



BEST PRACTICES GUIDE

How to get started with phishing-resistant MFA to secure state, local, tribal and territorial governments

Six deployment best practices to accelerate adoption at scale



\$4.45 million



global average data breach cost¹

82%



can be traced back to the human element including situations such as stolen credentials and phishing⁴

Up to 99.9%



protection offered through modern phishing-resistant MFA⁵

“Despite all the user training and password restrictions in place, usernames and passwords are not enough to secure access to critical systems these days. Bad actors can use password spraying or social engineering to gain access.”

Jackie Alexander |
Director of Information Technology |
City of Mission Viejo

Choosing the right MFA approach

State, local, tribal and territorial (SLTT) governments face mounting pressure to modernize authentication and implement Zero Trust in response to cyber threats, which are not only costly (\$4.45M USD global average data breach cost¹), but are a threat against the highly sensitive information they hold, the critical services they provide and the upstream risk to all levels of the government.²

Modern cybercriminals target state and local governments with the aim to steal information and to impede their ability to function. According to a nationwide cybersecurity survey of local governments, 28% report being attacked at least hourly.³ Further, looking broadly at all breaches, the majority (82%⁴) can be traced back to the human element including situations such as stolen credentials and phishing.

While any form of multi-factor authentication (MFA) offers better security than passwords, **not all MFA is created equal**. Basic or legacy forms of MFA such as SMS, push notification apps and one-time passcodes (OTP) 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%.⁵ In contrast, **modern phishing-resistant MFA** can offer protection up to 99.9%.⁶

Phishing-resistant MFA is a mandated requirement of Office of Management and Budget Memo 22-09⁷ as part of the federal move to Zero Trust under White House Executive Order 14028,⁸ a regulation which has downstream implications for SLTT governments. Furthermore, MFA is a required element as part of the SLTT Cybersecurity Plans to gain access to funds from the State and Local Cybersecurity Grant Program (SLCGP).⁹

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 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: **Smart Card/PIV** and the modern **FIDO2/WebAuthn** authentication standard.

The 2023 Multi-State Information Sharing and Analysis Center Phishing Guidance from CISA states that accounts using MFA without Fast Identity Online (FIDO) MFA or Public Key Infrastructure (PKI)- based MFA enabled, are susceptible to malicious actors using compromised legitimate credentials to authenticate as the user in legitimate login portals.¹⁰





YubiKey form factors




From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition, YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

YubiKey offers phishing-resistant MFA at scale

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

The YubiKey is a multi-protocol hardware security key, supporting both **Smart Card/PIV** and modern **FIDO2/WebAuthn** authentication standards along with OTP, FIDO U2F and Open PGP, integrating seamlessly into both legacy and modern environments and helping government organizations **bridge to a passwordless future** without a rip or replace of existing infrastructure. YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 1,000 applications and services out-of-the-box.

The YubiKey is proven to reduce risk by 99.9% and deliver significant business value including an **ROI of 203%**,¹¹ all while delivering a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

 <p>Strongest security Reduce risk by 99.9%</p>	 <p>Fast Decrease time to authenticate by >4x</p>	 <p>More value Reduce support tickets by 75%</p>	 <p>High return Experience ROI of 203%</p>	 <p>Durable IP68 certified, dust-proof, crush-resistant and water-resistant</p>
--	---	---	---	---

Hardware security keys such as the YubiKey are an ideal option for authentication because they don't require external power or batteries and can help **close any MFA gaps related to users that can't, don't or won't use mobile authentication** due to reasons such as union restrictions, personal preference, cellular connectivity or financial reasons. YubiKeys can be easily tracked, managed, and re-programmed, reducing IT support and supporting strong authentication even for temporary workers and contract staff.

State and local governments using YubiKeys for 100% MFA coverage





SPOTLIGHT: PASSKEYS

fido™

FIDO

An open security standard backed by the FIDO Alliance, a group focused on moving away from a password-based system.



CREDENTIAL

The unique ID a user has that “gets you through the gate” when you log on to any system.

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:

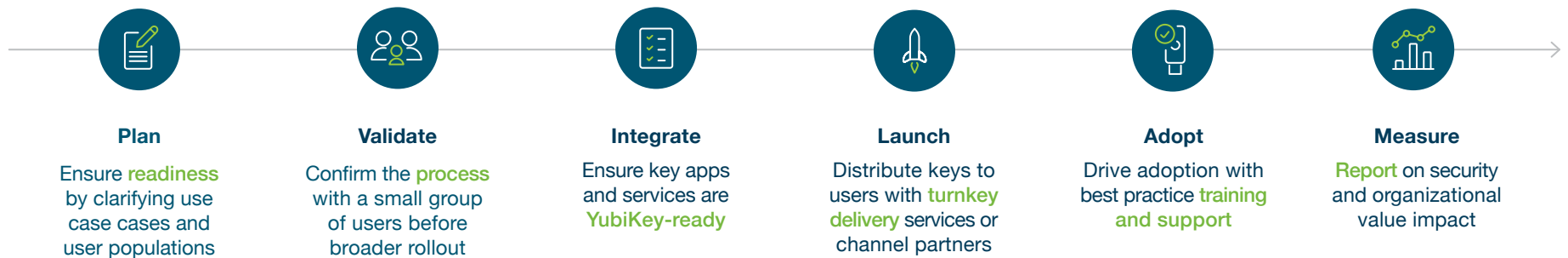
- **Synced passkeys** live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.
- **Device-bound passkeys** offer organizations 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 organizations with trusted credential lifecycle management and attestation abilities. With this passkey approach organizations can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent government requirements.

Given the threat landscape, the reasons for using modern, 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 state and local governments, 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, organizational 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 devices

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



Remote work

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



Elections infrastructure

Provide an extra layer of security for authorized personnel to access the voter registration database.



Software supply chain

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



Mobile-restricted

Secure sensitive environments where mobile devices are not allowed (e.g. call centers, corrections departments).

User groups



Office workers

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



First responders

Provide a highly portable, secure access to critical data for emergency operations.



Field workers

Provide public works professionals secure access to systems, services and data in the field, including secure and off-grid areas.



Third party

Protect third-party access to systems and data.



Citizen-facing public services

Protect citizen access to online services.



“ I like the YubiKey as opposed to phone authentication. We have a lot of users within our system that don’t have a state- or county-provided cell phone, and I certainly don’t want them using their own personal devices for agency or office business. The YubiKey was really the easy-to-use multifactor authentication of choice for us here in Washington state to achieve the additional security needs we had.”

Lori Augino | Elections Director | Washington State





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 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.

“ Training and support materials have been central to the high adoption of YubiKeys, both at the user and department level. Every department that has signed on has been successful in their deployment.”

Siddique Mohammed | IAM Solution Architect | City and County of San Francisco | Department of Technology



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/wwwyk.

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, DUO 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.

 Who	 What	 Where	 How
<p>Who needs access?</p> <p>Employees, contractors, third parties, supply chain</p>	<p>What authentication approach will you take?</p> <p>MFA (Password and strong second factor), passwordless</p>	<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>	<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.

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**

“ Without two-factor authentication, you’re leaving your network and your organization vulnerable. It’s really important to add this layer of security. This is one among many other layers cybersecurity experts should be adopting. This is the front line. Don’t start somewhere else without having this in place.”

Jackie Alexander |
Director of Information Technology |
City of Mission Viejo



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 organizational impact

We know **the truth is in the numbers**. Validate the pilot against these metrics, then expand to other users to increase the overall organizational 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.



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 trustworthy authentication future. For learn of our core services



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.

To download the Professional Services Solution Brief go to yubi.co/ps.

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

* 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 state and local government agencies against modern cyber threats and to solve the many critical authentication pain points. 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 organization as your needs grow. We include success guides and priority support to help you be successful as quickly as possible.

If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help you get started.



Contact us
yubi.co/contact



Learn more
yubi.co/statelocalgov

Sources

- ¹ IBM, [2023 Cost of Data Breach Report](#), (July 24, 2023)
- ² Deloitte-NASCIO, [2022 Deloitte-NASCIO Cybersecurity Study](#), (Nov. 3, 2022)
- ³ Donald F. Norris, et. al., [Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity](#), (Feb. 21, 2019)
- ⁴ Verizon, [2023 Data Breach Investigations Report](#), (May 10, 2023)
- ⁵ Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ⁶ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (Sept. 2022)
- ⁷ OMB, [M-22-09](#), (Jan. 26, 2022)
- ⁸ The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- ⁹ CISA, [FY 2023 State and Local Cybersecurity Grant Program FAQs](#), (Nov. 2, 2023)
- ¹⁰ CISA, [Multi-State Information Sharing and Analysis Center Phishing Guidance](#), (Oct. 2023)
- ¹¹ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (Sept. 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.