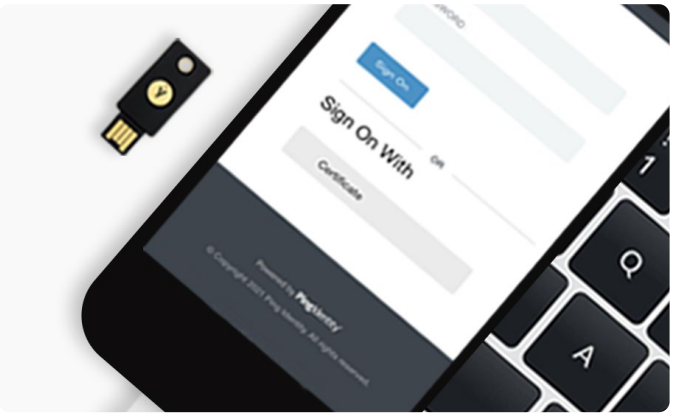
PingIdentity | yubico



Strong phishing-resistant MFA for EO 14028 compliance

Executive Order (EO) 14028 and OMB memo M-22-09 shift the cybersecurity principles for federal agencies, their staff, contractors, and partners from perimeter-based defenses to a Zero Trust architecture strategy that includes the requirement for phishing-resistant MFA.

Phishing-resistant MFA refers to an authentication process that is virtually immune to sophisticated attacks that could intercept or trick users into revealing access information. Phishing-resistant MFA establishes an authenticated protected channel with the verifier, protecting against verifier impersonation attacks through impostor websites or fraudulent push authorization attempts.

As defined by the Federal Information Processing Standards (FIPS) 140-2 and NIST SP 800-63B, only two authentication technologies currently meet this requirement: the federal government's Personal Identity Verification (PIV) standard/ smart card and the modern FIDO2/WebAuthn standard.

According to this guidance, agencies and their supply chain partners must move beyond authentication methods that fail to resist phishing, including passwords, as well as those that rely on SMS or voice calls, one-time codes, or mobile push notifications.

61% of data breaches are traced to credentials[1]

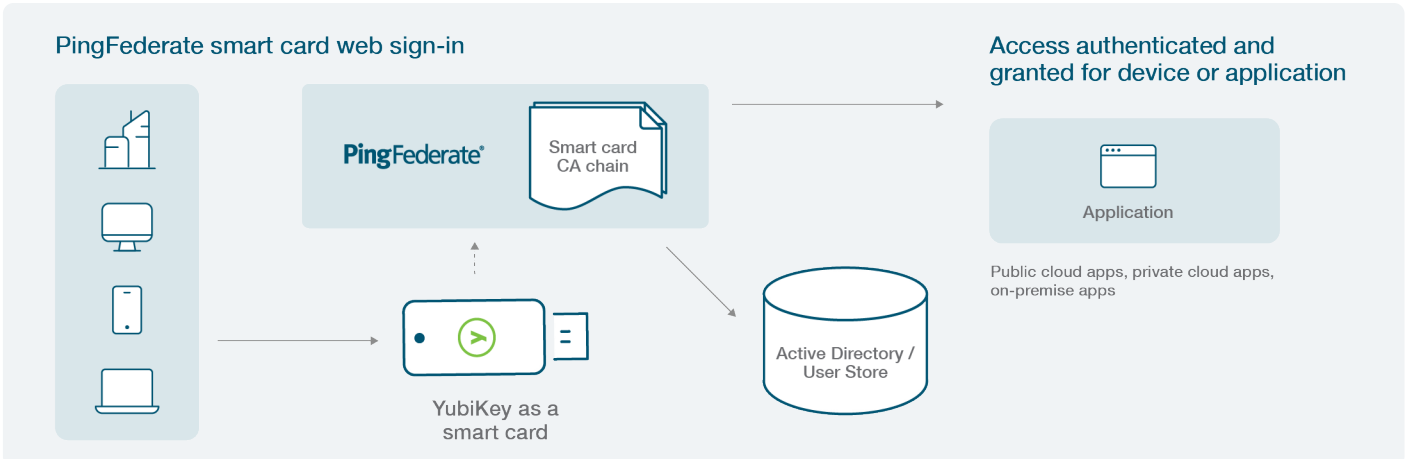
Achieve federal compliance with YubiKeys and Ping Identity

Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key proven to stop 100% of account takeovers in independent research. Ping Identity users, leveraging PingFederate, can take advantage of native support for the YubiKey for immediate compliance with the authentication requirements of OMB M-22-09 in a Zero Trust framework:

- FIPS 140-2 validated (overall level 1 and level 2, physical security level 3)
- Validated to NIST SP 800-63-3 Authenticator Assurance Level (AAL) 3 requirements

With Ping Identity and the YubiKey, government agencies can deploy federally validated, hardware-backed MFA across multiple applications and operating systems, as well as modern devices, with single-sign-on (SSO) capabilities. With certificate-based authentication, a user can leverage the YubiKey as a smart card with PingFederate to access web applications like Office 365. Yubico, Ping Identity, and EntryPoint have also teamed up to offer a solution to enable phishing-resistant Derived FIDO2 Credentials along with identity proofing and centralized identity management.

The easy and highly-secure solution has been tested and proven in the most security conscious government and enterprise environments. Global organizations such as PayPal, Geisinger Medical Center, and Capital One trust Ping Identity and YubiKey to protect their users.



[1] Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021)

Stronger together

Yubico and Ping Identity together offer the best of both worlds—modern, phishing-resistant MFA to protect against account takeovers, as well as a simplified user experience. YubiKeys are also durable, don't require batteries or need a cellular connection, and are water-resistant and crush-proof. Here are some additional benefits to using YubiKeys with PingFederate together:

Enhance security posture with streamlined deployment

PingFederate and the YubiKey add strong authentication to identity platforms to bring a complete, easy-to-scale offering to organizations of all sizes, supported by YubiEnterprise subscription and delivery options.

Secure privileged users, mobile-restricted environments

Improve security and productivity for privileged users or those sharing workstations and provide support for remote workers, contractors, air-gapped/isolated networks, cloud services, high-risk military scenarios, and mobile-restricted environments.

Superior authentication

Ping Identity works with YubiKey 5 FIPS Series, certified FIPS 140-2 validated security keys that meet the highest level of authenticator assurance (AAL3) of NIST SP800-63B guidelines.

Attestation support

Yubico and Ping Identity work together with EntryPoint's credential management system and identity binding to provide an off-the-shelf no-code solution that confirms Derived FIDO2 Credentials consistent with NIST SP 800-157 and 800-79-2.

Convenient login for higher employee productivity

Organizations can enhance security and simplify logins with PingFederate's consistent SSO experience and the YubiKey authentication, reducing support calls and downtime.

Adaptive and risk-based authentication

Administrators can define advanced authentication, pairing and device posture policies to trigger intelligent step-up MFA or to accept trust within geo-fenced or other defined scenarios.

Supply chain and customer access

Provide federated support to partners, 3rd party entities and even customers to prevent breaches.

Enable the bridge to passwordless authentication

Yubico and Ping Identity with EntryPoint work together to meet organizations where they are on their journey to passwordless, seamlessly supporting legacy infrastructures with multi-protocol flexibility as well as modern, cloud-based systems that leverage the latest FIDO2/WebAuthn standards.

Does the EO impact you?

While the Executive Order mandates requirements for federal agencies, it reaches far beyond. It has critical implications for many regulated and private sector industries such as defense, supply chain, healthcare, technology, and financial services.

Talk to us

www.yubico.com/contact-us

Learn more

yubi.co/eo-hub

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088