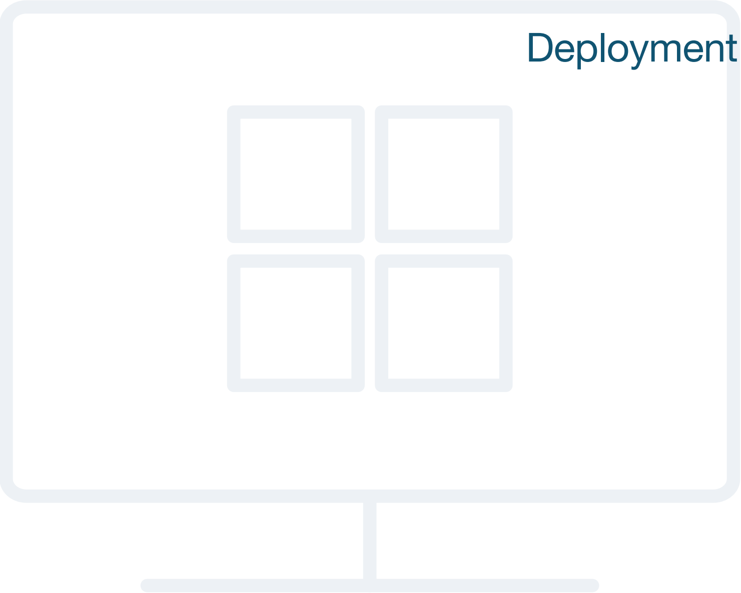
yubico | Microsoft

BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA for your Microsoft environment

Deployment best practices to accelerate YubiKey adoption at scale



$4.88 million

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

Accelerate Zero Trust with phishing-resistant MFA

Organizations face mounting pressures to implement **Zero Trust to support their Microsoft environments.** Work from home and modern work environments have become the target of new cyber threats which are not only costly ($4.88M USD global average data breach cost[1]) and disruptive, but the majority of which (74%[2]) can be traced back to the human element including situations such as stolen credentials and phishing.

With their increased use of advanced tools like machine learning and artificial intelligence to craft predatory emails that are nearly indistinguishable from the expected real message, the threat of cyberattacks looms larger than ever. These breaches not only disrupt operations which can lead to significant financial losses and reputational damage, the longer term impacts provide a further unknown and risk to your organization. Remove the threat that stolen credentials pose for your organization with a Zero Trust policy that enforces all individual or thing access is properly verified before being given access to the network and data.

This guide will provide you with best practices to enhance your organization's security posture, focusing on the critical role of phishing-resistant multi-factor authentication (MFA) and how it fits within the deployment of your planned or existing Microsoft ecosystem.

Respectfully enforcing identity and creating phishing-resistant users

The journey to Zero Trust is multifaceted and, depending on the size of your organization, can span months to years. Identity is a core building block that can help jumpstart your journey and offers immediate ROI in terms of security, operational efficiency and user productivity. Enterprises across the globe are turning to MFA to protect against cyber attacks and support Zero Trust initiatives (25%), but also to support remote access (34%), support privileged access (26%), improve user convenience (24%), and meet compliance requirements (21%).[3] While any form of MFA will offer better security than passwords, **not all MFA is created equal** and Zero Trust requires a movement away from legacy forms of MFA.

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 at a penetration rate of 10-24%.[4] In contrast, modern **phishing-resistant MFA** can offer protection up to 99.9%.[5]

Phishing-resistant MFA is a mandated requirement of Office of Management and Budget Memo 22-09[6] as part of the federal move to Zero Trust under White House Executive Order 14028,[7] but it is also a requirement for other industries (e.g. any subject to the PCI DSS v4.0 standard[8]) and is the end-goal state for any organization on the path to Zero Trust.[9]

> “At Microsoft, we are committed to providing the highest levels of protection for our customers. Phishing-resistant multi-factor authentication (MFA) is a critical component to a healthy and secure cybersecurity practice for any organization. Through our FIDO2 Provisioning API integration with Yubico solution, our enterprise customers can quickly implement YubiKey, enhancing employee protection more efficiently. Together, we are empowering our customers to safeguard their digital identities and protect their data against ever-evolving threats.”
>
> **Natee Pretikul** |
> Principal Product Management Lead |
> Microsoft Security Division

For more than a decade, Yubico has partnered with Microsoft to ensure businesses worldwide and the Microsoft solutions they rely on remain secure and resistant to phishing attacks. Recognizing the critical importance of MFA and as part of their Secure Future Initiative, Microsoft has mandated MFA for all Azure users. This decisive move underscores the necessity of robust authentication measures to safeguard end users against phishing threats. Yubico fully supports this mandate and urges organizations to not only comply with it but to also broaden the implementation of modern MFA across their entire infrastructure.

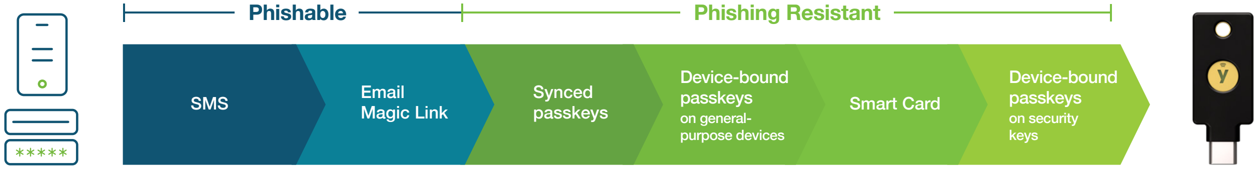
Phishing-resistant users are the core element to a phishing-resistant organization. When each user can work confidently knowing that they are resistant to the phishing attacks that level other organizations with debilitating attacks, your help desk, IT departments, sales, marketing, and others can work together knowing their credentials are secure. From phishing-resistant registration to authentication to account recovery, modern hardware security keys secure all points in the account lifecycle to create phishing-resistant users that bring your organization to Zero Trust, passwordless operations.

The YubiKey also respects user privacy by ensuring that no personal data is stored on the device itself. It operates without the need for any personally identifiable information (PII) to be transmitted during authentication, safeguarding user identities to your organization Identity Provider (IdP) or Identity and Access Management (IAM) provider of choice. By delivering phishing-resistant multi-factor authentication (MFA), the YubiKey provides a robust security solution that protects both organizational assets and individual privacy. This balance of security and privacy makes the YubiKey an essential tool for modern enterprises.

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.


Phishable
Phishing Resistant
*****
SMS
Email Magic Link
Synced passkeys
Device-bound passkeys on general-purpose devices
Smart Card
Device-bound passkeys on security keys

YubiKey offers phishing-resistant MFA

Microsoft and Yubico are FIDO Alliance members, helping to deliver strong phishing-resistant authentication solutions based on **FIDO2** and **certificate-based authentication** (CBA) standards. These solutions, coupled with Microsoft's **Conditional Access** policies, play a key role in supporting organizations on the journey to Zero Trust.

Yubico is maker of 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 standards along with OTP and OpenPGP, integrating seamlessly into both legacy on-premises and modern cloud environments, helping organizations **bridge to a passwordless future** across their entire Microsoft ecosystem.

A user can use a single YubiKey for secure access to Windows Hello for Business (WHfB) and Microsoft Entra ID protected workstations, applications and services, as well as over 1,000 other products, services and applications, with the secrets never shared between services. The YubiKey is the **only external device that supports CBA on Android and iOS** and is the **only FIPS-certified phishing-resistant solution available for Entra ID** on mobile.

The YubiKey is proven to deliver significant business value to large enterprises at scale, delivering an ROI of 203%,[10] while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

What about passkeys?

Passkeys are a new name for FIDO2 credentials, a standard that's replacing password-only 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 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.
- **Hardware-bound passkeys** exist only on a hardware key purpose-built for security, e.g. a **YubiKey,** suitable for the highest levels of authentication security and compliance assurance.
- **Software-bound passkeys** are a type of authentication credential that uses public-private key cryptography, where the private key is stored in the user's filesystem and used to verify a challenge from the application. Susceptible to malware attacks, if a user's operating system is compromised, the private key stored in the filesystem could potentially be exposed.passkeys.

Given the threat landscape and the shift to modern work environments, the need for modern phishing-resistant MFA is essential. **But how do you start the journey to phishing-resistant MFA and Zero Trust?** The remainder of this guide will detail six key best practices for a successful MFA and YubiKey deployment to your on-premise and cloud-based Microsoft ecosystem.

The total economic impact of YubiKeys:

Strongest Security
Reduce risk by
99.9%[5]

High Return
Experience ROI of
203%

More Value
Reduce support tickets by
75%

Faster
Decrease time to authenticate by
>4x

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

Getting started is easy. Based on Yubico's experience assisting customers to deploy phishing-resistant MFA, we have enhanced this six-step deployment process to plan for and accelerate the adoption of phishing-resistant MFA at scale that will get you to an organization of phishing-resistant users securely using your selected suite of Microsoft solutions.

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. 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.

Determine use cases

> "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

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 estricted

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 departments shown below can positively influence the implementation of Yubico's phishing-resistant MFA across the organization. It's important to have buy-in across all teams to ensure a smooth rollout, so working across stakeholders to create a detailed plan that outlines the steps, timeline, and resources needed for MFA deployment will be vitally important to a successful rollout.

IT	Security	Finance	Help Desk	HR/Learning & Development	Leadership	Team Leads

Engage Yubico experts as needed

With a tried and true process successfully proven across thousands of organizations worldwide, and with a 'YubiKey as a Service' model, Yubico offers flexible and cost-effective solutions to streamline authentication. No matter where you are on your Microsoft deployment and 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	
YubiKeys as a Service	YubiEnterprise Delivery	Deployment 360	Deployment planning
Simplifies how organizations 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.

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:

Select Pilot Users:

Focusing on various departments, roles, and levels of technical proficiency, begin by carefully selecting a diverse group of users to participate in the pilot testing of the Multi-Factor Authentication (MFA) implementation using YubiKeys.

By including a wide range of users, you will ensure that the feedback and insights gathered will be comprehensive and applicable across the entire organization that will help identify any potential issues or challenges that different user groups might face during the deployment.

Conduct Pilot Testing:

Proceed with onboarding the test group users using Microsoft's new API that will enable them to directly configure their YubiKeys and integrate them with your existing Microsoft solutions, such as Microsoft Entra ID or Microsoft 365.

During this phase, be sure to closely monitor the onboarding process and gather detailed feedback from the pilot users.

Pay attention to any difficulties they encounter, questions they have, or suggestions they offer.

This feedback is crucial for identifying areas that may need improvement or additional support.

Refine Process:

Based on the feedback collected from the pilot group, refine and adjust the implementation process to address any issues or concerns.

With the goal of ensuring a smooth and seamless rollout to prepare for full YubiKey deployment across your organization, this may involve updating documentation, providing additional training, or making technical adjustments to the integration.

Consider conducting follow-up sessions with the pilot group to validate that the changes have effectively resolved any issues and to gather further insights.

Phishing Simulation Exercises:

Designed to test the users' ability to recognize and respond to phishing attempts along with further enhancing the security readiness of the pilot group, conduct phishing simulation exercises.

By simulating real-world phishing scenarios, you can assess the effectiveness of the YubiKey implementation and identify any gaps in user awareness.

Use the results of these simulations to provide targeted training and improve overall security awareness.

This proactive approach will help ensure that users are well-prepared to handle phishing threats and can effectively utilize their YubiKeys to protect sensitive information.

03. Integrate

Ensure your Microsoft environment is YubiKey-ready

Microsoft and YubiKey work seamlessly together to help prevent account takeovers and help you and your teams go passwordless. Organizations can use the YubiKey with Microsoft Entra ID, Azure, GitHub, and Windows Hello for Business (WHfB) to securely authenticate to both on-premise and cloud environments along with other applications and services to secure your users' work and personal digital lives.

YubiKeys support MFA across the Microsoft ecosystem

With no shared secrets between the services, the YubiKey enables high security and privacy at scale. Organizations with existing PKI deployments can leverage the YubiKey as a smart card with Entra ID.

Integrating YubiKey with your Microsoft environment

Whether your identity directory is on premises or in the cloud, accessing personal or business accounts with Microsoft is smooth and efficient. YubiKeys provide strong two-factor, multi-factor and passwordless authentication for securing the identity access management infrastructure. The same YubiKey used for on-premises smart card deployments can be used to authenticate access to apps in the cloud through FIDO2.

Top scenarios for modern, phishing-resistant authentication

Certificate-based authentication (CBA)	CBA on iOS and Android	Conditional Access	Azure Virtual Desktop (AVD) and Remote Desktop	Passwordless authentication	Windows Hello for Business (WHfB)
Use a YubiKey as a smart card with Entra ID for application and browser sign-in.	Leverage the same YubiKey + Entra ID sign-in experience on mobile devices. **Available option:** YubiKey 5 FIPS Series.	Leverage authentication strengths or custom policies to require phishing-resistant MFA via YubiKeys (CBA or FIDO2), CBA or WHfB as well as specific key use (e.g YubiKey 5 FIPS Series)	Leverage Entra ID + YubiKey (CBA or FIDO2) to sign into AVD, remote desktop or an application inside the virtual desktop.	YubiKeys + WHfB or Entra ID provide phishing-resistant passwordless login flows to Windows 11 and Windows 10 workstations, native apps, web applications and remote desktops.	WHfB + YubIKey provides high assurance and FIDO2 phishing-resistant authentication in a portable form factor and extends phishing-resistance to use cases that lack TPM.

Works with YubiKey

In addition to Microsoft, the YubiKey works with hundreds of applications, devices, platforms, and services that you may already be using today. Check out the Works with YubiKey catalog for more information on existing integrations and how to set up your YubiKey with the countless integrations that exist.

To ensure that YubiKeys are integrated seamlessly with key applications and services you wish to secure, 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, ZTNA

How

How does location impact deployment?

Remote, hybrid, on-premise, shared workstations, multi-office

What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone, tablet

Prepare to deploy

With ready to go technical and operational workshops to help your organization achieve a smooth and seamless integration of the YubiKey, our Professional Services team offers best-in-class guidance designed to give you the knowledge and expertise to plan your YubiKey deployment from distribution to launch and fully support of your YubiKey implementation and rollout.

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

> “Our goal at Hyatt is to have every application in our stack fall under Azure single sign on. So once you’re using the YubiKey for app one, you’ll be using it for app two and three and four…”
>
> **Art Chernobrov** | Director of Identity, Access and Endpoints | Hyatt

Why users love the YubiKey

- Faster
- Easier
- More Secure

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.

Tap your security key
Christian Cartier
Tap your security key on the reader or insert it into the USB port
Sign-in options

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 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 **‘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

yubico

YubiKey as a Service

Flexible enterprise plans that help you move away from broken MFA and create phishing-resistant users at scale.

Enabling strong security while driving business acceleration

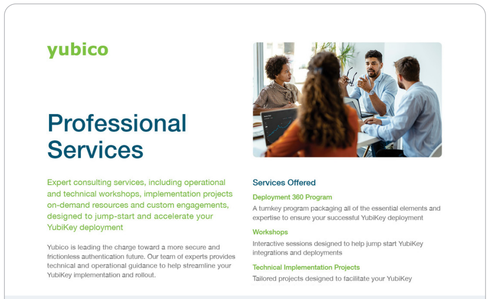
Organizations are looking for better and more efficient ways to improve security while making it easier for users to adopt best practices and enhance productivity. A single corporate security breach in 2022 cost an average of $4.35M.[1] And with compromised credentials via phishing being the most common initial attack vector, stronger and more phishing-resistant approaches such as those with modern hardware security keys offer the highest level of protection. Yubico, building on its years of helping secure some of the most

Simplify security against an ever changing cyber threat landscape

YubiKey as a Service greatly simplifies the acquisition and roll out of phishing-resistant authentication for organizations with 500 users or more, with additional cost savings.

Your business and employees are constantly evolving, from new hires and employee turnover, to remote and hybrid work environments, and support for new infrastructure needs. And with users working across desktop, mobile, shared workstations, and using the latest devices and modern authentication, you

Read the solution brief here.


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

Read the 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*

YubiKeys 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

Ready to get started?

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

YubiKeys 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.

YubiEnterprise Services*

YubiKeys as a Service
FIDO Pre-reg

YubiEnterprise Delivery

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

Yubico Professional Services

Deployment 360
Service hour bundles

Workshops
Implementation projects

Contact us yubi.co/contact

Learn more yubi.co/microsoft yubi.co/wwyk yubi.co/yes

Sources

[1] IBM, 2024 Cost of Data Breach Report, (Accessed August 5, 2024),

[2] Verizon, 2023 Data Breach Investigations Report, (June 6, 2023)

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

[4] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

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

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

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

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

[9] CISA, Zero Trust Maturity Model v 2.0, (April 2023)

[10] 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.