



WHITE PAPER

Protecting Federal Systems Integrators against modern cyber threats with highest-assurance security

Win more contracts, stop account takeovers, and meet CMMC and FedRAMP requirements with phishing-resistant MFA



Contents

Table of Contents	2
Executive Summary—The critical need for modern, strong authentication	3
The drawbacks of legacy authentication	4
Shifting cybersecurity standards for federal contractors	5
The federal shift to phishing-resistant MFA to support Zero Trust	6
How does NIST define phishing-resistant MFA?	6
YubiKey offers FIPS-validated phishing-resistant MFA	7
Authentication scenarios supported by the YubiKey	9
Privileged access	9
Hybrid and remote work	9
Mobile / BYOD	9
Shared workstations	10
Air-gapped networks & SCIFS	10
Supply chain integrity	10
Deploy highest-assurance security at scale	11

79%



of DOD contractors **lack comprehensive MFA**⁸

72%



of the top 100 defense contractors **leaked at least one credential** in a 90 day span⁹

“ Nation state targeting of IT service providers might enable the threat actors to exploit other organizations of interest by taking advantage of trust and access granted to these supply chain providers.”

Microsoft Digital Defense Report 2022¹⁰

Executive Summary

Attacks against identity are pervasive; 72% of the top 100 defense contractors had at least one leaked credential between March and May 2022.¹ The Colonial Pipeline and SolarWinds attacks were linked to compromised authentication as the primary attack vector. The former resulted in a shutdown of 45% of the fuel for the east coast of the United States.² The latter software created a backdoor into corporate and federal networks.³

While the federal government is making strides in mandating the use of phishing-resistant multi-factor authentication (MFA) across the executive branches, progress is unclear with federal system integrators (FSIs), which serve as an extension of the government. FSIs have access to critical systems and hold large volumes of sensitive and Controlled Unclassified Information (CUI), making them targets of sophisticated attacks that combine malware, phishing, and/or hacking.

Cyberattacks from nation-state groups have been on the rise.⁴ Raytheon Technologies, for example, fends off two million hack attempts per week⁵ while Lockheed Martin was targeted with a DDoS attack by pro-Russian group Killnet.⁶ China has repeatedly been accused of stealing U.S. technology from contractors to benefit its own stealth fighter jet program.⁷

A major challenge for both government and FSIs is that integrators may not have the same level of security as the agencies they serve—providing adversaries with an alternative attack point to compromise the integrity of products being delivered or the security and privacy of the data or code being exchanged. Either could have negative repercussions on federal operations and national security—not to mention internal operational disruptions, monetary loss, damage to brand, the loss of intellectual property (IP) and safety issues.

While any form of MFA will offer better security than password-based authentication alone, the truth is that not all MFA is created equal. Legacy authentication technologies—such as SMS, one-time passcodes (OTP), and push notification apps—remain highly susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle incidents.

As a result, FSIs face mounting pressure to implement modern, phishing-resistant MFA to secure identities and corporate secrets as well as modern cryptographic protection to secure servers, applications and computing devices. Although this pressure applies most specifically to federal access and data, times are changing and it's important to choose the right form of authentication.

The drawbacks of legacy authentication

10-24%



attack penetration rate
for mobile authentication¹¹

\$1 million



per year **cost for password
resets** alone¹²

Legacy mobile authentication solutions create **security** gaps and **usability** concerns. Further, the MFA strategy you choose can deliver on a vastly different ROI in terms of cost, compliance and coverage.



Security



Cost



User experience



Compliance



360° coverage

As cyber attacks have become more sophisticated, FSI organizations need to implement phishing-resistant MFA that provides the **greatest protection from attack** so they don't become the weakest link in the chain. Legacy MFA are susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle attacks at a penetration rate of 10-24%.¹³ In fact, the risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication in 2016.¹⁴

Legacy authentication also carries many **hidden governance and support costs** around setting and managing password policies at scale, productivity costs associated with account lockouts and time-consuming workflows to generate and enter OTP/TOTP/push app codes, and of course the costs associated with the risk of a potential data breach. Further, cyber insurers have countered their business liabilities with higher premiums,¹⁵ sub limits and exclusions,¹⁶ suggesting FSIs be prepared to provide evidence of cyber risk mitigation efforts, including MFA strategy, to make the organizational security profile more attractive to cyber insurers.

While security is a key driver for MFA adoption, 43% of organizations cite **user experience as the top obstacle to using MFA**,¹⁷ particularly when organizations combine the challenges of passwords (hard to remember, IT complexity) with mobile authentication (delays, availability issues, environmental considerations, MFA fatigue). Further, there are always **coverage gaps where mobile authentication does not work**—where users lack devices, availability or mobile-restrictions may apply, among other scenarios.

MFA investments must provide organizations with protection that evolves as **risk** and **compliance** requirements do. To be **future-proofed**, the MFA investment should reflect the growing regulatory requirement for phishing-resistant MFA, the need to implement Zero Trust, and modern login flows such as passwordless.



Shifting cybersecurity standards for federal contractors



Government contractors are required to implement the mandatory controls for CUI detailed by National Institute of Standards and Technology (NIST) SP 800-171.¹⁹ The draft NIST SP 800-171r3 will require a shift to MFA, specifically **phishing-resistant authentication** (aka replay-resistant authentication), for access to **system accounts**—not just for privileged accounts.²⁰ In fact, the most recent self-assessment methodology reflects a deduction in scoring if MFA is implemented only for remote and privileged users rather than all users and adds an additional point if MFA is phishing-resistant.²¹

The Cybersecurity Maturity Model Certification (CMMC)²² is the Department of Defense’s (DOD) unified standard for implementing cybersecurity across the defense industrial base, consisting of fourteen domains and three maturity levels that align to NIST standards. In July 2023 the DOD sent the CMMC 2.0 framework to the OMB Office of Information and Regulatory Affairs for final rulemaking.²³

CMMC Model 2.0		
	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110+ practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation

According to a CyberSheath study, 87% of DOD contractors have a sub-70 Supplier Performance Risk System (SPRS) score, below both the Defense Federal Acquisition Regulation Supplement (DFARS) as well as Cybersecurity Maturity Model Certification (CMMC) minimums.²⁴

While CMMC certification is only required for DOD contracts, CUI protection requirements apply across the federal government and CMMC is considered an asset in any federal contract. For any FSIs whose solutions include cloud service offerings, it’s also important to align with the Federal Risk and Authorization Management Program (FedRAMP) Cloud Security Technical Reference Architecture guide, revised to include security requirements in line with Zero Trust.²⁵

Further, CISA has made clear that any contractor developing software for the federal government should be using phishing-resistant MFA for all employees as part of making their products secure-by-design and by-default.²⁶

The federal shift to phishing-resistant MFA to support Zero Trust

In the past two years, the White House has pushed forward new regulations focusing on Zero Trust and phishing-resistant MFA, including White House Executive Order (EO) 14028,²⁷ the Office of Management and Budget (OMB) Memo M-22-09,²⁸ and National Security Memorandum (NSM)-8.²⁹

While OMB M-22-09 directs federal agencies to adopt the exclusive use of phishing-resistant MFA for all users, employees and contractors, these requirements reflect the new baseline standard for protecting against cyber attacks.

The DOD Identity, Credential, and Access Management (ICAM) Strategy³⁰ and CISA's Zero Trust Maturity Model³¹ have subsequently been developed to support the shift to Zero Trust. In particular, the DOD has expressed a continued commitment to credential quality, including innovative capabilities such as hardware security keys and phishing-resistant MFA.



How does NIST define phishing-resistant MFA?

Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process.

According to the NIST Special Publication (SP) 800-63 and Draft 800-63-4,³² two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.



YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers the phishing-resistant FIPS 140-2 validated YubiKey, a DOD-approved³³ hardware security key that offers highest-assurance multi-factor authentication at scale and meets the FIDO2/WebAuthn standard. The YubiKey is CMMC Level III and FedRAMP compliant and supports NIST SP 800-171.



The YubiKey is:

FIPS 140-2 validated to
AAL 3 requirements
Overall Level 1 (Certificate #3907)
and Level 2 (Certificate #3914),
Physical Security Level 3

CMMC Level III compliant

DFARS / NIST SP 800-171
compliant

Manufactured securely
in the US



Works with YubiKey

YubiKeys, the industry's
#1 security keys, work
with hundreds of products,
services, and applications.
Browse YubiKey
compatibility → [here](#)

Benefits of the YubiKey



Federal compliant

FIPS 140-2 validated
Overall Level 1
(Certificate #3907) and
Level 2 (Certificate
#3914), Physical
Security Level 3 to
NIST SP 800-63B AAL3
requirements, CMMC
Level III and FedRAMP
compliant, supports
NIST SP 800-171



CMMC requirements

The YubiKey helps
DOD contractors and
sub-contractors meet
CMMC requirements
across Identification
and Authentication,
Access Control, Audit
and Accountability,
Maintenance, and Media
Protection domains



Multi-protocol

YubiKeys support
multiple authentication
protocols on a single
key such as SmartCard/
PIV, FIDO2, FIDO U2F,
OTP, OpenPGP, offering
a single solution across
legacy and modern
environments and a
bridge to modern
FIDO2 passwordless



Broad ecosystem

YubiKeys work with
over 1,000 leading
applications and
services including
Identity and Access
Management (IAM)
solutions, password
managers and more.
Deploy seamlessly with
Centrify, Microsoft,
Okta, Ping, DUO,
Google and others



Easy to use

Users can simply touch
or tap to authenticate.
YubiKeys come in
different form factors
for USB-A, USB-C,
Lightning and offer
NFC capabilities. No
battery or network
connectivity required, no
broken screens. Crush
resistant and dust proof



Configurable

Easily configure multiple
protocols across
computers, mobile
devices/BYOD, tablets,
networks, and online
applications and services

The YubiKey uses modern protocols such as FIDO U2F and FIDO2 open authentication standards and additionally support protocols such as OPT, PIV/Smart Card and OpenPGP, with the hardware authenticator protecting the private secrets on a secure element, entirely eliminating phishing-driven credential-based attacks.

Hardware security keys such as the YubiKey are an ideal option for strong phishing-resistant MFA because they don't require additional hardware or software, external power or batteries, or a network connection—a single key secures hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.

As a portable hardware root of trust, the YubiKey is proven to reduce risk against phishing attacks and account takeovers by 99.9%³⁴ and serves as a user-friendly, cost-effective enabler of a Zero Trust security architecture. The YubiKey can also help bridge to modern login flows such as passwordless.

The total economic impact of YubiKeys:



Strongest Security

Reduce risk
by
99.9%



High Return

Experience ROI
of
203%



More Value

Reduce support
tickets by
75%



Faster

Decrease time to
authenticate by
>4x



Cyber insurance

Meets
requirements
100%



Authentication scenarios supported by the YubiKey



Note, while authentication use cases have been itemized to help identify common authentication challenges and to help FSIs prioritize a risk-based deployment process, authoring agencies may require contractors to adopt secure-by-design and -default practices that include phishing-resistant MFA for all employees and all scenarios.³⁵

With the YubiKey, FSIs can deploy highest-assurance, phishing-resistant MFA to support a variety of authentication scenarios, including privileged access, hybrid and remote work, mobile / BYOD, air-gapped networks & SCIFS and the integrity of the supply chain.



Privileged access

Privileged access to classified, secret and personal information places key contractors to the government (e.g. security, network and database admins) at risk of compromise. Any unauthorized access to ICT systems or data, including defense plans, budgets, and strategic planning docs, can place missions and national security at risk.

The YubiKey's hardware design enables the authentication secret to be stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen, offering the highest security for authenticating privileged users. The YubiKey can also be used as an additional form of validation for highly classified systems and documents, to quickly re-verify the user before access is granted or a required action is taken.



Hybrid and remote work

Many FSIs have adopted a hybrid and remote work approach that moves security from a perimeter-based approach to a per user and per device approach. Remote work introduces new vulnerabilities such as unsecured home networks, unpatched devices, shared devices, and weak/reused passwords—vulnerabilities that persist when connecting to Virtual Private Networks (VPN), Identity-Aware IdentityProxies (IAP), IAM and Identity Provider (IdP) platforms.



Mobile / BYOD

PIV/CAC authentication is not practical for mobile scenarios and storing credentials on that device further introduces security concerns if it is lost or stolen. With the YubiKey as a portable root of trust, contractors and DIB partners can authorize their personal mobile devices to access approved DoD services. Devices need to be authorized only a single time, with optional support for users to re-authenticate (step-up authentication) to specific government apps and services.

As the number of devices per employee increases, having a single portable external authenticator that can work across all computing devices helps make these transitions seamless.



Shared workstations across manufacturing floors

The YubiKey provides phishing-resistant MFA in a portable form factor for users that need to securely authenticate across shared workstation environments.

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 between devices, and helping you deploy phishing-resistant MFA at scale. YubiKeys are IP68 certified and are also easily re-programmed, making them suitable for rotating-shift and temporary workers across these environments.



Air-gapped networks & SCIFS

Air gap 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 username and password or a combination of passwords and a digital identity since the use of a Smart Card would require additional, expensive readers and would introduce security concerns for the air gap network.

YubiKeys don't need any network connectivity, cellular connection or batteries to work. YubiKeys ensure that air gap networks stay secured against breaches by providing a multi-factor authentication solution that works well in isolated network and mobile restricted environments. With a YubiKey, users can be authenticated without transfer of information across a Cross Domain Solution (CDS).



Supply chain integrity

Federal agencies subject to EO 14028 and OMB M-22-09³⁶ are adopting a Zero Trust Architecture strategy that requires them to trust no one or no thing unless properly verified before being given access to sensitive resources, requirements that are increasing the scrutiny on FSIs and their own downstream supply chain practices in three key areas: Third-party access to systems, code or IP, Software supply chain and IP and product integrity.

Draft NIST SP 800-171r3 specifically adds new requirements for supply chain risk management, including the use of defective components, counterfeits, theft, malicious development practices, improper delivery practices, and the insertion of malicious code.³⁷

Third-party relationships with vendors, contractors, and partners require ongoing exchanges of data that introduce risk. FSIs can reduce the risk in the supply chain with the YubiKey for any third-party user who has upstream access to the network. It is also important to ensure any vendor in the supply chain has proper chain-of-custody and disposal processes for secrets.

While the YubiKey provides secure, phishing-resistant MFA for third-party access and secure code signing capabilities to protect the software supply chain, ensuring the integrity of IP and product parts involves the use of digital cryptographic signing keys and encryption.

Since cryptographic keys stored in software are highly vulnerable to a variety of attack vectors including online channels, FSIs can leverage the YubiHSM 2 FIPS, a hardware security module (HSM) that provides a secure way to generate, store and protect both cryptographic keypairs and X.509 certificates on secure, purpose-built hardware.

Key areas for supply chain integrity



Third-party access to systems, code or IP



Software supply chain



IP and product integrity



The YubiHSM 2 FIPS

The YubiHSM 2 FIPS can be applied to any process where secrets and the authenticity of components needs to be managed, and where tampering needs to be prevented, in accordance with NSA guidance on how to harden on-premise systems.³⁸ It can be easily deployed to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices.

Deploy highest-assurance security at scale

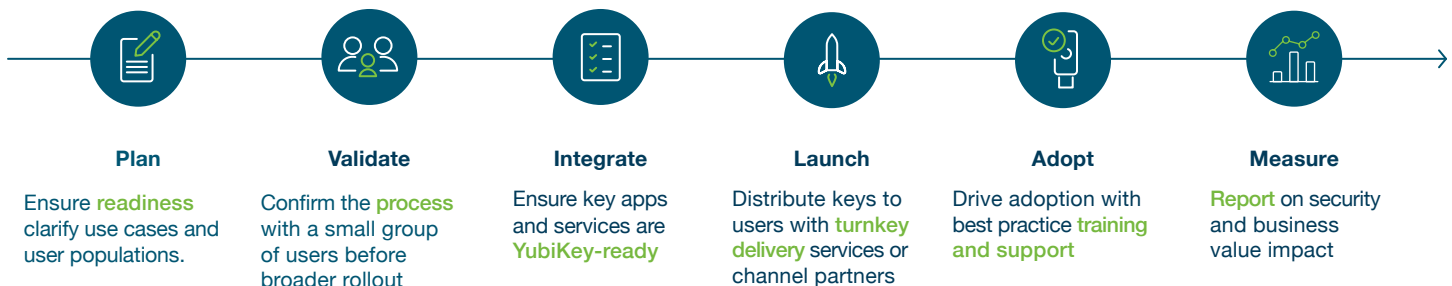
To protect against the growing number of cyber threats and shifting requirements and regulations for government contracts, FSI's need a modern solution to provide phishing-resistant MFA at scale and across a wide variety of complex authentication scenarios.

We have made it easy to deploy phishing-resistant MFA with the YubiKey. We offer a simple [6 Step Best Practice Deployment Guide to help accelerate modern MFA adoption at scale](#).

To streamline and simplify planning, purchasing and delivery, Yubico offers professional services and as-a-service options and works with many channel partners to make getting started easy.

FSI's can leverage security as a service through Yubico solutions. YubiKeys as a service simplifies the process of scaling YubiKeys to additional use cases and leveraging the insight from working with over 150 U.S. government implementations to date.

[Yubico's Professional Services](#) team is here to help with each implementation step.



yubico

Professional Services

Expert consulting services, including operational and technical workshops, implementation projects on-demand resources and custom engagements, designed to jump-start and accelerate your YubiKey deployment.

Yubico is leading the charge toward a more secure and riskless authentication future. Our team of experts provides technical and operational guidance to help streamline your YubiKey implementation and rollout.

Services Offered


Deployment 360 Program
A turnkey program packaging all of the essential elements and expertise to ensure your successful YubiKey deployment.


Workshops
Interactive sessions designed to help jump start YubiKey integration and deployment.

National Implementation Projects
Tailored projects designed to facilitate your YubiKey

Read the solution brief [→ here](#).

YubiEnterprise Services*

**YubiEnterprise Subscription**


**YubiEnterprise Delivery**


Yubico Professional Services

**Deployment 360**
Service hour bundles

**Workshops**
Implementation projects

* YubiEnterprise Services are available for organizations of 500 or more users.

 **Contact us** yubi.co/contact

 **Learn more** yubi.co/si

YubiEnterprise Subscription

With YubiEnterprise Subscription, agencies receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support and more.

YubiEnterprise Delivery

With YubiEnterprise Delivery, agencies experience turnkey authentication with shipping of YubiKeys, tracking, and returns processing of Yubico products handled seamlessly by logistics experts, so organizations can focus on what matters—securing the workforce.

Sources

- ¹ BlackKite, [Centralizing Supply Chain Cybersecurity: US Federal Government Risk in 2022](#), (May 24, 2022)
- ² Stephanie Kelly and Jessica Resnick-ault, [One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators](#)
- ³ Kim Zetter, [The Untold Story of the Boldest Supply-Chain Hack Ever](#), (May 2, 2023)
- ⁴ Microsoft, [Microsoft Digital Defense Report 2022](#), (November 2, 2022)
- ⁵ Harvard Business Review, [Raytheon CEO Gregory Hayes: How Ukraine Has Highlighted Gaps in US Defense Technologies](#), (March 25, 2022)
- ⁶ Kevin Townsend, [Killnet Releases ‘Proof’ of Its Attack Against Lockheed Martin](#), (August 12, 2022)
- ⁷ Sakshi Tiwari, [Chinese ‘Stealth’ Espionage! How Beijing-Backed Hackers ‘Acquired’ Sensitive US Tech Used In Its F-35 Fighter Jet?](#), (February 3, 2022)
- ⁸ CyberSheath, [More than 87% of Pentagon Supply Chain Fails Basic Cybersecurity Minimums](#), (November 30, 2022)
- ⁹ BlackKite, [Centralizing Supply Chain Cybersecurity: US Federal Government Risk in 2022](#), (May 24, 2022)
- ¹⁰ Microsoft, [Microsoft Digital Defense Report 2022](#), (November 2, 2022)
- ¹¹ Kurt Thomas and Angelika Moscicki, [New research: how effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ¹² Forrester Research, Inc, [Optimize User Experience With Passwordless Authentication](#), (March 2, 2020)
- ¹³ Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ¹⁴ Rob Lemos, [The state of two-factor authentication by text: What security pros need to know](#), (Accessed Sept 14, 2021)
- ¹⁵ Marsh, [Global Insurance Market Index First quarter 2023](#), (July 31, 2023)
- ¹⁶ Frederic Lee, [Cyber insurance rate hikes slow - but exclusions expand](#), (Accessed August 7, 2023)
- ¹⁷ 451 Research, [2021 Yubico and 451 Research Study](#), (April 2021)
- ¹⁸ NIST, [Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#), (February 2020)
- ¹⁹ NIST, [NIST SP 800-171r3 ipd](#), (May 2023)
- ²⁰ NIST, [NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1](#), (June 24, 2020)
- ²¹ DOD CIO, [CMMC 2.0](#), (Accessed August 8, 2023)
- ²² OMB, [Pending EO 12866 Regulatory Review](#), (July 24, 2023)
- ²³ CyberSheath, [More than 87% of Pentagon Supply Chain Fails Basic Cybersecurity Minimums](#), (November 30, 2022)
- ²⁴ CISA, [US Digital Service, FedRAMP, Cloud Security Technical Reference Architecture v 2.0](#), (June 2022)
- ²⁵ CISA, [Security-by-Design and -Default](#), (June 12, 2023)
- ²⁶ The White House, [Executive order on Improving the Nation’s Cybersecurity](#), (May 12, 2021)
- ²⁷ OMB, [M-22-09](#), (January 26, 2022)
- ²⁸ White House, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#), (January 19, 2022)
- ²⁹ DOD, [Identity, Credential, and access Management \(ICAM\) Strategy](#), (March 30, 2020)
- ³⁰ CISA, [Zero Trust Maturity Model v 2.0](#), (April 2023)
- ³¹ NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (December 2022)
- ³² DOD OCIO, [Memo](#), (December 20, 2019)
- ³³ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- ³⁴ CISA, [Security-by-Design and -Default](#), (June 12, 2023)
- ³⁵ OMB, [M-22-09](#), (January 26, 2022)
- ³⁶ NIST, [NIST SP 800-171r3 ipd](#), (May 2023)
- ³⁷ NSA, [Detecting Abuse of Authentication Mechanisms](#), (December 2020)



About Yubico

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.