Microsoft | 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 immune to sophisticated attacks that could intercept or trick users into revealing access information. 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%

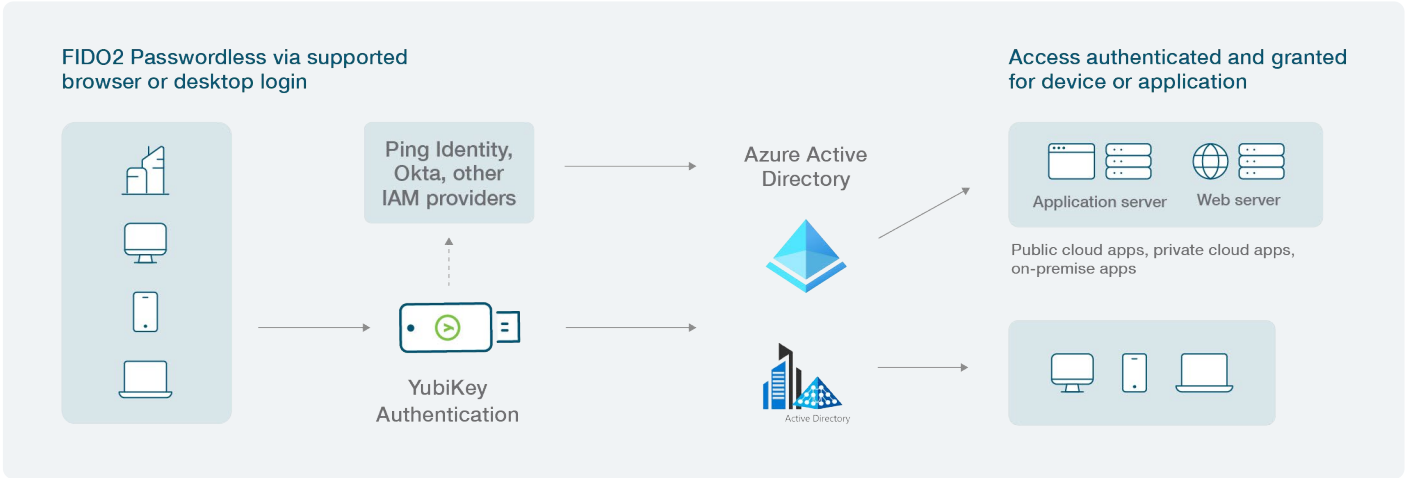
of data breaches are traced to credentials[1]

Achieve federal compliance with YubiKeys and Microsoft

Both Yubico and Microsoft are FIDO Alliance members and leading contributors to the FIDO2/WebAuthn authentication standards that meet the technical requirements for EO 14028. Yubico offers the YubiKey—a FIPS 140-2 validated hardware security key proven to stop 100% of account takeovers in independent research. Microsoft users, either Azure, Azure Active Directory (Azure AD), or Microsoft 365, 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 Microsoft and the YubiKey, government agencies can simply deploy federally validated, hardware-backed MFA across multiple applications and operating systems, as well as modern devices, with single-sign-on (SSO) capabilities. The easy and highly-secure solution has been tested and proven in the most security conscious government and enterprise environments. With certificate-based authentication, a user can leverage the YubiKey as a smart card with AD/FS to access Azure directly without the need for a 3rd party Identity and Access Management (IAM) product such as Ping Identity or Okta.



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

Stronger together

YubiKeys 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 for your Microsoft applications:

Enable the bridge to passwordless authentication

Government agencies can deploy a smart card/PIV passwordless solution today without the need for smart card readers—and get ready for a FIDO2/WebAuthn passwordless experience in the future.

Enhanced security posture with streamlined deployment

Deploying the YubiKey is a fast, simple, and inexpensive process thanks to seamless compatibility with existing infrastructures and YubiEnterprise subscription and delivery options.

Secure access to Microsoft apps

Microsoft 365 collaboration and productivity tools with Azure AD or AD FS are secured with the YubiKey solution that exceeds compliance requirements.

Convenient login for higher employee productivity

Organization can enhance security and simplify logins, reducing support calls and downtime.

Privileged users, remote workforce, and shared workstations

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

Multi-protocol flexibility

Microsoft works with the multi-protocol YubiKey 5 FIPS Series, ensuring a single solution across legacy and modern applications and devices. Authentication protocols include FIDO2/WebAuthn and certificate-based authentication.

Integrated with leading IAM solutions

YubiKeys secure authentication to Microsoft Office applications that are federated via IAM solutions such as Ping Identity, Okta, Duo, and more.

Third party/vendor access

YubiKeys can secure corporate system access to Microsoft 365 workloads by 3rd party entities to prevent breaches.

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