yubico

WHITE PAPER

Modernizing MFA and going passwordless across the healthcare sector

Prioritizing the human layer to protect against modern cyber threats

Contents

The critical need for security and efficiency across the healthcare sector

$10.93 million

cost of data breach[1]

61%

of breaches attributed to external attacks[2]

57%

of significant security incidents involved **phishing**[3]

66%

of organizations were hit by **ransomware**[4]

61%

of data breaches traced back to **credentials**[5]

The Healthcare and Public Health (HPH) sector is large, spanning public and private sectors including healthcare facilities, research centers, manufacturers, health plans and payers, and suppliers. Across the sector, organizations are facing a growing rate of cyberattacks, up in volume (69%) and complexity (67%) over the prior year.[6]

According to a HIMSS cybersecurity survey, the most significant security incidents in healthcare can be attributed to either a phishing attack (45%) or ransomware (17%).[7] Most cyberattacks in healthcare focus on weaknesses such as the low implementation of security controls, with only 34% of healthcare respondents applying multi-factor authentication (MFA) across the organization.[8] These unsecured touch points across the healthcare ecosystem are putting data—and patient lives—at risk.

An analysis of the U.S. Department of Health and Human Services (HHS) data demonstrates an 84% increase in the number of data breaches in healthcare between 2008 and 2021.[9] Further, data breaches in the first five months of 2022 nearly doubled from the same period the year prior.[10] Healthcare organizations impacted by cyber attacks face not only data breach costs, but additional risks to the privacy and confidentiality of medical information that could compromise care or interrupt care delivery, in the case of ransomware. Across the sector, additional risks include loss of production time, or risks to intellectual property and product integrity.

Healthcare organizations have identified the critical need to modernize authentication and security to protect sensitive healthcare information and the specific Information Technology (IT) and Operational Technology (OT) environments that vary widely across the sector. However, the unique sets of challenges faced across the healthcare sector have resulted in many organizations not keeping pace with the evolving cybersecurity attack landscape.

Authentication & security challenges faced across healthcare sectors

Health plans and payers

- Mobile-restricted areas
- Legacy infrastructure
- Big data
- Remote work
- Shared workstation environments
- Supply chain

Pharmacies

- Shared workstation environments
- PPE, gloved environments
- Highly targeted privileged users
- Remote work
- E-prescription

Health technology (devices)

- Product component integrity
- Protecting manufacturing and design IP
- Medical device regulations
- Unauthorized access to devices

Healthcare delivery organizations (HDOs)

- Legacy, siloed infrastructure
- Shared workstation environments
- PPE, gloved environments
- Mobile-restricted areas
- Work disruption concerns

Looking for information specific to the pharmaceutical industry? Refer to the Yubico white paper Maximizing security across Pharma's digital transformation with phishing-resistant MFA.

Across the healthcare sector, organizations need solutions that can offer modern security capabilities, helping transition to a more secure, passwordless workflow for a better user experience and overall efficiency. A passwordless workflow replaces insecure passwords with a form of authentication that doesn't require the user to provide a password at login such as SMS verification, smart card, or hardware security key. On the journey to passwordless, healthcare CISOs must design a security strategy that speaks to the organization's particular risk landscape and security needs, complex infrastructure, and usability goals.

Health plans and payers

Health plans and payers are entrusted with large volumes of sensitive data, including PHI as well as other forms of personal information. With legacy infrastructure, security and access controls such as MFA may be inadequately applied and enforced, with additional challenges presented by big data, mobile-restricted and shared workstation environments (call centers), and the growing levels of remote work. At the same time, health plans and payers are consistently under pressure to reduce costs, which involves a greater use of third-party software to identify cost saving opportunities.

With a growing focus on the software supply chain, many health plans and payers are focusing on efforts to protect third-party access to their systems.

Pharmacies

Pharmacy retailer organizations are one of the latest targets of cyber threat actors, including the recent breach by pharmacy retailer Dis-Chem that affected the personal details of 3.6 million customers.[11] As pharmacies collect personal details and 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. For those with active Salesforce CRM implementations, a new MFA requirement is accelerating this shift to modern authentication standards.[12]

Health technology (devices)

For health technology organizations who create medical devices or assistive technology such as medical robotics, concerns mirror those of manufacturing organizations, with additional concerns related to the stringent requirements of medical device regulations (see below).

From a manufacturing perspective, it is crucial to ensure authenticity of all components to avoid unsolicited replication and theft, but also for quality assurance, since an assembly line should only consist of genuinely sourced products, which may come from different manufacturing plants and third-party manufacturing facilities around the world. Product integrity challenges can occur if component firmwares aren't digitally signed and certified to ensure component authenticity and integrity at the end of respective production lines.

Health technology organizations need solutions that can be quickly and easily deployed to support the quality, integrity, and intellectual property (IP) of all components in the end-to-end process—from production and assembly, to repair and replacement.

Healthcare delivery organizations (HDOs)

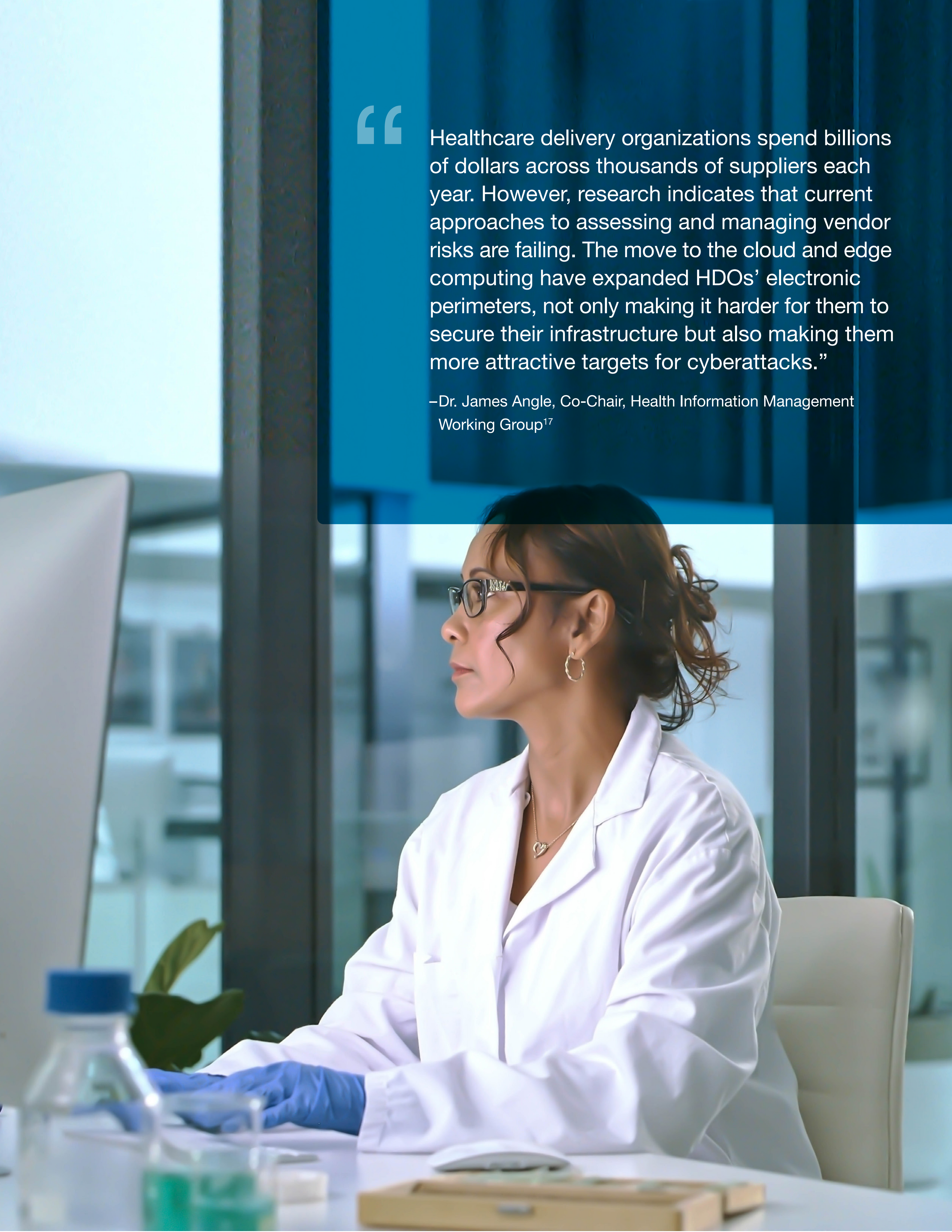
In the care delivery setting, cyberattacks are not only a privacy and confidentiality concern, but hold the potential to disrupt the care delivery process. In the case of ransomware, there is a direct link to mortality rates following a ransomware attack.[13] In 2017, a ransomware attack against the United Kingdom's National Health Service (NHS) caused disruption to over 200,000 systems across 150 countries.[14] Since then, cyberattacks against HDOs have been on the rise, particularly during the pandemic, with CISA recently putting hospitals on high alert to potential Russian cyberattacks.[15]

Health care systems struggle with legacy and siloed infrastructure, with authentication a primary challenge for not only EHRs, but all the other systems required to support and coordinate care across the care team. Many hospitals struggle to enforce authentication on personal devices for clinical communication, with workarounds to computer access common in order to support more efficient clinical processes.[16]

HDOs 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. Further, this solution should extend beyond the clinical floor to address the authentication needs of privileged users such as administrative and IT.

The Yubico white paper Protecting manufacturing with highest-assurance security provides specific advice on securing the health technology supply chain.

> “Healthcare delivery organizations spend billions of dollars across thousands of suppliers each year. However, research indicates that current approaches to assessing and managing vendor risks are failing. The move to the cloud and edge computing have expanded HDOs’ electronic perimeters, not only making it harder for them to secure their infrastructure but also making them more attractive targets for cyberattacks.”
>
> –Dr. James Angle, Co-Chair, Health Information Management Working Group[17]



> “It is unsettling to know that hackers are not only eager to take advantage of the pandemic crisis, but that they’re feeding off of a highly profitable supply chain of stolen digital assets to do so. While hospitals are the target, the patient is ultimately the true victim of this cyber attack machine.”[18]
>
> **David Sygula | CPO Magazine**

Evolving security regulations

The HPH sector is subject to strict security requirements and an increasing regulatory burden. The number of global regulations continues to increase, with new changes emerging to industry frameworks and standards as well as state, federal and global levels including the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA). In healthcare specifically, there have been recent updates to the Health Insurance Portability and Accountability Act (HIPAA), 21 CFR Part 11 (code of Federal Regulations Title 21) by the Federal Drug Administration, SUPPORT Act / EPCS, and the CURES Act Final Rule.

The health technology industry is subject to a variety of additional regulations, including the Medical Device Single Audit Program (MDSAP), the EU Medical Device Regulations (EU MDR) and ISO 13485:2016, which governs quality management systems for medical devices, and the FDA’S recommendations for the postmarket management of cybersecurity in medical devices.

In response to rising rates of cyberattacks against critical infrastructure, the White House issued Executive Order (EO) 14028 and OMB memo M-22-09, setting a new bar for cybersecurity for federal agencies, their staff, contractors, and partners—including those in healthcare and, in particular, medical device manufacturers. These directives include a requirement to adopt a Zero Trust architecture strategy and implement phishing-resistant MFA consistent with NIST SP 800-63B.[19]

Phishing-resistant MFA refers to an authentication process that is virtually immune to sophisticated attacks that could intercept or trick users into revealing access information. As defined by the Federal Information Processing Standards (FIPS) 140-2 and NIST SP 800-63B, only two authentication technologies currently meet this requirement: the federal government’s Personal Identity Verification (PIV) standard/ SmartCard and the modern FIDO2/WebAuthn standard.

Prioritizing the human layer

Given the many incentives and imperatives to tighten healthcare cybersecurity postures, it's clear that traditional models aren't going to suffice. It's time to focus more intently on 'the human layer'—the authentication layer that allows individuals to securely and efficiently access any system, app or data.

Traditional security models focus on protecting, managing and controlling access to the many layers that make up our enterprise architecture, as 61% of data breaches can be traced back to credentials in some way.[20] Privileged users (administrative or IT staff) who have legitimate access to critical systems and sensitive and valuable PHI are a prime target for cyber criminals. Phishing is the initial point of compromise in 71% of cyberattacks in healthcare, underlining the importance of updating access controls consistent with Zero Trust principles as the first line of defense.[21]

The Zero Trust framework is a journey, and implies that an organization should trust no individual or thing unless properly verified before being given access to the network and data. Strong authentication is a foundational aspect of that journey, enabling phishing-resistant user identity verification before access is provided.

Prioritizing the human layer is about challenging the drawbacks of conventional MFA, which falls short on security, user experience, and leads to IT complexity to procure and manage devices and ongoing password resets.

The challenges with legacy MFA

Conventional authentication and security solutions, including usernames and passwords and mobile-based authenticators, are no longer effective to protect healthcare organizations against modern cyber threats. Beyond security, legacy mobile authentication creates friction in the user experience if users are not able to seamlessly authenticate. Authentication is a mission-critical service, and if users can't log into the apps or devices they use, they can't do their job.

Drawbacks of mobile-based authenticators

Vulnerable to attack
Every mobile authenticator can be phished

Expensive to maintain
$1840/user in enterprise mobility costs

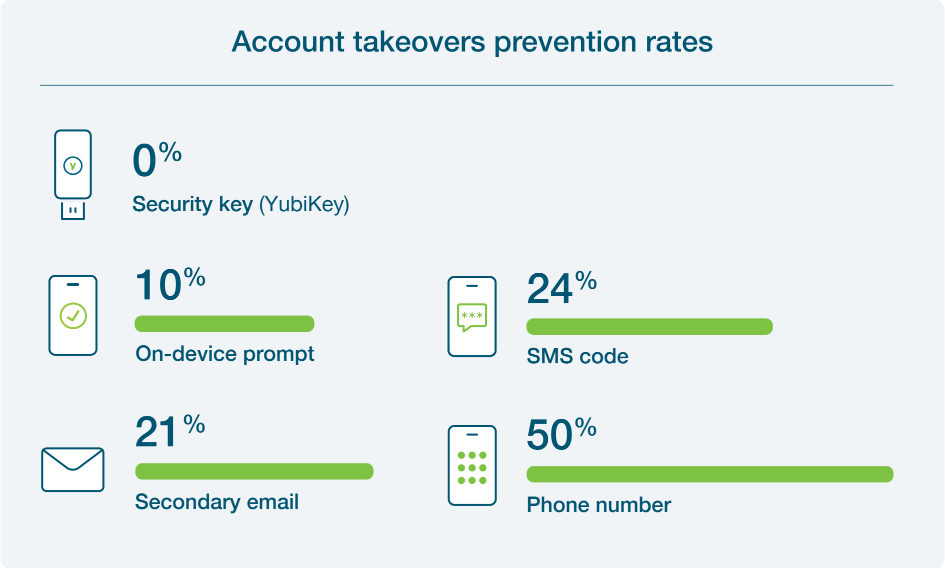
Poor user experience
Complex to operate and manage

Security gaps
Many users can't or won't use it

Short-term solution
Legacy MFA isn't built for the future

Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based one-time-password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%.[22] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of *if* you will be attacked – it's a matter of *when*.

With legacy MFA such as SMS, OTP, and push app, the second factor is tied to the mobile device. This is a red flag, because of four aspects. (1) There can be availability challenges with mobile devices sending codes in a timely manner due to poor connectivity or unreliable services. (2) There is no real guarantee that the private key ends up on a secure element on the mobile device. (3) The OTP or private key could be intercepted in some way (such as via SIM swapping), and (4) It is impossible to ensure proof of possession—or in NIST terms—impossible to prove it is impersonation-resistant.


Account takeovers prevention rates

Google: How effective is basic account hygiene at preventing hijacking

> “Look at it from the patient perspective, not just username and password. Every point of access is a potential threat to security and could allow hackers to find back channels. Providers must protect all security gaps.”[23]
>
> **Erin Benson | Senior Director of Market Planning, LexisNexis Health Care**

The journey to passwordless authentication

Passwordless authentication is any form of authentication that doesn’t require the user to provide a password at login. There are many different implementations of passwordless authentication today. While traditional MFA approaches are highly phishable and vulnerable to remote account takeover attacks, modern MFA approaches, including passwordless MFA, offer strong phishing resistance and are proven to stop account takeovers in its tracks.

Traditional MFA alternatives		Modern authentication & the passwordless future
☎ SMS/Voice	123 TOTP	**YubiKey:** Phishing-resistant MFA and passwordless authentication

Organizations can choose to implement smart card passwordless, FIDO2 passwordless using a biometric or a PIN, or a hybrid passwordless approach involving a mix of smart card and FIDO2 passwordless, depending on their existing infrastructure and user scenarios. And, the user can simply authenticate using a passwordless device, such as a hardware security key that can support both smart card and FIDO2 protocols to verify their credentials with the application or system.

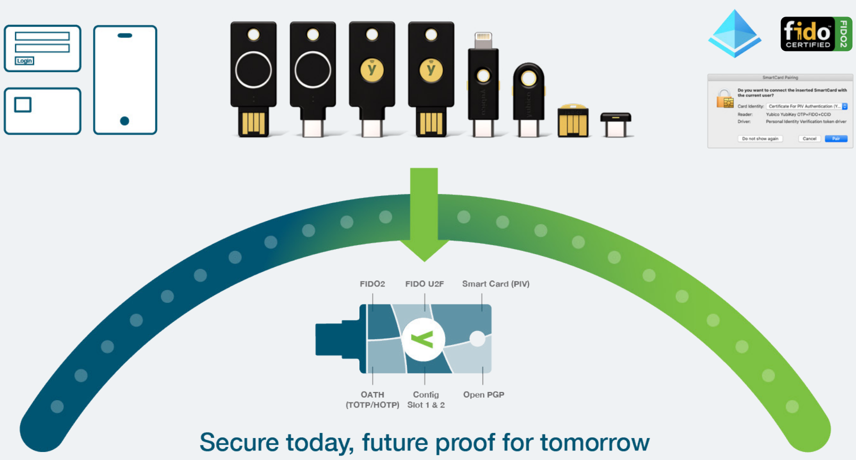
As new passwordless authentication methods are constantly evolving, passwordless solutions should support open standards for maximum interoperability, having an authenticator that can work across the board for all IdP/IAM vendors to provide consistency, usability and security.

YubiKeys offer healthcare organizations modern, phishing-resistant MFA and a bridge to passwordless

The YubiKey provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware authenticator protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[24] The YubiKey uses modern authentication protocols such as FIDO U2F and FIDO2/WebAuthn open authentication standards to help eliminate phishing-driven credential attacks and meet the requirements of EO 14028 and OMB M-22-09. YubiKeys also support SmartCard, OTP, and OpenPGP protocols, enabling the use of a single security key across a variety of modern and legacy systems, regardless of where healthcare organizations are in their journey to strong authentication and passwordless.

> “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**

Bridge to Passwordless with the YubiKey


Login
fido CERTIFIED
FIDO2
SmartCard Pairing
Do you want to connect the inserted SmartCard with the current user?
Card Identity: Certificate For PIV Authentication (Y...
Reader: Yubico YubiKey OTP+FIDO+CCID
Driver: Personal Identity Verification token driver
Do not show again
Cancel
Pair
FIDO2
FIDO U2F
Smart Card (PIV)
OATH (TOTP/HOTP)
Config Slot 1 & 2
Open PGP

Secure today, future proof for tomorrow

The versatile YubiKey requires no software installation, battery, or cellular connection, making it ideal for mobile-restricted environments and shared workstation environments. Users can benefit from a frictionless authentication workflow—a user plugs the YubiKey into a USB port and touches a button to authenticate.

To further improve the user experience and speed of authentication, Yubico also offers the YubiKey 5C NFC edition, supporting tap-and-go authentication on NFC-enabled devices or to authenticate to an IAM (Ping, Okta, Duo) to perform SSO to other applications. When combined with a silicone wristband, the YubiKey can solve critical pain points around sanitation and efficiency.

For regulated environments, the YubiKey 5 FIPS series is a FIPS 140-2 validated security key that meets the highest authenticator assurance level 3 (AAL3) requirements from NIST SP 800-63B.

YubiKey use cases in healthcare

With the YubiKey, healthcare organizations can implement FIDO2 passwordless, smart card passwordless or a hybrid strategy, depending on the infrastructure and use cases that need to be addressed. A common practice is to deploy YubiKeys first where there are MFA gaps, such as users who can't use mobile authentication (e.g. call centers), remote workers or visiting physicians and to privileged users with direct access to high-risk systems and applications. Next, YubiKeys can be deployed across the supply chain to protect third-party access as well as the integrity of products, IP and the software supply chain. Finally, the YubiKey can replace insecure mobile-based authentication methods with hardware-backed TOTP before being deployed organization-wide to address various risk profiles.

The YubiKey is uniquely designed to support every use case in the healthcare setting, including:

Privileged accounts
Secure privileged account users to access sensitive patient data and critical IT systems

Shared workstations
Protect shared workstation users such as nurses stations or pharmacy POS systems while maintaining convenience and patient security

Remote workforce
Enable secure access in mobile working environments

Mobile restricted
Secure clean room environments and parts of the healthcare facility where mobile is not an option

Office workers
Improve UX and security for hospital workers accessing their emails and productivity tools

3rd party user
Protect system access by 3rd parties operating withuin the healthcare facility

Summary

Modern healthcare organizations require modern solutions to drive security and efficiency and to minimize costs—and ultimately protect patient privacy and health.

The high value of health data, and the increasing rate of cyber attacks against the entire healthcare sector has underscored the need for a secure, scalable solution that works with a variety of legacy and modern infrastructure to help create a bridge to passwordless authentication to protect against modern cyber threats.

The YubiKey is a secure, portable, easy-to-use solution designed to meet healthcare organizations where they are today on their journey to passwordless, with phishing-resistant MFA as the first step in the journey and offering a bridge to passwordless, all while helping to seamlessly support legacy infrastructure as well as modern, cloud-based systems. The YubiKey makes authentication effortless for all users, helping patch critical weaknesses in the human layer of security, and putting the human layer first.

The YubiKey

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition, YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

Contact us
yubi.co/contact

Learn more
yubi.co/healthcare

Sources

[1] IBM, 2023 Cost of Data Breach Report, (Accessed November 1, 2023)

[2] Verizon, 2022 Data Breach Investigation Report, (Accessed June 27, 2022)

[3] HIMSS, 2021 HIMSS Healthcare Cybersecurity Survey, (January 28, 2022)

[4] Sophos, The State of Ransomware in Healthcare 2022, (June 1, 2022)

[5] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021)

[6] Sophos, The State of Ransomware in Healthcare 2022, (June 1, 2022

[7] HIMSS, 2021 HIMSS Healthcare Cybersecurity Survey, (January 28, 2022)

[8] HIMSS, 2021 HIMSS Healthcare Cybersecurity Survey, (January 28, 2022)

[9] Critical Insight, 2021 H2 Healthcare Data Breach Report, (Accessed June 29, 2022),

[10] Peyton Doyle, Healthcare breaches on the rise in 2022, (June 20, 2022)

[11] Benjamin David, Pharmacy Giant Hit by Data Breach Affecting 3.6 Million Customers, (May 18, 2022)

[12] Salesforce, Multi-Factor Authentication FAQ, (Accessed July 6, 2022)

[13] Rebecca Pifer, Quarter of providers saw mortality rates rise after ransomware attacks, survey finds, (September 24, 2021)

[14] Roger Collier, NHS ransomware attack spreads worldwide, (June 5, 2017)

[15] CISA, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, (April 20, 2022)

[16] Ross Koppel, et al, Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient?, (Accessed July 6, 2022)

[17] Cloud Security Alliance, Healthcare Supply Chain Cybersecurity Risk Management, (May 12, 2022)

[18] David Sygula, Inside the Cyber Attack "Machine": What Hospitals Need to Know about the Dark Web and Post-Pandemic Threats, (April 22, 2021)

[19] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021); OMB, Moving the US Government Toward Zero Trust Cybersecurity Principles, (January 26, 2022)

[20] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021)

[21] HIMSS, 2021 HIMSS Healthcare Cybersecurity Survey, (January 28, 2022)

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

[23] HealthITSecurity, Can MFA help healthcare's security posture?

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.