



# Phishing-resistant MFA for your hybrid and remote workforce

## Five steps to improve security and productivity

Hybrid and remote work are here to stay. 70% of employees want a hybrid or remote working style, according to the 2021 State of Remote Work Report.<sup>1</sup> Yet, adapting to the flexible nature of hybrid and remote work can create IT security challenges which accelerates the need to be agile, and embrace digital transformation. With geographically dispersed employees, traditional perimeter security and legacy forms of authentication—such as usernames and passwords and mobile-based authenticators—are no longer adequate to protect access to networks, applications, and data. Usernames and passwords can be easily breached, and mobile-based authenticators are susceptible to phishing, malware, SIM swaps, and man-in-the-middle (MiTM) attacks, putting your organization at risk of a breach.

Protect your hybrid and remote employees against modern cyber threats, with the YubiKey—a multi-protocol hardware security key from Yubico that provides phishing-resistant two-factor (2FA), multi-factor (MFA), and passwordless authentication. The YubiKey comes in multiple form factors and provides a portable and simple user experience across desktops, laptops, mobile devices, and tablets. The YubiKey also enables self-service password resets which significantly reduces IT support costs. Organizations worldwide are deploying YubiKeys to their employees to ensure secure access to business networks, data, applications, and reduce operating costs.



Take the following five steps to protect your employees, network, and devices with the YubiKey:

### 1 Enable MFA access for Identity and Access Management (IAM) systems and Identity Providers

Most leading hybrid and cloud environments leverage IAM solutions to enable employees to work without the hassle of multiple usernames and passwords for different corporate applications and services. Enabling MFA on your IAM platform will enhance your security posture.

Strengthen security across your entire organization by turning on MFA with the YubiKey. Leading IAM platforms such as Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, OneLogin, Ping Identity platform and RSA SecurID® Suite natively support YubiKeys, and can be used for Single Sign-on (SSO) to messaging and video conferencing apps such as Microsoft Teams, Google Hangouts and Zoom.

### 2 Eliminate reliance on mobile-based authentication to protect against account takeovers

Two-step authentication methods such as one-time passcodes and on-device prompts are tied to mobile devices which can be compromised by malware, SIM-swapping, and MiTM attacks. Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts has proven that SMS and mobile authenticators are not very effective in preventing account takeovers and targeted attacks.<sup>2</sup>

## YubiKey integrations that help secure your hybrid and remote workforce



Protect your employees against account takeovers by replacing legacy mobile-based authenticators with the YubiKey. By leveraging modern FIDO2 and WebAuthn open authentication standards, you can provide the highest level of security assurance to protect workers against phishing and man-in-the middle attacks.

### 3 Secure remote access technologies with MFA

Virtual Private Networks (VPN) or Identity-Aware Proxies (IAP) are used across many organizations for access to corporate networks, protected resources or specific applications. Connecting via VPN or IAP provides security after connections are established, but connecting from unsecured home or public wifi can still be risky if VPNs or IAPs are secured using legacy forms of authentication.

The YubiKey secures remote access by enabling phishing-resistant 2FA or MFA for leading [VPN applications](#) such as [Pulse Secure](#) and [Cisco AnyConnect](#), as well as other [remote access applications](#), using smartcard (PIV), one-time password (OTP), FIDO U2F, or FIDO2 capabilities.

### 4 Protect computer login with MFA

If employee laptops are not secured properly, they can provide entry points for external threats leading to


a security breach, which can have financial, legal, and reputational repercussions for your business.

YubiKeys secure computer logins, protecting on-device applications and critical business data. Multiple login options include authentication for [Macs and Windows computers](#) including those connected via [Azure Active Directory](#), Active Directory and Microsoft Accounts. One of the most effective ways to secure computer access is to leverage the YubiKey smart card functionality, requiring a YubiKey and a PIN.

### 5 Enable step-up authentication for password managers

In a recent [SANS Report](#) on password management and 2FA, passwords are still the most used authentication method. Almost 100% of the respondents indicated that passwords are in use, even though passwords are susceptible to phishing attacks. Having phishing-resistant 2FA or MFA is very important to protect your employees and infrastructure.

The YubiKey integrates with [several enterprise-grade password managers](#)—including 1Password, Dashlane, Keeper Security, LastPass, and more, ensuring that lax password management policies don't cause a security breach.

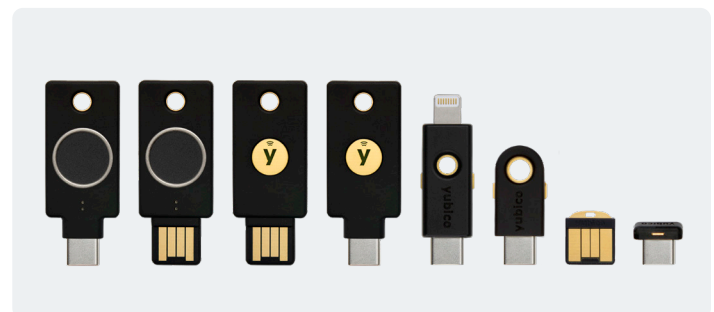


**YubiKeys deployed in:**

- 9 of the top 10 global technology companies
- 4 of the top 10 U.S. banks
- 5 of the top 10 global retailers

## Get started today and seamlessly deploy YubiKeys to your hybrid and remote workforce

Yubico makes it very convenient to get phishing-resistant MFA directly into the hands of your employees regardless of where they reside with [YubiEnterprise Delivery](#). This cloud-based service lets you streamline the distribution of YubiKeys and deliver to residential addresses in more than 49 countries across the USA, Canada and Europe.<sup>3</sup> By offering highest-assurance security, an accessible solution, and the best user experience, YubiKeys help drive high productivity for your employees, while minimizing cyber risk and operational costs. Stop your employees from becoming a cyber risk and instead, empower them with the YubiKey.



Contact the Yubico sales team today.

1. State of Remote Work Report 2021

2. Google Security Blog: New research: How effective is basic account hygiene at preventing hijacking

3. Customers outside of North America should contact their local Yubico rep for details

**About Yubico** As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: [www.yubico.com](http://www.yubico.com).

**Yubico AB**  
Kungsgatan 44  
2nd floor  
SE-111 35 Stockholm  
Sweden

**Yubico Inc.**  
530 Lytton Avenue, Suite 301  
Palo Alto, CA 94301 USA  
844-205-6787 (toll free)  
650-285-0088