BEST PRACTICES GUIDE

How to get started with passwordless using device-bound passkeys

Six deployment best practices to adopt the most secure passkey authentication strategy for your organization

$4.35 million

average cost of **data breach**[2]

$1 million

costs associated with **annual password reset**[3]

$5.2 million

additional costs in lost productivity due to **account lockouts**[4]

Only FIDO and Smart Card/PIV (PKI) are phishing-resistant

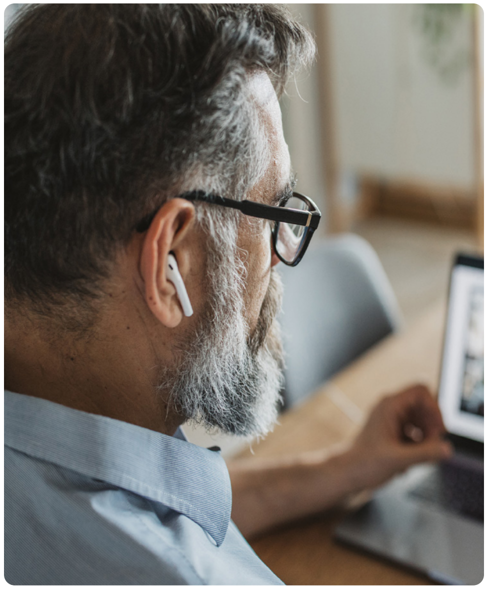
Choosing the right passwordless approach

Passwords remain the most common form of user authentication, used by 91% of organizations[1]—but passwords are fundamentally broken, offering weak security, increased support costs and a poor user experience. Data breaches carry a high cost across the globe ($4.35M USD[2]), with an additional $1M USD[3] associated with annual password reset costs and $5.2M USD[4] in lost productivity due to account lockouts. In response, 66% of organizations have deployed, are piloting, or are planning to deploy **passwordless authentication** within the next year.[5]

Passwordless authentication is **any form of authentication that doesn't require the user to provide a password at login.** Going passwordless is a journey for most organizations—first moving away from passwords and legacy forms of MFA, which are all highly vulnerable to phishing, and moving to a modern MFA approach which offers strong phishing-defense. Once there, an organization is well poised to move to passwordless.

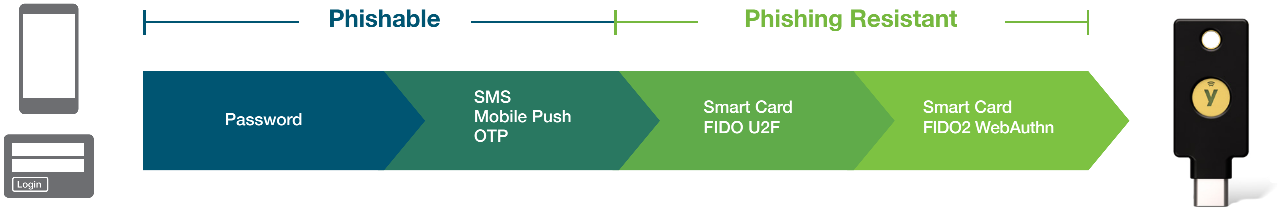
While any form of multi-factor authentication (MFA) offers better security than passwords, **not all MFA is created equal.** Basic or legacy forms of MFA passwordless such as SMS, mobile authentication and one-time passcodes can be easily bypassed by malicious actors, making them susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks. The only truly phishing-resistant and passwordless authentication methods involve either Smart Card or FIDO2-based authentication protocols.

> “Phishing resistance is the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber.”
>
> NIST **NIST 800-638-4** | Dec. 16, 2022



What are passkeys?

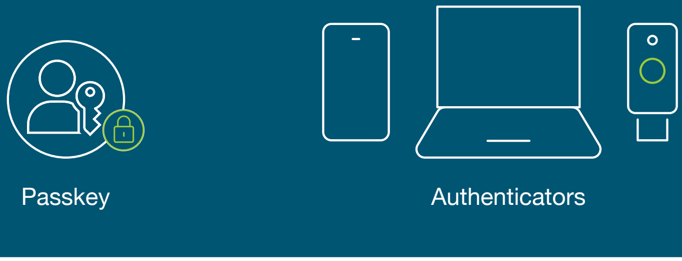
Passkeys are the modern, convenient replacement for passwords—a secure passwordless experience, based on phishing-resistant FIDO2 authentication protocols, that is easy and available for individuals and organizations alike.



A passkey is just a new name for a passwordless-enabled **FIDO2/WebAuthn credential**, which is good at blocking phishing attacks. The passkey is the credential itself, a digital file. The passkey lives in an authenticator such as a phone, laptop, or a device purpose-built for security such as a hardware security key. This distinction is important when choosing a passkey implementation for an enterprise environment.

What's the difference between a passkey and an authenticator?

A passkey is the credential itself, a digital file. An authenticator is where the passkey lives. For example, on a phone, laptop, hardware key, or other device.

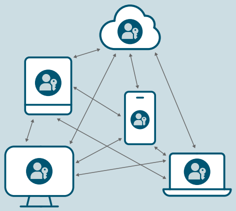


Passkey implementations

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

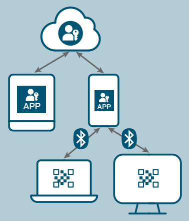
Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

Synced passkeys



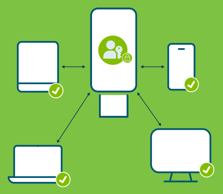
- Lives on a smartphone, tablet, etc.
- Copyable/shareable
- Consumer grade; lower security and compliance assurance

Device-bound passkeys on general-purpose devices



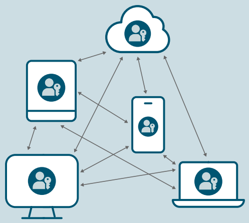
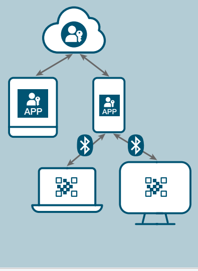
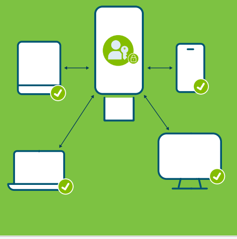
- Lives in general purpose devices such as smartphones and tablets. For example using an authenticator app
- Middle ground option for enterprises; but less secure than device-bound passkeys on hardware security keys

Device-bound passkeys on hardware security keys



- Lives on a security key or other hardware separate from everyday devices
- Best option for enterprises; meet higher security and compliance assurance
- Only passkeys that meet Authenticator Assurance Level 3 (AAL3)

Which passkey approach is right for you?

If you need	Synced passkeys 	Device-bound passkeys on general-purpose devices 	Device-bound passkeys on hardware security keys 
Synced/shareable between devices	Unmanaged syncing	Managed syncing	No syncing between devices
Works across Apple/Google/ Microsoft	May not work	Works across all platforms	Works across all platforms
User registration/onboarding	Weak; backed by password	Weak; app backed by password	Most secure as user registration not reliant on a password
Credential recovery	Easy to recover	Time to replace phone and costly	Fastest with a backup key
Compliance and audit	Authenticator Assurance Level 2 (AAL2) No attestation; unsure if user controls passkey	Authenticator Assurance Level 2 (AAL2) Supports software attestation	Authenticator Assurance Level 3 (AAL3) Supports hardware attestation
Risk/Costs	Perceived as “free”; high IT/ helpdesk costs and higher risk exposure is costly	Perceived as cheaper than HW; but risk exposure gaps can be costly in long run	Perceived as higher cost upfront; but less costly due to lowered breach risk and reduced IT burden
Works across enterprise scenarios	Not in mobile-restricted, shared workstations	Not in mobile-restricted, shared workstations	Works across all enterprise scenarios

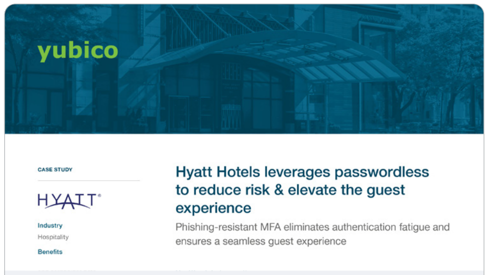
The total economic impact of YubiKeys:

Strongest Security
Reduce risk by
99.9%

High Return
Experience ROI of
203%

More Value
Reduce support tickets by
75%

Faster
Decrease time to authenticate by
>4x



yubico

CASE STUDY

HYATT

Industry
Hospitality

Benefits

Hyatt Hotels leverages passwordless to reduce risk & elevate the guest experience

Phishing-resistant MFA eliminates authentication fatigue and ensures a seamless guest experience

To read the case study go to yubi.co/hyatt.

YubiKeys enable passwordless with the most secure passkey authentication approach

Yubico created the **YubiKey**, a hardware security key that houses device-bound passkeys and delivers **phishing-resistant MFA and passwordless authentication at scale with with a seamless user experience.**

The YubiKey is a multi-protocol security key, supporting a range of authentication protocols, passwordless authentication via both Smart Card/PIV and passkey (FIDO2/WebAuthn), along with OTP and OpenPGP, integrating seamlessly across legacy on-premises and modern cloud environments to help organizations **bridge to a passwordless future.** YubiKeys work with over 1,000 products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services. The YubiKey is proven to reduce risk by 99.9% and deliver significant business value to large enterprises at scale, delivering an ROI of 203%[6], with a frictionless user experience, a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

Unlike synced passkeys that reside in devices not purpose-built for security, and delivering the ease of copying and sharing which introduces risk for the enterprise, device-bound passkeys residing in YubiKeys are not shareable or copyable, enabling the enterprise to better track and trust the FIDO credential, which is critical at scale, for compliance and for audits. Device-bound passkeys that live on a portable security key such as the YubiKey, also ensure that users can seamlessly and securely work across a range of platforms and devices, and across the ecosystem (e.g. Apple, Google, Microsoft).

Device-bound passkeys enable enterprises to implement passwordless and meet the most strict security and wregulated industries. Any other passkey available today supports only up to Authenticator Assurance Level 2 (AAL2).

Given the threat landscape, the need to move toward passwordless gets clearer on a daily basis. **But how do you start the journey to passwordless authentication?** The remainder of this guide will detail six key best practices to implement the highest-assurance path to passwordless using device-bound passkeys residing in the YubiKey.

> “The biggest benefit that Hyatt is going to receive from deploying YubiKeys is to be able to get rid of passwords in our environment. You can’t compromise what you don’t have. I think we’re going to have a great big party once we turn that button off and there’s no more passwords anywhere in the environment.”
>
> **Art Chernobrov** | Director of Identity, Access, and Endpoints | Hyatt Hotels Corporation

Six key best practices to accelerate the adoption of passwordless using device-bound passkeys

Getting started is easy. Getting started is easy. Based on Yubico's experience assisting hundreds of customers to optimize authentication security, we have created a six step deployment process to plan for and accelerate passwordless adoption using device-bound passkeys at scale.

Plan

Ensure readiness by clarifying use case cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact

01. Plan

Clarify use cases and ensure readiness

A **phased approach** is the best way to ensure a frictionless deployment. Put your **high value users and data first**, then expand. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

Deploy the right passkey approach for the right user groups and risk profiles:

Consumers

Synced passkeys or app-based passkeys on their devices are probably ok

Consumers at risk

High-risk users—e.g. journalists—may require extra security for passkeys, such as those residing in security keys

First line workers

Need a soultion that is not dependent on thier personal device to authenticate

Office workers

Require security keys with hardware attestation to ensure credentials cannot be copied

Privileged users

Highest risk users—require security keys with hardware attestation to know where the credentials are stored

Remote work

Protect against passkeys being shared to other devices or compromised by other devices attached to the iCloud account

Mobile restricted

Hardware keys can go where mobile devices are not allowed (e.g. call centers, manufacturing environments, server rooms, clean rooms, hardened rooms)

Supply chain

Require a solution that cannot be shared among employees or compromised if attached to personal iCloud accounts

Assemble key stakeholders

While the amount of resources committed to the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can positively influence the implementation of the YubiKey across the organization. It’s important to have buy-in across all teams to ensure a smooth rollout:

IT	Security	Finance	Help Desk	HR/Learning & Development

Engage Yubico experts as needed

With a tried and true process that hundreds of organizations have followed already, and with a ‘YubiKey as a Service’ model, Yubico offers flexible and cost-effective solutions to heighten solutions and streamline authentication. No matter where you are on your journey to passwordless, we’ll meet you there, offering best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.

YubiEnterprise Services*		Yubico Professional Services	
YubiEnterprise Subscription	YubiEnterprise Delivery	Deployment 360	Deployment planning
Simplifies how businesses procure, upgrade and support **YubiKeys**	Global turnkey YubiKey **distribution** through YubiEnterprise Delivery or local channel partners	**Turnkey** planning, technical integration and deployment support	Jump start your rollout with workshops & **projects** to review use cases and develop a customized strategy

* YubiEnterprise Services are available for organizations of 500 or more users.

> “I am all about making the adoption of technology as easy as possible. If I can hit the easy button using YubiKeys and also using their subscription model to ensure all my users have YubiKeys, that is a big win for me!”
>
> **Brent Deterding** | CISO | Afni

02. Validate

Confirm the process with a small group of users

Validate with a small group of users across a priority use case for confirmation and feedback, leveraging Yubico best practice resource guides, videos and engagements. **Practice, learn and then move forward with expansion.**

Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. To browse YubiKey compatibility go to **yubi.co/wwyk**.

03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys can work with over 1,000 applications and services, including leading IAM platforms such as Microsoft, Okta, Ping and Google. YubiKeys offer platform flexibility between Apple, Google and Microsoft for your passkey implementation. To ensure that YubiKeys are integrated seamlessly across your technical stack, below are some critical questions to think about. It's considered a best practice to first answer these questions for your pilot program, then circle around for each expanded deployment.

Who

Who needs access?

Employees, contractors, third parties, supply chain

What

What passwordless approach will you take?

Smart Card, synced or device-bound passkeys

Where

Where in your environment do you require strong authentication?

Corporate systems and E-comm hardware/servers, shared workstations and POS terminals, network, apps, and dev tools

How do you manage access?

IAM, IdP, PAM, SSO, VPN

How

How does location impact deployment?

Remote, hybrid, on-premise, multi-location

What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone, tablet, POS terminals, inventory scanners

Prepare to deploy

After ensuring that your environment is YubiKey ready, it's time to create a plan to deploy YubiKeys across your organization. Optimizing deployment involves organizational change management through effective communication, training and support. Yubico offers a variety of Professional Services to help you deploy quickly:

Yubico Professional Services

Deployment planning
Rollout plan development

Integration services
Architecture and infrastructure review, vendor integration analysis

Implementation projects
Technical engagements to implement YubiKeys in your environment

Service bundles
Flexible consulting hours for when & how you need them

04. Launch

Get keys in hands and plan Go Live events

We want your deployment to be as frictionless as possible for all teams and all users. This includes simplifying deployment plans, helping you answer critical questions about how you will distribute keys to users and how you will manage the YubiKey lifecycle.

Distribution	Key management
Self-service | Channel Partner | YubiEnterprise Delivery	Onboarding | Support | Offboarding

What?

Increase awareness
Build up **user training and support** materials

Why?

Boost engagement
Demonstrate value to the **organization** and the **user**

YubiKey rollout best practice recommendations

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. We recommend that each user has a second YubiKey as a backup, and if users cannot locate a YubiKey, revoking and replacing keys is the recommended next step. If a user leaves the organization, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKeys and continue using it for their own personal accounts.

- Offer flexibility and choice since **YubiKeys are available in a variety of form factors**
- **Two YubiKeys per person** for backup
- Future-proof with **extra keys** to cover for churn or lost/ stolen keys
- Encourage **security** with personal use policies
- **Plan an event** to make the future of your organization's security exciting

Why users love the YubiKey

- Faster
- Easier
- More Secure

Go Live events

Support the launch with a series of kick-off communications that introduce the YubiKey to users—communicate early, often. The ideal Go Live communications make users **excited** about the modern features of the YubiKey.

How to?

Educate users
Have clear calls to action on **how to get started** and **how to get help**

05. Adopt

Support adoption and boost engagement

At Yubico, we believe success should not be measured by how many YubiKeys you have, but by **how many keys are being used**.

While the Go Live communications educate users on the '**what YubiKeys are**' and the '**why they are important**', support teams need to be prepared to explain the **how**, with FAQs available to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).

Effective education and awareness is important during this phase in order to showcase to your user community why the company invested in the YubiKey, and the direct benefits to users. The YubiKey's simple user experience requires minimal training and on-going support for users.

> "Folks that aren't really computer savvy are able to register so quickly, so painlessly, and then begin using their YubiKey so effortlessly and instantaneously—that's an easy win for us."
>
> **Art Chernobrov** | Director of Identity, Access, and Endpoints | Hyatt Hotels Corporation

06. Measure

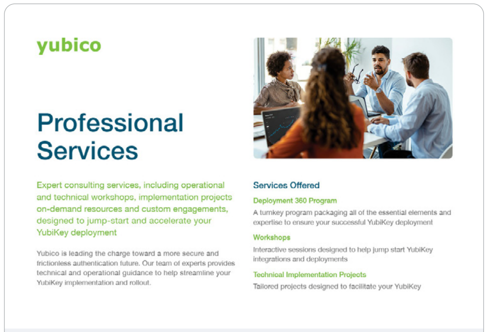
Report on security and business impact

We know **the truth is in the numbers**. Validate the pilot against these metrics, then expand to other users to increase the overall business impact.

Deployment metrics:	**Performance** metrics:	**Security** metrics:	**User** metrics:
Number of keys distributed, users activated, applications enabled	Support time reductions related to password resets, productivity increases related to login times	Security threats mitigated, simplified compliance or audit reporting	Ease of onboarding, ease of use, satisfaction

Ready for scale

Yubico offers expert consulting services, including operational and technical workshops, implementation projects, on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment at scale.



yubico

Professional Services

Expert consulting services, including operational and technical workshops, implementation projects on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment

Yubico is leading the charge toward a more secure and frictionless authentication future. Our team of experts provides technical and operational guidance to help streamline your YubiKey implementation and rollout.

Services Offered

Deployment 360 Program

A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment

Workshops

Interactive sessions designed to help jump start YubiKey integrations and deployments

Technical Implementation Projects

Tailored projects designed to facilitate your YubiKey

To download the Professional Services Solution Brief go to yubi.co/ps.

YubiEnterprise Services*		Yubico Professional Services		
YubiEnterprise Subscription	YubiEnterprise Delivery	Launch planning	Training & support	Analytics & reporting
Cost effective and flexible **YubiKey procurement**	**Global turnkey YubiKey distribution** through YubiEnterprise Delivery or local channel partners	Create a marketing and **communication plan** tailored to your users	Best practice **training & support** materials and processes	Customized **metrics** & dashboard design

* YubiEnterprise Services are available for organizations of 500 or more users.

YubiEnterprise Subscription

Gain leading, phishing-resistant authentication security for less than the price of a cup of coffee per user, per month. YubiKeys as a service, via subscription, delivers peace of mind in an uncertain world.

Learn more yubi.co/yes

YubiEnterprise Delivery

Yubico and trusted partners provide IT teams with powerful capabilities to manage delivery of hardware security keys to users globally and accelerate the adoption of strong authentication.

Learn more yubi.co/delivery

Ready to get started with passwordless?

While the path to passwordless can feel daunting, it doesn't have to be. There are many roads to passwordless and different passkey implementations offer tradeoffs for organizations and users alike. Therefore, **a 'one size fits all' approach for passkeys is sub-optimal** for an organization that houses critical customer and financial data with a range of security, compliance and scale requirements.

Device-bound passkeys using hardware security keys such as the YubiKey offer the most secure passkey authentication approach to meet the strictest compliance requirements. A set of deployment best practices that have already helped hundreds of organizations efficiently get on the bridge to passwordless can help you demystify how to get started.

Modern enterprises recognize that **security as a service** can take all the guesswork out of achieving success. When you choose YubiKeys as a Service, you get to make decisions as you go with custom insights and help from Yubico experts, simplifying the process of scaling YubiKeys and delivering passwordless experiences to wider circles of users as your business needs grow. We include success guides and priority support to help you be successful as quickly as possible.

If you want a closer partnership on any of the six steps of this plan, Yubico's Professional Services team is here to help.

Contact us
yubi.co/contact

Learn more
yubi.co/ps

Sources

[1] S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023

[2] IBM, 2022 Cost of Data Breach Report, (Accessed August 12, 2022

[3] Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (March 2, 2020)

[4] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (Accessed September 14, 2021)

[5] S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023

[6] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

yubico

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico’s solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, 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.

For more information, please visit: www.yubico.com.