yubico

Securing Federal Systems Integrators

with modern, phishing-resistant authentication

Rising data breach costs and evolving regulations

The 2023 average cost of a data breach was USD 4.45 million[1], with phishing and stolen or compromised credentials the two most prevalent attack vectors. Despite the growing tide and sophistication of modern cyber attacks and federal regulations such as White House Executive Order 14028 and CMMC 2.0, many federal systems integrators continue to use legacy multi-factor authentication (MFA) methods to secure access to critical federal and in-house applications and data.

Not all MFA is created equal

While any form of MFA is better than username and password based authentication, not all forms of MFA are created equal. Mobile-based MFA such as SMS, OTP, and push notifications are highly susceptible to phishing attacks, malware, SIM swapping, attacker-in-the-middle attacks, and account takeovers. Mobile authenticators also don't offer the best user experience. Users are required to wait for and enter codes, and are dependent on cellular connectivity and battery. They also aren't suitable for mobile-restricted areas such as manufacturing floors and other areas with heavy machinery.

What is 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 only two authentication forms currently meet the phishing-resistant MFA mark: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.

Yubico's security solutions for federal systems integrators

Yubico offers the YubiKey for modern phishing-resistant multi-factor and passwordless authentication, and the YubiHSM for protecting servers, applications, and computing devices.

YubiKeys deployed in:

9 of the top 10 global technology companies	**4 of the top 10** U.S. banks	**5 of the top 10** global retailers

The YubiKey from Yubico is a FIPS 140-2 validated hardware security key (Certificate #3517) that is purpose-built for high security and designed to stop phishing and account takeover in their tracks, delivering strong authentication at great scale. It's the only solution proven by independent researchers to stop 100% of account takeovers, including bulk and targeted phishing attacks[2].

Yubikeys offer modern, phishing-resistant MFA for office workers, privileged users, remote workers, mobile restricted environments, shared workstations and devices, air-gapped networks and SCIFS, and third party entities/supply chain.

YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 1,000 applications and services out-of-the-box.

A single YubiKey works across legacy and modern systems and applications with multi-protocol support for SmartCard(PIV), TOTP, OpenPGP, FIDO U2F, and FIDO2/WebAuthn, helping bridge to a modern passwordless future without a rip and replace.

Summary of benefits

(3 year risk adjusted)

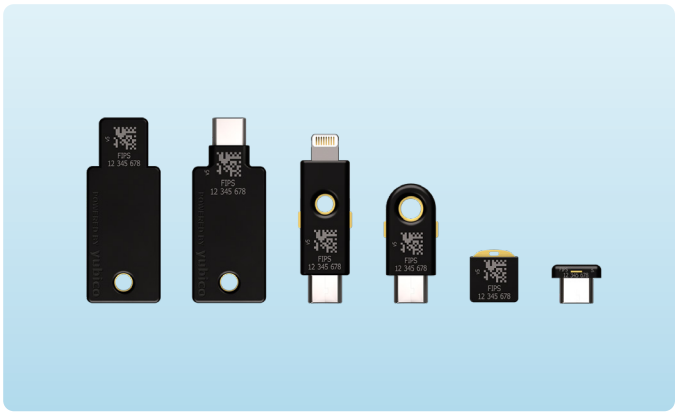
203%
return of investment

75%
reduced password related help desk tickets

17,500
hours saved for end-users by year 3

99.9%
blocked phishing-attempts

*Forrester Research, The Total Economic Impact Of Yubico YubiKeys, September 2022

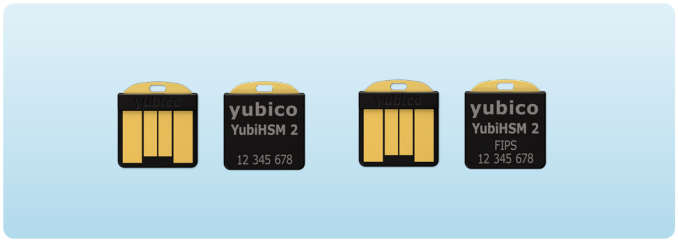


The YubiKey 5 FIPS Series is the first FIPS validated FIDO2/WebAuthn, multi-protocol authenticator lineup. From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS.

Benefits of the YubiKey

- FIPS 140-2 validated: Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914)
- Multi-protocol support for SmartCard (PIV), TOTP, FIDO2/WebAuth, FIDO U2F, and OpenPGP on the same device
- Portable external authenticator works across all computing devices with options to connect via NFC, USB-A, USB-C, and Lightening
- Secure United States manufacturing and supply chain processes, for trustworthy components and delivery
- YubiKeys are water resistant, crush resistant, dustproof and tamper proof, and require no battery or network connectivity

The YubiHSM 2 ensures uncompromised cryptographic hardware security for servers, applications, and computing devices at a fraction of the cost and size of traditional HSMs. It is a FIPS 140-2 validated, Level 3 solution, and is also available as a nonFIPS solution—both with the same capabilities. It can be easily deployed to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices.



The YubiHSM 2 and YubiHSM 2 FIPs

Benefits of the YubiHSM 2

- Ultra-portable, innovative 'nano' form-factor that allows for flexible deployment
- Cost-effective, enterprise-grade high cryptographic security and operations without the traditional HSM price tag
- Robust hardware protection that is FIPS 140-2 validated, ensuring the highest levels of data protection and compliance demands

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 multi-protocol FIDO2 authenticator.

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:

YubiEnterprise subscription

With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys in a way that meets technology and budget requirements, providing priority customer support, easy form factor selection, backup key discounts, and replacement stock benefits

YubiEnterprise delivery

With YubiEnterprise Delivery, organizations receive turnkey service with shipping, tracking, and returns of Yubico products—all securely handled by logistics experts. It also helps with inventory management with delivery of keys.

WATER RESISTANT | CRUSH RESISTANT | MADE IN US & SWEDEN

Contact us
yubi.co/contact

Learn more
yubi.co/fsi

1. IBM, 2023 Cost of Data Breach Report, (July 24, 2023)
2. Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA), and a creator and contributor to FIDO open authentication standards. The company is a pioneer in delivering hardware-based passkey authentication to customers in 160+ countries. For more information, visit: www.yubico.com.