yubico

Strong authentication for remote workers

Drive productivity while ensuring strong security

When remote work exploded in early 2020, many organizations scrambled to deploy security measures across their largely remote employee base. As the new security perimeter has expanded to include every employee's home network, shared devices, and BYOD, passwords and mobile-based authentication are not strong or secure enough to withstand the exponential rise in phishing and other cyber attacks.

To secure remote workers with convenient and strong authentication, Yubico offers the YubiKey—a multi-protocol hardware security key that protects against phishing attacks and account takeovers. Organizations worldwide are deploying the YubiKey for their remote workers, to ensure strong multi-factor authentication (MFA) access to business applications across company-owned and personal devices such as laptops, desktops, notebooks, and mobile devices. By offering highest-assurance security and the best user experience, YubiKeys help organizations drive high productivity for their remote workers, while minimizing cyber risk.

Five key steps to ensure strong authentication for remote workers

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.

Enhance security across your entire organization by turning on multi-factor authentication (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 Single On (SSO) to messaging and video conferencing apps such as Microsoft Teams, Google Hangouts and Zoom.

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 and SIM-swapping. 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.

Protect remote workers against account takeovers by replacing mobile authenticators and SMS 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.

YubiKeys deployed in:

9 of the top 10 global technology companies

4 of the top 10 U.S. banks

2 of the top 3 global retailers

Secure VPN access with MFA

VPN is used across many organizations for access to corporate networks, but connecting via VPN from unsecured home and public wifi can be risky, especially with authentication relying solely on passwords, as these are easily hacked.

The YubiKey ensures secure VPN access by acting as a strong second-factor authenticator. VPN applications such as Pulse Secure and Cisco AnyConnect, can be configured to work with a YubiKey as a smartcard (PIV) for remote access. Other VPN applications that offer native support for YubiKeys use the one-time password (OTP) capabilities.

Protect computer login with MFA

If remote 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.

Enable step up authentication for password managers

The majority of respondents in a recent Ponemon Institute report are still managing passwords with sticky notes and human memory. Whether your employees are remote or not, they need a simple and safe way to create, store, and manage multiple passwords.

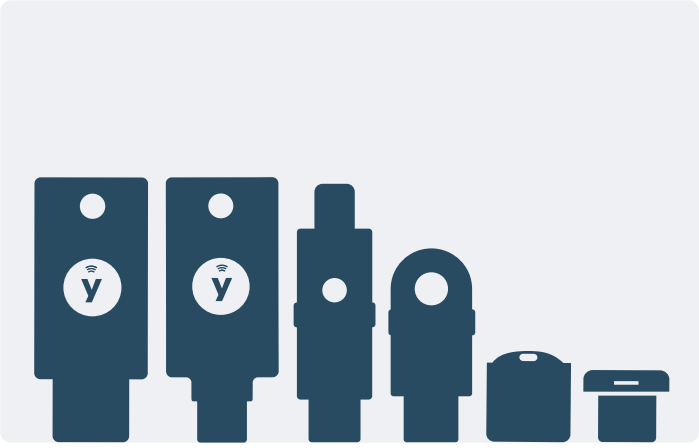
The YubiKey integrates with several enterprise-grade password managers including 1Password, Dashlane, Keeper Security, LastPass, and more, ensuring that lax password management policies don't cause a security breach.

YubiKey integrations that help secure remote workers

axiad · citrix · DUO · Google Cloud · Microsoft · okta · onelogin · PingIdentity · Pulse Secure · RSA

Deploy convenient and strong multi-factor authentication directly to remote employees

Yubico makes it easy to get convenient and strong authentication directly into the hands of your remote workforce with YubiEnterprise Delivery. This cloud-based service lets you streamline the distribution of YubiKeys and deliver to residential addresses in more than 30 countries across the USA, Canada and Europe. Don't let your remote workers become a cyber risk. Instead, choose the YubiKey with YubiEnterise Delivery for strong MFA security.



About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at 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