



BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA to secure healthcare

Six deployment best practices to accelerate adoption at scale



\$10.93M



global average data breach cost
(up 53% since 2020¹)

82%



breaches involve **data stored in
the cloud**²

Up to 99.9%



protection offered through **modern
phishing-resistant MFA**⁴

Phishing-resistant MFA is a mandated requirement of Office of Management and Budget Memo 22-09⁵ as part of the federal move to Zero Trust under White House Executive Order 14028,⁶ applicable to many healthcare organizations working across the public and private divide, but is also the end-goal state for any organization on the path to Zero Trust.⁷ In October 2023, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS) released a cybersecurity toolkit that includes recommendations for Zero Trust and MFA.⁸

Choosing the right MFA approach for healthcare

Healthcare and public health (HPH) organizations face mounting pressures to modernize authentication and implement Zero Trust in response to cyber threats, which are not only costly (\$10.93M USD global average data breach cost, up 53% since 2020¹) and disruptive, but the majority of which (82%²) can be traced back to the human element including situations such as stolen credentials and phishing.

While any form of multi-factor authentication (MFA) offers better security than passwords, **not all MFA is created equal**. Legacy forms of MFA including mobile-based authenticators such as SMS, one-time passcodes (OTP) and push notification apps are not phishing resistant and can be easily bypassed by malicious actors at a penetration rate of 10-24%.³

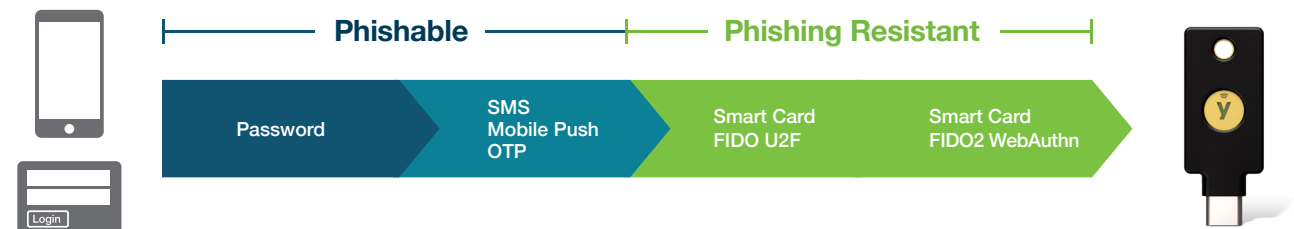
Further, the **MFA strategy you choose can deliver on a vastly different ROI** in terms of cost, user experience, and coverage at scale. In truth, legacy authentication carries many hidden governance and support costs as well as coverage challenges—where users lack devices, where mobile-restrictions apply within an environment, network connectivity challenges, and the challenges associated with clean rooms and gloved environments.

Modern, phishing-resistant MFA can help meet these complex authentication and security challenges across healthcare, offering protection up to 99.9%⁴ and modern login flows such as passwordless.

What is phishing-resistant MFA?

Phishing-resistant MFA refers to an authentication process that is highly resistant to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intention to initiate through deliberate action.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, referenced by the HPH Sector Cybersecurity Framework Implementation Guide,⁹ two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and the modern FIDO2/WebAuthn authentication standard.



“Speed is the operative word. With YubiKeys we have been able to speed up the login process from over 40 seconds down to less than 10 seconds, which means that healthcare personnel have more time to care for their clients.”

Matthias van Alphen | CEO & Founder, Adapt

YubiKey offers phishing-resistant MFA at scale

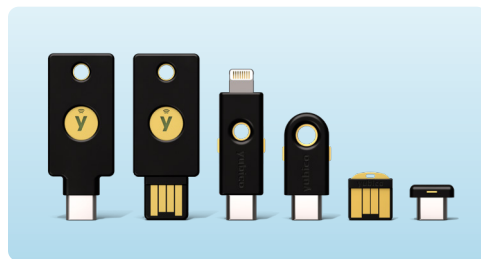
Yubico created the **YubiKey**, a hardware security key that supports **phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimized user experience.**

The YubiKey is a multi-protocol security key, supporting both **Smart Card/PIV** and **FIDO2/WebAuthn** standards along with OTP, FIDO U2F and OpenPGP, which integrates seamlessly into both legacy and modern environments, helping organizations **bridge to a passwordless future.**

Hardware security keys such as the YubiKey are an ideal option for **strong phishing-resistant MFA and passwordless** because they don't require external power or batteries, or a network connection—a user can use a single key to authenticate seamlessly across multiple devices and to over 1,000 products, services and applications, leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.

The YubiKey is highly durable, dust proof, crush- and water-resistant (IP68 certified), making it suitable for **shared workstation and clean rooms and gloved environments.** Yubico also offers the YubiKey 5C NFC edition, supporting tap-and-go authentication on NFC-enabled devices or to authenticate to an IAM (Ping, Okta, Duo) to perform SSO to other applications. When combined with a silicone wristband, the YubiKey can solve critical healthcare pain points around sanitation and efficiency.

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%**,¹⁰ all while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.



The YubiKey 5 Series

From left to right: YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano



Strong 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%



Durable

IP68 certified,
dust-proof,
crush-resistant and
water-resistant

What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are simply passwordless-enabled FIDO credentials that enable a move away from passwords, delivering phishing resistance. There are different passkey implementations:

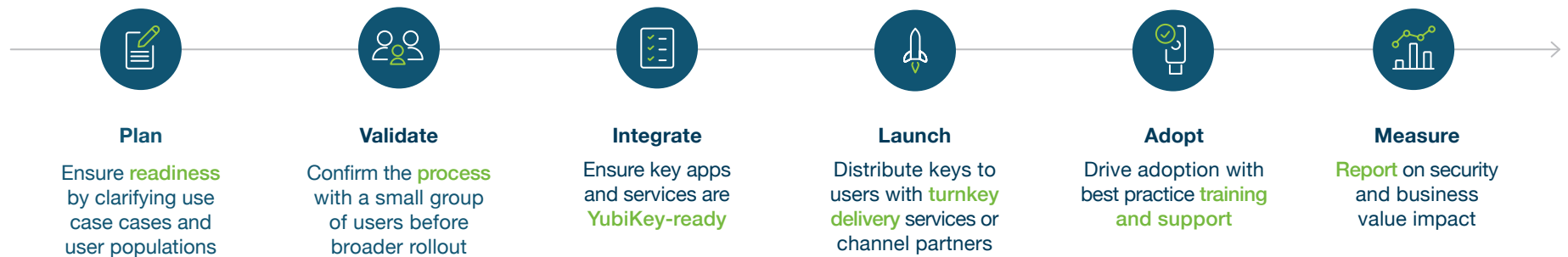
- **Synced passkeys** live on a smartphone, tablet or laptop and can be copied between devices. While synced passkeys enable easier account recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.
- **Device-bound passkeys** offer greater manageability than synced passkeys, and therefore better suited for the enterprise. However, there are different types of device-bound passkeys and those that live in hardware security keys are known to offer the highest security assurance and provide enterprises with the trusted credential lifecycle management and attestation abilities they need to have the strongest security, the simplest user onboarding and credential/account recovery experience across devices and platforms, and stay in compliance with the most stringent requirements across industries.

Given the threat landscape, the reasons for using modern, flexible phishing-resistant MFA grow on a daily basis. **But how do you start the journey?** The remainder of this guide will detail six key best practices for a successful YubiKey deployment.



Six key best practices to accelerate the adoption of the YubiKey

Getting started is easy. Based on Yubico's experience assisting hundreds of customers to deploy phishing-resistant MFA across healthcare environments, we have created a six step deployment process to plan for and accelerate adoption of the YubiKey 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. Rank use cases and user populations based on risk, workforce location, business impact and ease of technical integration.

Determine use cases



Privileged access

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



Shared devices

Protect shared workstation/device users while maintaining convenience and patient security.



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).



Software supply chain

Access and data exchange associated with third party software and code.



Clean rooms

Securely and quickly authenticate using a single tap of the YubiKey with a wearable, leveraging NFC capability.



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.



Digital patient services

Protect patient access to online healthcare and payment services; build brand loyalty and trust.

User groups

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 MFA 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 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 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	
 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 with workshops & projects to review use cases or develop a customized strategy

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

“It’s worth noting how simple it was to implement YubiKeys. You link a YubiKey on the back end, but the user doesn’t have to do anything themselves. So you don’t need steering committees or working groups to encourage user adoption.”

Matthias van Alphen | CEO & Founder, Adapt



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.**

03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys work with over 1,000 applications and services, including leading IAM platforms such as Microsoft, Okta, Ping and Google and VPN applications such as Pulse Secure and Cisco AnyConnect. 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 priority use cases, then circle around for each expanded deployment.

Browse the [Works with YubiKey](#) catalog

Who

Who needs access?

Employees, contractors, third parties, supply chain

What

What authentication approach will you take?

MFA (Password and strong second factor), passwordless

Where

Where in your environment do you require strong authentication?

Critical infrastructure elements, network, applications, developer tools.

How do you manage access?

IAM, IdP, PAM, SSO, VPN, ZTNA

How

How does location impact deployment?

Remote, hybrid, on-premise, multi-office

What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone, tablet

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.



Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. Browse YubiKey compatibility [here](#).

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 and 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

Self-service | Channel Partner | YubiEnterprise Delivery



Key management

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 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.





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



It's imperative to have that added level of security to protect our vulnerable clients. The YubiKey makes it extremely easy for us to have that oversight.”

Sylvia Rosemond | CEO, Independent Disability Services



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, 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).




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



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.

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.

Yubico is leading the charge toward a more secure and trustworthy authentication future. Our team of experts provides



Download the Professional Services Solution Brief [here](#)

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

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





Ready to get started?

There is no question that phishing-resistant MFA is the solution to secure healthcare organizations against modern cyber threats and to solve the many critical authentication pain points across IT and OT environments. Though the path to phishing-resistant MFA 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.

Security as a service can take all the guesswork out of achieving success. When you choose YubiKeys 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 you get started.



Contact us
yubi.co/contact



Learn more
yubi.co/healthcare

Sources

- ¹ IBM, [2023 Cost of Data Breach Report](#), (July 24, 2023)
- ² Verizon, [2022 Data Breach Investigations Report](#), (Accessed May 10, 2023)
- ³ Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ⁴ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- ⁵ OMB, [M-22-09](#), (January 26, 2022)
- ⁶ The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- ⁷ PCI, [PCI DSS: v4.0](#), (March 2022)
- ⁸ HHS, [Health Industry Cybersecurity Practices, 2023 Edition](#), (October 25, 2023)
- ⁹ HHS, [Health Care and Public Health Sector Cybersecurity Framework Implementation Guide Version 2](#), (March 2023)
- ¹⁰ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)



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.