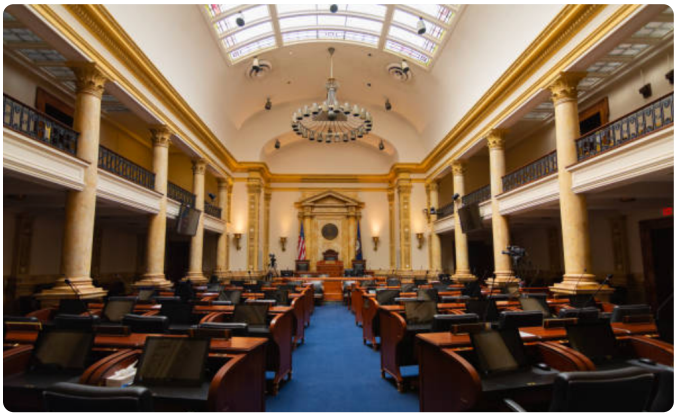
yubico

Achieve 100% MFA across state and local government

Protect against modern cyber threats



Mobile-based authentication is not phishing-resistant and creates MFA gaps

According to the 2022 IBM Security Cost of a Data Breach Report, the average cost of a data breach in public sector is $2.07 million,[1] with stolen credentials and phishing as top attack vectors. While MFA can be a strong first-line of defense against phishing and ransomware, not all forms of MFA are created equal. Legacy authentication such as usernames and passwords can be easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to modern phishing attacks, malware, SIM swaps, and man-in-the-middle (MiTM) attacks. Mobile-based authentication also creates gaps in your MFA strategy when users can't, don't, or won't use mobile authentication due to union restrictions, personal preferences, cellular geographic inconsistencies, financial reasons and more.

Secure critical access for employees and constituents with the YubiKey

To protect against modern cyberthreats, Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key for phishing-resistant two-factor (2FA), MFA, and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research,[2] and meets phishing-resistant MFA requirements in the 2021 White House Executive Order 14028 on Protecting the nation's cybersecurity.

YubiKeys are highly suitable for users that ***can't, won't, or don't*** use mobile authentication, and are simple to deploy and use—a single YubiKey can be used across legacy and modern applications, services, and devices, with multi-protocol support for Smart Card, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key, and don't require a battery or internet connection.

How the YubiKey can help you secure your technology, data, and users:

1. Meet your cyber insurance requirements

States, cities, and counties can face a shortage of cyber-security insurance capacity and increased cost for coverage if MFA coverage isn't satisfactorily deployed across the entire ecosystem. Restrictions could include reduced sublimits, higher deductibles, and narrower coverage terms. Cyber policy non-renewals may also be a potential outcome, which can expose an organization to significant risk if targeted by hackers, phishing attacks or ransomware attacks. YubiKeys offer the strongest MFA protection across the industry, ensuring compliance to your cyber insurance mandates.

2. Secure access to data from anywhere, and from any device

YubiKeys offer phishing-resistant MFA, ensuring only authorized users have access to the right applications and data. YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 700 applications and services out-of-the-box, including Google Suite, Microsoft Azure, Microsoft Office 365, Box, Jamf, and identity and credential management (ICAM) solutions, eliminating rip and replacement of existing solutions. A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations, enabling users to utilize the same key as they navigate between devices. They are also highly portable, ensuring users on the move such as law enforcement and first responders have secure and CJIS-compliant access to critical data for public safety operations, and employees that work in corrections departments can securely authenticate without the use of mobile devices.

State and local governments using YubiKeys for 100% MFA coverage

City of SACRAMENTO

WA.gov THE EVERGREEN STATE

gta GEORGIA TECHNOLOGY AUTHORITY

City of Louisville

MISSION VIEJO

> The biggest benefit is that you don't have to use your phone and wait for that phone call or wait for thatw text message with the OTP. The YubiKey is such a simpler solution where I just plug it in, tap the button and I'm done."
>
> Curtis Chiuu, Principal Systems Engineer, City of Sacramento

3. Secure election infrastructure

The election ecosystem is a prime target for cyber security threats and phishing-resistant MFA is an IT security best practice that states and counties should deploy.

The YubiKey provides strong hardware-based authentication to secure voter registration databases, e-pollbooks, election night reporting (ENR) systems, election management systems, as well as devices through which these systems are accessed such as laptops, desktops, and mobile devices, against hacking. Learn more here.

> I like the YubiKey as opposed to phone authentication, We have a lot of users within our system that don't have a state- or county-provided cell phone, and I certainly don't want them using their own personal devices for agency or office business. The YubiKey was really the easy-to-use multifactor authentication of choice for us here in Washington state to achieve the additional security needs we had."
>
> Curtis Chiuu, Principal Systems Engineer, City of Sacramento

4. Secure citizen-facing digital services

State and local government systems contain constituent information such as social security numbers and other sensitive data. Internal employees need secure access to this information, but external constituents also need to seamlessly and securely access digital services.

Building phishing-resistant authentication using FIDO2/WebAuth and YubiKeys into citizen-facing digital services offers citizens a secure and simple experience to help them stay protected against phishing attacks and account takeovers. YubiKeys can also bridge the digital divide for those constituents that don't have or cannot afford a mobile device.

Lifecycle management: Empower users with YubiKeys

Yubico makes it very convenient to deploy phishing-resistant MFA. You can leverage existing IAM, ICAM and IDP platforms to manage the issuance, revocation, and policy enforcement of YubiKeys. Yubico also makes it easy to get YubiKeys directly into the hands of your users, through services such as YubiEnterprise Subscription which provides a service-based and affordable model for purchasing YubiKeys, and YubiEnterprise Delivery which provides a turnkey distribution service with shipping and tracking of Yubico products.

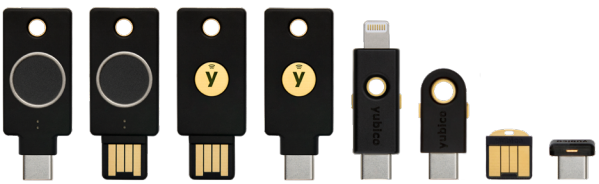
Key questions Yubico can help you with:

- ☐ How do I enroll a YubiKey in my MFA platform?
- ☐ Which YubiKey should my organization use?
- ☐ How does my help desk support the lifecycle of the YubiKey?
- ☐ Can I centrally manage distribution of the YubiKeys?

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. If a user leaves, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKey and continue using it for their own personal accounts.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator. YubiKeys are produced in the USA, maintaining security and quality control over the entire manufacturing process.



The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops, mobile devices and tablets.

[1] IBM, Cost of a Data Breach Report 2022

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

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.

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088