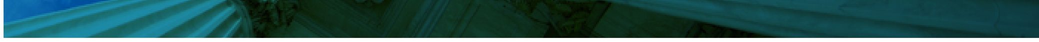
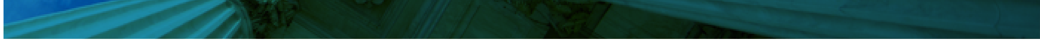


yubico

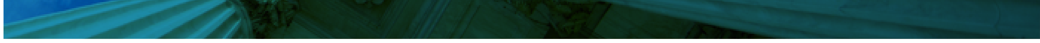
WHITE PAPER

Securing remote workers with phishing-resistant MFA

Modern, simple security-as-a-service right to your door



Contents



$4.45 million

global average cost of a data breach[1]

74%

of breaches tied to a human element

Social attacks, errors, misuse or credential theft[2]

62%

of organizations can partially attribute a **data breach to remote work**[3]

The critical need for modern, strong authentication for remote workers

For jobs that can be done remotely only 7% of employees worked remotely full-time prior to the pandemic. As of 2023, 35% remained remote and 41% hybrid[4] in the US and 60% combined globally.[5] While there is no question that work flexibility is here to stay, many organizations have yet to evolve their cybersecurity standards to address the risk of an expanded, distributed security perimeter.

Organizations faced 50% more cyber attacks per week in 2021 compared to 2020[6] and remained consistent at this new level before surging again in 2023 (8% increase).[7] Globally, two-thirds of organizations experienced a data breach due to remote work vulnerabilities, including insecure networks and devices.[8] IT often lacks visibility into the locations, timing and devices used by employees to log in, with an average 48% of endpoints escaping detection or lacking protection by IT.[9] Further, remote work amplifies the insider threat—threats that originate when authorized access is maliciously or negligently misused or compromised by cyber attacks.

While data breaches are always costly and disruptive ($4.45M globally, $9.48M US[10]), the impact increases by an average of $1 million when remote work is a contributing factor in the event.[11] The majority of data breaches (74%[12]) can be traced back to the human element including the use of stolen credentials, privilege misuse and phishing.

Enterprises across the globe are increasingly adopting multi-factor authentication (MFA) not only as a defense against cyber attacks, but also to facilitate secure remote access (34%), enable privileged access (26%), improve user convenience (24%), align with Zero Trust initiatives (25%) and meet compliance requirements (21%).[13]

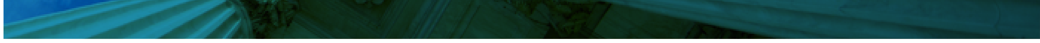
Despite the growing tide and sophistication of cyber attacks, many organizations still rely on legacy MFA such as mobile-based authenticators to secure remote access to critical and sensitive corporate applications and data. While any form of MFA offers better security than password-based authentication alone, the truth is that not all MFA is created equal when it comes to protecting against cyber threats such as phishing and account takeovers, meeting compliance requirements, or in terms of the friction created for end users and IT support teams.

In this whitepaper, we will explore remote work authentication vulnerabilities to help you re-evaluate your long-term remote work policy, and consider the shift to modern, phishing-resistant MFA.

Security risks from remote work

In addition to the rise in attacks, remote work exposes organizations to new vulnerabilities arising from unsecured home or public networks, unpatched personal devices, shared devices, and unrestricted access to personal devices or the internet. These factors increase both insider threats and the risks of cyber attacks. A lack of visibility, coupled with insufficient security of or gaps in MFA, increase the risk of threat actors exploiting vulnerabilities, installing malware, compromising credentials or intercepting shared files.

- **Expanded attack surface**
- **Insecure networks**
- **Insecure/ unmanned devices**
- **Insufficient technical controls**
- **Amplified insider threats**



10-24%

attack penetration rate for mobile authentication[14]

92%

of organizations were victims of **phishing**[15]

$1 million

per year cost for **password resets** alone[16]

The drawbacks of legacy authentication

While it's widely accepted that usernames and passwords are no longer effective to protect against modern cyber threats, the same holds true for more conventional MFA solutions including such as SMS, OTP, and push notifications. These methods are still susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks at a penetration rate of 10-24%.[17]

Convential MFA may be familiar but falls short on security

Vulnerable to attack

Every mobile authenticator can be phished

Expensive to maintain

$1840/user in enterprise mobility cost

Poor user experience

Complex to operate and manage

Security gaps

Many user can't or won't use it

Short-term solution

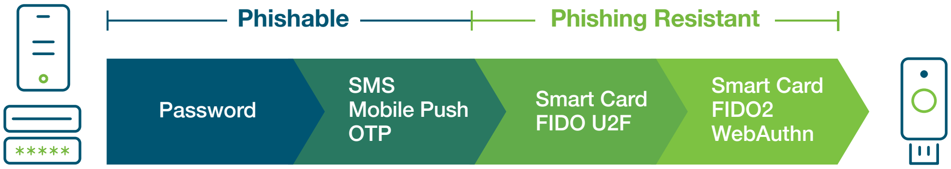
Legacy MFA isn't built for the future

To create a sustainable and secure long-term remote and hybrid work policy, organizations should invest in modern **phishing-resistant MFA** and modern login flows that eliminate passwords completely, such as **passwordless authentication**, to help advance towards a **Zero Trust security approach.**

What qualifies as 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: Smart Card/PIV and the modern FIDO2/WebAuthn authentication standard. The **modern FIDO authentication standard enables strong two-factor, multi-factor, and passwordless authentication.**



Phishable

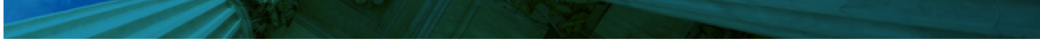
Phishing Resistant

Password

SMS
Mobile Push
OTP

Smart Card
FIDO U2F

Smart Card
FIDO2
WebAuthn



Remote work authentication scenarios and their vulnerabilities

As organizations examine their remote work policies, there are many authentication scenarios that need to be detailed to support employee productivity and minimize risk:

IAM and IdP access

Most leading hybrid and cloud environments leverage Identity and Access Management (IAM) and Identity Provider (IDP) platforms, typically leveraging Single Sign On (SSO) capabilities to enable employees to work without the hassle of remembering multiple usernames and passwords. However, the use of legacy MFA for access to IAM and IdP platforms can still leave organizations open to attack if credentials are misused or intercepted.

Mobile / BYODs

Storing credentials on a mobile device introduces security concerns if it is lost or stolen. As the number of devices per employee increases, having a single portable external authenticator that can work across all computing devices helps make these transitions seamless.

Remote access technologies

Connecting via Virtual Private Networks (VPN) or Identity-Aware Proxies (IAP) to access corporate networks, protected resources or specific applications from unsecured home or public wifi can be risky if using legacy forms of authentication.

Computer login

If employee laptops are not secured properly, they can provide entry points for external threats leading to a security breach. Securing computer logins protects on-device applications and critical business data.

Privileged access

Privileged users have elevated access to systems, software, data or infrastructure, including privileged IT users such as engineers, IT admins, security admins, network or database admins, and privileged business users who may have elevated access to sensitive or confidential data.

Forrester estimates that 80% of data breaches have a connection to compromised privileged credentials[21]. Storing SSH private keys on local devices leaves them at risk of being stolen, copied or accessed by malware on the device. Additionally, manually typing OTP codes for MFA slows down productivity as it takes users away from their workflows.

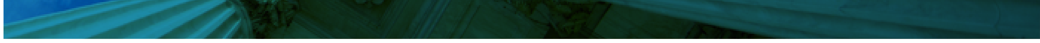
It is critical that privileged users and accounts have varying levels of access according to their specific roles and responsibilities within systems. Ideally, this access should follow the principle of least privilege, and such access must be protected with strong authentication and additional step-up authentication for the highest-risk actions. Learn more about the critical strong authentication needs for privileged users.

What about passkeys?

Passkeys are a new name for FIDO2 passwordless-enabled 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.

Device-bound passkeys offer greater manageability than synced passkeys, and therefore better suited for the enterprise. However, there are different types of device-bound passkeys and those that live in hardware security keys are known to offer the highest security assurance and provide enterprises with the trusted credential lifecycle management and attestation abilities they need to have the strongest security, the simplest user onboarding and credential/account recovery experience across devices and platforms, and stay in compliance with the most stringent requirements across industries.



> “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

Step-up authentication for password managers

Despite the risks, passwords remain the predominant authentication method, used by nearly 100% of organizations.[22]

As organizations move towards replacing passwords with modern MFA and passwordless login flows, they can leverage password managers to generate unique, strong passwords and to enforce two-factor authentication. Incorporating a phishing-resistant hardware security key adds an extra layer of protection, offering step-up authentication for the central password manager.

Cloud-based software

While it may seem obvious to protect privileged users first, in today’s modern cyber threat landscape, every user can be seen as having some level of privilege. Advanced threat actors exploit stolen credentials to traverse the network, attempting to acquire or phish for additional credentials that can escalate their access to high-value data assets and systems. A recent Google Cloud report indicates that weak passwords were a factor in 50% of compromises of enterprise cloud environments in Q4 2022.[23]

How to secure the remote and hybrid workforce with phishing-resistant multi-factor and passwordless authentication

To address these challenges, Yubico created the **YubiKey**, a hardware security key that offers **phishing-resistant MFA and passwordless authentication at scale with an exceptional user experience.**

The YubiKey is a multi-protocol key, supporting both Smart Card/PIV and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy and modern environments, helping organizations bridge to a **passwordless future.**

Modern hardware security keys, such as the YubiKey, are an ideal option for remote work and to support an organization’s Zero Trust strategy. The YubiKey is proven to **reduce risk of account takeovers by 99.9%**[24] while delivering a great user experience. The YubiKey allows users to securely log into leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and hundreds of cloud services—all with a single tap or touch.

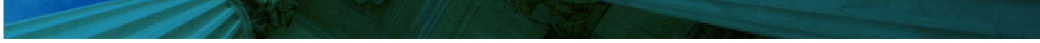
The total economic impact of YubiKeys[4]:

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



Remote authentication scenarios supported by the YubiKey

Organizations across a variety of industries have already deployed the YubiKey to solve for a growing number of remote use cases, starting with high risk user groups and scenarios and then gradually extending its use to provide more value by streamlining authentication and reducing support costs:

Top scenarios for phishing-resistant MFA

IAM and IDP access

Provide a consistent, secure and controlled authentication flow for critical applications and services. Native support from Axiad, Duo, Microsoft Azure Active Directory, Okta Adaptive MFA, OneLogin, PINGID and RSA SecurID Suite.

Privileged access

The YubiKey design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied, stolen or intercepted remotely. Good for primary, back-up or step-up authentication.

Cloud based software

YubiKeys can be used for Single Single On (SSO) access to productivity and collaboration software including Microsoft 365, Google Hangouts and Zoom.

Remote access technologies

Enable phishing-resistant MFA for leading VPN applications such as Pulse Secure and Cisco AnyConnect, as well as other remote access applications, using Smart Card/PIV, one-time password (OTP), FIDO U2F, or FIDO2 capabilities.

Computer login

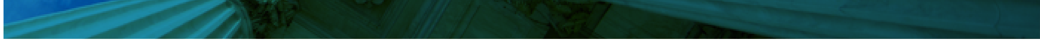
Secure computer logins for Macs and Windows computers, including those connected via Azure AD, AD and Microsoft Accounts. Option to use a YubiKey as a Smart Card + PIN.

Mobile / BYOD

Ensure phishing-resistant access via FIDO2/WebAuthn.

Step-up authentication for password managers

Integrate with enterprise-grade password managers including 1Password, Dashlane, Keeper Security, LastPass.



Getting started

To protect against the growing number of cyber threats that target remote and hybrid workers, organizations need a modern solution that provides phishing-resistant MFA at scale while also being easy-to-use and deploy. We have made it easy to deploy phishing-resistant MFA and passwordless authentication with the YubiKey. We offer a simple 6 Step Best Practice Deployment Guide to help accelerate modern MFA adoption at scale.

Plan

Ensure readiness by clarifying use 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

Yubico also offers YubiEnterprise Services, consisting of **YubiEnterprise Subscription** and **YubiEnterprise Delivery**, to help simplify procurement and distribution of YubiKeys into the hands of your distributed workforce.

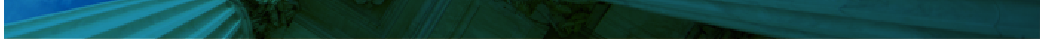
Yubico offers best-in-class industry deployment expertise and consulting to help guide you through all facets of a YubiKey implementation and deployment.

YubiEnterprise Services*		Yubico Professional Services		
YubiEnterprise Subscription	YubiEnterprise Delivery	Deployment 360	Workshops	Implementation projects
Simplifies how businesses procure, upgrade and support YubiKeys	Global distribution to remote and in-office locations through Yubico and trusted partners	Service hour bundles	Custom engagements	Technical engagements to implement YubiKeys in your environment

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

Contact us
yubi.co/contact

Learn more
yubi.co/remotework



YubiKeys in action

Real-world remote work success stories:

Halborn protects its global, remote workforce with YubiKeys

MAs a fully remote organization and a leading blockchain cybersecurity firm, Halborn consistently places a high priority on its security architecture. So, when co-founders Behnke and Walbroehl established Halborn as a fully-remote organization, they opted for the YubiKey. The YubiKey is now a standard component of every employee's onboarding process, even as the team has expanded to include members from over 50 different countries.

"The YubiKey provides that control and protection on the access layer," notes Steve Walbroehl, CTO and CoFounder of Halborn. "If there were a SIM swap or two-factor breach, the hardware piece—something you need—is now there so you can't use those credentials."

In the early days of the organization, Halborn reimbursed its employees for their choice of laptop and two YubiKeys, with the second spare key to be stored securely to protect against loss. Today, Halborn is shifting to a company-owned model to provide additional endpoint control, and leveraging dropshipping to supply pre-imaged laptops and YubiKeys directly to employees. Employees then follow Yubico's guided tutorials to set up their YubiKeys, which is often the "easiest component in onboarding," according to Walbroehl.

READ CASE STUDY →

yubi.co/halborn

> "As a blockchain security firm, securing information with strong MFA is non-negotiable. YubiKeys provide a really safe way to do this for every team member's account. Access and identity are the true perimeter of a remote organization. There's nothing better than a hardware device for protecting this."
>
> **Steve Walbroehl** | CTO and coFounder | Halborn

Figma protects remote workers with Okta and the YubiKey

In the last quarter of 2020, Figma, the maker of a cloud-based collaborative design tool, was looking for ways to implement strong authentication protection against potential phishing attacks for its remote employees.

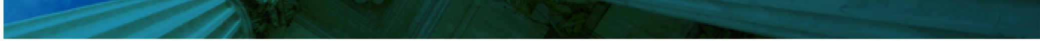
After careful consideration of all the authentication methods available in Okta, its identity provider (IdP), Figma landed on FIDO2/WebAuthn and the YubiKey as the only method to prevent account takeovers at scale. With geographically distributed employees and the stress of a newly remote workforce, Figma wanted to ensure onboarding caused as little disruption as possible.

The YubiEnterprise Delivery (YED) solution from Yubico simplified the procurement process and handled all the logistics of sending keys to remote employees, and the YubiKey integration with Okta gave Figma the ability to set security by risk level. Users were required to use FIDO2/WebAuthn when accessing critical-risk applications like AWS to start, eventually transitioning to FIDO-only authentication, including on mobile devices. Users were permitted to voluntarily self-register their FIDO security keys, which is a simple and fast process that happens in minutes.

READ CASE STUDY →

yubi.co/figma

> "I recommend signing up for YubiEnterprise Delivery, Yubico's service that ships YubiKeys to your employees anywhere in the world."
>
> **Devdatta Akhawe** | Head of security | Figma



Sources

[1] IBM, 2023 Cost of Data Breach Report, (July 24, 2023)

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

[3] Fortinet, 2023 Work-from-Anywhere Global Study, (March 7, 2023)

[4] PEW Research Center, About a third of U.S. workers who can work from home now do so all the time (March 20, 2023)

[5] Fortinet, 2023 Work-from-Anywhere Global Study, (March 7, 2023)

[6] Check Point, Check Point Research: Cyber Attacks Increased 50% Year Over Year, (January 10, 2022)

[7] Check Point, Check Point 2023 Mid-Year Security Report, (August 23, 2023)

[8] Fortinet, 2023 Work-from-Anywhere Global Study, (March 7, 2023)

[9] Ponemon Institute and Adaptiva, Managing Risks and Costs at the Edge, (July 13, 2022)

[10] IBM, 2023 Cost of Data Breach Report, (July 24, 2023)

[11] IBM, 2021 Cost of Data Breach Report, (July 28, 2021)

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

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

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

[15] Egress, Email Security Risk Report 2023, (March 8, 2023)

[16] Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (March 2, 2020)

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

[18] 451 Research, 2021 Yubico and 451 Research Study, (April 2021)

[19] Andras Cser, et. al., The Forrester Wave: Privileged Identity Management, Q4 2018, (November 2018)

[20] SANS, SANS 2021 Password Management and Two-Factor Authentication Methods Survey, (August 12, 2021)

[21] Google Cloud, April 2023 Threat Horizons Report, (April 2023)

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

[23] 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 modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.