yubico

Modern Authentication for Academic Medical Centers and Clinics

Hardware passkeys ensure cyber resilience with phishing-resistant MFA and exceptional UX

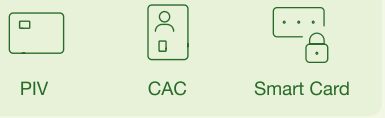
Advancing cybersecurity across academic healthcare

In any care delivery setting, cyberattacks are not only a privacy and confidentiality concern, but hold the potential to disrupt the care delivery process, posing a public health concern. In the case of ransomware, there is a direct link to mortality rates and complications for patient care following a ransomware attack. Securely accessing and sharing information in real-time across multiple platforms can be a matter of life and death, and enabling secure access to patient records to know previous diagnosis, allergies, and other healthcare information is critical for caregivers.

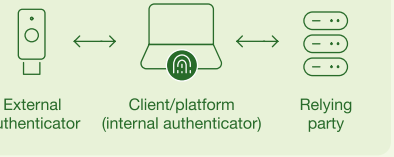
One of the first steps to stop cyber attacks is to ensure that phishing-resistant authentication is in place across the academic healthcare ecosystem to protect against cyber attacks and ensure cyber resiliency.

What qualifies as pishing-resistance MFA?

Channel binding PIV/CAC/Smart Card



Verifier name binding FIDO2/Web/Authn

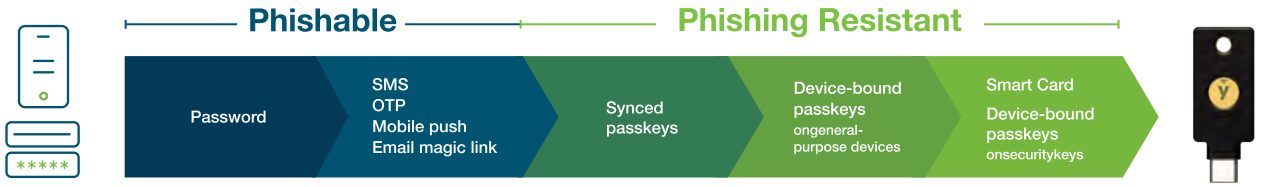


Rethink cybersecurity in the age of AI

Agentic AI and Generative AI make cyber attacks faster and more dangerous. AI allows for automation and accelerates the entire initial entry and attack lifecycle, compressing what used to take days or weeks into a matter of minutes. This significantly reduces the window for human defenders to detect and respond to an attack.

The use of legacy authentication, while still prevalent, puts healthcare ecosystems at risk of being breached. Usernames and passwords are easily hacked, and legacy mobile-based authentication, such as OTP, SMS, and push notification apps, are not phishing-resistant. Any user account that relies on legacy MFA that is not phishing resistant is susceptible to having credentials stolen.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64, only two forms of authentication meet the phishing-resistant mark: PIV/Smart Card and the modern FIDO2/WebAuthn (passkey) authentication standard.



The YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers the phishing-resistant FIPS 140-2 validated YubiKey. The YubiKey is a hardware security key that offers the most secure form of passkey, for highest-assurance multifactor and passwordless authentication.

The YubiKey provides the highest levels of security needed to protect against modern-day attacks, along with the flexibility to secure even the most complex scenarios all from a single key. With multiprotocol support, including Smart Card (PIV/CAC), FIDO U2F, FIDO2, OTP, and OpenPGP, the YubiKey supports both legacy and modern architectures with a single solution, providing a future-proof bridge to modern FIDO and passwordless authentication standards. With the YubiKey, healthcare institutions can implement FIDO2 passwordless, Smart Card passwordless or a hybrid strategy, depending on the infrastructure and use cases that need to be addressed.

By adopting YubiKeys, healthcare leaders can ensure they meet the highest cybersecurity standards while protecting against evolving cyber threats. Deploying YubiKeys is not just an IT decision, it's a critical step in safeguarding critical healthcare, PII, and financial data. YubiKeys enable secure and simple access to systems and data for all users, whether employees, contractors, shift workers, shared devices, laboratories, and clean rooms.

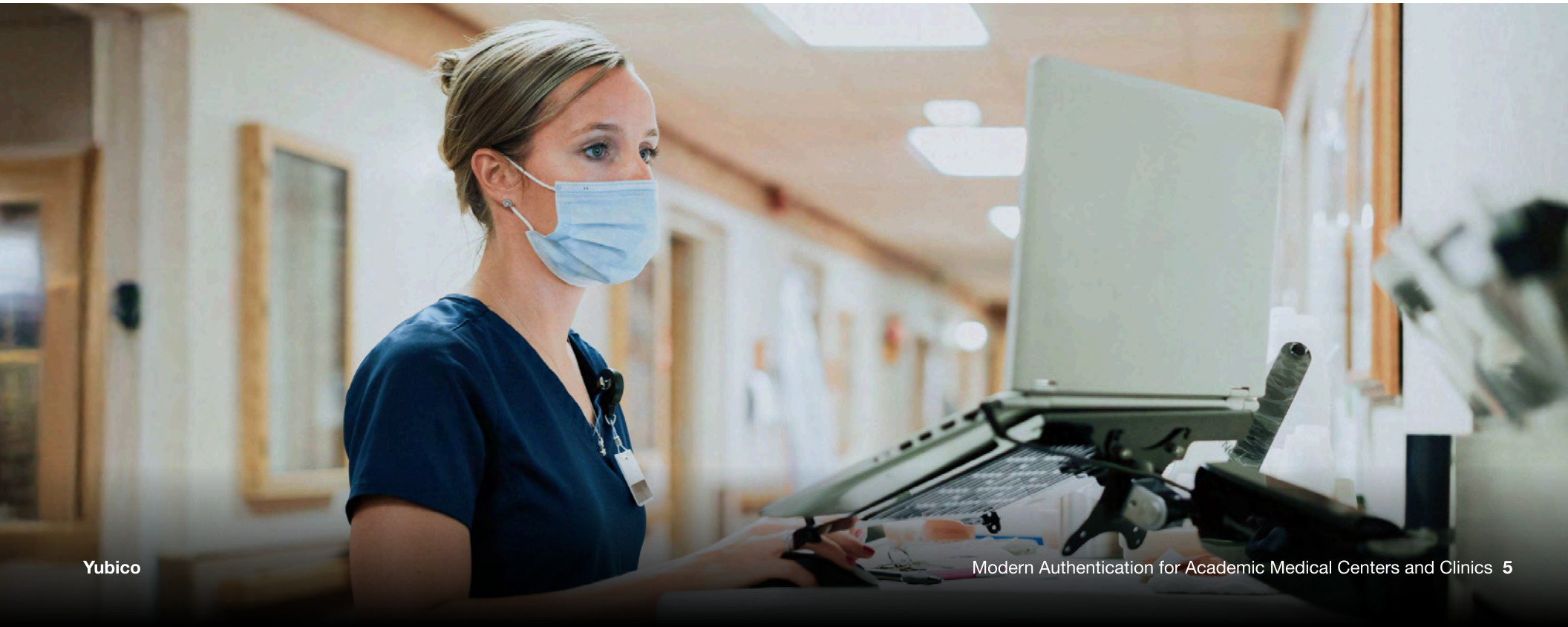
Securing caregivers and medical personnel

Healthcare systems struggle with legacy and siloed infrastructure, with authentication as a primary challenge for not only electronic health records (EHRs), but also other critical systems that support care across the care team. Hospitals struggle to enforce authentication on personal devices for clinical communication, with workarounds to computer access common to support more efficient clinical processes. Healthcare organizations need solutions that offer the highest authenticator assurance level with the lowest level of friction to support the clinician experience across multiple use cases and devices and serve as an alternative or supplement to existing smart card implementations.

YubiKeys offer the highest level of authentication security assurance and a simple user experience and serve as a portable root of trust. The credentials enable medical staff to authenticate securely to systems across shared workstations and devices that are common across this landscape.

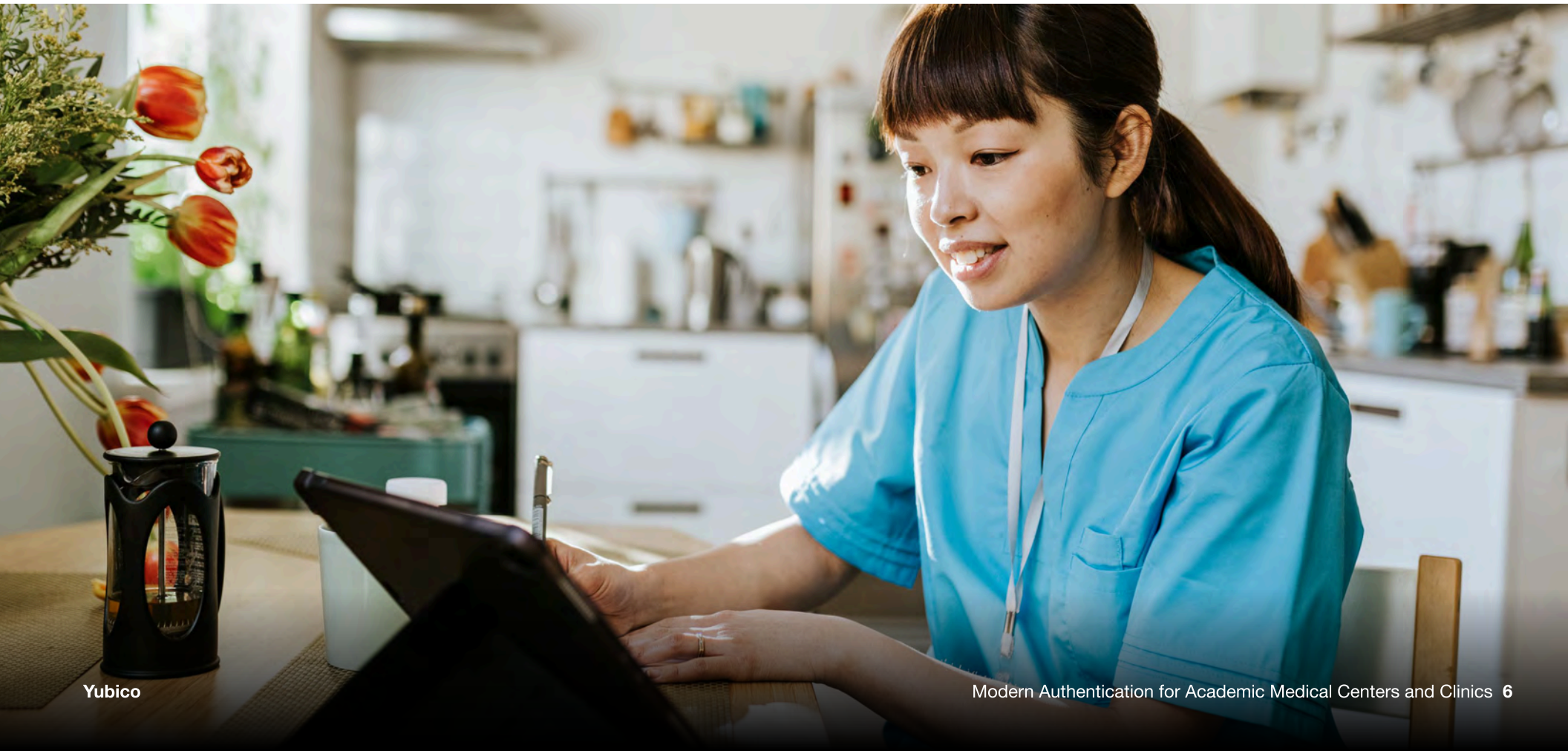
Securing shared workstations and mobile-restricted areas

The healthcare setting typically has multiple caregivers sharing the same system(s) to enter information, (order tests, coordinate care, and other purposes. Shared systems and shared devices that are common across hospitals and clinics, laboratories, and even clean rooms and restricted areas can benefit. For clean rooms it is important to consider solutions that don't require degloving and where fingerprint biometrics are impractical. Additionally, the authentication solution needs to work for non-employee providers and mobile-restricted areas such as call centers where mobile and personal devices may be restricted. Users can authenticate to the network across shared workstations and mobile-restricted areas with a single tap or touch of the YubiKey, proving they are a trusted user. A single YubiKey works across multiple shared devices, including desktops, laptops, mobiles, tablets, and notebooks, enabling users to utilize the same key as they navigate across devices. YubiKeys require no battery or internet connectivity and can be easily used by users wearing Personal Protective Equipment (PPE). They are are also easily reprogrammed, making them suitable for rotating-shift and temporary users across these environments.



Securing telework and personal devices

While password-based authentication may simplify remote access, relying on single-factor authentication does not satisfy zero trust security and phishing-resistant authentication requirements. Fortunately, YubiKey works with leading Identity and Access Management (IAM) and Identity Provider (IdP) solutions to enable phishing-resistant access for remote and hybrid employees, and across their personal devices, without the need for supporting infrastructure. The YubiKey is able to meet the demands of your employees' movements, providing a convenient solution that is portable. The purpose-built hardware on the YubiKey, including a touch sensor, provides a mechanism that can verify that the person logging in is a real human, and not a trojan or remote hacker.



Securing pharmacy ecosystems

Pharmacy retailer organizations are one of the latest targets of cyber threat actors, including the breach of Change Healthcare that affected the personal information of 190 million individuals. As pharmacies collect personal details and personal health information (PHI) from customers to dispense prescription medications, they are subject to a variety of strict regulations with varied challenges associated with privileged users and data protection challenges associated with legacy systems at the retail point-of-sale (POS) level.

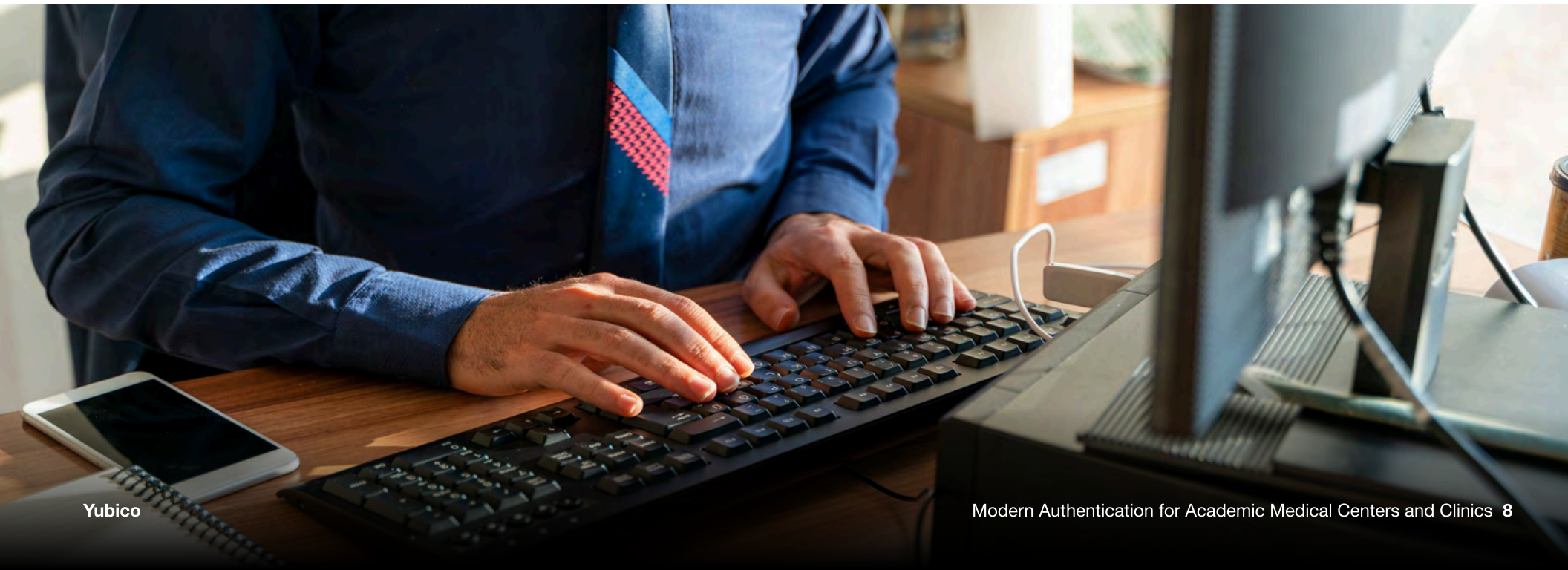
Pharmacy organizations have identified the critical need to modernize authentication to improve corporate access to data, as well as to streamline and secure shared workstation access at the retail level. The YubiKey enables phishing-resistant authentication to pharmacy systems to secure them and protect patient data.

Securing privileged users

Privileged users that require step-up authentication can use a Yubikey for access. The YubiKey offers the highest-assurance security that can be used to authenticate privileged users to both legacy and modern applications and secure access to devices. Further, the YubiKey supports multiple protocols, enables public key cryptography and URL binding, stores authentication secrets on a secure hardware chip, and restricts data from being copied or exported—all of which amounts to best in class security for authenticating privileged users across the enterprise. As an example, Microsoft Entra ID now supports the enrollment of YubiKey as a FIDO2 authenticator. With this feature, system administrators are able to quickly enroll YubiKeys on behalf of their privileged user roles, to solidify enterprise security and meet phishing-resistant authentication requirements.

Securing office and administrative workers

Administrative staff can easily use the YubiKey for access to resources regardless of the device being used to connect. Having a provisioned YubiKey offers flexibility to use both office desktops and personal laptops for access, providing a strong productivity workflow for daily tasks. The YubiKey comes in multiple form factors and can be used across desktops, laptops, and mobile devices without the need for an additional smart card reader peripheral device.



Securing third-party medical suppliers and supply chain

Healthcare partners often need access to systems to provide service updates, update records, and provide other information. These suppliers may have access to sensitive information and access should be secure via phishing-resistant authentication. Protecting downstream supply chains is not easy given the hundreds (if not thousands) of entry points that need to be monitored along the way and there is an urgent need to ensure that the right steps are taken from a security perspective. Organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain. The YubiKey provides modern phishing-resistant authentication at scale across the supply chain, ensuring that all suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical IP handoffs.

Ready to get started?

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 use cases and leveraging the insight from over thousands of implementations to date. We have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale.

Plan

Ensure **readiness** clarify use cases and user populations

Validate

Confirm the **process** with a small group of users before broader rollout

Intergrate

Ensure key apps and service are **Yubikey-ready**

Launch

Distribute keys to users with **turnkey delivery** service or channel partnerx]s

Adopt

Drive adoption with best practice **training and support**

Measure

Report on security and business value impact

The YubiKey 5 Series –
from left to right: YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

The YubiKey 5 FIPS Series –
from left to right: YubiKey 5C NFC FIPS, YubiKey 5 NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS

Bailment agreement can be established to obtain Not for Resale (NFR) YubiKeys for proof of concept (POC) programs. These YubiKeys are not required to be returned and, as a condition of use, are not to be continued for enterprise use at the conclusion of the POC. Yubico also offers solutions engineering support for architecture design and review, and IDP configuration guidance through the POC.

Organizations can purchase YubiKeys via a one-time perpetual purchasing model or can opt for greater flexibility with a subscription model:

- With YubiKey as a Service, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets their technology and budget requirements. This service also provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits. Organizations automatically gain access to the Customer Portal, a centralized, web-based dashboard for IT teams to efficiently deploy, track, and manage YubiKey deployment, with real-time visibility into inventory, rollout progress, and user activation. Organizations also have access to turnkey Enrollment and Delivery services that help IT get users quickly onboarded with YubiKeys to fast track to phishing-resistance and then get YubiKeys to end users across the world, including corporate and residential addresses. Users can even experience self-service ordering of YubiKeys, giving them the freedom to have the keys shipped to their preferred address anytime they need. YubiKey as a Service customers receive continual enhancements to available and new services assuring a smart and future-proofed security investment.
- Yubico's Professional Services team can help you with a successful implementation. Yubico offers a wide variety of advisory services in support of your YubiKey implementation and deployment, including best practices workshops, technical implementation packages, on-demand consulting resources and custom engagements. Our Professional Services team is comprised of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector. From standard implementations to complex enterprise rollouts, Professional Services has the skills and

yubico
The Key to Trust

Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, the original passkey, we set the gold standard for secure and simple login, stopping account takeovers with phishing-resistant, hardware-backed authentication.

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone's reach. Learn more at www.yubico.com.