yubico

BEST PRACTICES GUIDE

How to get started with modern, phishing-resistant MFA

Six deployment best practices to accelerate adoption at scale

$4.88 million

cost of data breach[2] in 2024

$1 million

cost for employee password resets

$5.2 million

cost for lost productivity due to account lockouts

Choosing the right MFA approach

Passwords remain the most common form of user authentication, used by 91% of organizations[1]—but passwords are fundamentally broken, offering weak security and a poor user experience. Globally, the average data breach carries a high cost ($4.88M USD[2]), not to mention the annual costs associated with employee password resets ($1M USD[3]) and lost productivity due to account lockouts ($5.2M USD[4]). Currently, weak passwords account for 50% of compromises of enterprise cloud environments.[5] While any form of multi-factor authentication (MFA) will offer better security than passwords, **not all MFA is created equal.**

Basic or legacy forms of MFA 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. In fact, 68% of data breaches involve the human element, with stolen credentials now the most popular entry point for breaches.[6]

Enterprises across the globe are turning to MFA to protect against cyber attacks, but also to support remote access (34%), support privileged access (26%), improve user convenience (24%), support Zero Trust initiatives (25%) and meet compliance requirements (21%).[7] MFA, and more specifically phishing-resistant MFA is now a standard requirement for many global cybersecurity regulations and is a growing requirement for organizations to either qualify for cyber insurance or eliminate costly increases in premiums, sub-limits or exclusions.

Multiple pressure points drive organizations toward MFA

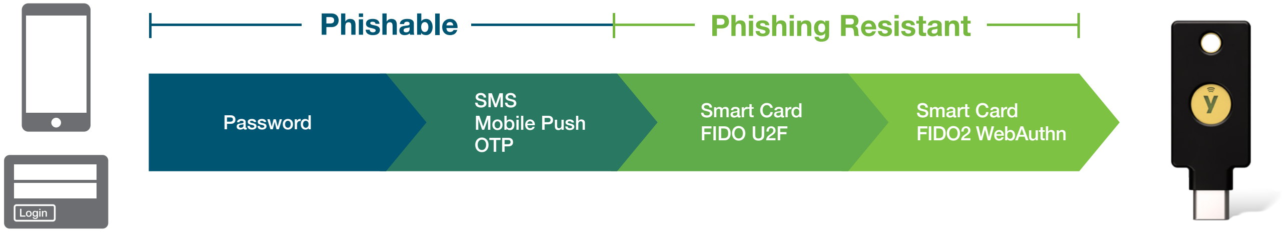
External pressures			Internal pressures				
Cyber threats	Compliance	Cyber insurance requirements	Remote access	Privileged access	Support complexity	User convenience	Zero Trust initiatives

Every organization has different business scenarios, third parties they work with and end users. Whether you're supporting shared workstations, remote employees, external vendors and even end-customers, it's important to choose an MFA approach that is secure, flexible and agile to support evolving business needs. To meet these enterprise needs and to stop phishing attacks, ransomware and account takeovers before they start, organizations are turning to phishing-resistant MFA.

What is phishing-resistant MFA?

Phishing-resistant MFA refers to an authentication process that is immune 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, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/smart card and the modern FIDO2/WebAuthn authentication standard, also known as passkeys.



Global mandates for phishing-resistant MFA have emerged: White House Executive Order 14028,[8] Office of Management and Budget (OMB) Memo 22-09[9] and the National Security Memorandum/NSM-8[10] in the US, NIS2[11] for the EU and the global PCI DSS v4.0 standard.[12]

Contact center specialist Afni was able to reduce its cyber insurance premiums by 30% by demonstrating how YubiKeys reduced its risk profile.

To read the Afni Case Study
go to yubi.co/Afni

> “When I’m going down by a third and others are going up by 20% or higher, that’s a really big win. In fact, I estimate our premiums are nearly half of what others are having to pay.”

Brent Deterding | CISO | Afni

YubiKey offers phishing-resistant MFA

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 key, supporting both PIV/smart card and FIDO2/WebAuthn/passkey 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 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 cultivates phishing-resistant users which then creates phishing-resistant enterprises.

Modern hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require external power or batteries, or a network connection—a user can use a single key for secure access to multiple applications and services with the secrets never shared between services. The YubiKey is proven to deliver significant business value to large enterprises at scale, delivering an ROI of 203%,[13] while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

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

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

> "Any form of MFA is better than just a username and password, but most MFA can still be phished. It didn't take long to realize we needed stronger authentication for all employees that couldn't be phished. YubiKeys made the most sense. And when I first used a YubiKey Nano, I loved the experience—I left it in my computer and simply touched it to authenticate."
>
> **Daniel Jacobson** | Senior Director of IT | Datadog

What makes the YubiKey phishing-resistant?

1. YubiKeys use secure public key cryptographic technology to generate unique public and private key pairs for each service. Private keys are stored securely on the YubiKey, making them hardware-bound and non-copyable, unlike legacy MFA.

2. Once users register a YubiKey to a service, it is bound to that specific URL, and the registered credential cannot be used to log in to a fake website. So, even if a user is fooled, the YubiKey never is.

3. The touch sensor on the YubiKey verifies that the user is a real human and that the authentication is done with real intent. This prevents remote and man-in-the-middle attacks.

4. YubiKeys authenticate through the phishing-resistant FIDO open standard (in addition to smart card), enabling access to personal and work applications and services, providing high security and privacy at scale.

What are passkeys?

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

Given the threat landscape, the need for modern phishing-resistant MFA gets clearer on a daily basis. To enhance flexibility and agility, modern organizations are pivoting to hardware-based phishing-resistant MFA as a service, an option that allows organizations to adopt right-sized solutions to their environment, as their business needs evolve. But how do you start the journey to phishing-resistant MFA?

The remainder of this guide will detail six key best practices for a successful MFA and YubiKey deployment.

Six key best practices to accelerate the adoption of phishing-resistant MFA

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

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 workstations

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, & 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 as part of an effort to effectively secure the supply chain.

End customers

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

Assemble key stakeholders

While the number of resources on 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.

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 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 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 and **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. **Practice, learn and then move forward with expansion.**

03. Integrate

Ensure your environment is YubiKey-ready

YubiKeys can work with a range of applications and services including leading IAM platforms such as Microsoft, Okta, Ping and Google and offer the best security for access to sensitive data and applications for corporate and remote employees. YubiKeys enable phishing-resistant MFA for leading VPN applications such as Pulse Secure and Cisco AnyConnect, as well as other remote access applications. 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.

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

How

How does location impact deployment?

Remote, hybrid, on-premise, multi-office

What types of devices need to be supported?

Desktop, laptop, smartphone (BYOD or owned)

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**.

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 and ongoing assistance

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

What?

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

Why?

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

> We’re going down the same path as the most advanced organizations in the world. And we’re all rolling out YubiKeys.”
>
> **Mike Schwermin** | CIO | Afni

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 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

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.

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 and videos 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.

How to?

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

06. Measure

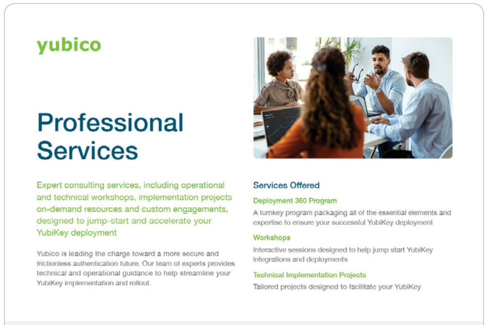
Report on security and business impact

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		
YubiKey as a Service	YubiEnterprise Delivery	Launch planning	Training and support	Analytics and 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 and support** materials and processes	Customized **metrics** and dashboard design

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

YubiKey as a Service

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/YKSvc

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?

There is no question that phishing-resistant MFA is the solution to secure enterprises 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.

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.

Yubico Professional Services

Deployment 360

Service hour bundles

Workshops

Implementation projects

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

Learn more
yubi.co/ps

Contact us
yubi.co/contact

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, 2024 Cost of Data Breach Report, (Accessed August 2, 2024)

[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] Google Cloud, April 2023 Threat Horizons Report, (April 2023)

[6] Verizon, 2024 Data Breach Investigations Report, (Accessed May 28, 2024)

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

[8] The White House, Executive Order on Improving the Nation's Cybersecurity, (May 12, 2021)

[9] OMB, M-22-09, (January 26, 2022)

[10] The White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 2020)

[11] European Parliament, The NIS2 Directive, (February 2023)

[12] PCI, PCI DSS: v4.0, (March 2022)

[13] 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 hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

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