



BEST PRACTICES GUIDE

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

Six deployment best practices to accelerate adoption at scale



\$3.58 million



global average data breach cost¹

82%



can be traced back to the human element including situations such as stolen credentials and phishing³

Up to 99.9%



protection offered through modern phishing-resistant MFA⁵

Globally, regulators are aligning on the need for strong MFA, including, the Telecommunications (Security) Act in the UK,¹⁵ the Cybersecurity Act 2018 in Japan,¹⁶ IT Security Act 2.0 and the BSI Ordinance Determining Critical Infrastructures (BSI-KritisV) in Germany. In Australia, the Essential Eight Maturity Model (E8MM) guidelines, referenced by the Security of Critical Infrastructure Act (SOCl Act) for critical infrastructure and soon to include telecommunications,¹⁷ suggests the use of phishing-resistant MFA at maturity level two and above.¹⁸

Choosing the right MFA approach for telecommunications

Telecommunications organizations (telecoms) providing voice and data services face mounting pressure to modernize authentication and implement Zero Trust in response to cyber threats, which are not only costly (\$3.58M USD global average data breach cost¹), but are a threat to the critical services they provide. Further, insight from industry and consumer surveys indicates that privacy, security and trust are a top threat facing telecoms,² underscoring the importance of consumer expectations.

Looking broadly at all breaches, the majority (82%³) can be traced back to the human element including situations such as stolen credentials and phishing. In response, telecoms are implementing Zero Trust and strong multi-factor authentication (MFA). Although the journey to **Zero Trust** is multifaceted and can span many 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.

While any form of 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 at a penetration rate of 10-24%.⁴ In contrast, modern **phishing-resistant MFA** can offer protection up to 99.9%.⁵ Furthermore, telecoms are also driven by the need to **reduce the friction in the authentication experience** to support customer service in call center and retail environments and to support technicians in the field.

Phishing-resistant MFA is a **mandated requirement** of Office of Management and Budget Memo 22-09⁶ as part of the federal move to Zero Trust under White House Executive Order 14028,⁷ but it also has downstream implications for telecoms and is further required by the Enduring Security Framework,⁸ FTC standards,⁹ and the PCI DSS v4.0 standard.¹⁰ As phishing-resistant MFA is the end-goal state for any organization on the path to Zero Trust,¹¹ it is also a consideration under the revised Network and Information Security (NIS) 2 Directive in the EU¹² and can help simplify the implementation of standards such as ISA/IEC-62443¹³ and ISO 27001.¹⁴



“ Proactively securing our global supply chain was an important step as properly tested and approved products are counted on by our customers who buy and deploy them.”

Chad Lloyd | Director of Cybersecurity Architecture for Energy Management | Schneider Electric

What are the options for 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 intent to authenticate 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



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 **PIV/Smart Card** and **FIDO2/WebAuthn** standards along with OTP, FIDO U2F and OpenPGP, integrating seamlessly into both legacy and modern environments and helping telecoms **bridge to a passwordless future.**

Hardware security keys such as the YubiKey are an ideal option for **IT, OT and ICS access** because they don't require additional hardware or software, external power or batteries, or a network connection—a single key secures hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services. Keys can be easily numbered, tracked, managed and re-programmed, making them an ideal solution for retail environments



The YubiKey

Is proven to reduce risk of successful phishing and credential theft attacks by 99.9% and create significant business value to large enterprises at scale, delivering an **ROI of 203%**,¹⁹ all 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%



Fast

Decrease time to authenticate by
>4x



More value

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 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.

YubiHSM 2 protects corporate secrets and OT environments

The YubiKey helps secure authentication from external sources and between IT and OT systems, while the YubiHSM 2 (hardware security module) and YubiHSM FIPS enable secure key storage and operations on a physical device. The YubiHSM and YubiHSM FIPS provides the same philosophy of low cost, high security and simplicity to cryptographic protection for servers, applications and IoT devices used to monitor and support smart energy grids.

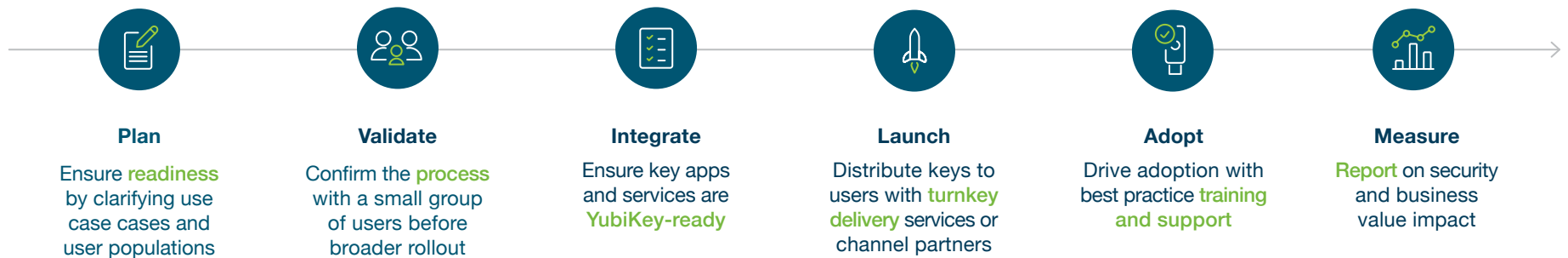
The small format YubiHSM 2 can be integrated into any process where secrets need to be managed, and the authenticity of components guaranteed or tampering needs to be avoided. The YubiHSM 2 can be easily deployed to a USB slot on servers, databases, production platforms and IoT devices.



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 telecom 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

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 workstation environments (retail, call center, OT).



Remote work

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



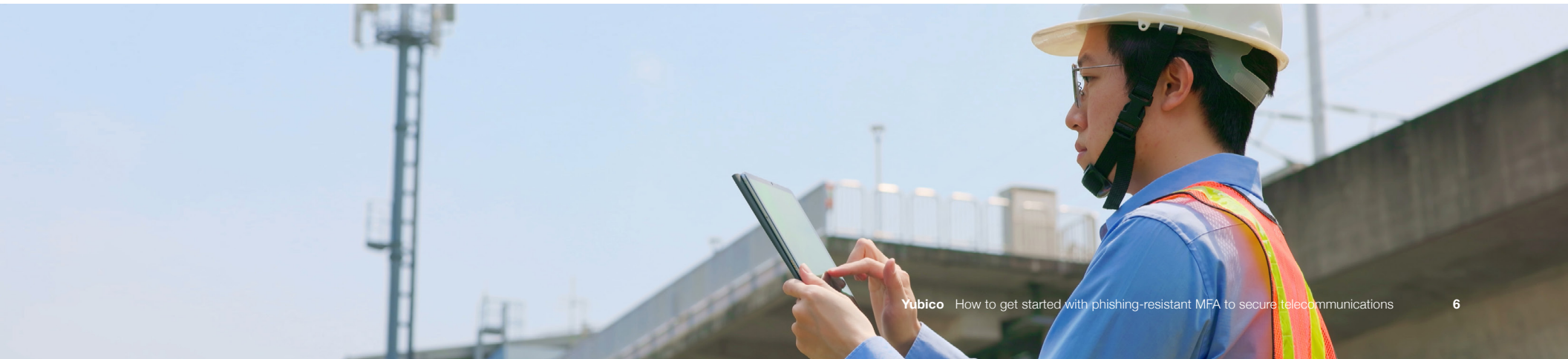
OT and mobile-restricted environments

Secure air-gapped networks, sensitive, isolated, and closed environments without transfer of information across a CDS & no need for network or cellular connectivity.



Software supply chain

Protect code access and implement trusted code-signing.





User groups



Office and hybrid workers

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



Call center

Verify call center agent identity to provide access to key systems and shared workstations, in mobile-restricted environments.



Retail environments

Use shared devices that tie into the brand's corporate environment (e.g. retail stores).



Field workers

Provide a durable MFA access via Smart Card and FIDO2/WebAuthn for employees in the field.



Third party

Protect third-party or franchisee access to systems and data.



End customers

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

Corporate secrets and OT environments



OT access

Provide secure access to critical systems, including ICS and SCADA, by verifying every user or device, including between IT and OT systems.



IoT devices & PKI environments

Protect cryptographic keys, avoid hostile takeovers and ensure secure access to intelligent systems with a combination of YubiKey + YubiHSM 2.



Product & IP integrity

Ensure product authenticity and protect corporate IP with YubiHSM 2.



Discover how to secure telecommunications in our white paper
yubi.co/telecom-wp

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.



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.



Works with YubiKey

YubiKeys, the industry's #1 security keys, work with hundreds of products, services, and applications. Browse YubiKey compatibility yubi.co/wwwyk.



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.

Yubico Professional Services			
 <p>Deployment planning Rollout plan development</p>	 <p>Integration services Architecture and infrastructure review, vendor integration analysis</p>	 <p>Implementation projects Technical engagements to implement YubiKeys in your environment</p>	 <p>Service bundles Flexible consulting hours for when and how you need them</p>

04. Launch

Get keys in hands and plan Go Live events

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

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

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



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:

Number of keys distributed, users activated, applications enabled

Performance metrics:

Support time reductions related to password resets, productivity increases related to login times

Security metrics:

Security threats mitigated, simplified compliance or audit reporting

User metrics:

Ease of onboarding, ease of use, satisfaction




Yubico's role in the industry is unique, the solutions that Yubico offers today are the next generation of identity security. The rest of the world needs to catch up with Yubico and not the other way around."

Steve Brasen | Research Director
Architecture for Energy Management

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.

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 resilient authentication future. Our focus is on secure, reliable.

[Download the Professional Services Solution Brief **yubi.co/ps**](#)

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

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



YubiEnterprise Subscription

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

[Learn more **yubi.co/yes**](https://yubi.co/yes)



YubiEnterprise Delivery

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

[Learn more **yubi.co/delivery**](https://yubi.co/delivery)



Ready to get started?

There is no question that phishing-resistant MFA is the solution to secure telecoms against modern cyber threats. 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, or want more detailed information on how to safeguard your OT systems and telecommunications with YubiHSM 2, [Yubico's Professional Services](#) team is here to help you get started.



Contact us
yubi.co/contact



Learn more
yubi.co/telecom

Sources

- ¹ IBM, [2023 Cost of Data Breach Report](#), (July 24, 2023)
- ² Ernst & Young, [Top 10 Risks in Telecommunications](#), (Nov. 29, 2022)
- ³ Verizon, [2022 Data Breach Investigations Report](#), (May 17, 2019)
- 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](#), (Accessed May 10, 2023)
- ⁶ OMB, [M-22-09](#), (Jan. 26, 2022)
- ⁷ The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- ⁸ CISA and the NSA, [Enduring Security Framework](#), (Accessed Oct. 23, 2023)
- ⁹ James Dempsey, [The FTC's rapidly evolving standards for MFA](#), (Nov. 8, 2022)
- ¹⁰ PCI, [PCI DSS: v4.0](#), (March 2022)
- ¹¹ CISA, [Zero Trust Maturity Model v 2.0](#), (April 2023)
- ¹² European Parliament, [The NIS2 Directive](#), (Feb. 2023)
- ¹³ IEC, [IEC 62443-4-2:2019](#), (Feb. 27, 2019)
- ¹⁴ ISMS, [ISO 27001:2022 Annex A Control 8.27](#), (Accessed Oct. 24, 2023)
- ¹⁵ UK Legislation, [Telecommunications \(Security\) Act 2021](#), (Nov. 17, 2021)
- ¹⁶ Cyber Security Agency of Singapore, [Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition](#), (Accessed Oct. 30, 2023)
- ¹⁷ Australian Government, [2023-2030 Australian Cyber Security Strategy](#), (Nov. 22, 2023)
- ¹⁸ Australian Signals Directorate, [Essential Eight Maturity Model](#), (Nov. 24, 2023)
- ¹⁹ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (Sep, 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.