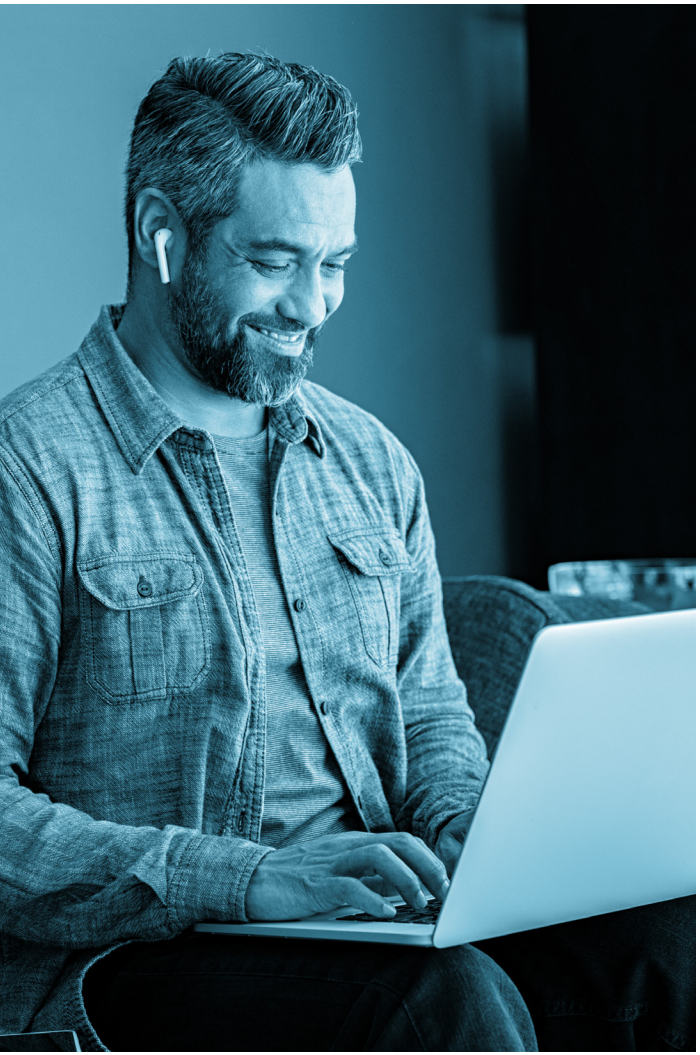
yubico

Considering synced passkeys for your enterprise?

Avoid the pitfalls that increase risk and cost exposure



Different passkey implementations

Passkeys are passwordless-enabled FIDO credentials that live in authenticators, whether they be smartphones, tablets or laptops or in authenticators that are purpose-built for security such as FIDO hardware security keys.

Passkeys are more secure than passwords and enable a move to passwordless authentication that enables greater security and efficiency. To learn more about passkey basics click here.

There are two types of passkeys, synced and device-bound. Synced passkeys are copyable credentials that can travel across various devices such as smartphones, laptops, and tablets connected to a user account. This may create some chilling failure points for the enterprise.

A few common scenarios when your synced passkeys might be vulnerable at work:

1. **Remote work risks**—Security risks arise when employees work from home and an attacker's device is used for employee credentials due to synced passkeys copying easily
2. **Supply chain vulnerability**—Insider threats emerge and supply chain integrity breaks down when employees share synced passkey credentials across accounts and devices
3. **Compliance and support complexity**—Passkey ecosystem sprawl opens up an enterprise to multiple passkey providers, making it challenging to track and trust the credential needed for compliance, and also increases IT helpdesk burdens and cost.

Read each of these scenarios below to see how synced passkeys can increase risk and costs for the enterprise.

Synced vs. device-bound passkeys

Synced passkeys

Lives on a smartphone, tablet, laptop or other device where it can be copied and synced across many devices.

Device-bound passkeys

Live on authenticators purpose-built for security, such as hardware security keys, and offer the highest security assurance.

Scenario 1

Remote work risks

A passkey syncs between all owned devices on a single iCloud account. Here's a story of how that proved dangerous for Jim, a full-time remote worker for a tech company. Jim works at home, where his whole family uses the same iCloud account with six different devices. Let's see how an attacker can take advantage of synced passkeys.

1. Jim logs onto his work account using a passkey on his phone. He has added his phone to his personal iCloud account, which is also shared with other devices used by his family.

2. Jim's son, Ben, gets an email with a cool link about an app-based game he likes to play. He clicks the link.

3. Ben is tricked into supplying his iCloud username and password—which are intercepted by the attacker. Ben accepts the request to add a new device allowing the attacker to register their own device to the family's iCloud account.

4. Because Jim's work phone is already synced to the cloud, his work passkey automatically syncs with all devices on the iCloud account. That includes the attacker's device!

5. Once the attacker has Jim's work credentials, they can log onto work sites as Jim and then seek other credentials with higher privileges.

DID YOU KNOW?

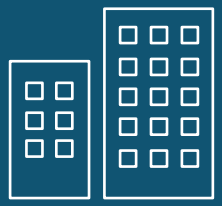
89% of organizations experienced a phishing attack in the past year.

HYPR, 2022 State of Passwordless Security Report

Scenario 2

Supply chain vulnerability

A synced passkey can be easily shared outside of a user's direct control with another device through the AirDrop feature on iPhone. And while a passkey's shareability is convenient in some situations, it can create significant security gaps such as insider threat if employees share credentials carelessly. This contributes to increased risk and loss of trust within the overall supply chain. Listen to Kira's story.



1. A large retailer with a complex supply chain allows their HVAC system monitor (an outside vendor) to log into essential systems to check real-time conditions.

2. Kira is a new employee at the vendor. She has not yet completed the setup of her account with the retailer, but needs to work the next shift, so she has a co-worker share their passkey using Airdrop over bluetooth.

3. A few months later, Kira quits but she still has her co-worker's passkey as there is no automated way to revoke the co-worker's shared passkey on Kira's device.

   The organization cannot enforce deleting the passkeys from Kira's device.

4. A setting misadjustment on the HVAC system suddenly causes a significant outage.

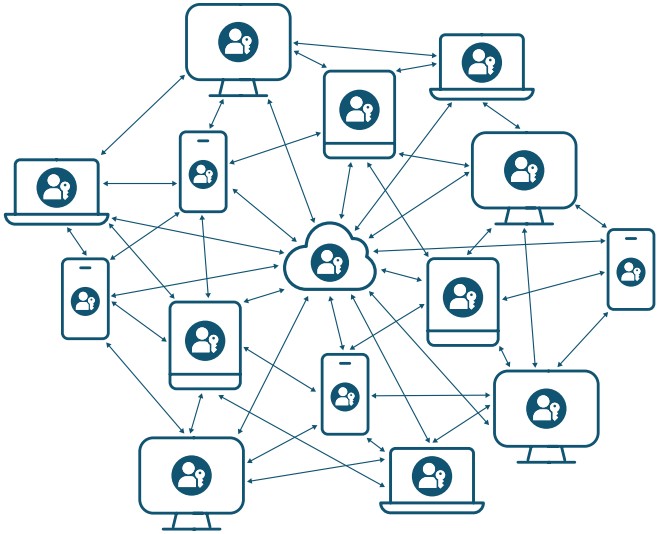
   The passkey exists in at least two locations—The audit logs show the passkey credential was used but the logs cannot determine whether login was made by Kira or her co-worker.

5. Legal risk exposure increases as audit logs are less reliable and the vendor loses control of where the passkey credentials are stored and managed.

Scenario 3

Compliance and support complexity

Passkeys are implemented across a variety of different vendors and products. Users are not required to use only one of these. That means an enterprise is faced with the risk that users have many passkeys across different platforms and password managers. How will the enterprise track which passkey is being stored where, and how will they help users who encounter passkey-related support issues if the enterprise has no visibility?



1. Frank is asked by IT to register passkeys as a way to improve security on his corporate login.

2. Frank decides to use 3 different passkey service providers (Apple, Google, password manager) in order to make it convenient so that Frank can log into the corporate system with any one of his synced passkeys.

3. Months later, a data breach incident is disclosed highlighting that one of Frank's passkey service providers had a security incident on the passkey management system.

4. Due to ecosystem over exposure, Frank's identity is vulnerable for attackers to exploit. Frank now needs to remove all the synced passkeys from the 3 different providers and re-enroll passkeys for his corporate login.

5. The corporate help desk will struggle to help workers like Frank resolve access issues as they do not have any knowledge of the various passkey service providers. Enterprises will need to consider the support cost for enabling synced passkeys.

Which passkeys are right for your organization?

Top 5 takeaways

Passkeys are better than passwords because they're based on modern FIDO protocols and offer stronger defense against phishing.

Here are the top 5 things to remember about synced passkeys and why device-bound passkeys that reside on hardware security keys offer a more secure and compliant option for enterprise needs! Not all passkeys are created equal and enterprises should avoid the pitfalls of synced passkeys.

- Passkeys enable a FIDO enabled world but for enterprises that require strict control of user identity, synced passkeys may actually lead to increased risk for your organization.
- Synced passkeys can travel so they more closely reflect a "sign in with" mechanism rather than a true second factor.
- Synced passkeys may cause enterprises to trust 3rd parties who are not dedicated security vendors.
- Synced passkeys provide easier paths for users to share credentials and users may default to that if enabled.
- Device-bound passkeys, such as the ones that reside in modern, portable FIDO security keys, provide a higher degree of protection and better meet enterprise compliance needs.

Contact us
yubi.co/contact

Learn more about the different types of passkey options for your enterprise
yubi.co/passkey

How to choose the right passkey solution

SERVICE PROVIDERS	**Consumers** Most consumers can use synced passkeys on their devices as it's a better option than passwords	**Consumers at risk** High risk users—e.g. journalists—may benefit from passkeys that deliver higher security assurance, such as those residing in hardware security keys
ENTERPRISES	**First line workers** Many of these workers can't use personal phones or laptops on the work floor and need a passkey solution that is not dependent such devices	**Office workers** These workers require security keys with hardware attestation to ensure passkey credentials cannot be copied
		Privileged users Users who are the highest risk targets require security keys with hardware attestation to know where the passkey credentials are stored

yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.