Say Goodbye to Passwords

New IDG Research Finds That IT Leaders View Mobile Devices as the Future of Secure Authentication

An April 2019 survey conducted by IDG and sponsored by MobileIron shows that enterprise users and security professionals alike are frustrated by the inefficiency and lax security of passwords for user authentication. But it also pointed the way toward solutions and the next generation of authentication that's more user-friendly and secure.

The survey polled 200 IT security leaders in the US, UK, Australia, and New Zealand working in a range of industries at companies with at least 500 employees. The aim was to discover the major authentication pain points facing enterprises.

The survey found that nearly half of all enterprise help desk tickets request password resets or result from users getting locked out of their accounts by multifactor authentication (MFA) processes. Passwords and MFA clearly represent major frustrations for users as well as the IT professionals who support them.

Along with the user experience challenges presented by passwords, they also pose a security risk, according to those surveyed. Although a majority (64%) of the respondents feel that passwords provide sufficient means for authenticating users, that leaves 34% who disagree, with the rest undecided.

It's no wonder: Almost half of enterprise users recycle passwords for multiple logins, in a clear case of compromised security, according to respondents. And nearly all of the respondents (90%) have witnessed security incidents stemming from theft of credentials.

As the survey results demonstrate, it's time for a new approach to security. The findings indicate that leveraging mobile devices for user authentication rather than relying on passwords and MFA is a more robust and easier alternative. This approach is more effective than using conventional passwords and MFA, in part because of the changing relationship between users and enterprise data.

"In the enterprise, more and more users are not getting on the enterprise network to go to their applications and get to their data," explains Brian Foster, SVP of product management at MobileIron. "Instead, they're accessing apps and company data via their own mobile devices."

Although that's a concern for IT departments used to managing network access from endpoints they control and have visibility into, it also represents an opportunity to do identity and access management (IAM) better—using the devices themselves for authentication.

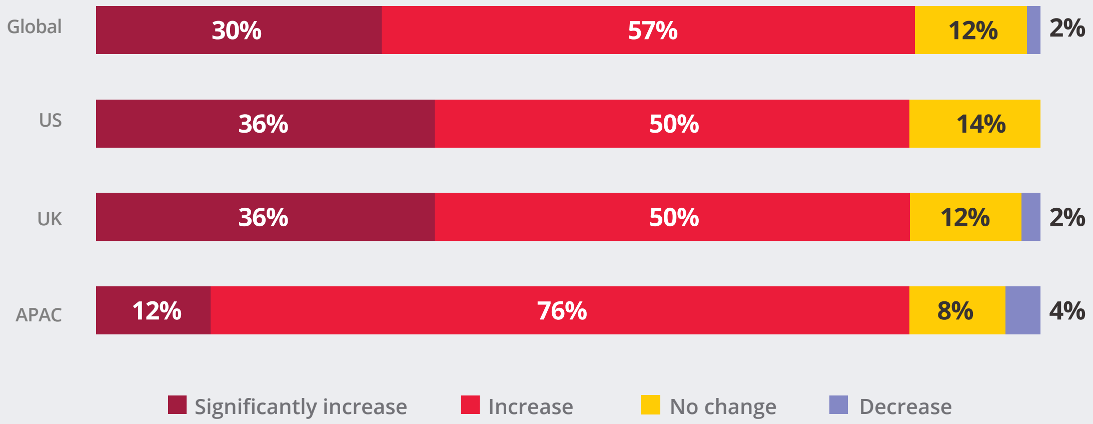
The Rise of Mobile

The use of mobile business apps is on the rise. It seems clear that the shortcomings of passwords and the rise of mobile apps for business use present an opportunity to leverage the power of secure mobile devices to provide stronger, more user-friendly, device-based authentication.

Nearly all of the survey respondents (94%) reported that millennials are driving the push for broader access to business services on mobile apps.

In the next 2 years, almost all organizations expect to see continued expansion of the use of business apps

Change in the Percentage of Access to Mobile Business Apps in the Next 24 Months



Q20: How will the percentage of your workforce that needs access to business apps from a mobile device change over the next 12 months?

Base: 200 (100 US; 50 UK; 50 APAC)

Although just under half of end users rely on mobile enterprise apps daily, usage is on the rise. Among the respondents, 85% reported seeing an increase in the number of users who need to access business apps from a mobile device over the past 12 months. This trend is expected to continue, with 87% anticipating an increase in users needing business app access over the next 24 months.

Respondents also estimated a high rate of increase. On a global basis, security leaders expect users requiring mobile apps to increase by 25%. In the US, they expect user adoption of mobile apps to increase by 33%.

Other research backs that up. A recent survey by Gartner, for example, found that mobile apps are the most common type of application developed by enterprises, as reported by 91% of the respondents. The survey also found that enterprise leaders expect mobile apps to contribute more than any other type of application to the success of their business.

The Sorry State of Passwords

The survey clearly concludes that passwords don't provide robust enough security. Among the security leaders, 86% would dump password use as an authentication method if they could. In fact, nearly half of those surveyed cited eliminating passwords as a way to cut almost half of all breach attempts.

Perceived security shortcomings are a key reason why almost three-quarters of these security leaders say they're actively looking for replacements for passwords for authentication.

User frustration with passwords is also a key factor. Well over half (62%) of the respondents reported extreme user irritation with password lockouts. The percentage of respondents who reported extreme user frustration at password lockouts rose to 67% at companies with more than 5,000 employees.

Using multifactor authentication is one way to strengthen the security of passwords, since it requires verifying a login through alternative means (for example, through a code sent by text message). But here again, the IDG survey reveals shortcomings. Even though 95% of the respondents reported MFA deployment at their organization, they also said that MFA covers only a little more than half of their users.

Among the reasons cited for not providing MFA to everyone: doubts about the security benefits (36%), expense (33%), and the top reason: a determination that users don't access sensitive information (45%).

"By and large, there are two issues that come up with the concern about passwords," says Foster. "The first is just the friction and the costs of passwords in the enterprise. (That includes people's calling support staff because they've forgotten their password.) And part 2 is that passwords are not enough for authentication."

The key challenge here, according to Foster, is supplementing passwords in a way that remains user-friendly.

"How do I implement that in an enterprise so that it doesn't cause so much friction for the users that they complain and revolt?" That, says Foster, is the key challenge facing today's security leaders. And it's a valid concern. The majority of the respondents (69%) reported that users would be relieved or even excited about ending passwords as a means of authentication.

Clearly, something must replace passwords and MFA for optimal security and user-friendliness, but what?

Finding Solutions

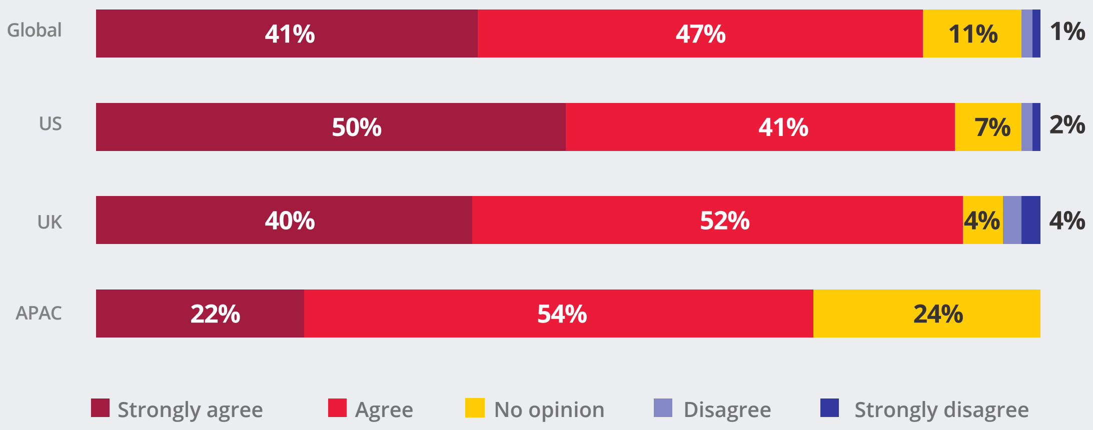
More than 75% of those surveyed said mobile devices secured by biometric authentication methods present the best option for replacing passwords. The majority (61%) also see hardware tokens as viable password replacements.

"I do think that we're going to get to seamless authentication based on your cell phone," says Foster. For the foreseeable future, he says, "the mobile phone remains at the center of enterprises in

In the near future, most security leaders assume that mobile devices will authenticate IAM

STATEMENT:

"In the near future, mobile devices will searve as your digital ID to access enterprise service and data."



Q24: To what extent do you agree or disagree with the following statement?
"In the near future, mobile devices will serve as your digital ID to access enterprise services and data."

Base: 200 (100 US; 50 UK; 50 APAC)

terms of where business is done, how access is given, and how authentication is done."

In this light, the phone itself becomes the user's identity, with no password entry or MFA—along with all the associated challenges—required.

A large majority of the IDG survey respondents agree. Globally, 88% of security leaders feel that in the near future, mobile devices will serve as a digital ID for accessing enterprise apps and data. In the US, the percentage rises to 91%.

With cyberattacks on the rise and the disadvantages of passwords and MFA apparent to security leaders—from both a user and a security standpoint—it seems clear that new authentication methods are needed.

Hardware tokens, seen by many security leaders as a more secure option for authentication than passwords, take a hit on user-friendliness compared to biometrics on a mobile device, as evidenced by the IDG survey. Among the security leaders, 72% see biometrics as more user-friendly than passwords, versus just 58% favoring tokens over passwords for ease of use.

"Nobody wants to carry additional dongles or keycards in addition to their cell phone," Foster says. That, along with the rise of mobile devices in the enterprise, is why he thinks ongoing innovations put the mobile phone front and center when it comes to unlocking enterprise apps and data by providing robust and user-friendly IAM. "If I put my prognosticator hat on, I think that the phone remains at the center," he says.

For more information about how mobile-centric authentication can provide stronger and more user-friendly security for your enterprise, go to **Mobileiron.com**