Phishing-resistant MFA for your hybrid and remote workforce
Five steps to improve security and productivity

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.

YubiKey integrations that help secure your hybrid and remote workforce

---

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

**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 ifVPNs 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.

**Protect computer login with MFA**

If employee laptops aren’t effectively secured, they can provide entry points for external threats leading to a security breach that 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**

Many enterprise employees rely on password managers, but if your password manager isn’t secured with phishing-resistant MFA, it is vulnerable to attack, offering attackers a repository of passwords for all your enterprise applications and data.

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.

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

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With YubiEnterprise Subscription, organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as YubiEnterprise Delivery, a global turnkey hardware key distribution service to residential and office locations across 49 countries.

Contact the Yubico sales team today.

---

**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.