PASSWORDLESS: The Future of User Authentication

IDG Survey of IT leaders shows the impact of 2020 on security and how they're responding

By any measure, 2020 was the most tumultuous year in modern history. Front and center was a pandemic of proportions not seen in 100 years. And one of the ways that COVID-19 has disrupted lives and upended businesses the world over has been through its impact on IT infrastructure. A new survey from IDG sponsored by Okta highlights the impact on IT security, in particular, and how IT leaders are adapting.

As employees and customers hunkered down at home away from company networks, the IT executives who responded to the survey in late 2020 addressed the problem of user authentication. On the face of it, the picture wasn't pretty.

The majority of respondents (53%) reported that their organizations had been hit with data breaches directly related to mismanaged employee credentials. The consequences were severe; 44% reported financial loss stemming from these breaches, and nearly half (48%) said their companies had suffered reputational damage. Just 8% of those surveyed reported no negative consequences from mismanaged employee credentials.

Despite these apparently grim findings, however, the survey also revealed hope for the future as enterprises continue to adapt to the new reality of ongoing work from home and the accompanying increase in IT vulnerabilities. These findings should point the way forward well beyond the pandemic since organizations expect to continue to support larger numbers of employees working from home than ever before.

Key to achieving this goal is a shift in focus for IT security, starting with a zero-trust stance for enterprise networks and other IT assets.

A zero-trust enterprise has no "trusted" internal IT infrastructure in the traditional sense of a perimeter separating it from "untrusted" outside networks. Instead, security comes from an identity-centric mindset. Such a mindset secures access to enterprise IT resources by trusted users no matter where they log in, on what device, or from what network. That's ideal for a world of clouds, hybrid clouds, and employees working on a menagerie of devices on a constellation of home networks.

A zero-trust, identity-centric mindset depends on secure methods of user authentication. Passwords alone, with their well-documented vulnerabilities, won't cut it. What's needed in an environment where identity forms the core of security is passwordless, and includes multifactor authentication (MFA).

Because of its ability to secure access to corporate assets regardless of network, a zero-trust approach can help enterprises and their employees adapt to long-term remote work. And while organizations still have ground to cover in reaching zero trust across their IT stack, the IDG/Okta survey shows they're making progress.

To complete the transition, though, they'll have to overcome the challenges of the current state of user authentication at most organizations.

User Authentication Shortcomings

IDG surveyed 300 IT and IT security leaders at director-level and above in the US, the UK, and the Asia-Pacific region in September and October 2020. The objective: to gauge the current state of passwordless authentication in today's enterprise. In other words, how close are enterprises to the zero-trust state that provides the most security for enterprise IT?

First, the bad news. Respondents reported a range of severe consequences stemming from mismanaged user credentials, indicating they haven't achieved the kind of security they need to move forward through the pandemic and the work-from-home environment beyond with confidence.

Data breaches topped the list of consequences of authentication stumbles. Most respondents reported breaches stemming from credential mismanagement. That should, on its own, give companies plenty of motivation for getting this issue under control.

70% of respondents to that survey said they expected remote work to increase the cost of a breach. The study also found that compromised credentials resulted in the most expensive breaches.

As the 2020 Cost of a Data Breach Report from IBM Security and the Ponemon Institute shows, a data breach's average cost is close to $4 million. Nearly three-quarters (70%) of respondents to that survey said they expected remote work to increase the cost of a breach. The study also found that compromised credentials resulted in the most expensive breaches.

A host of equally serious consequences to credential mismanagement followed close behind breaches in the IDG survey. These ranged from lost employee productivity (49%) and reputational or brand damage (48%) to financial loss (44%) and legal and regulatory penalties (43%).

Other findings hint at hidden costs in addition to the more obvious hits.

- 41% of respondents reported having to divert internal resources, including staff time and budgets, to addressing the consequences of credential mismanagement. That means they're pulled away from more productive activities such as innovation and digital transformation projects.
- An average of 32% of help desk support requests are related to password issues, again pulling staff away from areas in which they could provide greater value, according to the survey.

All in all, user authentication emerges as a critical area that enterprises need to shore up to forestall a range of negative consequences.

Moving Beyond Passwords

A look at the current state of authentication at most enterprises reveals two factors contributing to failure. Nearly three-quarters (72%) of IT leaders report that passwords are the most common authentication factor used as part of MFA strategies at their organizations. That was closely followed by security questions, another weak authentication method, reported by 68% of respondents.

Although so many IT leaders reported relying on passwords for authentication, they expressed the view that passwordless authentication offers significant benefits.

"It cannot be copied and therefore prevents fraud from occurring," said one respondent. Many others commented that passwordless authentication provides a more user-friendly experience as well as more robust security. Accordingly, said one respondent, "It can help secure information from financial fraud and theft and increases productivity."

IT leaders also acknowledged that passwordless authentication puts less strain on helpdesks. That saves everyone the kind of frustration expressed by a respondent who commented that with passwordless authentication, "users can't forget or mistype [a] password."

IT leaders cited reduced security risk via the elimination of credential attacks as the top potential benefit of passwordless authentication. More respondents cited that benefit in the US, at 56%, versus 47% in the UK, and 43% in the APAC region.

Improving user experience was the second-most-cited benefit, with respondents in the APAC region citing it at the highest rate (43%), followed by those in the US (41%) and UK (32%).

Reducing the burden on IT resources and staff was the third-most-cited benefit of passwordless authentication, named by about a third (35%) of respondents in all regions.

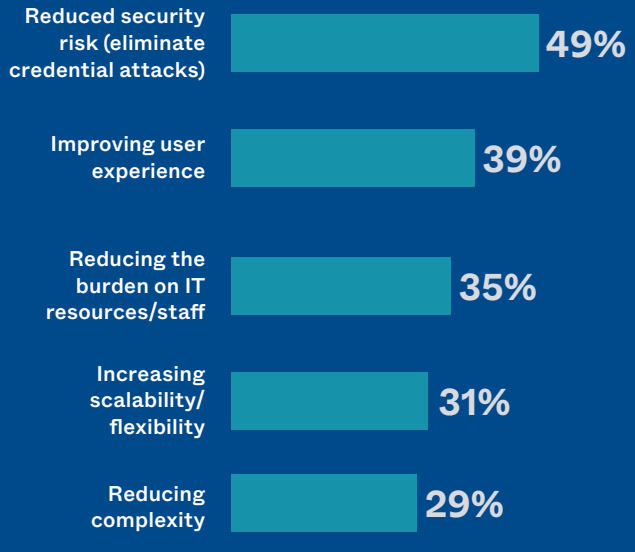
IT leaders also see passwordless authentication as a critical part of a zero-trust strategy. Nearly nine in ten (87%) of respondents expressed the view that passwordless authentication is "critical" or "very important" to a zero-trust strategy. Only 1% said it was "not very important," and no one said passwordless authentication was "not at all important" for a zero-trust strategy.

US-based IT executives called passwordless authentication "critical" for zero trust at the highest rate, with 40% of respondents. Respondents in the APAC region logged the highest percentage of those calling passwordless authentication "very important," at 68% of respondents.

The good news is that nearly all survey respondents (95%) reported familiarity with passwordless authentication technology, and the majority of their organizations have deployed technology for enabling it.

FIGURE 1.

The most appealing potential benefits of a passwordless employee authentication solution



	U.S.	EMEA	APAC
Reduced security risk (eliminate credential attacks)	56%	47%	43%
Improving user experience	41%	32%	43%
Reducing the burden on IT resources/staff	35%	39%	30%
Increasing scalability/ flexibility	21%	33%	39%
Reducing complexity	28%	28%	32%

Source: IDG

Multifactor Authentication

Along with passwordless authentication, MFA provides critical benefits on the road to achieving zero-trust security. An average of 60% of enterprise users rely on multifactor authentication, according to IT leaders surveyed. That means that many organizations that use passwords don't rely on them exclusively. Instead, they back them up with authentication methods such as smartphone codes and biometrics, greatly enhancing security in the process.

The most-cited benefit for MFA used in the enterprise is increased security for employees working from home, with about three quarters (74%) of IT leaders naming this benefit. That result remained steady across regions, with 76% of US IT leaders and 78% of those in the APAC region espousing MFA's work-from-home benefits. Results from the UK dipped slightly, with 67% of respondents citing this benefit, but still amounted to the most-cited benefit of MFA for UK respondents.

Secure single sign-on (SSO) is another top-cited benefit of MFA, suggesting that many organizations see value in an integrated SSO and MFA solution. This perceived benefit just edged out security for remote work in the APAC region, cited by 79% of respondents there. Well over half of respondents in the US (65%) and the UK (62%) named SSO as a critical benefit of MFA.

It seems clear that IT leaders appreciate SSO's user-friendly nature, since it requires users to enter credentials only once to access an array of services and apps. "There isn't a need to memorize multiple passwords or store them for future use," explained one respondent. "Employees can stop worrying about their information and be more productive."

An enhanced ability to meet compliance obligations (cited by 66% of respondents), cost savings (53%), and a decrease in credential-related breaches (52%) also got high marks as perceived benefits of MFA.

And while passwords and security questions remain the top authentication methods, more secure and user-friendly factors have gained traction. After passwords and security questions, one-time password (OTP) emerged as the third-most-popular authentication method, used by 65% of survey respondents. Close behind were mobile authenticator apps such as Google Authenticator and Okta Verify. Organizations deployed authenticator apps at the rate of 63% of those surveyed. Half (50%) of respondents reported sending OTP tokens to users via SMS or voice. Just 31% reported using biometrics, perhaps as a result of increased costs in deploying hardware that supports biometrics.

The APAC region reported the heaviest use of OTP, at 74% of organizations, versus 66% in the US and barely more than half (55%) in the UK. The APAC region is also ahead in using authenticator apps, with 72% of respondents there relying on them as part of an MFA strategy. The US and the UK just about tied in authenticator apps, at 58% and 60%, respectively.

But even though more than half of all IT departments surveyed use some form of MFA, the survey also revealed why organizations still have some distance to go for widespread adoption of passwordless authentication as part of their MFA strategies.

Challenges to Passwordless Adoption

Survey respondents cited numerous challenges to implementing passwordless authentication, chief among them integration issues due to technological complexity, reported by 41% of respondents. Respondents in the US cited integration issues at the highest rate (53%), followed by those in the APAC region (39%). Not quite a third (30%) of respondents in the UK cited this issue.

Data privacy concerns, most likely specific to the use of biometrics, came next, cited by a third of respondents (33%). This concern was highest in the APAC region, cited by nearly half (47%) of IT leaders there. US respondents expressed

> **"Passwordless authentication provides a more user-friendly experience as well as more robust security. It cannot be copied and therefore prevents fraud from occurring."**
>
> IDG SURVEY RESPONDENT

concern about privacy at the lowest rate, with just over a quarter (26%) of respondents reporting it, but UK respondents were very close at 27%.

Following data privacy concerns, nearly the same percentage overall (30%) expressed concern about pressure on IT resources. That finding was very similar across regions, followed by cost concerns (28% overall). But significantly more APAC (33%) and UK (34%) respondents cited concerns about cost as a factor inhibiting implementation than in the US (18%).

A quarter (25%) said that resistance to change and fear of the unfamiliar got in the way of implementation, the same rate as those having difficulty selecting the appropriate technology. That was followed closely by the related problems making the case for ROI (21%). US respondents reported the most difficulty selecting technology, at 29% versus just 20% in both the UK and APAC regions.

Despite the challenges with implementing passwordless authentication, the prevalence of multifactor authentication in organizations will help to kickstart passwordless authentication when ready.

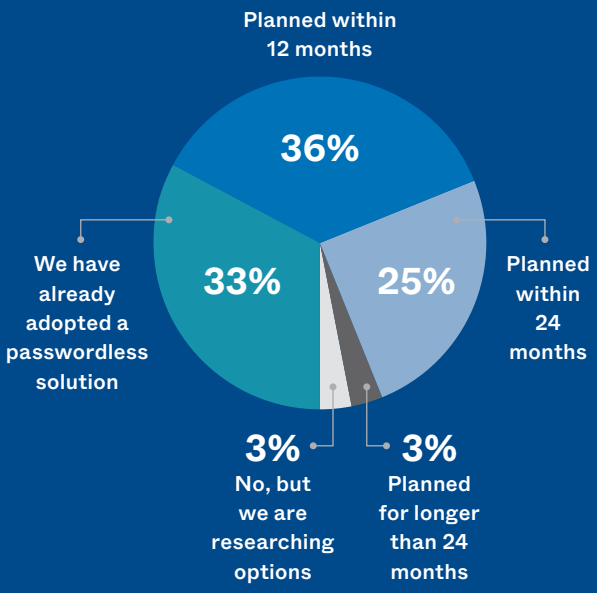
Modern User Authentication Solutions

Nearly one-third (33%) of IT departments have already adopted passwordless authentication, with the APAC region reporting the highest adoption rate, at 41%. The US lagged the furthest behind, with 26% reporting adoption versus 31% for the UK.

However, the US appears to be catching up, with more than half of respondents (52%) reporting that their organizations plan to adopt passwordless authentication within 12 months, versus 26% in the UK and 29% in the APAC region.

FIGURE 2.

Organizations' plans to adopt a passwordless authentication solution for employees



	U.S.	EMEA	APAC
We have already adopted a passwordless solution	26%	31%	41%
Planned within 12 months	52%	26%	29%
Planned within 24 months	22%	30%	23%
Planned for longer than 24 months	0%	5%	5%
No, but we are researching options	0%	6%	2%

Source: IDG

> **There isn't a need to memorize multiple passwords or store them for future use. Employees can stop worrying about their information and be more productive."**
>
> IDG SURVEY RESPONDENT

Among the majority of organizations deploying MFA solutions, those from Okta received the highest marks in key areas. Among other benefits, Okta allows organizations to build authentication into the applications and platforms they already use, including the Microsoft Office suite, G Suite, Zoom, and Salesforce. It also extends security to the customer experience, helping to smooth transactions while fostering trust.

- ☑ **Security for remote work,** the top perceived benefit of MFA, was cited as a benefit of Okta solutions by 78% of IT leaders versus 72% of leaders deploying solutions from other vendors.
- ☑ **Secure login** with SSO was cited by 74% of Okta users versus 67% of users of other solutions.
- ☑ **Better compliance** with regulations was cited by 73% of Okta users versus 63% of others.
- ☑ **Decreased or no credential breaches** was cited as an important benefit of their chosen solution by 67% of respondents using Okta versus 45% for other solutions.
- ☑ **Okta was also competitive for cost savings,** tied with other solutions at 53% of respondents reporting this is as an important benefit of the MFA solutions in use at their organizations.

Moving Forward

The challenges to business as usual by the events of 2020 have forced enterprises around the world to make lasting changes to the way they secure their workforces, their customers, and their data—wherever in the world they happen to be, on whatever device or network they use.

Passwords and "what you know" forms of authentication lack the robust, modern security capabilities that organizations need to secure employees and customers on diverse and perimeterless networks. They also put heavy burdens on helpdesks and employees forced to cope with the consequences of mismanaged user credentials, as revealed by the survey.

Fortunately, passwordless authentication as part of a robust multifactor strategy can overcome the challenges of today's work-from-home environment and its attendant security concerns. The Okta Identity Cloud can help by providing secure, single sign-on and multifactor authentication for enterprise workforces and customers.

For more about how passwordless user authentication and MFA benefit global enterprises in the new normal, visit **https://okta.com**.