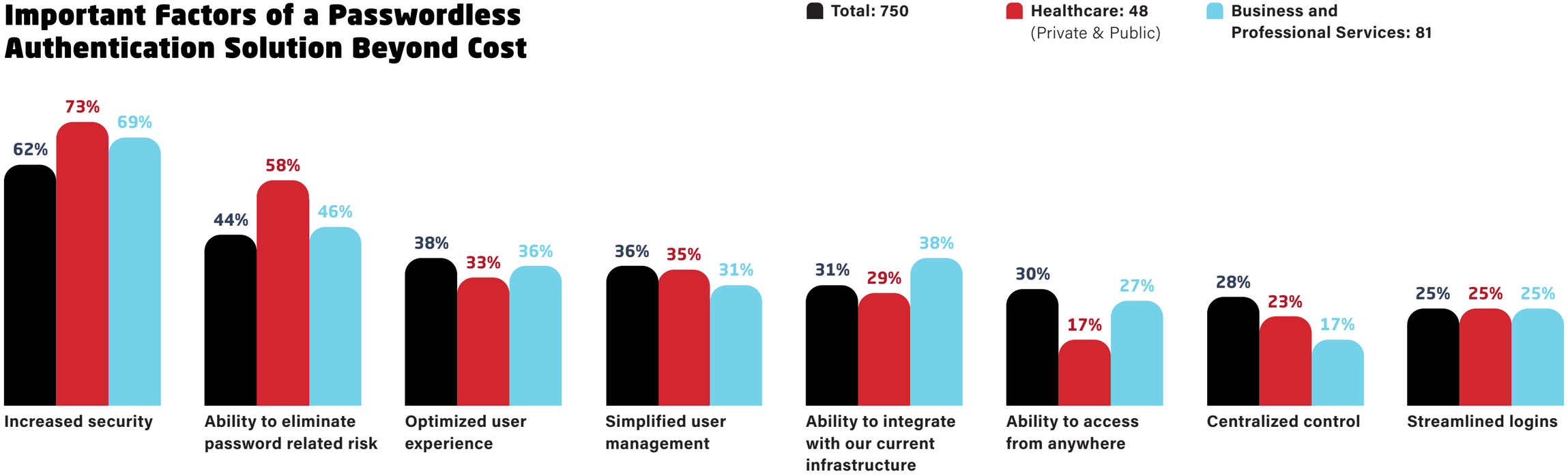
Passwords or passwordless?

Security, Security, Security.

Security trumps any other factor when it comes to choosing a passwordless authentication solution. Beyond cost, when asked what they believe to be the most important factor of a passwordless authentication solution for their organization, respondents are most likely to report increased security (62%) or the ability to eliminate password related risk (44%). Increased security was deemed to be even more important for those within the healthcare (73%) and business and professional services (69%) sectors, likely stemming from the confidential data these types of organizations hold.

It's clear that going passwordless is the ultimate solution when it comes to a stronger, more secure authentication method, and it can also offer a greater level of ease for end-users. As we already know the move to remote work has uncovered an array of new security risks, so the need for introducing this stronger method is even more important now. And similarly, during these difficult times, anything that organizations can do to simplify the lives of their end-users will ultimately bring about wider benefits.

Important Factors of a Passwordless Authentication Solution Beyond Cost



What Does This Mean for the Humble Password?

Given they've always been the foundation of authentication it's not as simple as getting rid of the password forever; our surveyed respondents don't believe this is the end for them either. When it comes to identity and access management, 85% don't think passwords are going away completely. The same proportion (85%) believe there is a need for a combination of passwordless authentication and password management.

This matches up with the reality of what a passwordless authentication model involves. Passwordless reduces the need for employees to type a password upon login, making their experience much more streamlined and allowing them to focus on their work. However, passwords will still be used in some way throughout the business, and these will still need to be managed securely and efficiently. It's therefore critical that, alongside the implementation of a passwordless authentication model, a simple and efficient password management solution is also put in place. This is the only way to truly eradicate those frustrations and problems that passwords bring to you and your IT teams.

The Importance of Combining Passwordless Authentication and Password Management:

1% Don't understand enough about the link between passwordless authentication and password management

13% Don't believe there is a need for a combination of passwordless authentication and password management

85% Believe there is a need for a combination of passwordless authentication and password management

Looking to the Future.

Just as work from anywhere has become the new normal, a passwordless future is inevitable. The days of remembering and typing long-winded passwords may soon be behind us.

The ability it has to maintain absolute security and allow for complete visibility is reason enough to migrate your organization's authentication mechanism to this type of model.

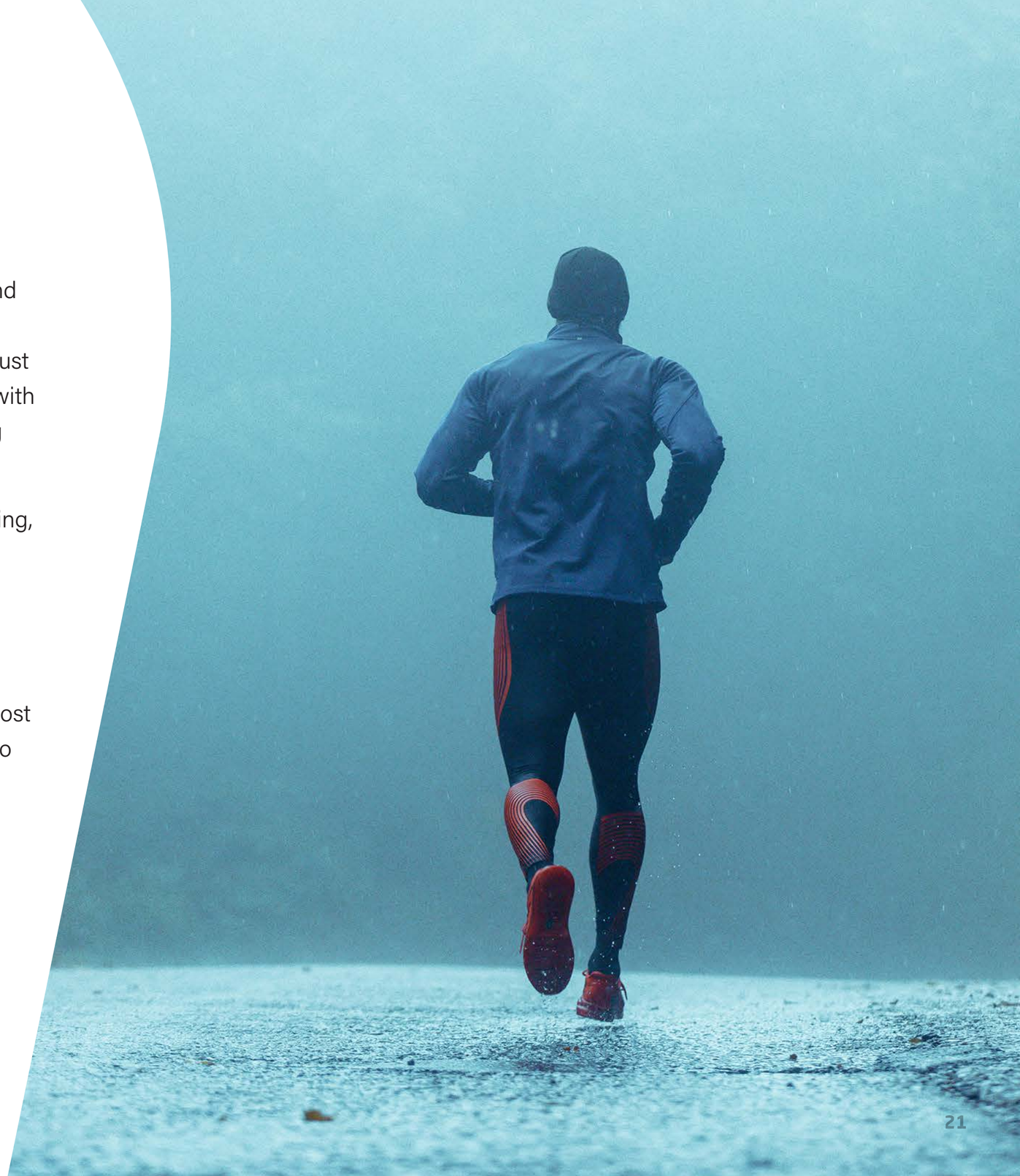
92% **Over nine in 10 respondents believe that delivering a passwordless experience for end-users is the future for their organization.**

Passwordless in the Future.

The need for migration away from traditional passwords is ever-growing, and as we've seen from our surveyed IT and security professionals, that need is still, if not even more, apparent in a remote working world. Organizations must look to eliminate the frustrations had by stakeholders across the business, with passwordless authentication a clear "win win" when it comes to addressing these problems for all.

It solves the frustrations that you and the rest of your IT department are facing, and it also takes into account the convenience and ease that employees desire when it comes to identity and access management. Not only that, but passwordless technologies are deemed to be both more secure than passwords, and as, if not easier, to use.

Passwords may not be going away completely though, a view echoed by most of those surveyed. But, given that passwordless authentication is believed to be the future of their organization for most, the need to find a solution that combines password management and passwordless authentication is vital.



Security, simplified for your business.

Learn More

LastPass

For more than 70,000 businesses of all sizes, LastPass reduces friction for employees while increasing control and visibility for IT with an identity and access management solution that's easy to manage and effortless to use. From single sign-on and enterprise password management to adaptive authentication, LastPass gives superior control to IT and frictionless access to users to help support the transition to going passwordless. For more information, visit **LastPass.com**.

VansonBourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **vansonbourne.com**.