yubico

Modern authentication for Federal Systems Integrators and Sub-contractors

Hardware passkeys drive cyber resilience with phishing-resistant MFA and exceptional UX

MFA evolution across the FSI space

Federal Systems Integrators (FSIs), the Defense Industrial Base (DIB), and their sub-contractor supply chain remain under persistent cyberattack, often from threat actors who leverage sophisticated technologies and Artificial Intelligence (AI) kits that combine malware, phishing and/or hacking. These complex attacks are often linked with the use of stolen credentials and often target the supply chain as the weakest link.

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 FSIs, which serve as an extension of the government. FSIs and their sub-contractors 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. **A major challenge for both government and FSIs is that integrators and sub-contractors 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.

The Cybersecurity Maturity Model Certification (CMMC) 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. The CMMC domain—Identification and Authentication (IA. L2-3.5.3) in particular lists the requirement for multi-factor authentication. With CMMC, all sub-contractors are required to meet the same level of CMMC maturity as the awarded prime.

There is a growing need for phishing-resistant multi-factor authentication to address the cyber threats of today and tomorrow.

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

What is Fast Identity Online (FIDO)?

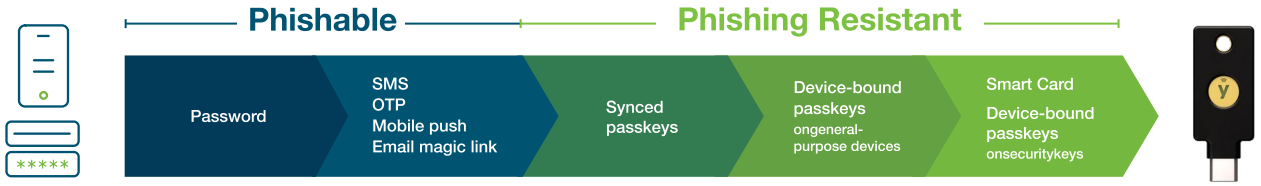
FIDO2 is an open authentication standard, created by the FIDO Alliance, that consists of the W3C Web Authentication specification (WebAuthn API), and the Client to Authentication Protocol (CTAP). CTAP is an application layer protocol used for communication between a client (browser) or a platform (operating 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.

Rethink cybersecurity in the age of AI

The introduction of **Agentic AI and Generative AI in general makes cyber attacks faster and more dangerous.** Generative AI allows for automation and accelerates the entire initial entry and attack lifecycle, compressing what used to take days or weeks into a matter of minutes. This significantly reduces the window for human defenders to detect and respond to an attack.

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. For those use cases where the Common Access Card (CAC) and Personal Identity Verification (PIV) is limited or not practical, falling back on username and passwords or legacy multi-factor authentication (MFA) is risky. Accounts using MFA that are not based on phishing-resistant protocols are susceptible to having credentials stolen.

The 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 Smart Card and verifier name binding such as using a Fast Identity Online (FIDO)-based credential and authenticator.



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

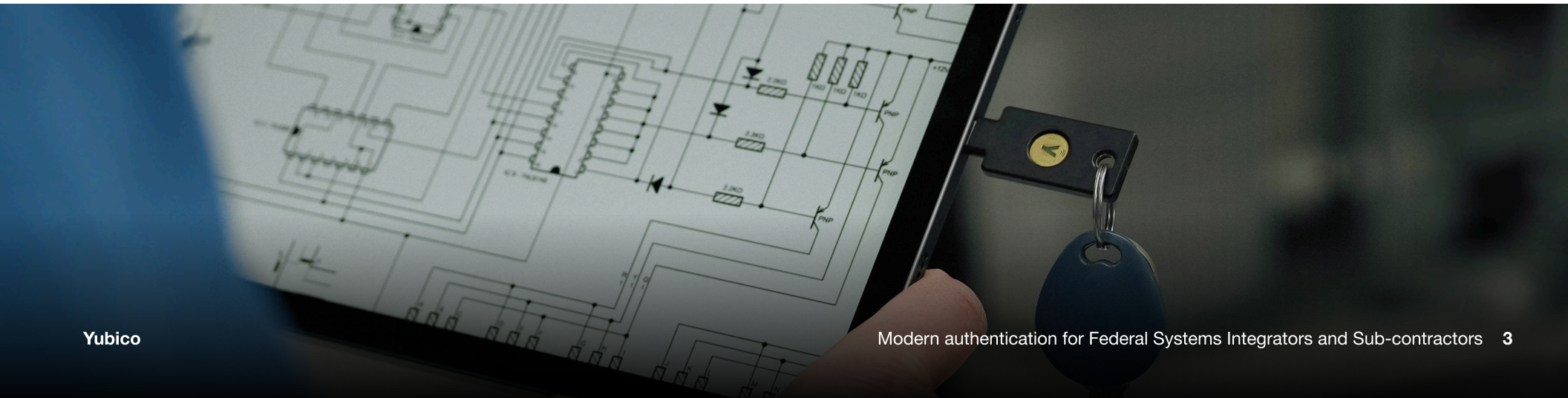
The YubiKey 5 Series –
from left to right: YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

The YubiKey offers FIPS-validated phishing-resistant MFA

Yubico offers the phishing-resistant FIPS 140-2 validated YubiKey. The YubiKey is a hardware passkey that is purpose-built for security and offers the highest-assurance multifactor and passwordless authentication. The YubiKey 5 FIPS Series meets NIST Authentication Assurance Level 3 (AAL3) and supports Zero Trust architecture initiatives. It is currently undergoing FIPS 140-3 validation, which is expected shortly.

The YubiKey provides the highest levels of security needed to protect against modern-day attacks, along with the flexibility to secure even the most complex scenarios all from a single key. With multiprotocol support, including Smart Card (PIV/CAC), FIDO U2F, FIDO2, OTP, and OpenPGP, the YubiKey supports both legacy and modern architectures with a single solution, providing a future-proof bridge to modern FIDO and passwordless authentication standards. With the YubiKey, FSIs and sub-contractors can implement FIDO2 passwordless, Smart Card passwordless or a hybrid strategy, depending on the infrastructure and use cases that need to be addressed.

By adopting YubiKeys, the FSI community and its sub-contractors can collectively meet contractual requirements while ensuring they meet the highest cybersecurity standards to protect against evolving cyber threats. Deploying YubiKeys is not just an IT decision, it's a critical step in safeguarding critical data. YubiKeys enable secure and simple access to systems and data for all users, whether an air-gapped network, SCIF, or other area where other authentication technology might not be enabled.



Phishing-resistant MFA scenarios

Securing privileged users

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 Informative and Communication Technology (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.

Securing telework & BYOAD

While password-based authentication may simplify remote access, relying on single-factor authentication does not satisfy zero trust security and phishing-resistant authentication requirements.

Fortunately, 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. YubiKeys have the flexibility to be used with a wide range of mobile devices and unmanaged and managed workstations, including Chromebooks and personal phones. In cases where remote and hybrid workers are sent company devices, the YubiKey can also be used as a portable root of trust to ensure the device hasn't been compromised enroute. 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.

READ THE WHITEPAPER →

Securing shared devices & workstations

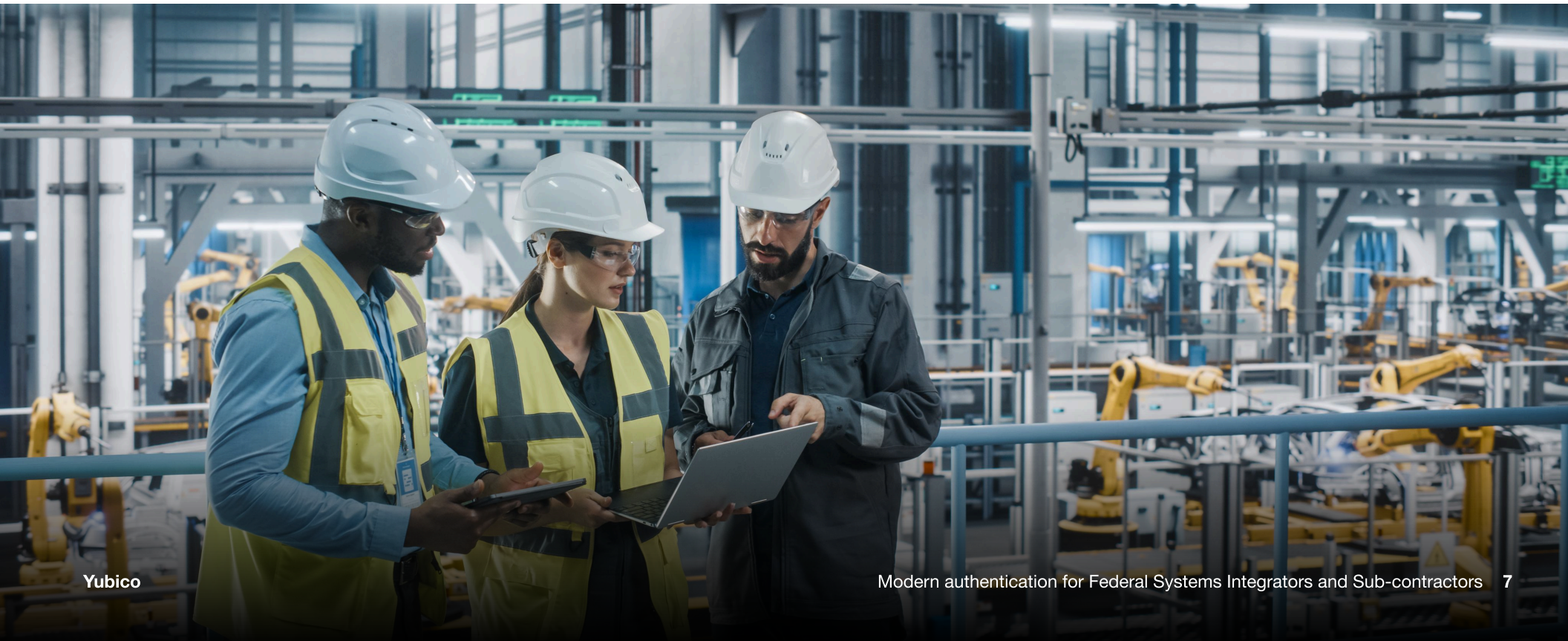
Shared workstations, kiosks, and devices are critical to the day-to-day operations of businesses within this sector, and often have a direct link to critical systems and data, including customer data, payment information, proprietary information, manufacturing or assembly lines. Shared devices have the challenge of supporting multiple users. 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.

READ THE WHITEPAPER →

Securing manufacturing floors

For manufacturers to ensure secure workflows across manufacturing floors that are typically mobile-restricted environments, while accelerating business, they need to consider an MFA solution that can easily overcome the unique security and productivity challenges. Any authentication solution used in a manufacturing facility must be able to withstand the daily rigors of that environment. The use of moving and heavy equipment, hard surfaces, and thick gloves all combine to increase the risk of damage to authentication solutions that enter the workplace. The chosen authentication solution should be highly durable, crush-resistant, and able to withstand regular sanitization.

The versatile and IP68 certified YubiKey requires no software installation, battery, or cellular connection, making it ideal for shared workstation and **mobile-restricted environments,** including isolated areas within manufacturing. They are also dust proof, crush resistant, water resistant, and highly durable. Users can benefit from a frictionless authentication workflow—a user plugs the YubiKey into a USB port and touches a button to authenticate, or simply taps the YubiKey using NFC against a device (highly suited for no spark environments).



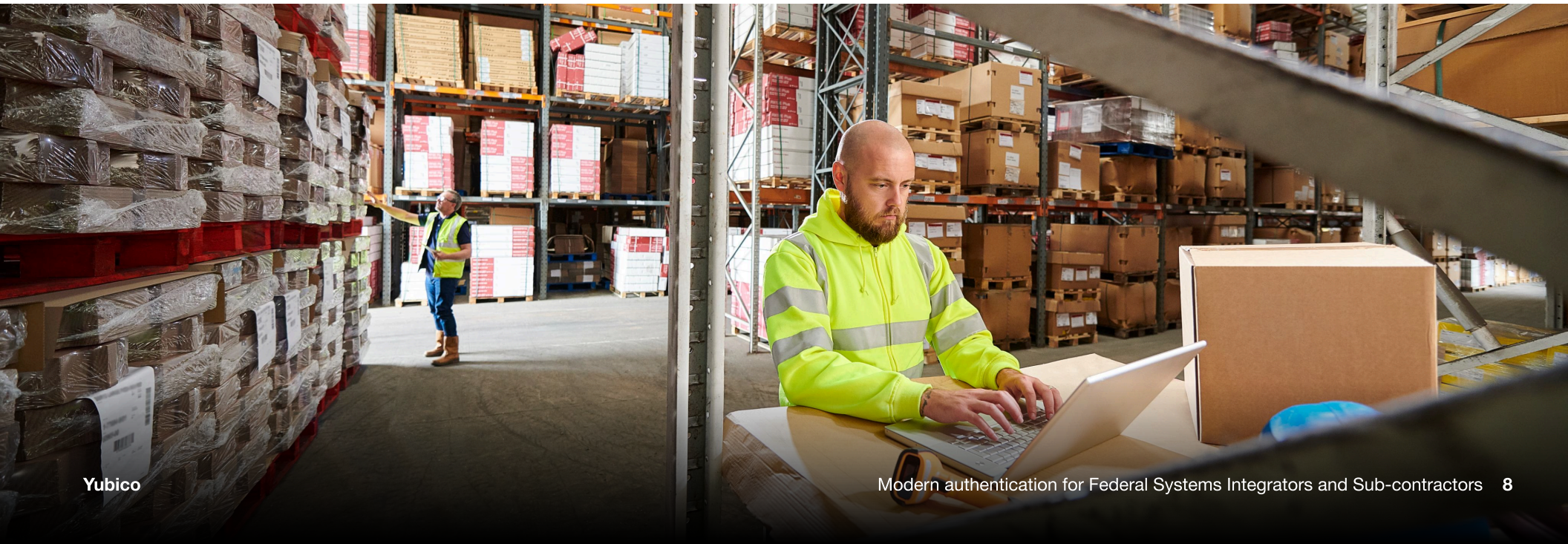
The YubiHSM2 FIPS

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

Securing supply chain

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. 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 key pairs and X.509 certificates on secure, purpose-built hardware.



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.

Plan

Ensure **readiness** clarify use cases and user populations

Validate

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

Intergrate

Ensure key apps and service are **Yubikey-ready**

Launch

Distribute keys to users with **turnkey delivery** service or channel partnerx]s

Adopt

Drive adoption with best practice **training and support**

Measure

Report on security and business value impact

FSIs and sub-contractors 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.

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

YubiKeys can be purchased via a one-time perpetual purchasing model or can opt for greater flexibility with a subscription model. You may work with Yubico on preferred pricing for your sub-contractors.

To make it easy to deploy passwordless authentication at scale to secure digital identities against modern AI-driven threats, Yubico offers YubiKey as a Service for fast and frictionless deployment of enterprise-grade security.

- With YubiKey as a Service, organizations can benefit from simple and scalable global deployments of YubiKeys for their workforce, supply chain, and end customers.
- YubiKey as a Service offers customers a choice of form factors, replacement stock, and priority customer support,all for less than the price of a cup of coffee per month. Customers also have access to turnkey Enrollment and Delivery services that help IT get users quickly onboarded with YubiKeys to fast track to phishing-resistance and then get YubiKeys to end users across the world, including corporate and residential addresses. **Users can even experience self-service ordering of YubiKeys via the End User Portal,** giving them the freedom to have the keys shipped to their preferred address anytime they need. YubiKey as a Service customers receive continual enhancements to available and new services assuring a smart and future-proofed security investment.

yubico
The Key to Trust

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

Our technology secures people in over 160 countries, delivering fast, passwordless access. Dual-headquartered in Stockholm and Santa Clara, we believe strong security should be within everyone's reach. Learn more at www.yubico.com.