



BEST PRACTICES GUIDE

# How to get started with phishing-resistant MFA for Zero Trust

Six deployment best practices to accelerate adoption at scale



**Organizations on the path to Advanced or Optimized levels of the ZTMM will progress toward authenticating all identities with phishing-resistant MFA<sup>6</sup>**

While only U.S. federal agencies are required to adopt Zero Trust in accordance with White House Executive Order 14028,<sup>7</sup> phishing-resistant MFA is a mandated requirement of Office of Management and Budget Memo 22-09<sup>8</sup> and evolving FTC standards<sup>9</sup> in the US, NIS2<sup>10</sup> for the EU and the Global PCI DSS v4.0 standard,<sup>11</sup> among others.

## Accelerate Zero Trust with phishing-resistant MFA

Organizations face mounting pressures to implement Zero Trust in response to cyber threats, which are not only costly (\$4.35M USD global average data breach cost<sup>1</sup>) and disruptive, but the majority of which (82%<sup>2</sup>) can be traced back to the human element including situations such as stolen credentials and phishing. A Zero Trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be verified and authenticated before access is granted. In 2023, 36% of global CISOs say they have started to implement components of zero trust.<sup>3</sup>

The **Zero Trust Maturity Model (ZTMM)** was developed by CISA (v 2.0 April 2023<sup>4</sup>) to assist organizations and federal agencies in developing zero trust strategies related to five distinct pillars: identity, devices, networks, applications and workloads, and data. For those organizations already on the path to Zero Trust, it is important to understand how the ZTMM addresses identity and multi-factor authentication (MFA).

The ZTMM recognizes that **not all forms of MFA are created equal**, requiring stronger forms of MFA be adopted for each subsequent stage. Legacy authentication methods, including SMS, mobile authentication and one-time passcodes, are susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks. A Google, NYU, and UCSD analysis of 350,000 real-world hijacking attempts revealed that a SMS-based OTP only blocked 76% of targeted attacks and a mobile push app only blocked 90% of targeted attacks.<sup>5</sup> In other words, the best case scenario was a 10% attack penetration rate.

**This deployment best practices guide specifically outlines Advanced or Optimal identity and multi-factor authentication considerations for organizations that are already on the path to Zero Trust, which more holistically considers:**



### Authentication support

Phishing-resistant MFA and passwordless supported by attestation of the authenticator



### Access management

Least privileged access controls supported by microsegmentation and continuous verification



### Risk assessments

Real-time signals for continuous risk assessments, e.g. to support step-up authentication



### Identity stores

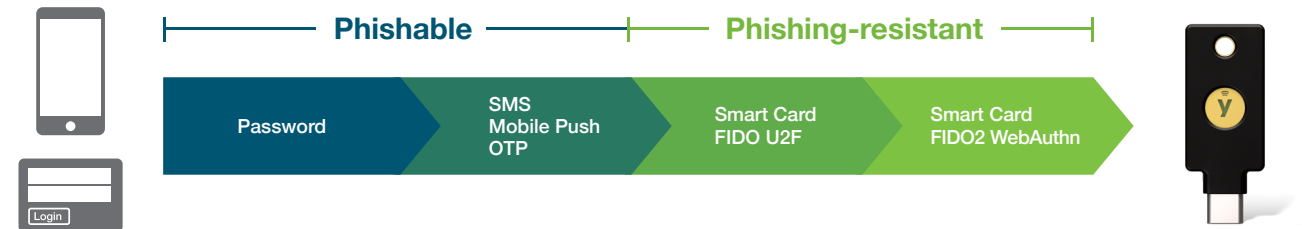
Integrated identity stores to manage identity information across cloud and on-premise environments

**NIST Special Publication 800-63B-4 defines phishing-resistance** as “the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber.”

## What is phishing-resistant MFA?

Phishing-resistant multi-factor authentication (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. In Zero Trust terminology, this helps establish trust in both the user and the authenticator.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B-4, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.



“

Any form of MFA is better than just a username and password, but most MFA can still be phished. It didn't take long to realize we needed stronger authentication for all employees that couldn't be phished.”

Daniel Jacobson  
Senior Director of IT, Datadog



“

The YubiKey complements our Zero Trust architecture and helps get us closer to Zero Trust.”

Morey J. Haber  
Chief Security Officer, BeyondTrust

## 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.

# YubiKey offers phishing-resistant MFA

Yubico created the **YubiKey**, a hardware security key that supports **phishing-resistant two-factor, multi-factor 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 and modern environments, helping organizations **bridge to a passwordless future.** YubiKeys work with over 1,000 products, services and applications including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services.

Modern hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA as part of an organization's Zero Trust security strategy. Unlike legacy MFA schemes such as SMS and email OTP or mobile push notifications, the YubiKey is proven to **reduce risk of account takeovers by 99.9%,<sup>12</sup>** doesn't require external power or batteries, and can even operate within environments without a network connection. A user can use a single key for secure access to multiple applications and services with the secrets never shared between relying parties, delivering a great user experience by enabling users to securely log in with a single tap or touch:



### Strongest security

Reduce risk  
by 99.9%



### High return

Experience ROI  
of 203%



### More value

Reduce support  
tickets by 75%



### Faster

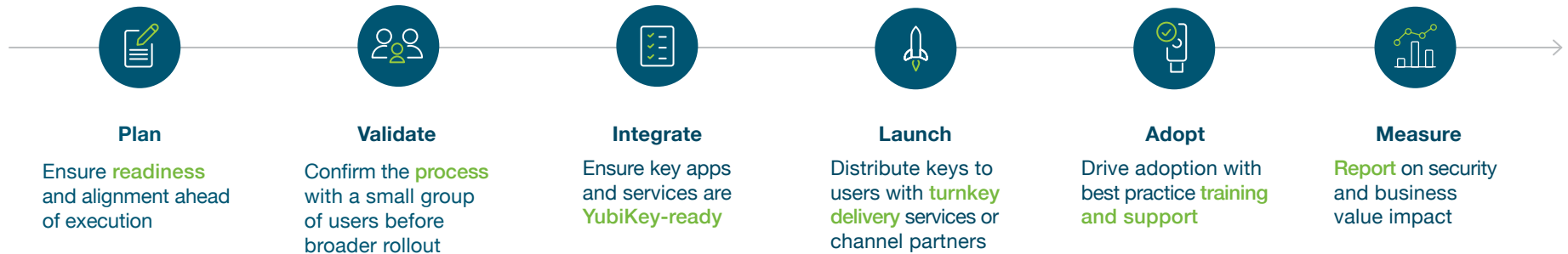
Decrease time to  
authenticate by >4x

\*Forrester Research, The Total Economic Impact Of Yubico YubiKeys, September 2022

Given the threat landscape, the need for modern phishing-resistant MFA gets clearer on a daily basis. **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.

# Six key best practices to accelerate the adoption of phishing-resistant MFA as part of Zero Trust

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

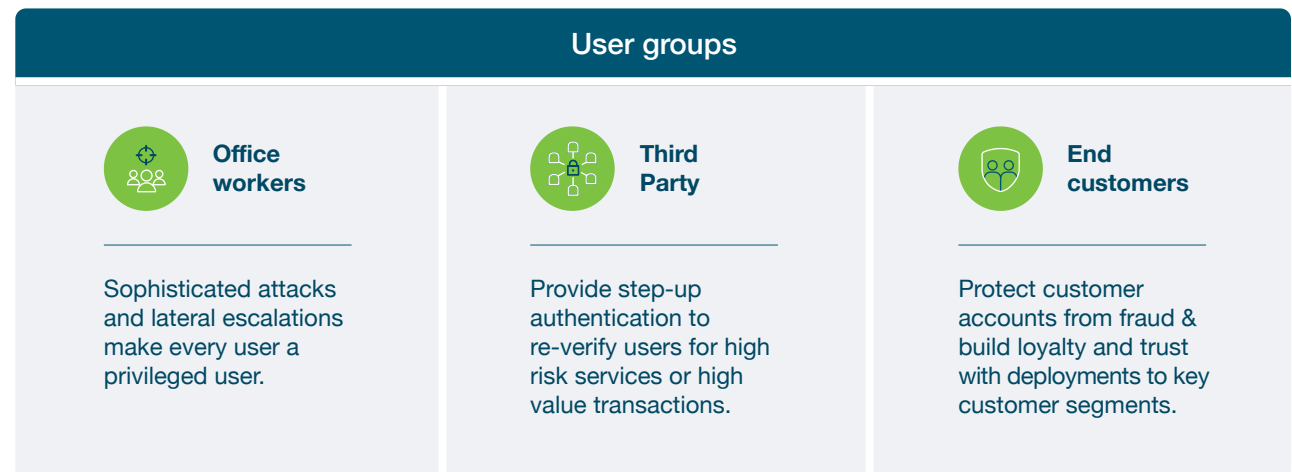
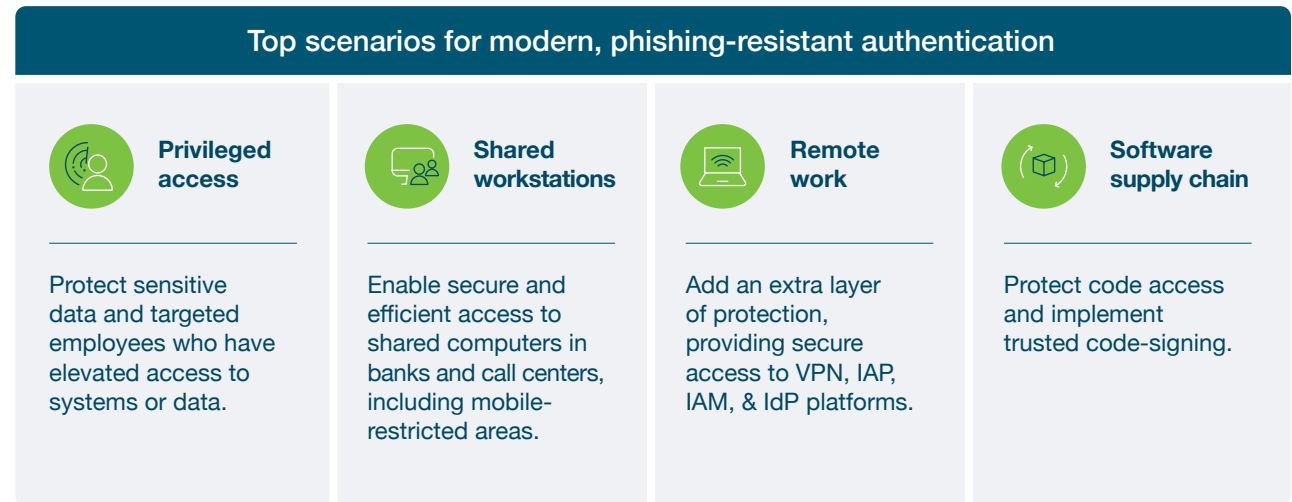
“

“We are taking great strides in protecting the safety of our guests and colleagues by requiring phishing-resistant MFA methods for all applications that can expose both PII and Card Holder data. We also believe that having Guest Services colleagues looking down at their phone to complete an MFA response or approval does not portray the message we want, to someone walking past the front desk. It lends itself to the perception the colleague is engaged in their cell phone for social media or other personal activity.

Using a YubiKey not only provides a more seamless experience for the colleague while keeping our data safe, but also allows those colleagues to keep their cell phones stored away while performing guest-facing roles.”

Art Chernobrov  
Director of Identity, Access, and Endpoints  
Hyatt Hotels Corporation

## Determine use cases



“

I am all about making the adoption of technology as easy as possible. If I can hit the easy button using YubiKeys and also using their subscription model to ensure all my users have YubiKeys, that is a big win for me!”

Brent Deterding,  
CISO, Afni







## 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

Yubico, building on its years of helping secure some of the most security conscious organizations in the world, is focused on helping businesses and governments easily access security products and services in a flexible and cost-effective way to heighten security. Organizations can benefit highly from a YubiKeys as a Service model and our Professional Services team offers best-in-class technical and operational guidance in support of your YubiKey implementation and rollout.

YubiEnterprise Services*		Yubico Professional Services	
 <b>YubiEnterprise Subscription</b>	 <b>YubiEnterprise Delivery</b>	 <b>Deployment 360</b>	 <b>Deployment planning</b>
Simplifies how businesses procure, upgrade and support <b>YubiKeys</b>	Global <b>distribution</b> to remote and in-office locations	<b>Turnkey</b> planning, technical integration and deployment support	Jump start with workshops & <b>projects</b> to review use cases or develop a customized strategy

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

## 02. Validate



### Confirm the process with a small group of users

**Validate** with a small group of users across a priority use case for confirmation and feedback, leveraging Yubico best practice resource guides, videos and engagements. **Practice, learn and then move forward with expansion.**

## 03. Integrate



### Ensure your environment is YubiKey-ready

YubiKeys can work with over 1,000 applications and services and secure your users' work and personal digital lives with no shared secrets between the services, enabling high security and privacy at scale. 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 pilot program, 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 → [here](#).



#### 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

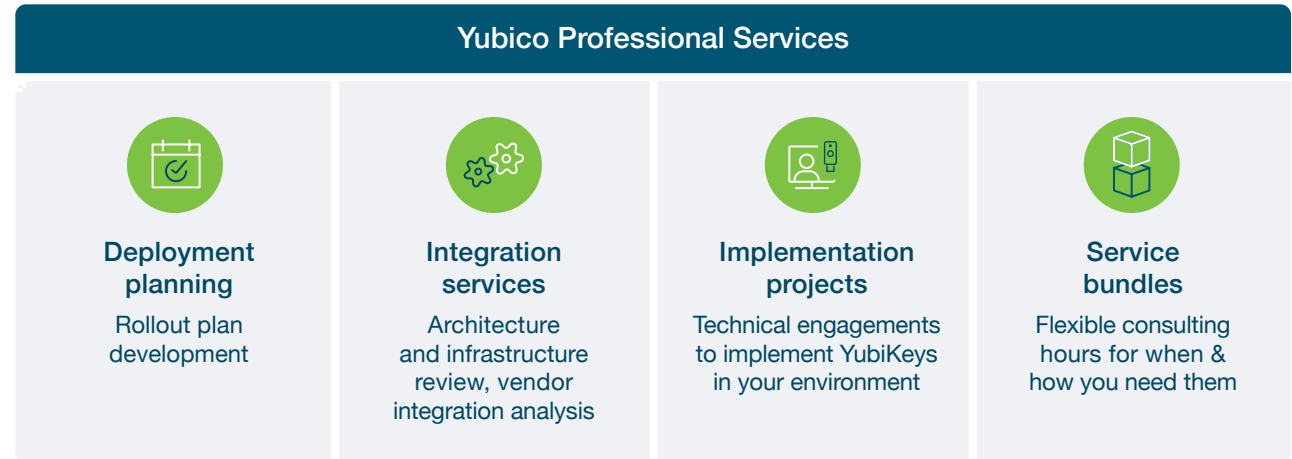
##### What types of devices need to be supported?

Owned, BYOD, desktop, laptop, smartphone



## 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:



## 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:



### What?

#### Increase awareness

Build up user training & support materials



### Why?

#### Boost engagement

Demonstrate value to the organization & the user

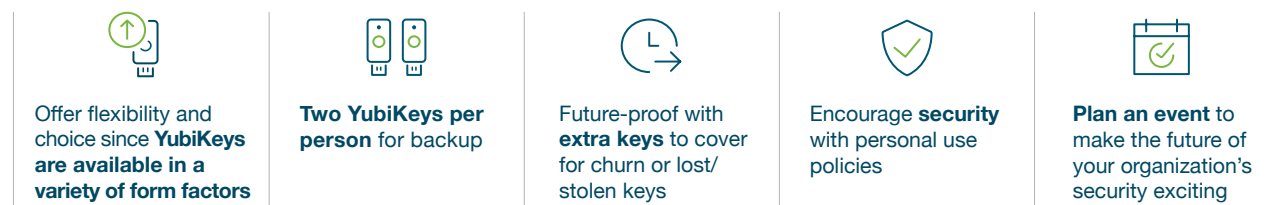
“

With the YubiKey, you can enforce training to 100% because you don't open or click, you're touching with your finger to validate with biometrics. We can finally say 'Don't click, don't open' and have no exceptions.”

Morey J. Haber  
Chief Security Officer, BeyondTrust

## 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.



## 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.



### How to?

#### Educate users

Have clear calls to action on how to get started & 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**, 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).

“

With regard to YubiKey deployment and usage, if our staff don't say anything, that's a sign they are generally happy. Given the silence, the YubiKey has been quite a success.”

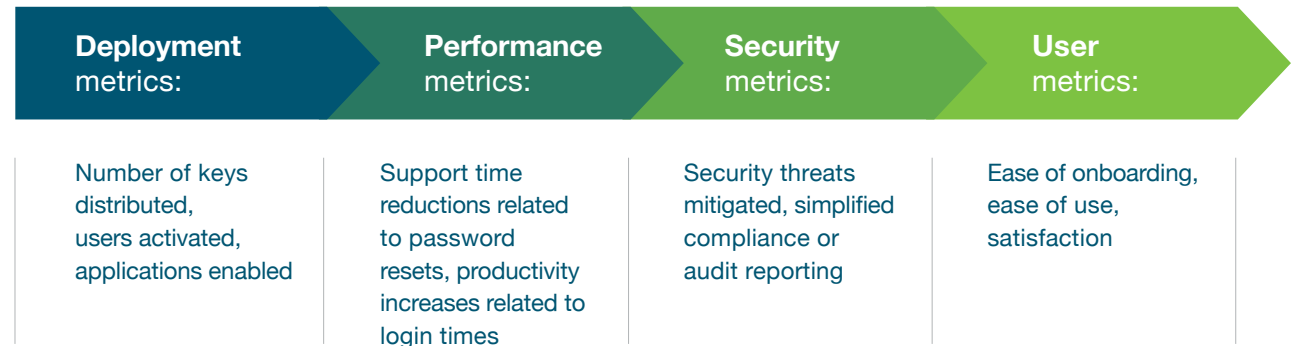
Stefan Lueders  
CISO, CERN

## 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

#### 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 Services*		Yubico Professional Services		
YubiEnterprise Subscription	YubiEnterprise Delivery	Launch planning	Training & support	Analytics & reporting
Cost effective and flexible YubiKey procurement	Global <b>distribution</b> to remote and in-office locations	Create a marketing and <b>communication plan</b> tailored to your users	Best practice <b>training &amp; support</b> materials and processes	Customized <b>metrics &amp; dashboard design</b>

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

## Yubico Professional Services



### Deployment 360

Service hour bundles



### Workshops

Implementation projects



## Ready to get started?

There is no question that phishing-resistant MFA is an integral part of the solution to secure organizations against modern cyber threats, to accelerate the journey to Advanced or Optimal Zero Trust implementations and to minimize any user friction associated with continuous authentication or verification. 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 and how to get them in the hands of employees.

Modern enterprises recognize that **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](https://yubi.co/contact)



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



Datadog believes in giving their employees everything they need to do their jobs and be safe. We encourage every employee to use their YubiKeys even for accounts outside of work, and if an employee ever leaves the company they keep their YubiKeys.”

Daniel Jacobson  
Senior Director of IT, Datadog



## Sources

1. IBM, [2022 Cost of Data Breach Report](#), (Accessed August 12, 2022)
2. Verizon, [2022 Data Breach Investigations Report](#)
3. PwC, [Global Digital Trust Insights 2023](#), (Accessed April 6, 2023)
4. CISA, [Zero Trust Maturity Model v 2.0](#), (April 2023)
5. Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
6. CISA, [Zero Trust Maturity Model v 2.0](#), (April 2023)
7. The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
8. OMB, [M-22-09](#), (January 26, 2022)
9. James Dempsey, [The FTC's rapidly evolving standards for MFA](#), (November 8, 2022)
10. European Parliament, [The NIS2 Directive](#), (February 2023)
11. PCI, [PCI DSS: v4.0](#), (March 2022)
12. Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)



## About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: [www.yubico.com](https://www.yubico.com).