



BEST PRACTICES GUIDE

How to create phishing-resistant users with fast, out-of-the box YubiKey FIDO activation with Okta

Six deployment best practices to accelerate phishing-resistant adoption at scale with Yubico and Okta



\$4.88 million



USD global average **account data breach cost**¹

74%



percentage of breaches that can be traced back to a human element



Phishing-resistant authentication has to be secure. But it also has to be IT and user-friendly. Okta and Yubico give customers the security and flexibility needed to protect their enterprise resources.”

Stephen Lee

VP Technical Strategies & Partnerships
Okta

Go passwordless with phishing-resistant users that create phishing-resistant enterprises

Individuals have always been the target of cyber threats, but these threats are at their highest levels since the pandemic. The **average cost of a data breach jumped to \$4.88 million** from \$4.45 million in 2023, the highest increase since the pandemic,¹ but that isn’t the only expense organizations face in the fight against cyber attacks. Annually, organizations spend \$1M USD² on employee password resets and \$5.2M USD³ on lost productivity due to account lockouts.

Because the majority of breaches (74%⁴) can be traced back to the human element, including situations such as stolen credentials and phishing, enterprises face tremendous pressure to not only adopt phishing-resistant multi-factor authentication (MFA), but to fortify it by combining the strength of leading security solutions from organizations like Okta and Yubico.

Despite investments in MFA and the implementation of phishing-resistant authentication, organizations remain susceptible to phishing attacks



“User carelessness” was the most common cause of sensitive information loss in worldwide organizations in 2023⁵



83% of organizations who experienced a phishing attack in 2023 had a form of MFA in place that cyber criminals bypassed⁶



Over 60% of compromise factors come from gaps in users’ credential lifecycle that attackers can exploit with relative ease⁷

Because phishing-resistance starts and ends with the user, enterprises need to think beyond phishing-resistant MFA and laser focus on creating **phishing-resistant users**. The only effective approach to remove phishing from an organization’s threat landscape is to ensure that every user within the organization becomes phishing-resistant—**and that resistance must move with the users no matter how they work, where they work, across devices, platforms and systems**. Deploying phishing-resistant authentication across the entire user lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

What about passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences.

- **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.
- **Device-bound passkeys on general purpose devices** such as smartphones, laptops and tablets offer enterprises greater control of their FIDO credentials compared to synced passkeys but are still backed by a password and offer weak security.
- **Device-bound passkeys on modern FIDO hardware security keys** offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach, organizations 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 regulated industries.

Creating phishing-resistant users with Yubico and Okta


As FIDO Alliance members, Yubico and Okta are dedicated partners in helping to deliver strong phishing-resistant authentication solutions based on **FIDO2** and **certificate-based authentication (CBA)** standards, while also simplifying access. Both Yubico and Okta's missions align to ensure we deliver the highest standards in phishing-resistant solutions that thwart security threats.

The YubiKey, made by Yubico, is a hardware security key that supports **phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimized user experience**. The YubiKey is a multi-protocol key, supporting both PIV/Smart Card and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy on-premises and modern cloud environments, helping organizations **bridge to a passwordless future**.


YubiKeys secure resources with Okta Adaptive MFA, protecting critical assets, and together, they give users complete control over identity and access. With just a simple insertion and finger tap of a YubiKey, a user can authenticate to Okta and access any enterprise application. Okta and YubiKey platforms support Microsoft Windows 7 or later, macOS x 10.10 or later, and mobile devices. Plus, Okta Desktop MFA for macOS supports all FIDO2 YubiKey models for authenticating into Apple computers with online access, which reduces friction by enabling passwordless desktop access without sacrificing security. Desktop MFA for Windows will also support FIDO2 Yubikeys in passwordless authentication flows, in addition to the support of OATH YubiKeys versions 5.0 and up for offline Windows access.

The total economic impact of YubiKeys⁸:


Strongest security
Reduce risk by
99.9%


Fast
Decrease time to authenticate by
>4x


Reduce costs
Reduce support tickets by
75%


High return
Experience ROI of
203%

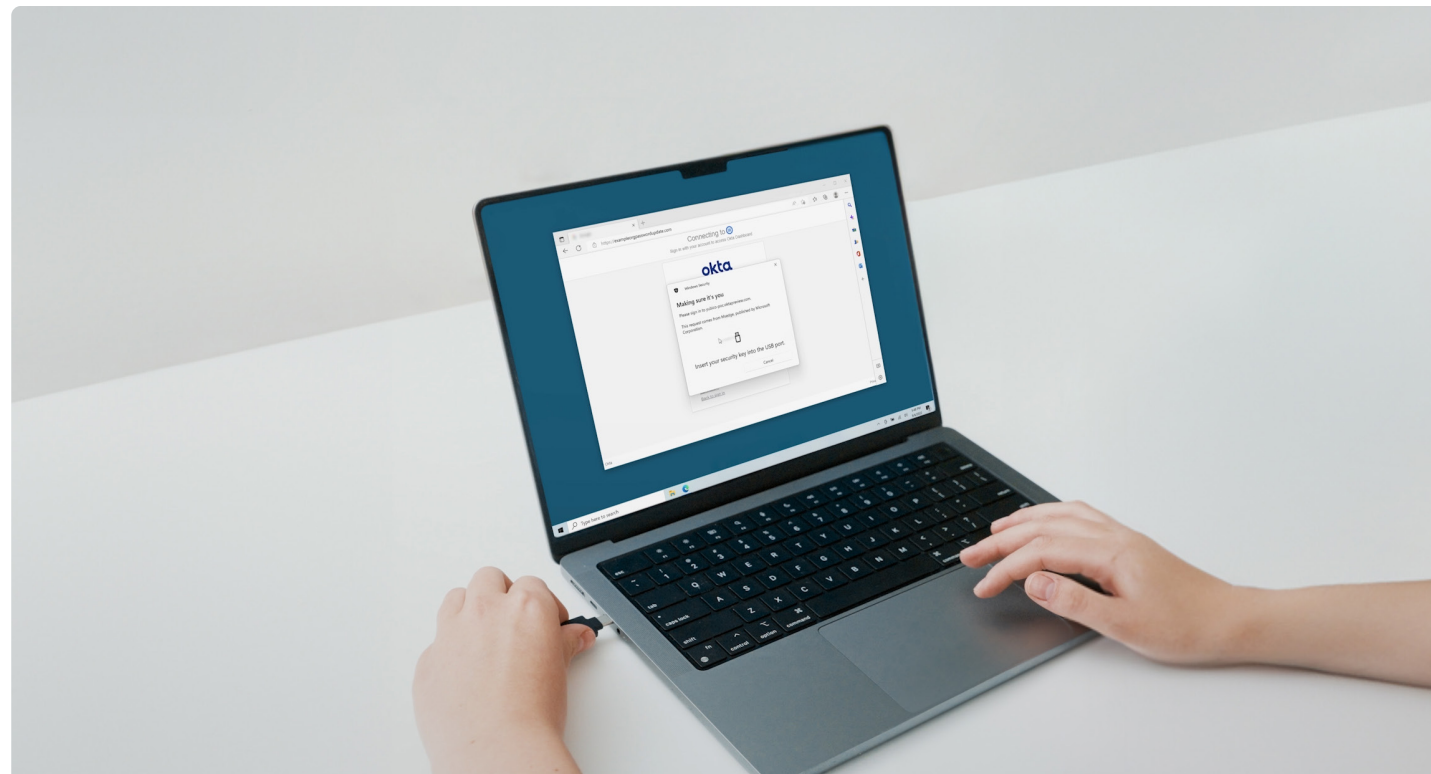
The YubiKey is proven to deliver significant business value to large enterprises at scale, delivering an ROI of 203%, while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

Yubico FIDO Pre-reg with Okta: The easiest way to create phishing-resistant users

Given the threat landscape and the shift to modern work environments, creating phishing-resistant users by combining the might of Okta's Adaptive MFA with a hardware security key like the YubiKey is a simple, streamlined way to create an enterprise that's truly phishing-resistant.

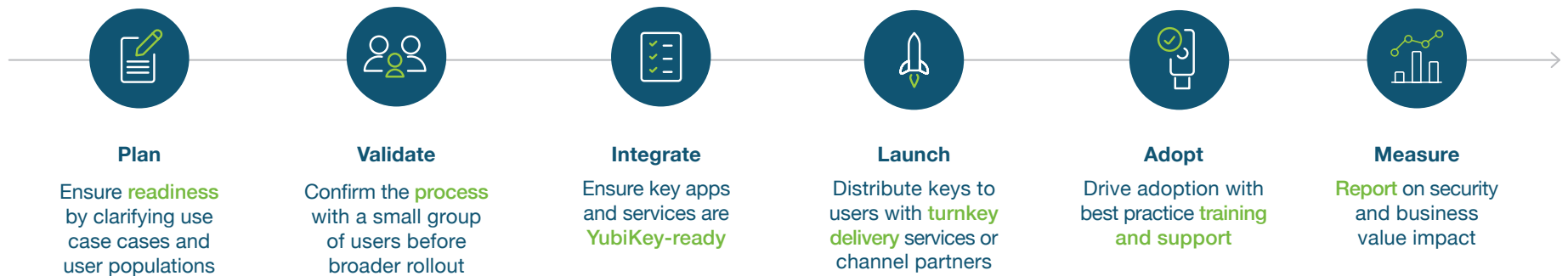
With Yubico FIDO Pre-reg, enterprise users can experience secure passwordless access to their online accounts in minutes using the most secure form of passkey authentication while reducing the burden on their admins and users. Manual user registration is eliminated, as users receive security keys that are pre-registered with Okta by Yubico during production and shipped directly to the user, whether in corporate or residential locations.

But how do you start the journey? The remainder of this guide will detail six key best practices for a successful YubiKey deployment in your Okta environment.



Six key best practices to accelerate the creation of phishing-resistant users at scale

Getting started is easy. Based on Yubico's experience assisting thousands of customers to deploy phishing-resistant MFA, we have created a six step deployment process to plan for and accelerate the creation of phishing-resistant users at scale.



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. While your end goal will be to implement phishing-resistant MFA to all users, it is important to rank use cases and user populations based on risk, workforce location, and business impact.

“ Our team uses mobile phones, tablets, and other devices. Through Yubico, I need to partner indirectly with Microsoft to understand what they have, what they offer, and how it works with the YubiKey. The YubiKey works to replace one-time passwords, it works as multi factor authentication, it factors all that into one easy to use device. I was able to implement it with my forward thinking methods. I feel like it’s put me in the top 1% of public sector for implementing this using certificate-based authentication that Microsoft provides. I am freed up to focus on servicing the people in my city.”

Jason Rucker
Director of Information Technology
City of Southgate, Michigan

Determine use cases

Top scenarios for modern, phishing-resistant authentication



Privileged access

Protect sensitive data and targeted employees who have elevated access to systems or data.



Shared workstation

Enable secure and efficient access to shared computers (e.g. customer facing and manufacturing environments, call centers).



Remote work

Add an extra layer of protection, providing secure access to VPN, IAP, IAM, and IdP platforms.



Mobile restricted

Secure sensitive environments where mobile devices are not allowed (e.g. call centers, manufacturing environments, server rooms, clean rooms, hardened rooms)

User groups



Office workers

Sophisticated attacks and lateral escalations make every user a privileged user. Improve security and productivity for office workers.



Third party

Protect third-party access to systems and data.



End customers

Protect customer accounts from fraud & build loyalty and trust with deployments to key customer segments.

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 phishing-resistant users across the organization. It's important to have buy-in across all teams to ensure a smooth rollout:



Engage Yubico experts as needed

With a tried and true process that thousands of organizations have followed already, and with the YubiKey as a Service subscription model that offers faster, more cost-effective rollouts to in-office and remote employees and third-party vendors, Yubico offers flexible solutions to streamline authentication. No matter where you are on your MFA journey, 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	
 YubiKey as a Service	 YubiEnterprise Delivery	 Deployment 360	 Deployment planning
Simplifies how organizations procure, upgrade and support YubiKeys i.e. Yubico FIDO Pre-reg	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Turnkey planning, technical integration and deployment support	Jump start with workshops & projects to review use cases or develop a customized strategy

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

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 throughout the process. Practice, learn, course correct where needed, then move forward with expansion and future rollouts of YubiKeys to the rest of your organization. Use the following steps to conduct a conclusive and easily repeatable process to begin testing and implementing the use of YubiKeys:

03. Integrate

Ensure your Okta environment is **ready for Yubico FIDO Pre-reg**

With security only being as strong as its weakest link, even the most stringent security measures would not be effective if users refuse to adopt it. Okta and Yubico have made adoption simple and seamless with Yubico FIDO Pre-reg.

To get started using Yubico FIDO Pre-reg with Okta and Okta Workflows, the following must be in place:

- YubiKey as a Service program with subscription pricing plan
- An Okta Identity Engine (OIE) tenant with Adaptive MFA and Okta Workflows entitlements
- The Yubico FIDO Pre-reg Okta Workflows template



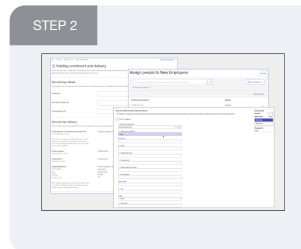
Yubico FIDO Pre-reg: Easier for admin team

No need for manual registration. Save on time, labor, and costs.

While the traditional YubiKey adoption process is designed for quick deployment, Yubico FIDO Pre-reg reduces the process even further to accelerate enterprises' creation of phishing-resistant users.



Your admin is preparing to deploy YubiKeys using Yubico FIDO Pre-reg with Okta.



They start the YubiKey request using an automation trigger...
*The Admin UI is one way to request a YubiKey; this solution has the flexibility to allow various request triggers.



...which initiates Okta Workflows behind the scenes.



Integration with your HR system provides shipping info for your employee to Okta Workflows.



The key is sent from Yubico Enterprise fulfillment pre-enrolled with the employee's Okta credentials.



Later, the employee is provided their PIN separate from the shipped YubiKey in order to prevent interception.



Your employee inserts their YubiKey, enters their PIN, taps the device, and is authenticated using secure FIDO2 credentials.



...and on Day 1 they can quickly and securely access everything they need to get started!

Additional support is always available

Yubico Professional Services			
			
Deployment planning	Integration services	Implementation projects	Service bundles
Rollout plan development	Architecture and infrastructure review, vendor integration analysis	Technical engagements to implement YubiKeys in your environment	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
Yubico FIDO Pre-reg Self-service YubiEnterprise Delivery Channel Partner	Onboarding Support Offboarding

YubiKey rollout best practice recommendations



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 employee turnover or lost/stolen keys



Encourage **security** with personal use policies



Plan an event to make the future of your organization's security exciting

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. Aside from being secure, durable, and reliable, the YubiKey is also a fun way to maintain security.

Impress on your end users how simple and fast it is to use. Encourage their confidence in doing their job more securely and faster, knowing that they are protected by a strong and modern authentication method while emphasizing the cool, sleek, and compact design of the YubiKey, which fits easily in your pocket or on your keychain. You might even want to share your experience with your colleagues or friends, and encourage them to try it out too.



Why users love the YubiKey



Faster



Easier



More Secure

Yubico FIDO Pre-reg: Turnkey for users

Easy 2-step activation. Secure passwordless access in minutes.



My company is providing a more secure and seamless sign-in experience, making it easier and faster for me to log in.



I receive a PIN from my company.



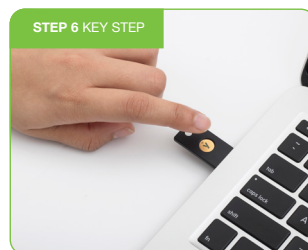
I receive my YubiKey shipped directly to me.



I log into my laptop.



I go to my company's Okta login page.



I insert my Yubikey.



I type in the PIN that I was provided and tap the YubiKey.



I successfully authenticate to Okta and can work securely in just a few easy steps.



What?

Increase awareness

Build up **user training** and support materials



How to?

Educate users

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



Why?

Boost engagement

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



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 users are using their YubiKeys.

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 '**how YubiKeys work**'. Using an FAQ to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key) is recommended and introduction sessions and team chats for follow-up questions with experts are helpful approaches to ensure a smooth onboarding of YubiKeys to your organization.



06. Measure

Report on security and **business impact**

We know the truth is in the numbers. Validate your initial deployment 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

YubiKey as a Service



Read the solution brief yubi.co/6ev

Yubico Professional Services



Read the solution brief yubi.co/6fu

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.

YubiEnterprise Services*

YubiKey as a Service

Cost effective and flexible
YubiKey procurement

YubiEnterprise Delivery

Global **distribution** to remote
and in-office locations

Yubico FIDO Pre-reg

Go passwordless at speed
and scale **with turnkey FIDO
activation** for YubiKeys.

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

Yubico Professional Services

Launch planning

Create a marketing and
communication plan tailored
to your users

Training & support

Best practice **training & support**
materials and processes

Analytics & reporting

Customized **metrics &**
dashboard design

YubiEnterprise Services*



YubiKeys as a Service

Yubico FIDO Pre-reg



YubiEnterprise Delivery

Simplified YubiKey distribution

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

Yubico Professional Services



Deployment 360

Service hour bundles



Workshops

Implementation projects



Ready to get started?

There is no question that phishing-resistant users are the solution to secure Okta environments against modern cyber threats. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

Don't know where to start? The good news is that you don't need to know all the answers upfront about how many keys to buy, what kind, how to integrate them into your environments, or how to get keys in the hands of end users. No matter where you are on your MFA journey, we'll meet you there and help to address your concerns, questions, and interest in what YubiKeys can do for your organization.

Security as a service can take all the guesswork out of achieving success. When you choose YubiKey as a Service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys 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/microsoft yubi.co/wwwyk yubi.co/yes

Sources

- ¹ IBM, [Cost of a Data Breach Report 2024](#)
- ² Forrester Research, Inc, [Optimize User Experience With Passwordless Authentication](#), (March 2, 2020)
- ³ Ponemon Institute, [2019 State of Password and Authentication Security Behaviors Report](#), (Accessed September 14, 2021)
- ⁴ Verizon, [2023 Data Breach Investigations Report](#), (June 6, 2023)
- ⁵ Statista, [Most common causes of sensitive information loss in worldwide organizations in 2023](#), (March 2024)
- ⁶ Egress, [Must-know phishing statistics for 2024](#), (January 2024)
- ⁷ Google Cloud, [Threat Horizons Report](#), (August 2023)
- ⁸ Forrester, [The Total Economic Impact™ Of Yubico YubiKeys](#), (September 2022)



About 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 hardware-based passwordless authentication using the highest assurance passkeys to customers in 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.