yubico

HOW THE YUBIKEY COMPLEMENTS NATIONAL GUARD, HOMELAND SECURITY, EMERGENCY MANAGEMENT AND PUBLIC SERVICE CYBERSECURITY RESILIENCY

Modern Authentication for Defense and Domestic Operations

Common use cases

- **Securing telework & personal devices**
- **Securing mission partners**
- **Securing privileged users**
- **Securing shared devices & workstations**
- **Securing non-CAC eligible users**
- **Securing office workers**
- **Securing SCIFs & air-gapped networks**

Advancing MFA for domestic operations and National Guard

Traditional authentication methods, such as usernames, passwords, or even Smart Cards, often fall short in the demanding environments that Homeland Security professionals, National Guard members, first responders, contractors, and mission partners face. Secure, seamless cross-platform functionality is critical—especially in a landscape shaped by nation-state cyberattacks, criminal organizations, and gray zone warfare. Recent guidance, including the National Security Memorandum-8 (NSM-8), has emphasized adopting phishing-resistant authentication methods as part of a comprehensive Zero Trust Architecture to modernize and secure operations.

Even widely trusted solutions like the Department of Defense's Common Access Card (CAC), which employs high-assurance Public Key Infrastructure (PKI), are proving less practical in modern scenarios. Whether it's remote work, Bring Your Own Approved Device (BYOAD) policies, coalition and mission partner environments, air-gapped networks, or tactical operations abroad, the CAC often presents limitations. For example, CAC reader support for mobile phones or tablets is limited or non existent, and teleworking with a CAC reader leaves the device open to potential malware. For these critical situations, alternative credentialing solutions—like YubiKey—are increasingly essential.

Why YubiKeys are mission critical

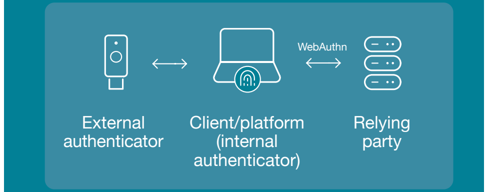
For National Guard and domestic operations personnel, securely accessing and sharing information in real time across multiple platforms can be a matter of life and death. During a crisis, teams must be able to connect from incident sites to national command centers without delay. A provisioned YubiKey enables interagency and cross-jurisdictional personnel to quickly access critical systems, share intelligence, and maintain situational awareness. YubiKey's compatibility across devices and platforms becomes a force multiplier, enhancing command, control, and communications at every level—from the Emergency Operations Center (EOC) to the field. Empowering part-time citizen Soldiers and Airmen, and Homeland Security professionals including Coast Guard, Emergency Management Services (EMS) and others with a YubiKey can unlock readiness bottlenecks, create pathways for real-time accountability in a disaster, and provide a conduit for vital information at the community level. Similarly, YubiKeys can also unlock the flow of essential information for secure mission partner environments that are increasingly vital for Federal, State and Local, allied, coalition, and State Partnership Program (SPP) activities.

What qualifies as phishing-resistant MFA?

PIV/CAC/Smart Card

PIV
CAC
Smart Card

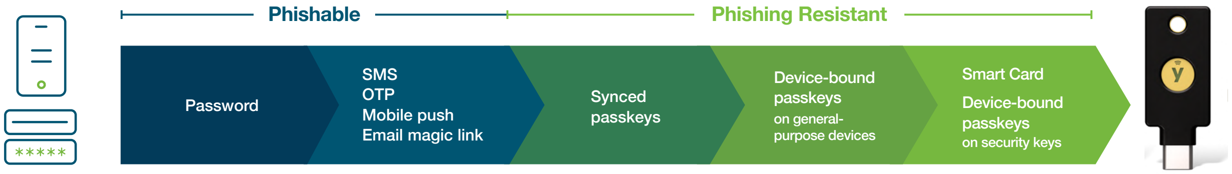
FIDO2/WebAuthn



NIST SP 800-63-4

Not all MFA is created equal

For use cases where the CAC is limited or not practical such as mobile and tactical scenarios, falling back on username and passwords or legacy multi-factor authentication (MFA) is risky. Usernames and passwords are easily hacked, and legacy mobile-based authentication such as OTP, SMS and push notification apps are not phishing resistant. Accounts using MFA that are not based on phishing-resistant protocols are susceptible to having credentials stolen.



By adopting YubiKeys, domestic operations and National Guard leaders can ensure they meet the highest cybersecurity standards while maintaining operational agility.

Deploying YubiKeys is not just an IT decision, it’s a critical step in safeguarding national security, enabling seamless interagency coordination, and ensuring that personnel can operate securely, no matter where the mission takes them.

fido™

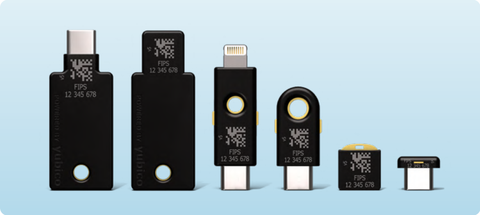
What is Fast Identity Online (FIDO)? FIDO2 is an open authentication standard, created by the FIDO Alliance, that consists of the W3C Web Authentication specification (WebAuthn API), and the Client to Authentication Protocol (CTAP). CTAP is an application layer protocol used for communication between a client (browser) or a platform (operating system) with an external authenticator such as a hardware security key. FIDO2 authentication options include strong single factor (passwordless), two-factor, and multi-factor authentication. Yubico is a core contributor to the FIDO2 open authentication protocol.

The YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers Yubico offers military-grade, phishing-resistant FIPS 140-2 validated YubiKey, a DoD-approved hardware security key that offers highest-assurance multi-factor and passwordless authentication in accordance with Homeland Security Presidential Directive 12 (HSPD 12). With a secure U.S. supply chain, the YubiKey is approved for use as an MFA authenticator for DoD Unclassified and Secret information systems that can meet use cases where the CAC is not available nor practical, by leveraging derived CAC credentials.

The YubiKey supports derived credentials and provides the highest levels of security needed to protect against modern day attacks along with the flexibility to secure even the most complex scenarios—from air-gapped networks to remote work and cloud services—all from a single key. With multi-protocol support including Smart Card (CAC), FIDO U2F, FIDO2, OTP and OpenPGP, the YubiKey supports both legacy and modern architectures with a single solution, and offers a future-proofed bridge to modern FIDO authentication standards.

A single YubiKey can provide both PKI and FIDO2/WebAuthn phishing-resistant authentication to securely authenticate users to applications and services across Government Furnished Equipment (GFE) or personal devices such as laptops, desktops, tablets, and mobile phones. Unlike managing multiple certificates across mobile devices and CACs, a YubiKey with Purebred derived credentials can be used as a portable root of trust across multiple devices including mobile and BYOD/BYOAD.



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

Federal compliant

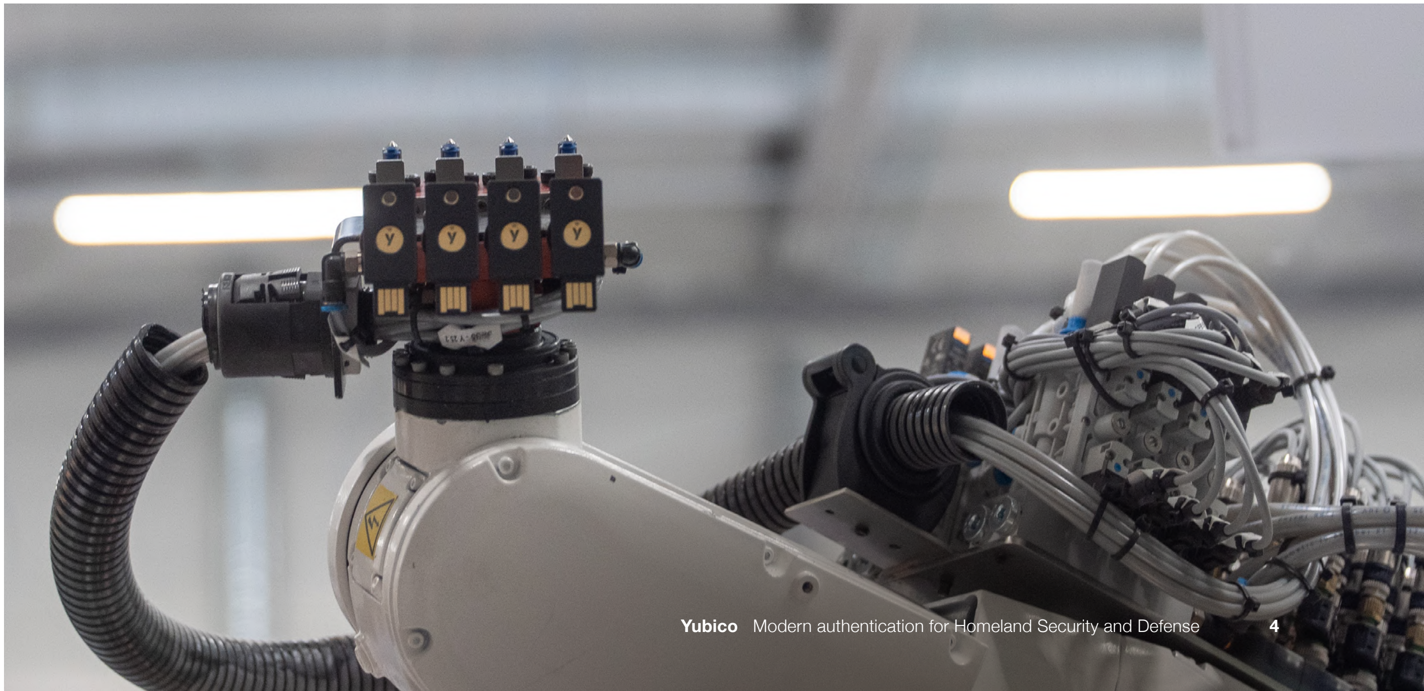
Simple to deploy and use

Built for portability

Reduced IT costs

High ROI

Secure supply chain

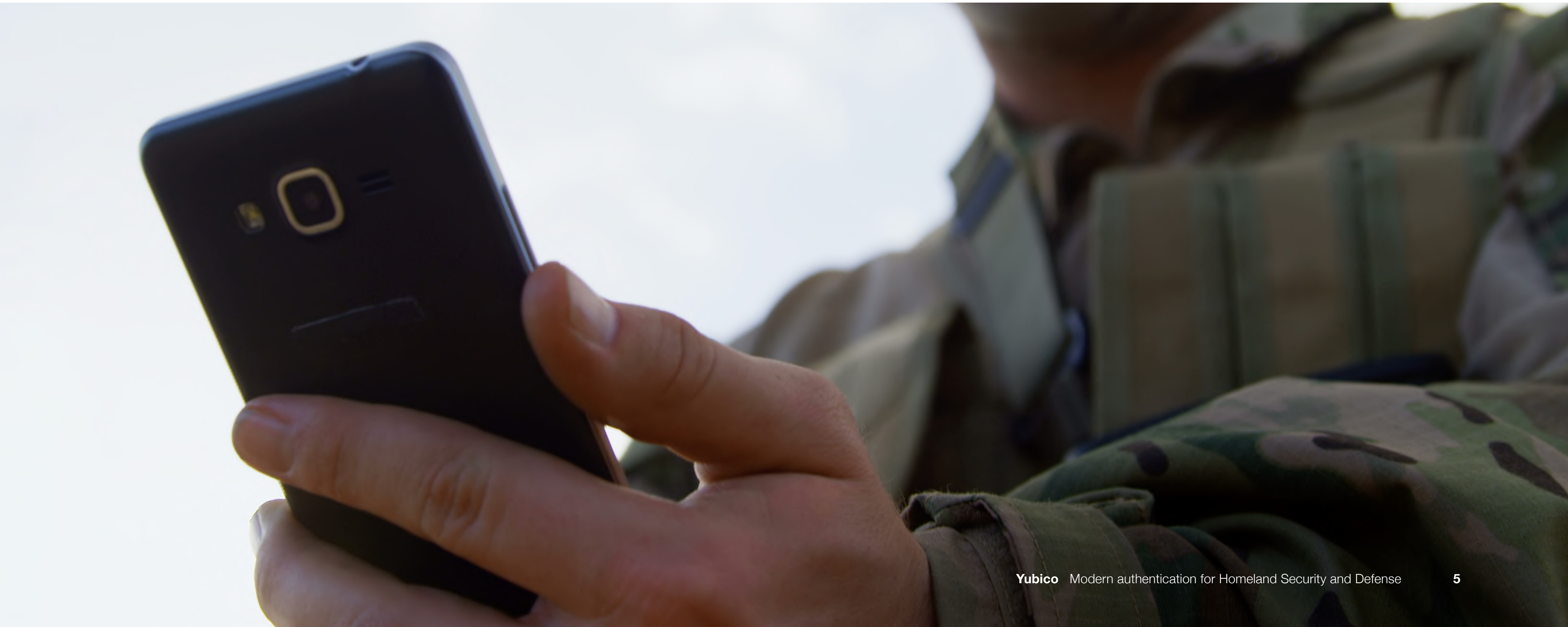


[2] YubiKey 5 FIPS Series latest 5.7 firmware has completed testing by our NIST accredited testing lab, and has been submitted to the Cryptographic Module Validation Program (CMVP) for FIPS 140-3 validation, Overall Level 2 and Physical Level 3

Securing telework & personal devices

Historically, personal device options for military personnel have been limited due to high costs and security concerns. Supporting teleworkers and personal devices adds complexity and expense, making widespread adoption difficult. YubiKeys simplify secure access by working seamlessly with leading Identity and Access Management (IAM) and Identity Provider (IdP) solutions.

For military members, first responders, civilian employees, contractors, and mission partners, YubiKey provides a reliable, flexible, and cost-effective way to securely access military and interagency resources using Purebred-derived credentials and other authenticator protocols. This means powerful tools like Microsoft's virtual desktop services, which allow service members to work from home, no longer require a CAC and external CAC reader. Even when government-issued (GFE) devices are provided for remote and hybrid workers, YubiKey serves as a portable root of trust, ensuring the device remains uncompromised during transit. YubiKeys are also highly adaptable, supporting a wide range of managed and unmanaged devices—including Chromebooks, personal phones, and workstations. When provisioned with DoD Purebred credentials, a YubiKey becomes a trusted authentication tool that enables secure access across multiple devices, eliminating the high costs traditionally associated with BYOD programs.



Securing mission partners

The YubiKey is a solution authorized domestic partners can use to secure access to critical information systems such as WebEOC, the Homeland Security Information Network (HSIN), or the National Guard's Joint Information Exchange Environment (JIEE).

Beyond domestic access, the YubiKey is a bridge for partner, coalition, and allied military personnel who are not CAC-eligible, providing a secure authentication solution for mission-critical environments. As a multi-protocol authenticator, the YubiKey offers the flexibility and personalization needed to support readiness training, operations, and State Partnership Program (SPP) activities.

Units can generate, manage, and provision local credentials to a YubiKey, ensuring secure access for personnel operating across multijurisdictional, interagency, allied, and coalition networks. This approach ensures that only locally issued credentials are used for authentication within approved systems, strengthening security and interoperability.

Securing privileged users

Ensuring secure phishing-resistant user access to confidential, classified, secret, and personal information is critical for privileged users who cannot authenticate using the CAC. The YubiKey offers the highest-assurance alternate authenticator that can be used to authenticate privileged users to both legacy and modern applications. The YubiKey's hardware design enables the authentication secret to be stored on a secure hardware chip that cannot be copied or stolen, offering the highest security for authenticating privileged users. The YubiKey can be used to step up authentication for high-security applications.

A top priority for CIOs is to ensure strong MFA in air-gapped or operational networks that cannot take advantage of the high assurance of PKI. These environments require innovation and creativity to add strong MFA for network admins, end users, and other privileged roles.

For example, DoD Microsoft 365 tenant admins cannot use their primary DoD credentials to authenticate for daily tasks and maintenance. As Microsoft Azure supports the enrollment of a YubiKey as a FIDO2 authenticator, admins can quickly enroll a YubiKey for their privileged user roles to meet phishing-resistant authentication requirements. A YubiKey as a FIDO2 token uses public/private keypairs bound to the tenant URL to ensure strong authentication is met.

Securing shared devices & workstations

The use of shared workstations and mobile devices are increasingly common across the military and public sector. By pooling resources for military members, civilian employees, contractors, and mission partners, device ownership and operating costs can be significantly cut. Shifting the storage of the credentials from the device to a hardware-based authenticator, like a YubiKey, everyone can be issued a security key for authentication on any device.

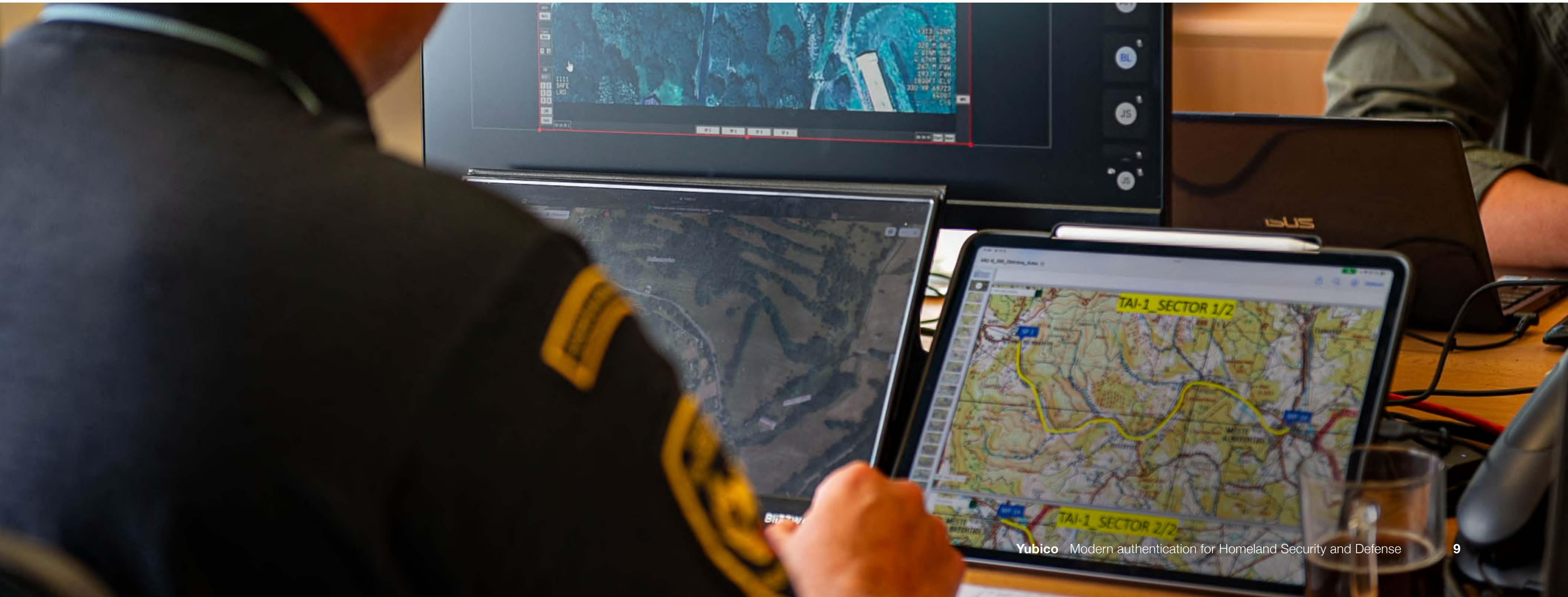
Soldiers, Airmen, civilian employees, contractors, and mission partners using shared workstations and devices benefit from using the YubiKey because it works across multiple shared devices, including desktops, laptops, mobile phones, tablets, and notebooks using the same key. Moreover, a YubiKey is easily re-programmed, making it suitable for rotating shifts and temporary users across these environments.

Securing non-CAC eligible users

Non-CAC eligible personnel such as dependents, contractors, SPP partners, and other users that require 3rd party access still require secure access to systems. To meet these needs, the DoD approved the YubiKey when PKI is infeasible—a FIPS 140-2 validated alternative to the CAC that allows non-CAC personnel or personal non-GFE devices in a BYOD environment to authenticate to DoD networks.

Securing office workers

With the Army deployment of Azure Virtual Desktop (AVD), YubiKeys have been embraced by Soldiers in the Guard and Reserve Soldiers because they provide access regardless of the device used. With multiple form factors and supported by the Army Enterprise Service Desk, YubiKeys can unlock the full potential of AVD for service members, personnel and users on laptops, and mobile devices without needing an additional smart card reader. Similarly, a YubiKey can unlock the full potential of Desktop Anywhere to deliver a consistent experience in the office or working remotely. A YubiKey provides registered users with a simple authentication experience no matter the device used to start the remote session.



Securing SCIFs & air-gapped networks

Air-gapped networks are closed off from the outside, making it difficult to authenticate users using data sent over a network. Many air-gapped systems still use a username and password or a combination of passwords and a digital identity. The multi-protocol capability of YubiKeys ensures that air-gapped networks stay secured against breaches by providing phishing-resistant MFA options that work well in isolated network and mobile restricted environments as they don't need any network connectivity, cellular connection, or batteries to work.

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 150 U.S. government implementations to date. We have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale. 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.

Agencies can obtain Not for Resale (NFR) YubiKeys for proof of concept (POC) programs. Yubico also offers solutions engineering support for architecture design and review, and IDP configuration guidance through the POC.

Plan
Ensure readiness by clarifying use cases and user populations

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

Integrate
Ensure key apps and services are YubiKey-ready

Launch
Distribute keys to users with turnkey delivery services or channel partners

Adopt
Drive adoption with best practice training and support

Measure
Report on security and business value impact

Agencies 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, agencies 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, easy of form factor selection, backup key discounts, and replacement stock benefits.

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, ondemand 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 expertise to help guide you through all facets of your YubiKey implementation and deployment.

Contact us
yubi.co/contact

Learn more
yubi.co/dod

yubico
The key to trust

Yubico (Nasdaq 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 hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, please visit: www.yubico.com.