yubico

YubiKey 5 FIPS Series
Phishing-resistant MFA and compliance for the Public Sector

Digital transformation raises data breach risks

Digital transformation is a challenge for any organization, but for government entities the complications are increased and the stakes are even higher. Numerous regulations need to be met and government employees are especially likely to be targets of cyber-attacks by hackers, hacktivists, and nation states.

YubiKeys offer federal compliant, highest assurance multi-factor authentication

YubiKeys offer phishing-resistant MFA and are FIPS 140-2 validated to meet the highest authentication assurance level 3 requirements (AAL3) of NIST SP800-63B guidelines (Certificate #3914). YubiKeys are also FIDO2/WebAuthn, FIDO U2F and DFARS/NIST SP 800-171 compliant, and are approved for use in DOD Non-Classified and Secret Classified Environments.

YubiKeys have been proven to offer the highest levels of security against account takeovers in independent research, preventing targeted attacks.

Account takeover rates

0[%] — Security key (YubiKey)

10[%] — On-device prompt

24[%] — SMS code

21[%] — Secondary email

50[%] — Phone number

Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

Strong hardware-based security

The YubiKey is a hardware-based solution that:

- Meets phishing-resistant MFA requirements in May 12, 2021 White House Executive Order 14028 and Jan 26, 2022 Office of Management and Budget (OMB) Memo M-22-09.

- Offers multiple authentication and cryptographic protocols including FIDO2/WebAuthn, FIDO U2F, Personal Identity Verification-compatible (PIV) Smart Card, OpenPGP, and Yubico One-Time Password (OTP) to secure legacy and modern applications and systems

- Provides DOD-approved, phishing-resistant authentication for remote and hybrid workers, non PIV/CAC eligible workers, mobile device users, citizen services, isolated/closed networks, and cloud services with a single tap or touch to authenticate.

- Is FIPS 140-2 validated (Certificate #3914), and accommodates derived PIV/CAC requirements

- Provides the option to modernize smart card deployments for future FIDO2/WebAuthn needs, and works across major operating systems including Microsoft Windows, macOS, Android, and Linux, as well as leading browsers

Government agencies can use YubiKeys to:

- Ensure strong security for non PIV/non CAC eligible users

- Deploy highest assurance authentication for mobile derived PIV and BYOD/BYOAD

- Modernize authentication for privileged users

- Secure user access to closed/air gap networks

- Deploy fast, one-touch authentication for first responders

- Secure sensitive information across government elections and political campaigns

---

The YubiKey 5 FIPS Series

From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS

YubiKey: Proven, easy-to-use security that's trusted by the world's leading companies
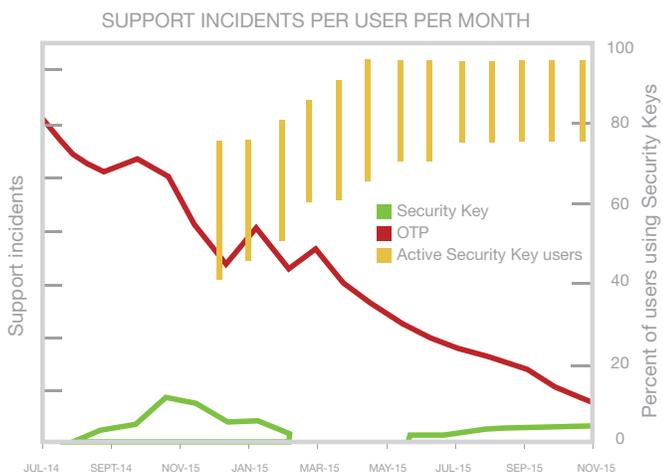
Phishing resistance for highest-assurance multi-factor authentication

The YubiKey stores the authentication secret on a secure element hardware chip. This secret is never transmitted and therefore cannot be copied or stolen.

Reduces IT costs

The YubiKey dramatically reduces the number one IT support cost—password resets—which cost Microsoft over $12M per month.[1]

By switching from mobile OTPs to YubiKeys, Google reduced password support incidents by 92% because YubiKeys are more reliable, faster, and easier to use.

SUPPORT INCIDENTS PER USER PER MONTH

Legend:
- Security Key
- OTP
- Active Security Key users

X-axis: JUL-14, SEPT-14, NOV-15, JAN-15, MAR-15, MAY-15, JUL-15, SEP-15, NOV-15

Y-axis (left): Support incidents

Y-axis (right): Percent of users using Security Keys (0, 20, 40, 60, 80, 100)

This graph illustrates how quickly Google reduced password support incidents after switching from OTP to YubiKey.[2]

Differentiators

Unlike managing multiple certificates across mobile devices and PIV/CAC cards, a YubiKey with one certificate can be used as a portable root of trust across multiple devices including mobile and BYOD/BYOAD.
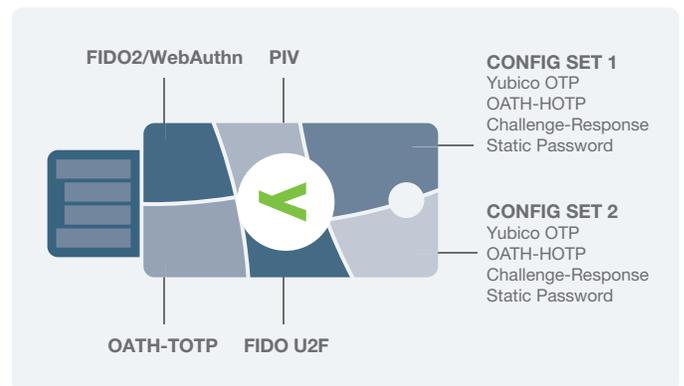
- Unlike mobile-based authenticators, YubiKeys are purpose-built for security and don't require Government Furnished Equipment (GFE) or a network connection. YubiKeys are also phishing and malware resistant, waterproof, crush-resistant, and dustproof.

[4] "Saying Goodbye to Passwords," Alex Simons, Manini Roy, Microsoft Ignite 2017
[5] Google Research, Security Keys: Practical Cryptographic Second Factors for the Modern Web

Easy to deploy

IT can deploy YubiKeys in days, not months. A single key can access several modern and legacy systems, which eliminates the need for separate keys or extra integration work.

FIDO2/WebAuthn PIV

CONFIG SET 1
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password

CONFIG SET 2
Yubico OTP
OATH-HOTP
Challenge-Response
Static Password

OATH-TOTP FIDO U2F

YubiKey 5 FIPS Series offers multi-protocol support. Technical specifications are available at yubico.com.

Trusted authentication leader

Yubico is a principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO Alliance and W3C, and is the first company to produce the U2F security key and a multi-protocol FIDO2/WebAuthn authenticator.

YubiKeys are produced in the USA, maintaining security and quality control over the entire manufacturing process.

Yubico SDK for iOS and Android:

Protect your organization with the FIPS 140-2 Overall Levels 1 and 2, Physical Security Level 3 validated version of the industry leading YubiKey multi-factor authentication solution. The YubiKey 5 FIPS Series enables government agencies and regulated industries to meet the highest authenticator assurance level 3 (AAL3) requirements from the new NIST SP800-63B guidance.