yubico

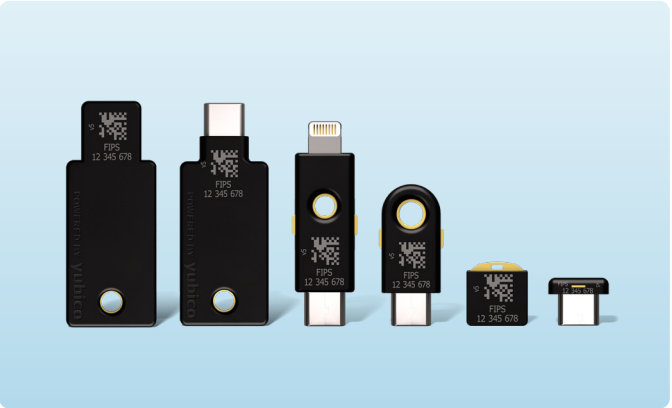
Capability Statement

Core Competencies

Yubico assists the federal government in its mission to deploy strong cybersecurity by providing highest-assurance multi-factor and passwordless authentication with the YubiKey, a FIPS 140-2 validated hardware security key that is an alternative to Personal Identity Verification (PIV) and Common Access Card (CAC). YubiKeys offer phishing-resistant MFA to meet the highest Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B guidelines.

Why is YubiKey the right solution?

- 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
- National Security Agency (NSA) Cybersecurity Information Guidance, Selecting Secure Multi-factor Authentication Solutions, October 2022: YubiKey listed in MFA evaluation guidance as an AAL3 capable authenticator
- FIPS 140-2 validated: Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914)
- Meets Zero Trust and phishing-resistant multi-factor authentication (MFA) requirements as listed in May 12, 2021 U.S. White House Executive Order 14028 on Protecting the Nation's Cybersecurity and recommended in Jan 19, 2022 U.S. White House National Security Memorandum/NSM-8 on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems
- WebAuthn, FIDO, FIDO2, DFARS/NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) compliant
- Support for Defense Information Systems Agency (DISA) Purebred derived credentials for credentialing of YubiKey for BYOD/BYOAD mobile devices
- Usable with both GFE/personal laptops, desktops, smart phones and tablets
- Supported protocols: PIV/CAC, OTP, FIDO U2F, FIDO2/WebAuth
- Secure United States manufacturing and supply chain processes for trustworthy components and delivery
- Strongest authentication: Non PIV/CAC eligible and mission partners, BYOD/BYOAD & closed/air-gapped networks



The YubiKey 5 FIPS Series is the first FIPS validated FIDO2/WebAthn, multi-protocol authenticator. 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.

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

In a commissioned study conducted on behalf of Yubico, Forrester Consulting interviewed security leaders from five enterprises using YubiKeys and found that for the composite organization, YubiKeys slashed exposure to security breaches from phishing and credential thefts by 99.9%. Further, YubiKeys reduced administrative overhead while providing a flexible, dependable user experience.

Past Performance

U.S. Government: Widely deployed in the U.S. Government with over 150 unique implementations

- FIPS 140-2 validated: Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914).

Industry: Many of the world's largest technology companies and financial institutions use YubiKeys.

- Google reduced account takeovers to zero with YubiKeys, used by over 114,000 employees
- 4 of the top 10 U.S. banks use YubiKeys. The nation's fifth-largest consumer bank expanded YubiKeys from mobile-restricted call centers to over 100,000 employees
- Facebook eliminated targeted attacks and expanded YubiKeys from engineering to over 50,000 employees
- One of the largest US insurance firms deployed YubiKeys to 155,000 employees for two-factor authentication today, and passwordless tomorrow

Technology Partners: Yubico works closely with technology partners to fuel growth, innovation and results that deliver strong authentication solutions and standards for our mutual customers:

Microsoft okta PingIdentity aws Google

Differentiators

- Multiple authentication protocols on a single key—PIV/CAC, OTP, FIDO U2F, FIDO2/WebAuthn
- FIPS 140-2 validated strong PIV/CAC alternative with a low total cost of ownership. YubiKeys are easier to deploy especially for remote workers—Yubico works with Sebastian Tech Solutions (STS) for secure logistics/shipping of YubiKeys directly to employees
- Unlike managing multiple certificates across mobile devices and PIV/CAC cards, a YubiKey can be used as a portable root of trust across multiple devices including mobile and BYOD/BYOAD, minimizing CapEx and OpEx costs
- Unlike mobile-based authenticators, YubiKeys are purpose-built for security and don't require Government Furnished Equipment (GFE) or a network connection. Phishing and malware resistant, waterproof, crush-resistant, and dustproof
- Unlike smart cards, YubiKeys offer anonymity with no visible amplifying personal information when in use

Getting Started

- Bailment agreement can be established to obtain Not for Resale (NFR) YubiKeys for proof of concept (POC) programs. Yubico 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 agencies easily access security products and services in a flexible and cost-effective way to heighten security:
  - 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, easy form factor selection, backup key discounts, and replacement stock benefits
  - With YubiEnterprise Delivery, agencies 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
  - Yubico's Professional Services team provides agencies with best-in-class technical and operational guidance in support of your YubiKey implementation and roll out including deployment planning, integration services and technical engagements

Company Information

Yubico puts an end to account takeovers for businesses, governments and individuals. The YubiKe—the world's #1 hardware security key is the most secure, easy-to-use, and affordable multi-factor authentication, and works with hundreds of applications and services including leading identity access management solutions such as Microsoft, Okta, Ping, and Duo.

YubiKeys are available for procurement through multiple convenient channels:

- Address: Yubico Inc. 5201 Great America Pkwy #122, Santa Clara, CA 95054
  - Phone: 844-205-6787 (toll free), 650-285-0088
- Purchase via GSA or SEWP V contract
- Carahsoft Technology Corporation = GSA Multiple Award Schedule Contract # 47QSWA18D008F
- Immix = GSA Contract # GS-35F-0511T / SEWP V NNG15SC16B (Category A, Group A) & NNG15SC39B (Category B, Group D
- DUNS: 046832835, CAGE Code: 6UUE2, NAICS Code: 423430

Contact us
yubi.co/contact

Learn more
yubi.co/federal

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.