yubico

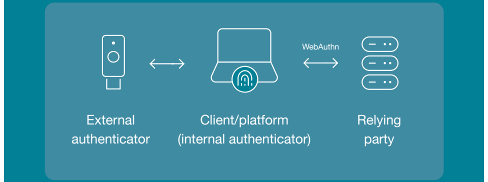
HOW THE YUBIKEY COMPLEMENTS THE CAC AND SOLVES U.S. NAVY MODERNIZATION USE CASES WITH PHISHING-RESISTANT MFA

Modern authentication for the modern naval war fighter

What qualifies as phishing-resistant MFA?

Channel binding PIV/CAC/Smart Card

Verifier name binding FIDO2/WebAuthn



MFA evolution across the Department of Defense

Using the Common Access Card (CAC) for authentication is not practical or possible for every U.S. Navy employee, contractor, mission partner and Reservist. Guidance such as the National Security Memorandum/NSM-8, and more importantly, cyber attacks from nation-states to criminal organizations have mandated the DoD to deploy phishing-resistant authentication as part of a Zero Trust Architecture and created requirements to modernize authentication across the entire Department of Defense (DoD).

While CAC meets the highest assurance of MFA when using DoD Public Key Infrastructure (PKI), there are a growing number of scenarios that have the same assurance requirements where CAC is not available or practical. These scenarios include secure access for telework, BYOAD (Bring Your Own Approved Devices), non-CAC eligible coalition and mission partner environments, air-gapped/isolated networks, and tactical scenarios overseas where relying on a CAC may inadvertently reveal identities. 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.

There is a growing need for cost-effective, turnkey solutions to address the needs of today and future-proof against the authentication needs of tomorrow—including those currently under policy review by the DoD such as Fast Identity Online (FIDO) authentication standards.

Not all MFA is created equal

For those use cases where the CAC is limited or not practical, 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.

The draft National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-4), designed to guide agencies with digital identity assurance and authentication, outlines the technical requirements for phishing-resistant authentication, recognizing two methods as being phishing-resistant: channel binding such as using a PKI-based SmartCard and verifier name binding such as using a Fast Identity Online (FIDO)-based credential and authenticator.

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.

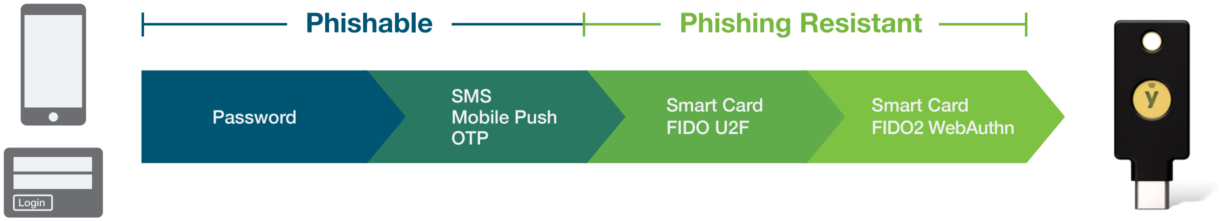
The YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers the 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). 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 DoD CIO memorandum on Approval of Multi-Factor Authentication Alternatives—RSA and YubiKey, 14 April 2017, certifies YubiKeys as DoD-approved alternative MFA and may be used to authenticate to non-privileged user accounts.

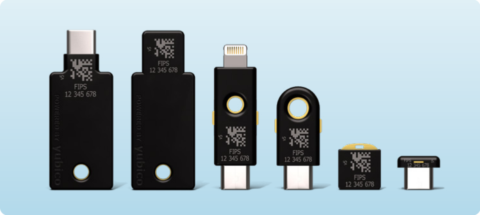
The YubiKey supports derived credentials and provides the highest levels of security needed to protect against modern day attacks along with the flexibility to secure even the most complex scenarios—from air-gapped networks to remote work and cloud services—all from a single key. With multi-protocol support including SmartCard (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.

> “Secure access to National Security IT assets and networks is paramount. The Department of Defense should follow the example set by many large commercial IT companies and investigate the use of YubiKey as a critical component of their network defense strategy.”*
>
> **Mr. Victor Gavin** | SES (Ret), U.S. Navy

**The quote expressed herein are solely those of the individual and do not necessarily represent the views of the Department of Defense.*



A single YubiKey can provide both PKI and FIDO2/WebAuthn phishing-resistant authentication to securely authenticate users to applications and services across GFE or personal devices such as laptops, desktops, tablets, and mobile phones. Unlike managing multiple certificates across mobile devices and CAC cards, a YubiKey with Purebred derived credentials can be used as a portable root of trust across multiple devices including mobile and BYOD/BYOAD. A single YubiKey can provide both PKI and FIDO2/WebAuthn phishing-resistant authentication, housing multiples of each credential. By meeting DoD mobile PKI credential storage requirements, a YubiKey can hold either DoD PKI credentials, issued by Purebred, or an organization can host their own PKI to provide credentials to non-CAC eligible personnel, or for air-gapped and other accepted networks.



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.

Securing telework & BYOAD

Supporting teleworkers and BYOAD using the CAC creates complexity. While password-based authentication may simplify remote access, relying on single-factor authentication does not cater to zero trust security and phishing-resistant authentication requirements.

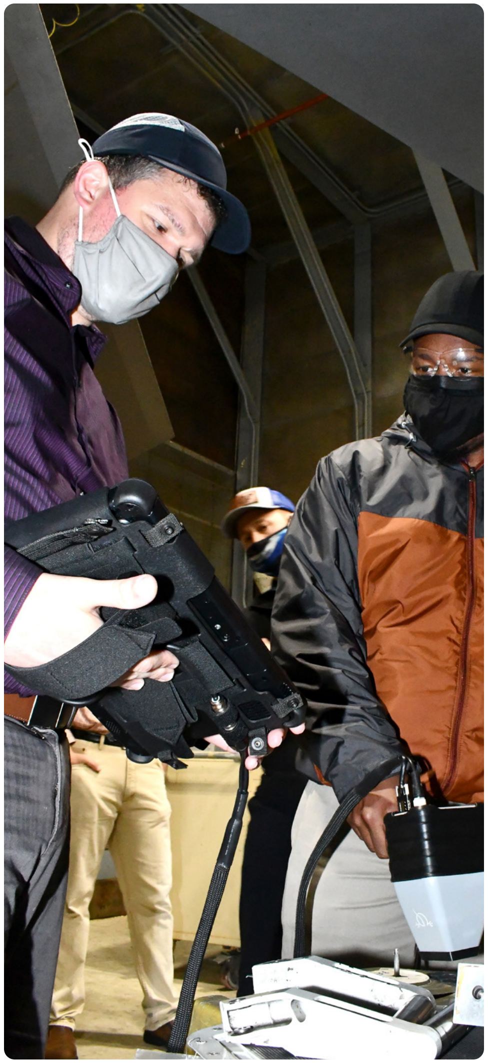
The YubiKey works with leading Identity and Access Management (IAM) and Identity Provider (IdP) solutions to enable phishing-resistant access for remote and hybrid employees without the need for supporting devices. In cases where remote and hybrid workers are sent GFE devices, the YubiKey can be used as a portable root of trust to ensure the device hasn't been compromised en route.

Most Navy Reservists are not issued dedicated government furnished laptops/PCs or mobile phones to conduct official business. More and more, Reservists have to rely on personally owned devices to access Navy resources and services. The Navy has deployed amazing new capabilities such as Flank Speed 365 and Nautilus Virtual Desktop that make it easier for service members to access these services from home, but are still reliant on a CAC and a separate CAC reader. These readers are not always compatible with mobile devices and there have been cases of malware found in CAC readers. With a YubiKey, Reservists would be able to take advantage of a YubiKey with Purebred derived certificates to securely authenticate to Navy resources on any of their personal devices.

Securing privileged users

Ensuring secure phishing-resistant user access to classified, secret and personal information is critical for those privileged users that cannot use the CAC to authenticate. The YubiKey offers the highest-assurance alternate authentication 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 for step-up authentication for high-security applications.

DoD O365 tenant admins cannot use their primary DoD credentials to authenticate for daily tasks and maintenance. Microsoft Azure supports the enrollment of a YubiKey as a FIDO2 authenticator. Admins are able to 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

Government workers that use shared workstations and shared devices such as tablets, can benefit from using the YubiKey as a portable root of trust for secure authentication They can authenticate to the network using the trusted smart card credential on their YubiKey, proving they are a trusted user.

A single YubiKey works across multiple shared devices including desktops, laptops, mobile, tablets, and notebooks, enabling users to utilize the same key as they navigate across devices. YubiKeys are also easily re-programmed, making them suitable for rotating-shift and temporary users across these environments.

The use of shared workstations and mobile devices are increasingly common across the Navy. By affording a pool of resources for maintainers, aviators, and crew, the Navy can lower the total cost of ownership of devices. However, shared devices still have the challenge of supporting multiple users, each requiring DoD credentials for authentication. By shifting the storage of the credentials from the device to a hardware-based authenticator, like a YubiKey, each individual can be issued a security key for authentication on any of the shared devices. Users do not have to worry about grabbing the right devices matching their stored soft credentials.

Securing mission partners

Coalition and Five Eyes (FVEY) mission partners use PKI credentials to authenticate to DoD systems, but are not always CAC-eligible. YubiKey is a solution that is managed at the unit level to support access to the data needed to conduct a mission, supporting strong, phishing resistant authentication for mission partners at the tactical edge.

A YubiKey, as a multi-protocol authenticator, provides flexibility and personalization to coalition networks that require DoD credentials for mission partners. Coalition networks can generate and manage local credentials, provision them to a YubiKey, and issue them to mission partners requiring access to DoD resources within a respective Area of Responsibility. This will ensure that only locally issued credentials can be used for authentication within the respective Combatant Command network. Additionally, options are available for the type of managed credentials—tactical PKI supports certificate-based credentials while other Identity Credential and Access Management (ICAM) components can issue FIDO2 credentials. Both types of credentials meet phishing-resistant authentication requirements.

Securing office workers

The Navy's deployment of Azure Virtual Desktop (AVD), Nautilus, has been welcomed with open arms by Active and Reserve service members. Active Duty service members can easily use the YubiKey for access to AVD regardless of the device being used to connect. Having a provisioned YubiKey offers flexibility to use both an office desktop and personal laptops for access to AVD, providing a strong productivity workflow for daily tasks. The YubiKey comes in multiple form factors and can be used across desktops, laptops, and mobile devices without the need for an additional smart card reader peripheral device.

Securing non CAC-eligible users

Non-CAC eligible personnel such as dependents, contractors and other users that require 3rd party access still require secure access to U.S Navy systems. To meet these needs,the DoD approved the YubiKey as one of three alternate MFA solutions 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 BYOAD environment to securely authenticate to DoD networks.

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. YubiKeys ensure that air-gapped networks stay secured against breaches by providing phishing-resistant MFA that works well in isolated network and mobile restricted environments as they don't need any network connectivity, cellular connection, or batteries to work. YubiKeys are compatible with Cross Domain Solution (CDS) and Multi-Level Security (MLS), and users can be authenticated without transfer of information.

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

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 case 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

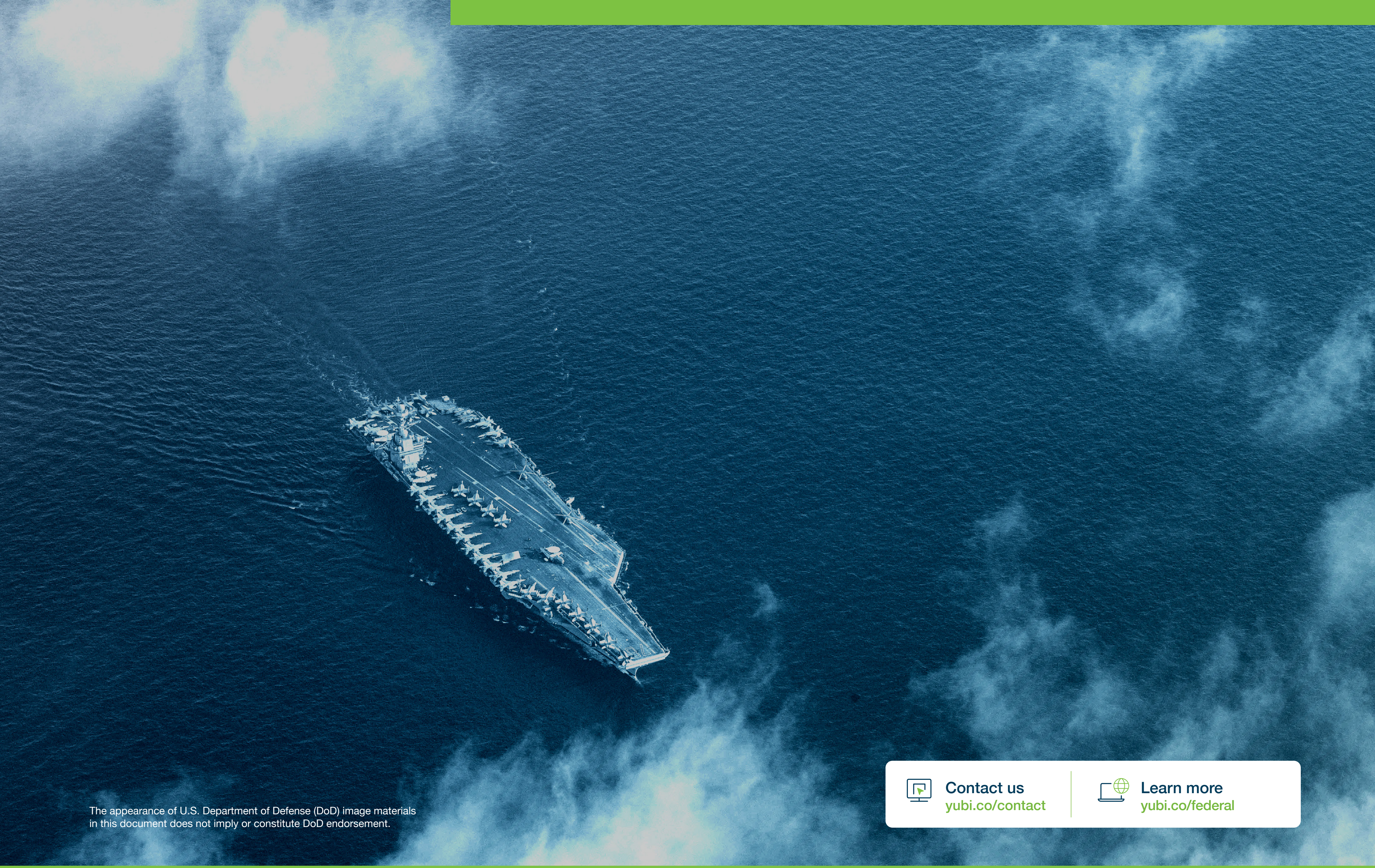
Adopt
Drive adoption with best practice training and support

Measure
Report on security and business value impact

Once ready to purchase, Yubico is focused on helping agencies easily access security products and services in a flexible and cost-effective way to heighten security:

Agencies can purchase YubiKeys via a one-time perpetual purchasing model or can opt for greater flexibility with a subscription model. With YubiEnterprise Subscription, 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, ease 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 sectors. 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.



The appearance of U.S. Department of Defense (DoD) image materials in this document does not imply or constitute DoD endorsement.

Contact us
yubi.co/contact

Learn more
yubi.co/federal

yubico
The key to trust

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.**