

[LEADERSHIP STRATEGIES](#)

Future of Authentication: What Enterprises Need to Know about Passkeys

Is it time to ditch passwords?

MARCH 22, 2024 - 7 MINS READ

[in](#) LinkedIn[Share on Twitter](#)

**Latest Research
Highlights and Trends**

Direct to Your Inbox

[Subscribe Now](#)



If I told you the single most effective step your business could take to improve cybersecurity is to stop using passwords, you might think I'm crazy. It's sort of like saying that the best way to make your car faster is to remove the tires, or that swearing off vegetables is key to losing weight.

But the reality is that by many measures, passwords are past their prime. There's a better solution – passkeys – and organizations looking

Why Disruptive Tech Vendors Partner with IDC



You're here to disrupt the tech industry. We're here to help. Learn more about IDC's approach to working with disruptive tech vendors & our newest solution, the Accelerator Program:

[WATCH VIDEO](#)

Are You Looking for Better Returns From Your IT Investments?

for ways to optimize their security stances would do well to consider passkey-based authentication in contexts where it makes sense.

That said, passkeys remain subject to a variety of challenges, which make it unrealistic for most businesses to shift entirely to passkey-based logins in the near future.

Plus, as passkeys grow in popularity, it will be increasingly important for business decision-makers to distinguish between hype and reality when it comes to passkeys. Expect to hear more and more in the near future about how wonderful passkeys are – especially from vendors who sell passkey solutions – but don't assume that passkeys are preferable to passwords for every use case and circumstance.

With those realities in mind, here's a balanced look at the pros and cons of passkeys, along with tips on when and how to take advantage of passkeys as part of your business's authentication strategy.

What are passkeys?

Passkeys are a way of authenticating with a website or app without requiring a username and password. Instead, passkeys confirm a user's identity using methods like biometric authentication or the entry of a PIN code.



Then look at IDC's services for cost benchmarking, analyst advice and IT optimization.

Get Data-driven Insight

Maximize Your Marketing ROI



Amplify your pipeline with high quality leads and effective content marketing. IDC's lead generation program, with Foundry, combines expert research and analysis with targeted outreach to drive your business forward.

Under the hood, passkeys rely on a set of keys – one public and one private – that are generated for each user. The user’s public key is shared with a website or app to which the user wants to log in. The private key is stored only on the user’s personal device (such as a phone or laptop).

To authenticate with a website or app, the user must unlock his or her private key from the device where it resides. Typically, the method for unlocking the key involves biometric authentication (like scanning the user’s face or fingerprint) or the entry of a unique PIN code that the user configured when setting up the passkey.

Advantages of passkeys vs. passwords

Compared to password-based authentication, which has been widespread for decades, the benefits of passkeys boil down to two main advantages:

- **Greater convenience:** Passkeys are more convenient for users, who don’t have to remember login names or passwords to login.
- **Enhanced security:** Passkeys improve security because, unlike passwords, they cannot be guessed or brute-forced by attackers (at least in most cases). In addition, because private passkeys reside only on users’ personal devices, passkeys eliminate the risk that

Get Better Leads

Recent posts

JUNE 26, 2024

Why Tech Startups Should Engage With Analyst Firms: Debunking Common Myths

JUNE 24, 2024

Unpacking the 2023 CIO Sentiment Survey

JUNE 21, 2024

The Rising Urgency for Telecom Innovation

JUNE 19, 2024

Empowering Sales Management with AI

JUNE 14, 2024

Apple Enters a New Era

Trending Topics

featured cognitive/artificial intelligence marketing

IoT COVID-19 data Internet of Things customer experience

generative ai future of trust AI cybersecurity IDC future

enterprise digital innovation future of work ESG Future of

threat actors could hack a server or database containing passwords and usernames, then use the information to compromise user accounts.

- **Spoofing/phishing protection:** Passkeys mitigate spoofing and phishing risks because a user's private key must be paired with the public key of a specific site or app when logging in. Therefore, attempts to trick users to log into malicious sites masquerading as legitimate ones won't work, because the malicious sites won't have the same public keys as the legitimate sites they are impersonating.

For these reasons, passkeys are a growing focus of identity and authentication providers like [Okta](#) and [Microsoft](#), according to recent IDC research. Businesses that use authentication products or services from vendors who have added passkey support can make passkey-based logins an option – or a mandatory requirement, if desired – for their employees and customers.

The pitfalls of passkeys

On the other hand, passkeys are not perfect. They are subject to several distinct drawbacks that could hinder the ability of enterprises to adopt passkeys in certain situations:

Websites and apps may need to be updated to support passkeys

Sites and apps that are already configured to integrate with third-party authentication providers who support passkeys can add passkey-based logins relatively easily. Otherwise, however, businesses will need to overhaul the authentication logic in their apps to make passkeys viable for employees and customers – a process that takes time and money.

Passkeys are tied to devices

Because passkey-based authentication depends on access to private keys stored on specific devices, it's not a good option for use cases where it's difficult to predict which device an employee or customer will use to log in. For instance, if a customer sometimes connects to your site using a mobile phone but also uses a personal laptop or work laptop, they'd need to configure separate passkeys.

The passkey vendor ecosystem is fragmented

To date, most solutions for configuring and managing passkeys work only on certain operating systems, devices or vendor ecosystems. For example, Apple's offerings do not support Android devices.

Passkeys only support certain devices and operating systems

Passkey-based authentication also only works on devices and operating systems designed to support it. Older devices are likely not to be compatible which could create confusion among users about which devices are supported

Passkeys can be hacked

Passkeys are substantially more secure than passwords, but they're not impervious against attack. Sophisticated threat actors who manage to obtain physical access to devices may find ways to [work around biometric authentication](#) or guess PIN codes in order to access passkeys stored on the device.

These types of attacks are much more challenging to carry out than conventional techniques for bypassing passwords, and to date, no major breach has occurred involving stolen passkeys. But they are plausible nonetheless.

Enterprise security policies don't accommodate passkeys

Currently, most enterprise security policies that govern authentication and authorization were not designed with passkeys in mind. Enterprises will therefore need to update their security policies (and associated security practices).

This is feasible, but updating security policies is likely to take some time, delaying enterprise passkey implementation.

A long horizon for passkey adoption

The nature of passkeys, and the challenges surrounding their implementation, mean that very few businesses are likely to migrate exclusively to passkey-based authentication anytime soon. To get to that point, organizations would need to overhaul all of their websites and applications to support passkeys

In addition, identity and authentication management vendors would need to make passkey-based authentication a first-class citizen within their solutions. To date, few have done that, although it's reasonable to expect that this will happen over the next two or three years.

When businesses should – and should not – use passkeys

Rather than approaching the question of “to passkey or not to passkey” as an either-or, binary choice, organizations should be thinking at present about specific situations where it does and doesn’t make sense to adopt passkeys as a primary means of authentication.

In general, shifting to passkeys is a good strategy for websites and applications that have well-defined sets of users with predictable behavior. If you know that the employees or customers who need to access a certain resource typically log in using specific types of devices, and they access those resources frequently, asking them to set up passkeys is reasonable – especially if the website or app already integrates with an identity management service that supports passkeys.

On the other hand, it’s harder to make a case for switching to passkeys in situations where the cost, complexity and hassle of configuring and maintaining them – from the perspective of both the business and users – outweigh the benefits. For example, legacy applications that can’t integrate with authentication services offering built-in passkey support are likely not worth updating just to enable passkey logins. Likewise, if you have a group of customers who access a website only a few times, they may view passkey requirements as more trouble than they’re worth.

Learn more about passkeys in the enterprise

Passkeys remain a fast-evolving topic as more and more identity and authentication management providers embrace the concept of passwordless logins, and as enterprises continue to evaluate use cases for passkeys.

IDC is following this scene closely and will be unveiling multiple resources in the coming months to offer actionable guidance on how enterprises can (and can't) benefit from passkeys. To learn more – or to request access to IDC assets and analysts focused on passkey authentication – [contact us](#).

If you're interested learning more about IDC's guidance around cybersecurity, watch the on-demand webinar, *Cybersecurity Norms and Trends: How Does Your Business Stack Up?*, by clicking the button below.

WATCH NOW

AUTHENTICATION

CYBERSECURITY

FEATURED



PASSKEYS

Christopher Tozzi, Adjunct Research Advisor



Christopher Tozzi, Adjunct Research Advisor

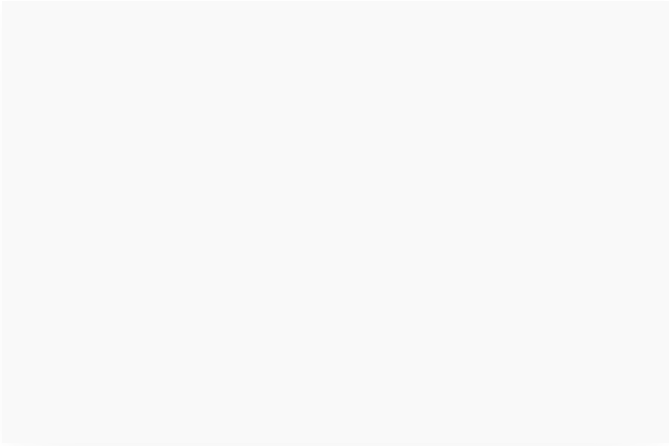
Christopher Tozzi, an adjunct research advisor for IDC, is senior lecturer in IT and Society at Rensselaer Polytechnic Institute. He is also the author of thousands of blog posts and articles for a variety of technology media sites, as well as a number of scholarly publications.

Related Posts



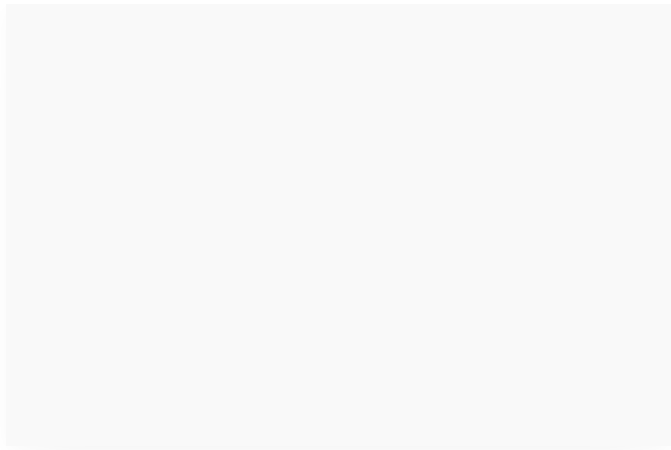
Why Tech Startups Should Engage With Analyst Firms: Debunking Common Myths

JUNE 26, 2024



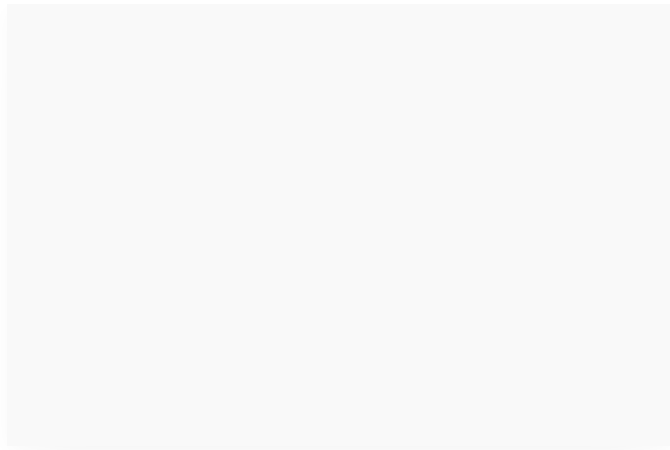
Unpacking the 2023 CIO Sentiment Survey

JUNE 24, 2024



The Rising Urgency for Telecom Innovation

JUNE 21, 2024



Empowering Sales Management with AI

JUNE 19, 2024

Copyright 2023 IDC. All rights reserved.