Yubico and Okta

Raising the bar for security and accelerating to passwordless

Turnkey modern authentication with Yubico
FIDO Pre-reg and Okta Adaptive MFA

yubico | okta

Abstract

Picture a cyber attacker slipping past your defenses due to inadequate phishing protection. Frequently, the simplest method to breach security is by taking advantage of human error and stealing user credentials. In fact, according to the latest Verizon DBIR report, 68% of breaches are caused by stolen credentials and hackers don't hack in…they simply log in, disguised as a legitimate user.

Yubico and Okta have long partnered together to offer solutions that overcome these challenges and to innovate together to offer trusted solutions to safeguard organizations from an ever-changing cybersecurity landscape.

This eBook demystifies the essentials of phishing-resistant MFA—how it works, the problems it solves, and how phishing-resistant users can be created that lead to phishing-resistant organizations that stay consistently protected from modern cyber threats. And, to help organizations stay agile and future-proofed against the evolving threat and regulatory landscape, authentication services such as YubiKey as a Service and Yubico FIDO Pre-reg revolutionize the way modern enterprises can stay ahead of modern attacks and move at market speed as their business evolves.

Modern cyber threats require stronger protection against phishing

Phishing is a gateway crime. More than 90% of cyber-attacks begin with phishing.[1] According to the most recent Phishing Landscape report,[2] the total number of phishing attacks grew by nearly 50,0000 attacks compared to the year before to just under 1.9 million incidents worldwide.

Cybercrime continues to grow at an alarming rate worldwide, and the impacts on consumers, businesses, and institutions are devastating. Cybercrime incidents and related monetary losses reached record highs in 2023. The U.S. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), for example, conservatively estimated over $12.5 billion in direct losses in the US alone, a 10% in cybercrime complaints and a 22% increase in financial losses compared to 2022.

With jaw-dropping growth numbers like these coming out every year, organizations who fail to modernize their security approach are bound to find themselves next in line.

Here's the bottom line:

Developing a phishing-resistant identity solution is essential to adequately protecting your organization, further justified by the continued growth of phishing attacks and pressures from the federal government to harden cybersecurity defenses.

[1] CISA, Be cyber smart: Get your "Shields Up"–Simple Steps for Safety Online

[2] Interisle, Phishing Landscape 2024 Report

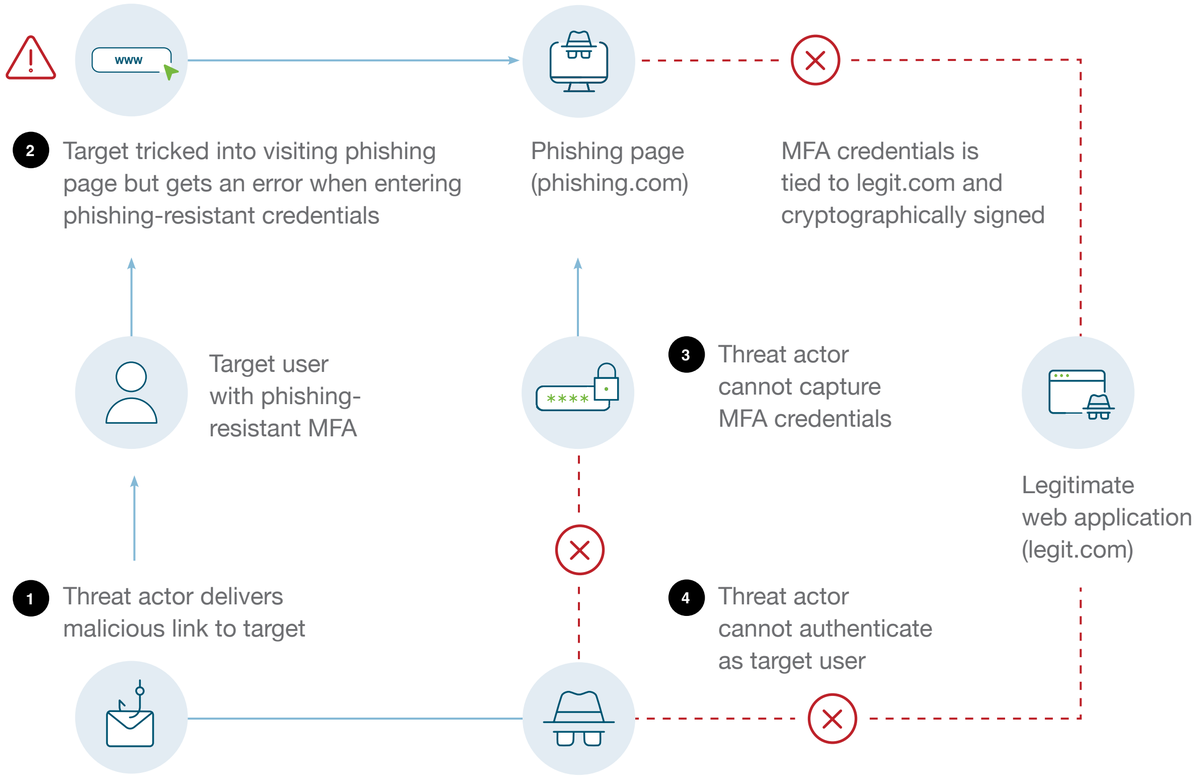
Demystifying phishing-resistant MFA and how it protects users

Possession and securing the credential is a critical component to any phishing-resistant approach. Moving to modern MFA also paves the way for organizations to eliminate passwords altogether and move to a secure, passwordless environment that enhances security and also efficiency.

According to the NIST 800-63B-4, “Phishing resistance is the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an imposter relying party without reliance on the vigilance of the subscriber”.

In other words, phishing-resistant MFA that’s effective should not require the user to have to make important security decisions that they are not inherently trained to make. And, even if the user is tricked into supplying their credentials in a phishing attack, their form of MFA should ideally not be circumvented.

Phishing-resistant MFA removes the human element from the authentication process. With phishing resistant MFA, the credential is *cryptographically bound to the domain*, which means it cannot interact with fake domains created by bad actors. Leveraging public key cryptography that is bound to a domain from a device, a user possesses very strong defense against these types of attacks.



Not all MFA is created equal. Legacy MFA is broken and easily breached.

Phishing attacks are on the rise, but not all forms of multi-factor authentication (MFA) are phishing-resistant. Legacy MFA, such as SMS, OTP and mobile authentication applications, have been proven to be vulnerable repeatedly as these methods are easily bypassed by attackers using phishing, malware, ransomware, SIM swaps, and attacker-in-the-middle attacks.

Modern, phishing-resistant MFA, offered only by FIDO or Smart Card/PIV protocols, have been proven to stop account takeovers in their tracks. And hardware-backed authentication, such as through modern hardware security keys that support both FIDO and Smart Card/PIV authentication protocols, have been proven to stop remote attacks and account takeovers every time.

FIDO Approach

FIDO/WebAuthn is an industry standard and widely available phishing-resistant authentication protocol. This method performs a cryptographic based authentication ceremony between the FIDO authenticator and the pre-registered relying party. The ceremony is only performed from requests initiated from registered domains thus blocking fake domain sites from capturing credential and access session information, making use of something you are, like your unique fingerprint, or something you know, like a PIN, to unlock the authenticator to perform the phishing-resistant authentication ceremony for an additional authentication factor.

Smart Card Approach

Smart card-based authentication offers strong phishing-resistant MFA and offers a path to passwordless. Smart cards leverage public key cryptography-based authentication that is bound to a domain. The smart card PIV standard is used heavily by governments and large enterprises.

Okta Adaptive MFA framework enables phishing-resistant MFA implementations

Supporting Smart Card-based authentication

Okta integrates with existing smart card infrastructures and systems, allowing organizations to leverage their current smart card investments to provide a passwordless phishing-resistant MFA. Okta's environment works seamlessly with modern hardware security keys that can act as smart card authenticators delivering a raised level of protection. The certificate that resides within a modern hardware security key is hardware-protected and cannot be copied.

Enabling FIDO-based authentication

Okta's Adaptive MFA framework supports FIDO/WebAuthn and works seamlessly with modern hardware authenticators to raise the bar for security during the phishing-resistant authentication ceremony. This FIDO approach can be leveraged for passwordless authentication or used as an additional factor in Okta's Adaptive MFA framework to allow for phishing-resistant MFA implementations.

Delivering Okta FastPass for secure access

The Okta FastPass journey begins with an enrollment (or adding an account) process on the Okta Verify app of your device. Okta Verify is an MFA authenticator app used to confirm a user's identity when they sign in to Okta or protected resources. After you add Okta Verify as an authenticator, you configure the options that control how end users interact with Okta Verify when they authenticate, such as enabling Okta FastPass. Okta FastPass is a proprietary device-bound solution that provides passwordless authentication and includes device compliance and risk signals, resulting in risk-aware access to Okta-managed applications.

Yubico YubiKeys deliver strong phishing defense and ransomware prevention and integrate seamlessly with Okta solutions.

Hardware security keys, such as YubiKeys, support multiple authentication protocols including FIDO U2F, FIDO2, and Smart Card/PIV, making them truly phishing-resistant, and passwordless-enabled, delivering peace of mind.

Wondering why it's worth it to carry one more thing?

Don't let the hardware form factor fool you! The YubiKey is a powerful next gen solution that will protect your online digital identity and stop modern cyber threats and account takeovers in their tracks.

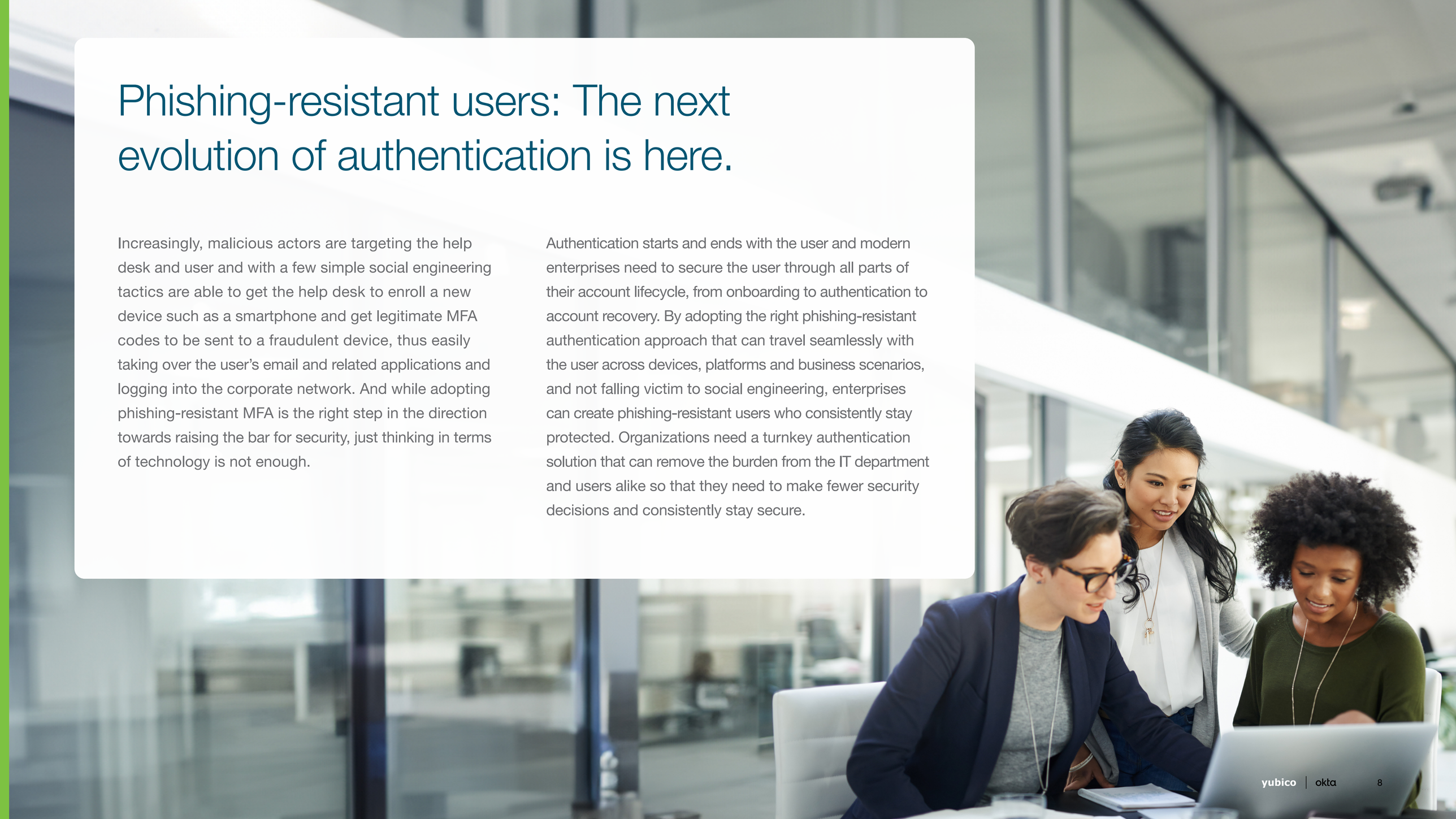
What’s a YubiKey?

YubiKeys are FIPS 140-2 validated hardware security devices that provide the highest security and compliance assurance. YubiKeys are purpose-built for security and support device-bound passkeys, ensuring compliance to Authenticator Assurance Level 3 (AAL3) standards. The YubiKey 5 FIPS series and YubiKey 5 Series support various protocols, including phishing resistant FIDO2/WebAuth and Smart Card, OATH, OpenPGP, OTP, and FIDO U2F protocols. As basic two-factor authentication methods (SMS, mobile apps, etc.) become increasingly vulnerable to attackers, YubiKeys offer a modern and future-proofed way of mitigating cyber risk.

Phishing-resistant users: The next evolution of authentication is here.

Increasingly, malicious actors are targeting the help desk and user and with a few simple social engineering tactics are able to get the help desk to enroll a new device such as a smartphone and get legitimate MFA codes to be sent to a fraudulent device, thus easily taking over the user's email and related applications and logging into the corporate network. And while adopting phishing-resistant MFA is the right step in the direction towards raising the bar for security, just thinking in terms of technology is not enough.

Authentication starts and ends with the user and modern enterprises need to secure the user through all parts of their account lifecycle, from onboarding to authentication to account recovery. By adopting the right phishing-resistant authentication approach that can travel seamlessly with the user across devices, platforms and business scenarios, and not falling victim to social engineering, enterprises can create phishing-resistant users who consistently stay protected. Organizations need a turnkey authentication solution that can remove the burden from the IT department and users alike so that they need to make fewer security decisions and consistently stay secure.



Yubico FIDO Pre-reg: Easily create phishing-resistant users and fast-track to passwordless

Yubico FIDO Pre-reg delivers modern authentication that moves seamlessly with the user, across devices, services and business scenarios, to create phishing-resistant users. With Yubico FIDO Pre-reg, organizations can go passwordless at speed and scale with a turnkey FIDO activation for YubiKeys, which offer strong phishing defense that stops account takeovers in their tracks. Raise the bar for security quickly and prevent damaging ransomware attacks and other threat vectors from taking hold in the organization. Enable secure login to online accounts and access to sensitive corporate systems and data with the most secure form of passkey authentication, all while reducing the burden on IT departments and their users.

Reduce IT burden

IT departments no longer need to register YubiKeys on behalf of their users or require users to self-enroll. Save on time and costs by eliminating the need to manually register security keys for each employee, one by one.

Simple and fast for users

Users can receive YubiKeys that are pre-registered with the organization's Identity Provider (IdP). No longer a need to self-enroll, leaving users free to enjoy secure, passwordless access to their online accounts in minutes.

Accelerate business securely

Yubico FIDO Pre-reg is available through the YubiEnterprise Subscription program which delivers greater business flexibility and agility with a YubiKeys as a Service model, which lowers the cost to entry, and dramatically raises the bar for security.

Turnkey YubiKey activation with Yubico FIDO Pre-Reg

Simple for your admin teams and your employees

As stated in Verizon's 2024 Data Breach Investigations Report (DBIR), credentials are vulnerable to breaches, with **68%** of data breaches resulting from stolen credentials and enterprises are often challenged with accelerating the adoption of phishing-resistant Multi-Factor Authentication (MFA) and passwordless methods. YubiKeys, which provide strong MFA and bridge to passwordless solutions, are effective in countering these threats. However, the adoption of YubiKeys can pose obstacles for some organizations due to manual registration processes by IT departments and user confusion during self-enrollment.

Both IT department-led registration and user self-enrollment options have limitations. Yubico FIDO Pre-reg, a new service launched by Yubico and Okta, involves a turnkey FIDO authentication approach for enterprises. This service eliminates manual user registration by providing pre-registered YubiKeys* and streamlines the adoption of phishing-resistant MFA by pre-registering YubiKeys with Okta. The problem of slow user adoption due to manual registration processes is addressed.

Utilizing Okta's Workflows automation platform and Yubico's YubiKey as a Service, the two companies now offer customers an easier way to deploy phishing-resistant FIDO2/WebAuthn YubiKeys by integrating these two services.

Users can now quickly access their online accounts without needing to create a traditional password. Instead, they follow a simple process involving a PIN provided by their IT department, eliminating the need for manual user registration, and reducing time and costs, while enhancing security and productivity for end users.

This service is available through the YubiKey as a Service subscription program, which offers increased business flexibility and lower costs. With Yubico FIDO Pre-reg, organizations can streamline the adoption of strong MFA and passwordless practices, improving security, efficiency, and user satisfaction within enterprise environments.

[1]Verizon, 2024 Data Breach Investigations Report

Yubico FIDO Pre-reg: Easier for admin teams

No need for manual registration. Save on time, labor and costs.

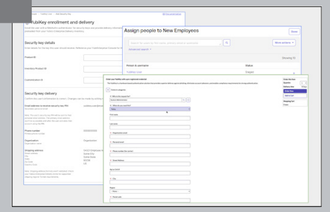
Secure access to your applications from day one with FIDO Pre-reg. Phishing-resistant MFA just got easier to get your new employees started quickly. Now you can have out-of-the-box YubiKey (FIDO) activation in minutes.

Only the highlighted steps are actions that need to be taken.

STEP 1 KEY STEP

***Your admin is preparing to deploy YubiKeys using Yubico FIDO Pre-reg with Okta.**

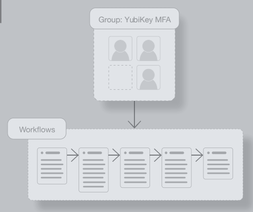
STEP 2



They start the YubiKey request using an automation trigger…

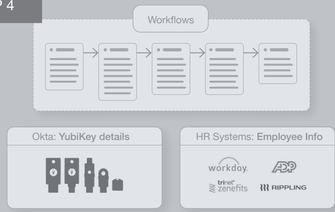
*The Admin UI is one way to request a YubiKey; this solution has the flexibility to allow various request triggers.

STEP 3



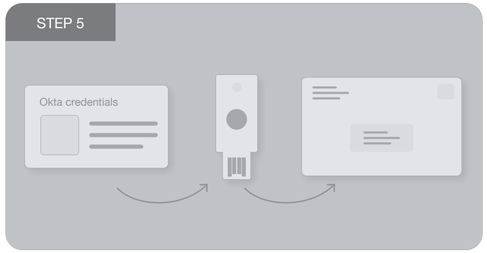
…which initiates Okta Workflows behind the scenes.

STEP 4



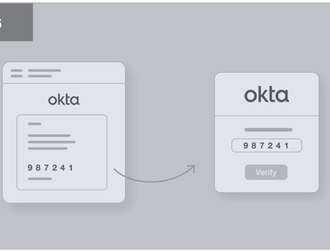
Integration with your HR system provides shipping info for your employee to Okta Workflows.

STEP 5



The key is sent from Yubico Enterprise fulfillment pre-enrolled with the employee's Okta credentials.

STEP 6



Later, the employee is provided their PIN separate from the shipped YubiKey in order to prevent interception.

STEP 7 KEY STEP

***Your employee inserts their YubiKey, enters their PIN, taps the device, and is authenticated using secure FIDO2 credentials.**

STEP 8

...and on Day 1 they can quickly and securely access everything they need to get started!

Yubico FIDO Pre-reg: Turnkey for users

Easy 2-step activation. Secure passwordless access in minutes.

Goodbye passwords, Hello hassle-free login. Protect your online accounts in minutes. Turnkey YubiKey activation—it just works.

Only the highlighted steps are actions that need to be taken.

STEP 1

My company is providing a more secure and seamless sign-in experience, making it easier and faster for me to log in.

STEP 2

I receive a PIN from my company.

STEP 3

I receive my YubiKey shipped directly to me.

STEP 4

I log into my new laptop.

STEP 5

I go to my company's Okta login page.

STEP 6 KEY STEP

*** I insert my Yubikey.**

STEP 7 KEY STEP

*** I type in the PIN that I was provided and tap the YubiKey.**

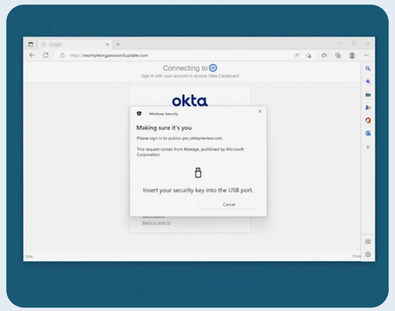
STEP 8

I successfully authenticate with Okta and can work securely in just a few easy steps.

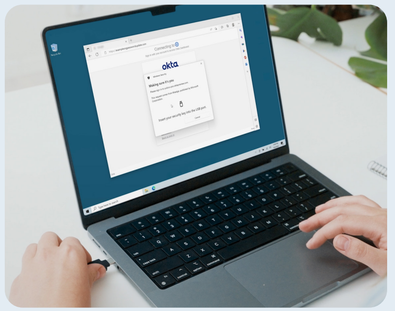
Yubico and Okta
Raising the bar for security together

Two complementary parts of a full cybersecurity program, Okta and Yubico, continue to work together to integrate your organization's identity solution across your entire technology ecosystem. By combining Okta's suite of MFA solutions with Yubico's hardware-based authentication services, organizations can streamline access controls while adding a much-needed layer of phishing protection.

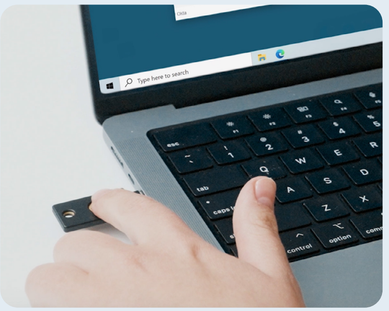
Enterprises can now empower their IT departments to raise the bar for security for Okta environments while delivering users a fast and efficient way to protect their online accounts in minutes:



1. Okta customers can empower their users to simply navigate to the Okta platform



2. Insert the pre-programmed YubiKey into their computer or phone



3. When prompted, enter the PIN provided by the IT team, and validate user presence by tapping the YubiKey

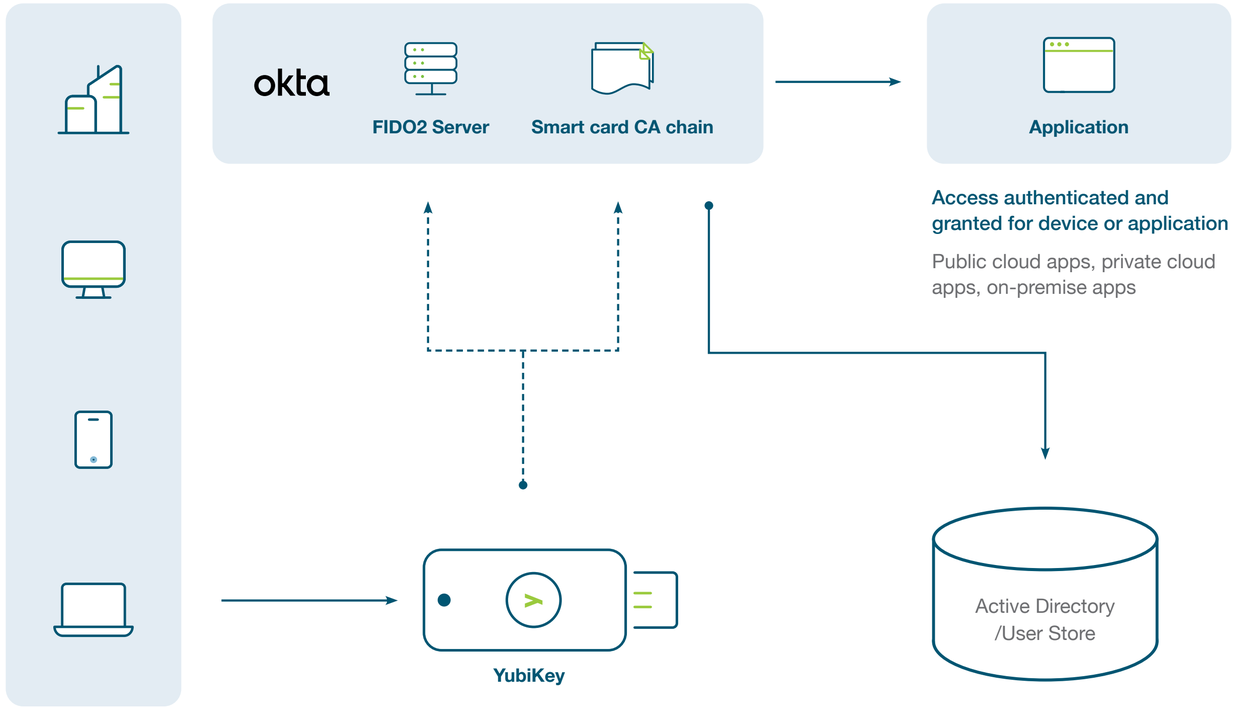
And they're in! Turnkey authentication with FIDO2/secure hardware-bound passkeys and passwordless-enabled faster than you could read this.

Okta and Yubico provide a means of enforcing authentication based on Zero Trust principals within your organizational environment. The YubiKey can be used as the primary or back-up authentication method in conjunction with Okta implementation, ensuring user access and reducing support when any of the devices are not accessible. The easy and highly-secure solution has been tested and proven in security-conscious government and enterprise environments.

The YubiKeys including the FIPS series are:

YubiKey FIPS series are FIPS 140-2 validated with overall level 1 and level 2 and physical security level 3

All YubiKeys meet NIST SP 800-63 Authenticator Assurance Level (AAL) 3 requirements



How are YubiKeys deployed?

Yubico offers flexible plans that help your company move away from broken or antiquated MFA and accelerate toward phishing-resistant MFA at scale, including a YubiKey as a Service subscription program for organizations with 500 users or more.

Lower cost to entry

Gain phishing-resistant MFA for less than the price of a cup of coffee per user per month (OPEX) with additional subscription-only entitlements and discounts built-in.

Flexibility and choice

Enable user choice to select preferred YubiKeys in the subscription tier over time with an option to upgrade as needs evolve.

Faster rollouts

Quickly protect your workforce, and your brand, and stay connected to security experts such as Professional Services, a dedicated Customer Success Manager, and Priority Support.

Future-proofed investment

Ensure security is always prioritized as your business evolves, you experience employee turnover, or simply need to replace lost or stolen keys.

Enjoy a secure, seamless transition

Okta and Yubico support a variety of authentication protocols that allow organizations to bridge any potential gaps between legacy and modern applications.

Here are some options:

1. ### Okta FIDO2/WebAuthn + YubiKeys

   YubiKeys can be used as a phishing-resistant Security Key authenticator once WebAuthn/FIDO2 has been enabled within an Okta organization.

2. ### Okta YubiKey OTP + YubiKeys

   The YubiKey supports one-time password (OTP). The YubiKey communicates via the HID keyboard interface, sending output as a series of keystrokes. This means OTP protocols can work across all OSs and environments that support USB keyboards, as well as with any app that can accept keyboard input.

3. ### Okta Smart Card (PIV/CAC) + YubiKeys

   YubiKeys can be used as a PIV-derived smart card authenticator. The YubiKey identifies itself as a smart card reader with a smart card plugged in so it will work with most common smart card drivers.

Meet your various compliance and regulation requirements

Many industries require various authentication requirements for different user groups and applications. And some regulations even require specific authenticators at specific assurance levels.

These regulations are met with ease by choosing from a range of assurance factors—including knowledge factors, possession factors, inherence factors, and time-based factors—that comply with your industry requirements. Authenticate your users with one click, one touch, or even a quick scan.

The YubiKey family

The combination of Okta Adaptive MFA and the YubiKey fits seamlessly into this broader ecosystem, offering users next-level identity authentication. Both are supported by hundreds of integrations across leading vendors in infrastructure and security, enabling the joint solution to work across different devices, apps, and services.

About Yubico

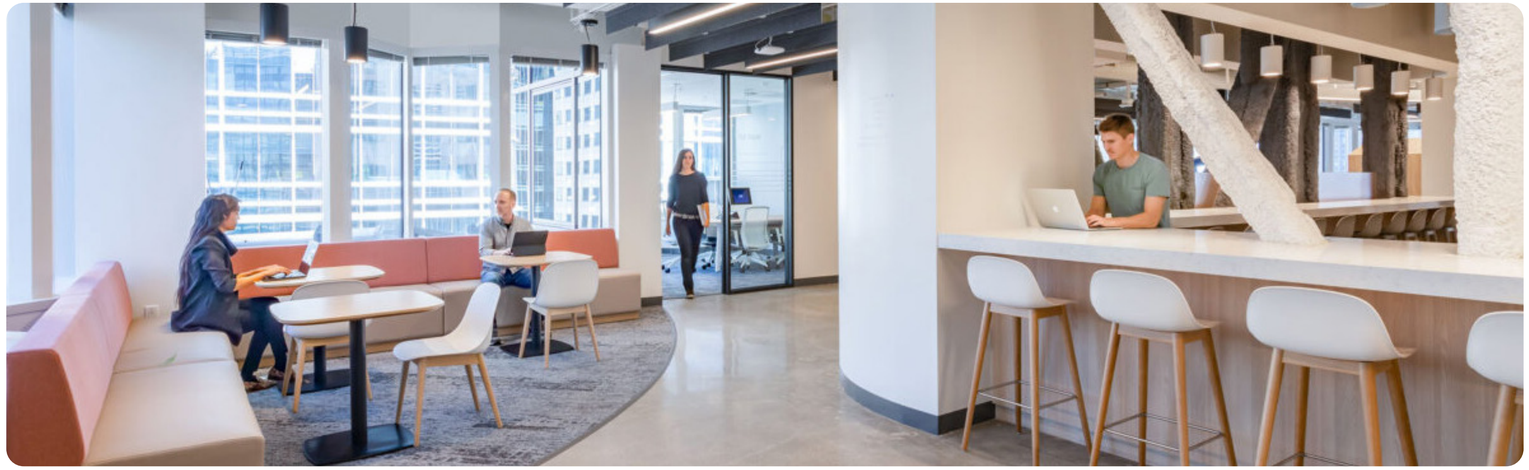
Yubico (Nasdaq First North Growth Market Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA.

For more information on Yubico, visit us at www.yubico.com.

About Okta



Okta is the World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success — all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.