Yubico and Okta:
Raising the bar for security

Modern and intelligent phishing-resistant authentication for state and local government

yubico | okta

Rising AI and nation-state threats underscore the need to fortify defenses against identity-related phishing

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.

In today's rapidly evolving digital landscape, state and local government agencies face an increasingly complex array of cybersecurity challenges. From defending against sophisticated nation-state actors to protecting sensitive citizen data, the stakes have never been higher. Yet, despite significant investments in cybersecurity infrastructure and awareness, one often-overlooked vulnerability continues to expose agencies to unnecessary risk: **legacy authentication protocols.**

Moreover, federal mandates and cybersecurity frameworks such as Zero Trust are pushing agencies toward modernization, making continued dependence on legacy methods not just risky, but increasingly non-compliant.

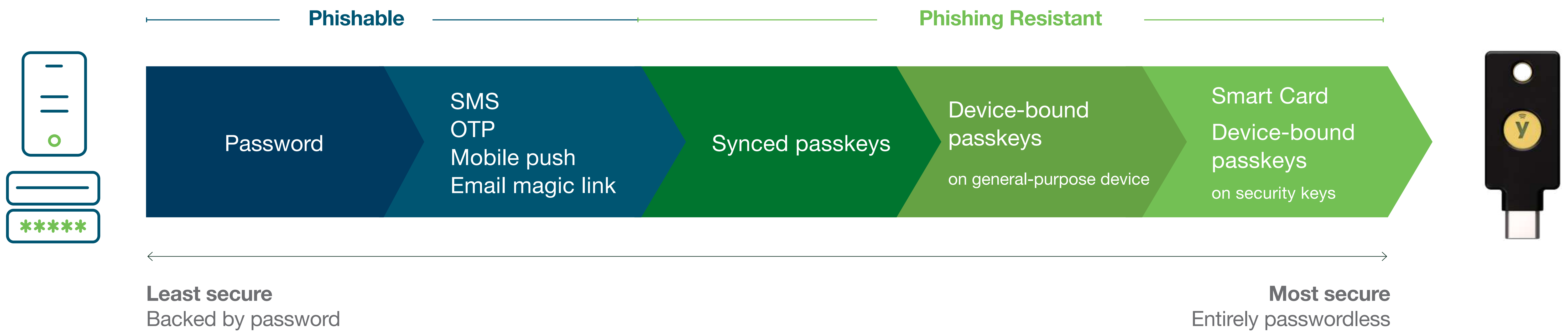
For years, Yubico and Okta have partnered together to offer solutions that overcome these challenges and continue to innovate together to offer quick, safe and trusted solutions to safeguard government agencies from an ever-changing cybersecurity landscape

Here's the bottom line: Developing a phishing-resistant identity solution is essential to adequately protect your organization, further justified by the continued growth of phishing attacks and pressures from the federal government.

What is phishing-resistant authentication?

Phishing attacks are on the rise, but not all forms of multifactor 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.

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 passkey (FIDO2/WebAuthn) authentication standard. Passkeys that reside in hardware security keys such as the YubiKey, have been proven to stop remote attacks and account takeovers every time.



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.

> "Phishing-resistant authentication has to be secure. But it also needs to be IT and userfriendly. Okta and Yubico give customers the security and flexibility needed to protect their enterprise resources."
>
> **David Bradbury** | Chief Security Officer | Okta

What is a YubiKey?

YubiKeys offer highest assurance, FIPS 140-2 validated (FIPS 140-3 pending) passkeys that reside in a hardware security key form factor. YubiKeys are purpose built for security, 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.

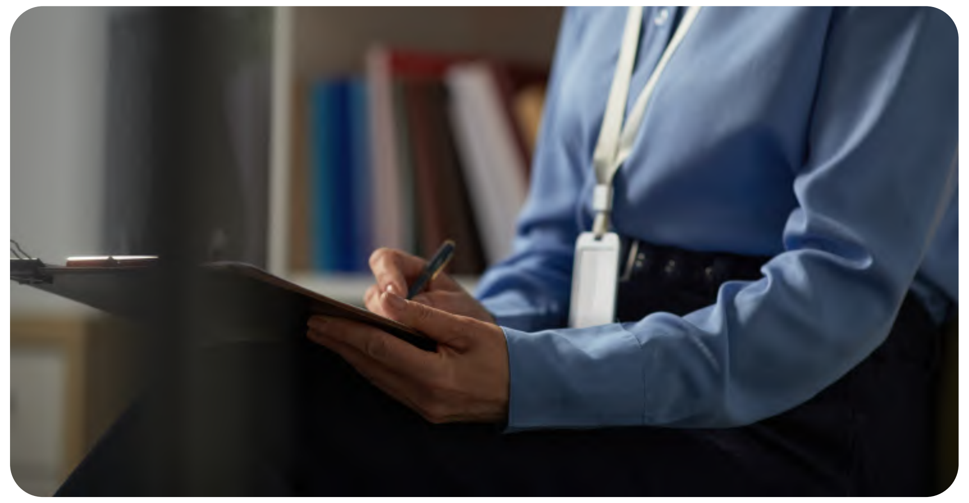
Yubico offers flexible plans that help your company move away from broken or antiquated MFA and accelerate toward phishing-resistant MFA at scale, including a YubiKey as a Service subscription program for agencies with 500 users or more.

Phishing-resistant authentication use cases across state and local government

Office workers
Secure every user across every device for end-to-end protection.

Privileged users
Protect every privileged user across the organization including C-suite, finance, HR, IT and more.

Hybrid and remote worker
Ensure highest-assurance security for all users—regardless of where they work.



Department of Corrections
Phishing-resistant authentication for mobile-restricted users, shared workstations and devices. Drive CJIS compliance.

Law enforcement and courts
Secure users across mobile-restricted locations and shared workstations and devices. Drive CJIS compliance.

Election infrastructure
Protect election infrastructure and voter registration databases. Secure shared tablets and devices used by temporary staff.

Citizen-facing digital services
Protect citizen financial and personal data from being hacked with highest-assurance security.

Temporary workers
Ensure cybersecurity hygiene for temporary staff and contract workers.

Highest levels of phishing-resistant assurance across the Okta ecosystem with Yubico

Workforce Identity Cloud

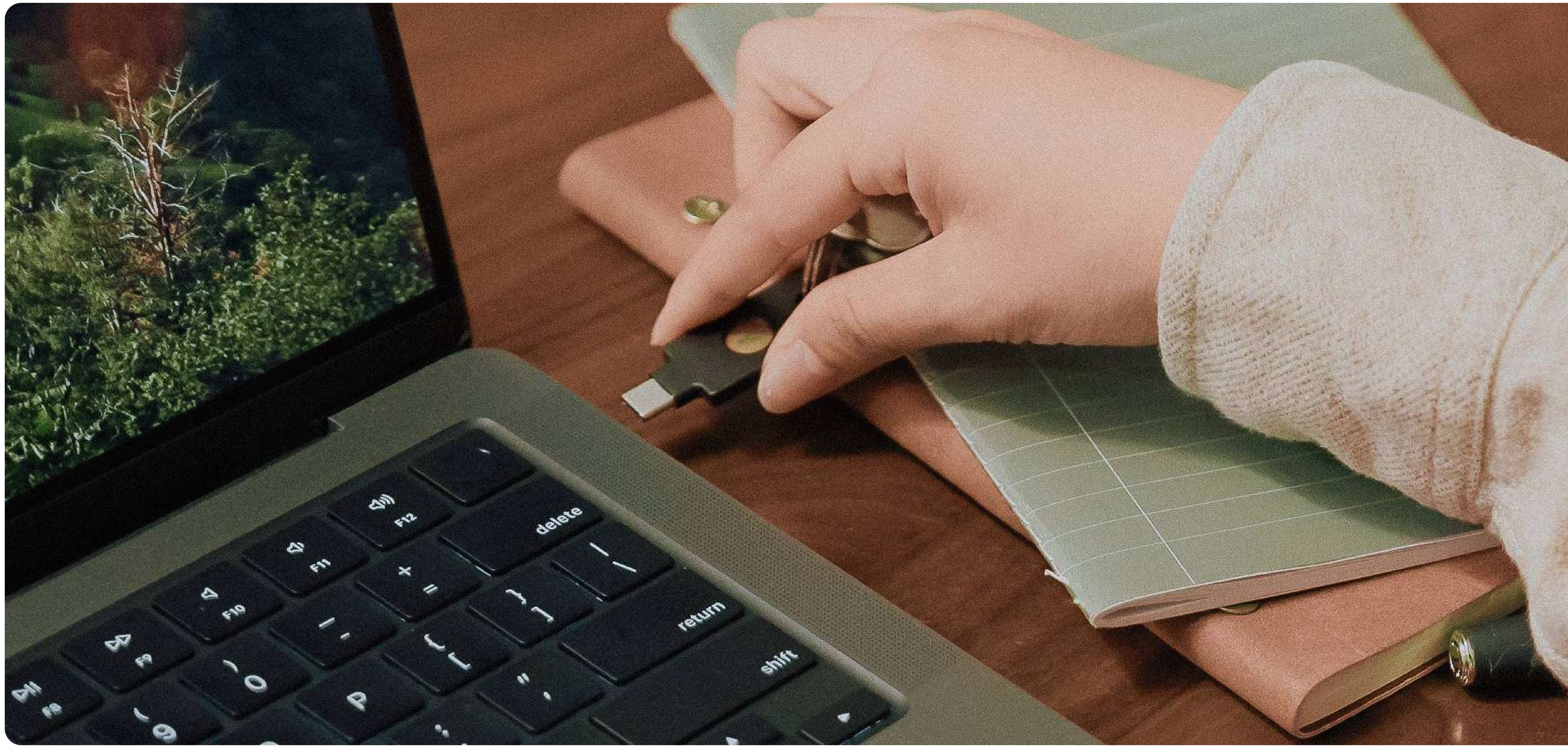
Workforce Identity Cloud, with YubiKeys, delivers phishing-resistant security using FIDO2/ WebAuthn and Smart Card/PIV. Its Adaptive MFA engine ensures strong authentication for high-risk logins, balancing security and user convenience. This powerful combo prevents account takeovers and enables passwordless experiences across all users and devices. Plus, YubiEnroll simplifies YubiKey setup for Okta admins, reducing friction.

Okta Device Access

Okta Device Access extends Okta's cloud identity to the Windows and macOS log-in screen. Okta Device Access currently integrates with FIDO2 YubiKeys and YubiOTP.

Okta Integration Network

The Okta Integration Network is a catalog of pre-built connectors. Yubico hosts the Yubico Connector that allows for Okta and Yubico customers to utilize Yubico FIDO Pre-reg, a feature of the Yubico Enrollment suite. Also within the Okta's Integration Network, customers can find the Yubico FIDO Pre-registration template, that makes deploying FIDO2 phishing resistant YubiKeys faster and at scale.



Yubico FIDO Pre-reg: Easily move to phishing-resistant security and fast-track to passwordless

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.

Reduce IT burden

IT departments no longer need to register YubiKeys on behalf of their users or require users to selfenroll. 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 security

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

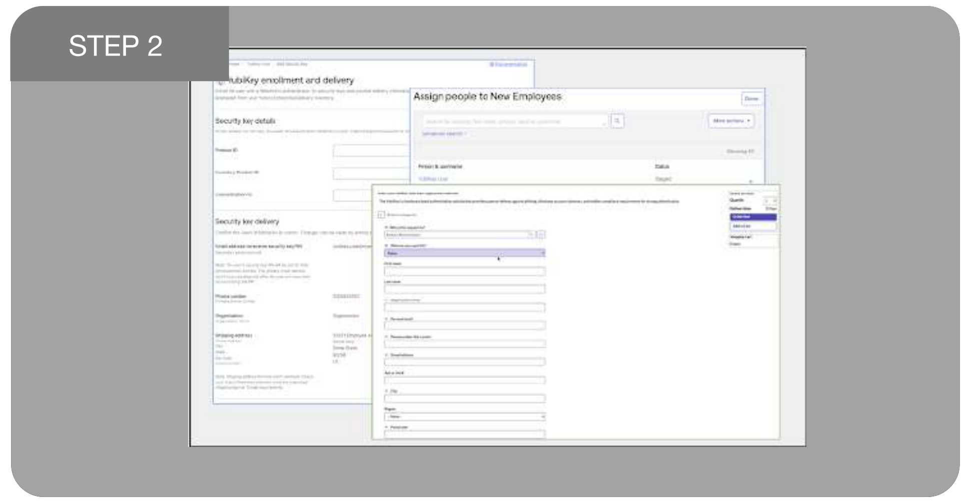
Yubico FIDO Pre-reg: Easier for admin teams

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.

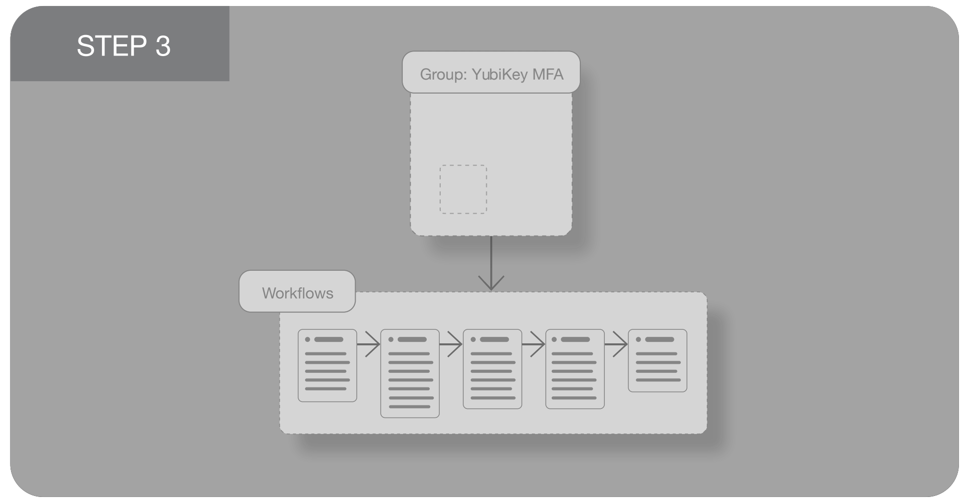
Only the highlighted steps are actions that need to be taken.

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

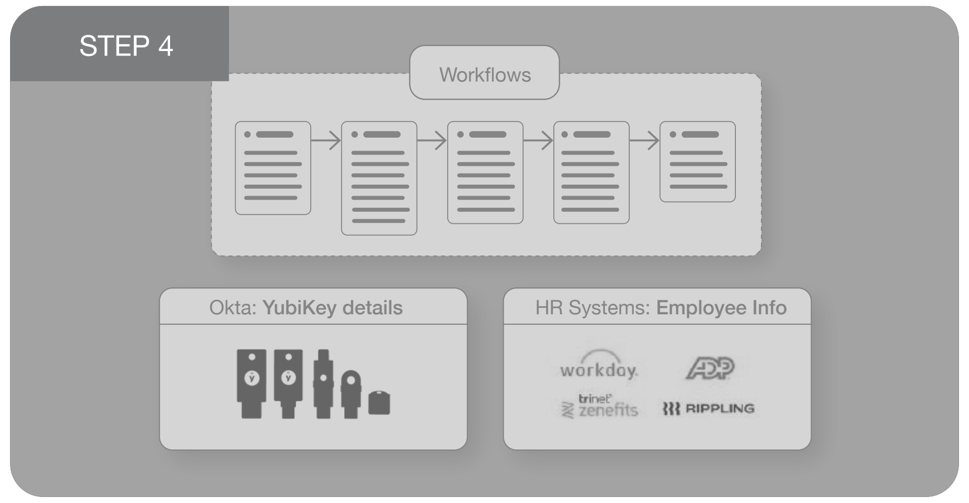

STEP 2
YubiKey enrollment and delivery
Assign people to New Employees

They start the YubiKey request using an automation trigger…

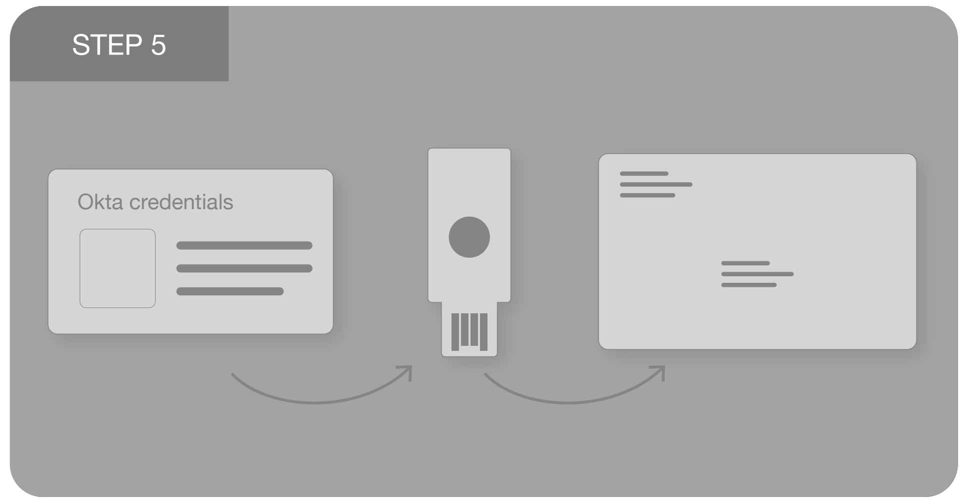
*The Admin UI is one way to request a YubiKey; this solution has the flexibility to allow various request triggers.



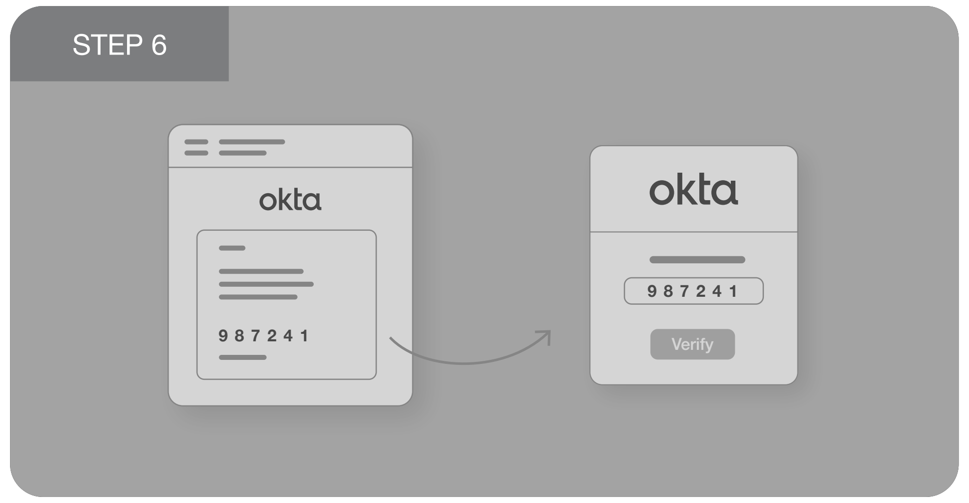
…which initiates Okta Workflows behind the scenes.



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



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



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

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

STEP 8
okta
Sign In
7

…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 agency 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 agency.

STEP 3

I receive my YubiKey shipped directly to me.

STEP 4

I log into my new laptop.

STEP 5

I go to my agency's Okta login page.

STEP 6 KEY STEP

*** I insert my YubiKey.**

STEP 7 KEY STEP

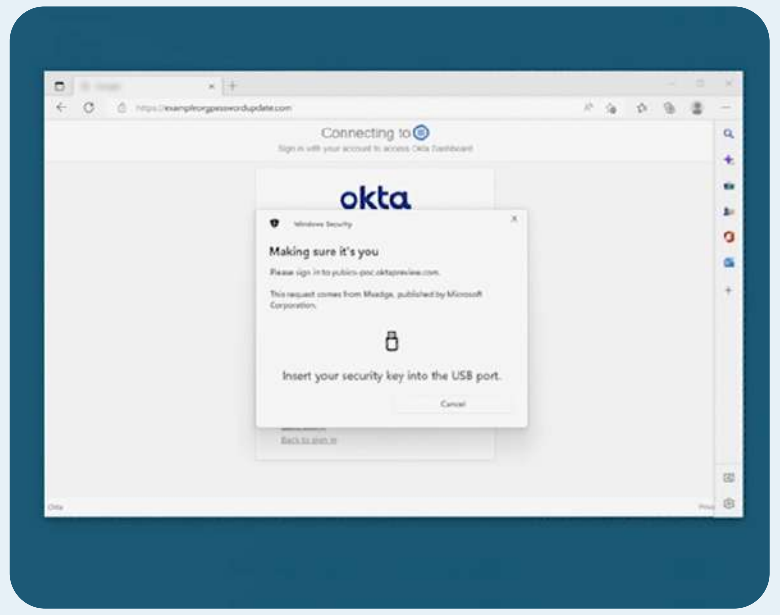
*** I type in the PIN that I was provided and tap the YubiKey.**

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



https://exampleorgpasswordupdate.com

Connecting to

Sign in with your account to access Okta Dashboard

okta

Windows Security

Making sure it's you

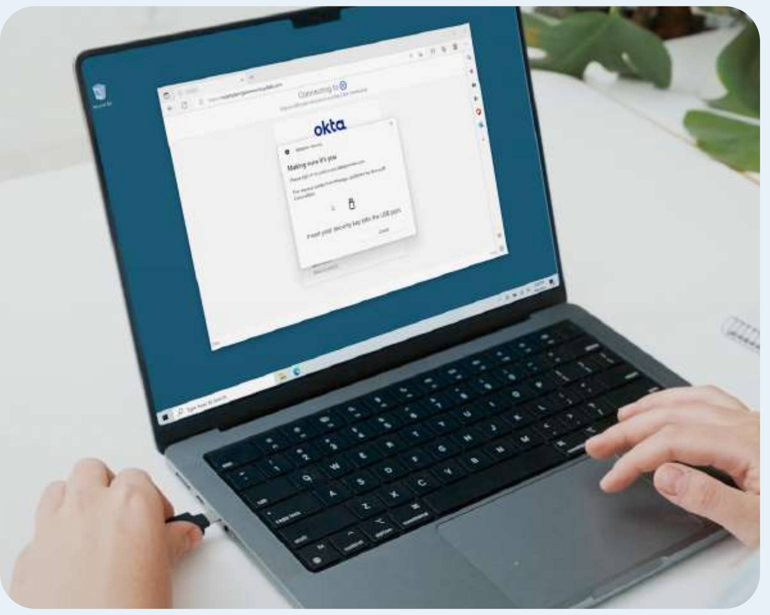
Please sign in to yubico-poc.oktapreview.com.

This request comes from Msedge, published by Microsoft Corporation.

Insert your security key into the USB port.

Cancel

Back to sign in



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

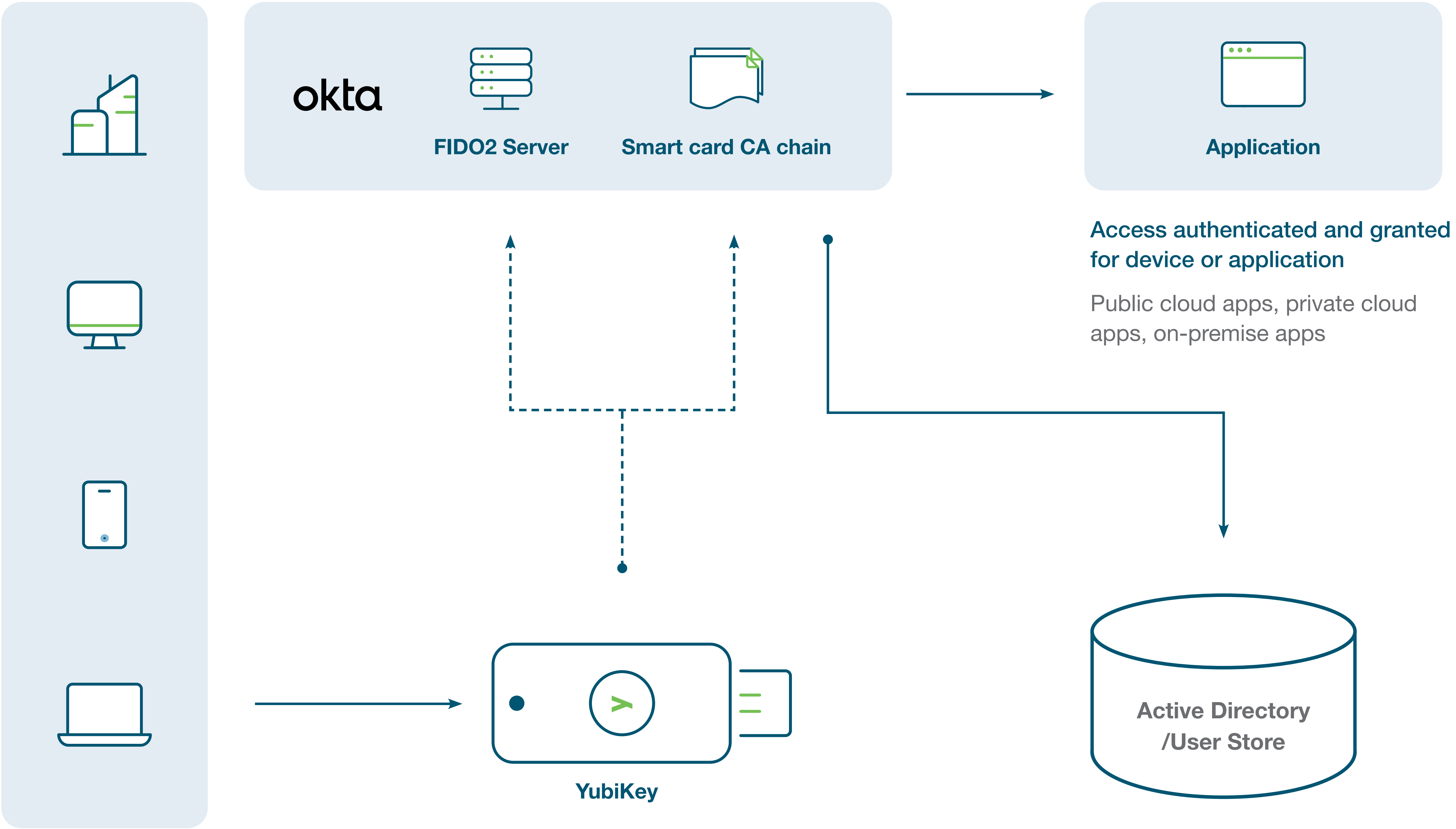
And they're in! Turnkey authentication with FIDO2/secure hardware-bound passkeys and passwordless-enabled faster than you could read this.

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:

FIPS 140-2 validated with overall level 1 and level 2 and physical security level 3, with FIPS 140-3 validation in process.

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



Access authenticated and granted for device or application

Public cloud apps, private cloud apps, on-premise apps

Accelerate Zero Trust and stop phishing attacks

Okta and Yubico support a variety of authentication protocols that allow agencies 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.

About Yubico

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, we set the gold standard for modern phishing-resistant, hardware-backed authentication, stopping account takeovers and making secure login simple.

Since 2007, we've helped shape global authentication standards, co-created FIDO2, WebAuthn, and FIDO U2F, and introduced the original passkey. Today, our passkey technology secures people and organizations in over 160 countries—transforming how digital identity is protected from onboarding to account recovery.

Trusted by the world's most security-conscious brands, governments, and institutions, YubiKeys work out of the box with hundreds of apps and services, delivering fast, passwordless access without friction or compromise.

We believe strong security should never be out of reach. Through our philanthropic initiative, Secure it Forward, we donate YubiKeys to nonprofits supporting at-risk communities.

Dual-headquartered in Stockholm, Sweden and Santa Clara, California, Yubico is proud to be recognized as one of TIME's 100 Most Influential Companies and Fast Company's Most Innovative Companies. Learn more 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.