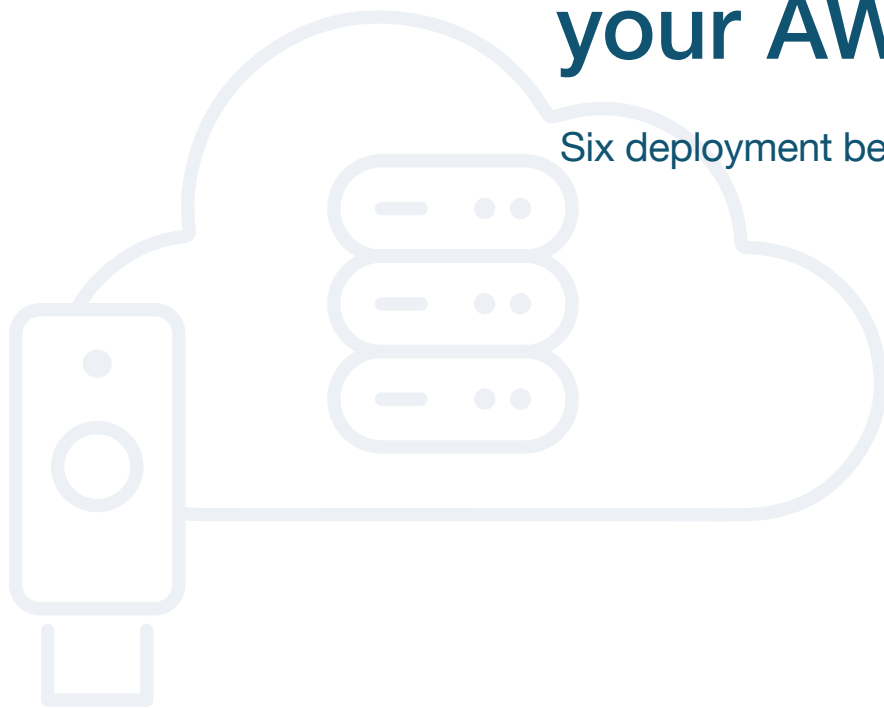




BEST PRACTICES GUIDE

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

Six deployment best practices to accelerate adoption at scale



82%



breaches involve **data stored in the cloud**¹

74%



can be traced back to **the human element** including situations such as stolen credentials and phishing.²

Up to 99.9%



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

Not all MFA is created equal

As organizations leverage Amazon Web Services (AWS) to mature their digital capabilities, they are exposed to new elements of risk that make perimeter-based security models and legacy authentication ineffective. Today, 82% of breaches involve data stored in the cloud¹ and 74% of breaches can be traced back to the human element including situations such as stolen credentials and phishing.²

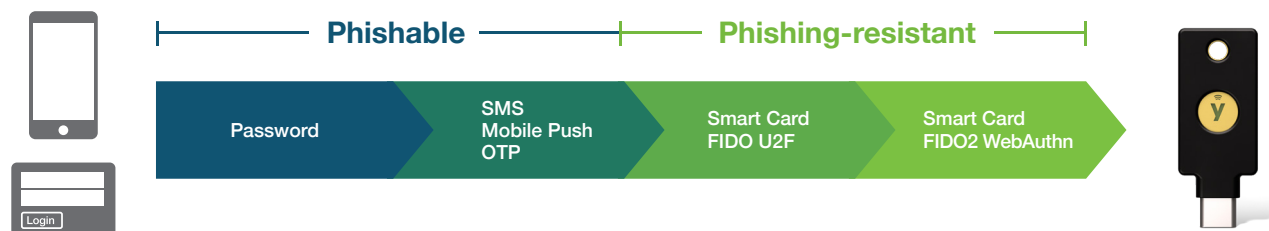
While any form of multi-factor authentication (MFA) will offer better security than passwords, **not all MFA is created equal**. Basic or legacy forms of MFA such as SMS, mobile authentication and one-time passcodes can be easily bypassed by malicious actors, making them susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks at a penetration rate of 10-24%³. In contrast, **modern phishing-resistant MFA** can offer protection up to 99.9%.⁴

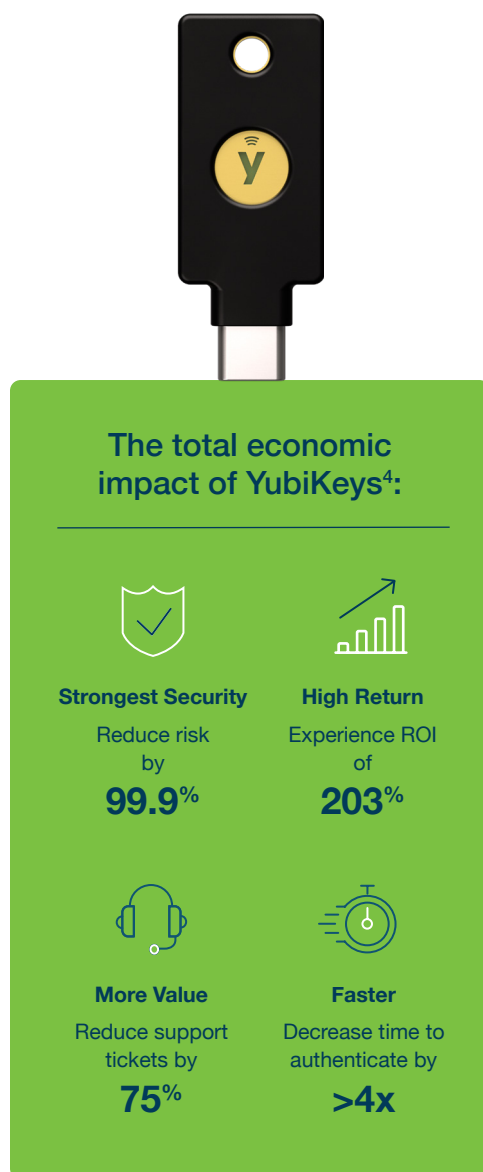
Phishing-resistant MFA is a mandated requirement of Office of Management and Budget Memo 22-09⁵ as part of the federal move to Zero Trust under White House Executive Order 14028⁶, but it is also a requirement for other industries (e.g. any subject to the PCI DSS v4.0 standard)⁷ and is the **end-goal state for any organization on the path to Zero Trust**.⁸

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, two forms of authentication currently meet the mark for phishing-resistant MFA: **PIV/Smart Card** and the modern **FIDO2/WebAuthn** authentication standard.





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 for AWS environments**.

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 AWS ecosystem.

A single YubiKey gives users secure access to AWS accounts and the AWS console—via a root account, IAM, commercial or AWS GovCloud, a desktop or a supported mobile platform—as well as [over 1,000 other products, services and applications](#), with the secrets never shared between services. The YubiKey can be used for **multiple credentials**, giving users flexibility to secure all AWS accounts as well as personal accounts—all on the same key.

For the highest level of security and AWS GovCloud users, the YubiKey 5 FIPS Series is FIPS 140-2 validated, FIDO Level 2 certified and DOD-approved⁹, meeting the highest authenticator assurance level 3 (AAL3) requirements and supported by AWS IAM device attestation in all regions.

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 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:

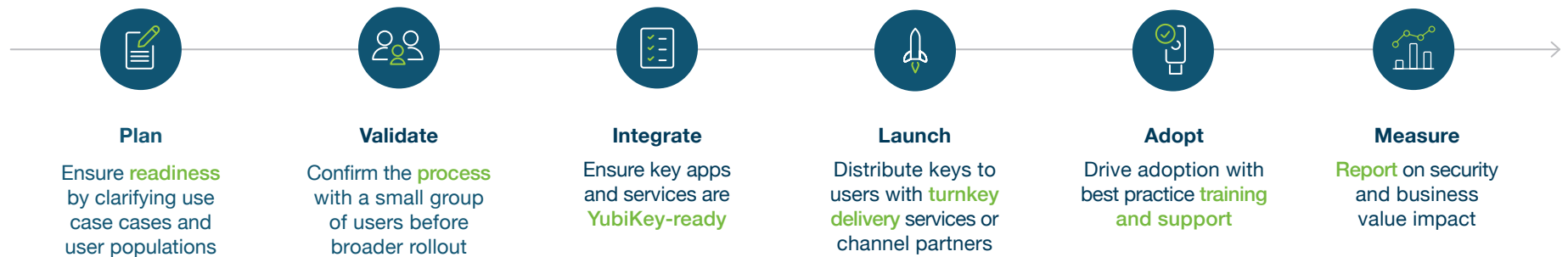
- **Synced passkeys** live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower 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 and the shift to modern work environments, the need for modern phishing-resistant MFA is essential. **But how do you start the journey?** The remainder of this guide will detail six key best practices for a successful MFA and YubiKey deployment to your AWS ecosystem.

Six key best practices to accelerate the adoption of passwordless using device-bound passkeys

Getting started is easy.⁴ Based on Yubico's experience assisting customers across the globe to optimize security, we have created a six step deployment process to plan for and accelerate passwordless adoption using device-bound passkeys 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, and business impact.

“ Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.”

John Kindervag | Creator of Zero Trust

Determine use cases

Top scenarios for modern, phishing-resistant authentication



Privileged access

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



Shared workstation

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



Remote work

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



Hybrid and remote work

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



High security

Federal and tightly regulated organizations who require a FIPS 140-2 validated solution.



Software supply chain

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

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 and built loyalty and trust with deployments to key customer segments.

Assemble key stakeholders





While the amount of resources committed to the project can vary based on the size and breadth of the YubiKey deployment, key stakeholders within the following departments can positively influence the implementation of the YubiKey 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 journey to passwordless, we’ll meet you there, offering best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.

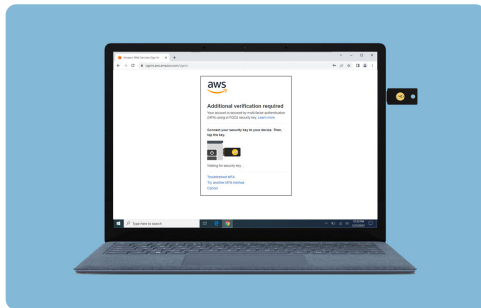


YubiEnterprise Services*		Yubico Professional Services	
 YubiEnterprise Subscription	 YubiEnterprise Delivery	 Deployment 360	 Deployment planning
Simplifies how businesses procure, upgrade and support YubiKeys	Global turnkey YubiKey distribution through YubiEnterprise Delivery or local channel partners	Turnkey planning, technical integration and deployment support	Jump start your rollout with workshops to review use cases and develop a customized strategy

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

Integrating the YubiKey within your AWS environment

Whether your identity directory is on premises or in the cloud, accessing personal or business accounts with AWS is smooth and efficient. YubiKeys provide strong, 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.



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 AWS environment is YubiKey-ready

AWS and Yubico work seamlessly together to help prevent account takeovers and go passwordless. Adding MFA for your AWS IAM users, AWS root users and Amazon Cognito immediately enhances your security posture and follows modern security best practices to effectively counter modern cyber threats, helping meet you wherever you are on your journey to MFA, passwordless and Zero Trust. With no shared secrets between the services, the YubiKey enables high security and privacy at scale.

AWS ecosystem + YubiKey

AWS root users

Use a YubiKey to protect privileged access to AWS services and resources

AWS SSO

Secure user access to AWS accounts and applications using the YubiKey

AWS IAM

Use a single YubiKey to access multiple IAM and root users across multiple AWS accounts

AWS GovCloud

Leverage the YubiKey 5 Series and YubiKey FIPS series for the highest level of security to AWS GovCloud

AWS IAM Roles Anywhere

Leverage the YubiKey to store cryptographic keys to support IAM roles to be used outside AWS

Amazon Cognito

Create enterprise and consumer apps that leverage built-in support for phishing-resistant MFA and the YubiKey

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 <p>Who needs access?</p> <p>Employees, contractors, third parties, supply chain</p>	 What <p>What authentication approach will you take?</p> <p>MFA (Password and strong second factor), passwordless</p>	 Where <p>Where in your environment do you require strong authentication?</p> <p>Critical infrastructure elements, network, applications, developer tools.</p> <p>How do you manage access?</p> <p>IAM, IdP, PAM, SSO, VPN, ZTNA</p>	 How <p>How does location impact deployment?</p> <p>Remote, hybrid, on-premise, multi-office</p> <p>What types of devices need to be supported?</p> <p>Owned, BYOD, desktop, laptop, smartphone, tablet</p>
---	--	--	---

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



What?

Increase awareness

Build up user training and support materials



Why?

Boost engagement

Demonstrate value to the organization and the user



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

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 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.

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.





How to?

Educate users

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



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 available to help with any questions that may arise for onboarding and troubleshooting (e.g. what to do in case of a lost key).

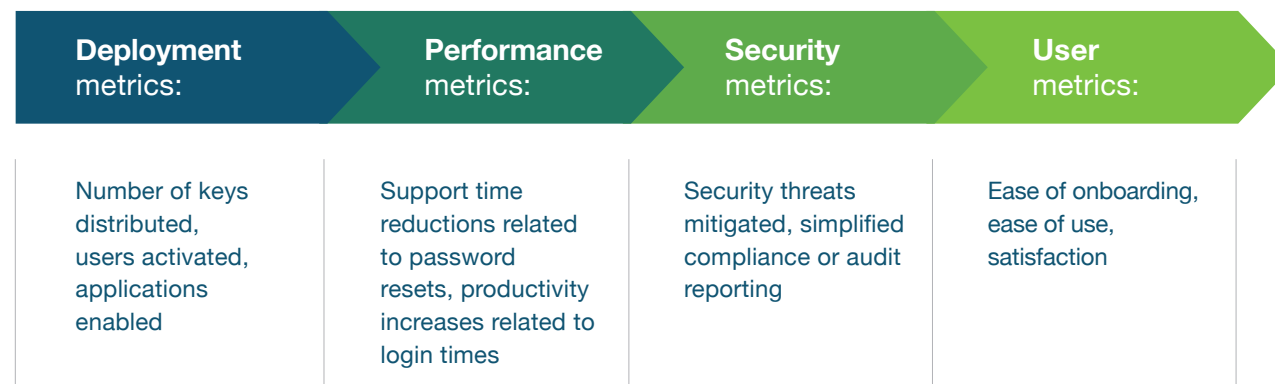
Effective education and awareness is important during this phase in order to showcase to your user community why the company invested in the YubiKey, and the direct benefits to users. The YubiKey's simple user experience requires minimal training and on-going support for users.



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.



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 riskless 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

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



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 here](#)



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 here](#)



Which YubiKeys are right for me?



We've made it easy for you to find out which YubiKey is right for you or your company. You will get a tailored recommendation based on the way you answer questions about your unique needs.

Take our quiz at yubi.co/quiz



YubiEnterprise Services*

YubiEnterprise Subscription
YubiEnterprise Delivery



YubiEnterprise Professional Services

Deployment 360

Service hour bundles

Workshops

Implementation projects

* 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 AWS environments against modern cyber threats. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

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

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



Contact us
yubi.co/contact



Learn more
yubi.co/ps

Sources

- ¹ IBM, [2022 Cost of Data Breach Report](#), (Accessed August 12, 2022)
- ² Verizon, [2023 Data Breach Investigations Report](#), (June 6, 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 CISA, [Zero Trust Maturity Model v 2.0](#), (April 2023)
- ⁹ DOD OCIO, [Memo](#), (December 20, 2019)
- 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.