Transform Zero Trust from a CISO-only journey to an organization-wide priority

Accelerate your strategy with phishing-resistant MFA

U.S. federal agencies are required to meet specific Zero Trust goals by the end of fiscal year 2024[1], and the private sector which serves government agencies is inevitably impacted and challenged with raising the bar for security as well—which gives CISOs a prime opportunity to be the accelerator.

A Zero Trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be verified and authenticated before access is granted.

yubico

CISOs have a duty to make Zero Trust an organization-wide priority, especially since the path to it varies so greatly from one enterprise to the next:

"With every user having a YubiKey, I don't have to worry about leakage of credentials. That's a very, very good place to be as a CISO."

Brent Deterding
AFNI CISO
Yubi.co/Afni

36% of CISOs have started their journey to Zero Trust (Source)

25% of IT leaders who have either partially or fully implemented Zero Trust struggle to get the internal buy-in needed to scale it across the organization (Source)

83% of cybersecurity leaders are not "extremely confident" in their ability to implement Zero Trust (Source)

10% of large enterprises are expected to have a mature and measurable Zero Trust program in place by 2026 (Source)

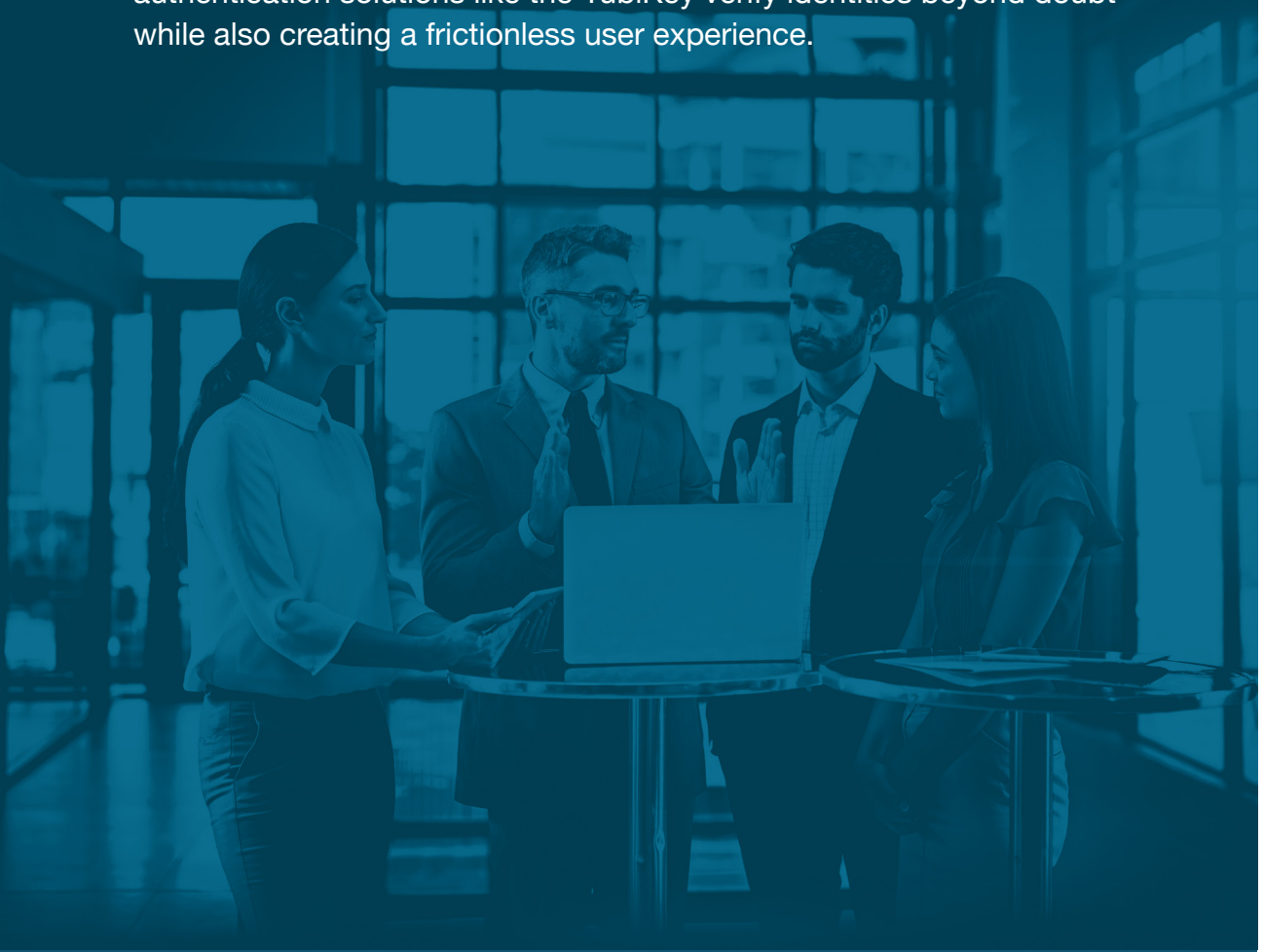
65% of cybersecurity leaders are prioritizing multifactor authentication (MFA) as they implement a Zero Trust framework (Source)

82% of cyber attacks can be traced back to the human element, including stolen credentials and phishing (Source)

yubico

Every CISO's Zero Trust strategy should start with phishing-resistant MFA

Multi-factor authentication (MFA) is a critical factor for Zero Trust success, **but not all forms of MFA are created equal**. As part of long-and intermediate-term plans to apply Zero Trust principles, CISA encourages all organizations to implement phishing-resistant MFA. Hardware-based authentication solutions like the YubiKey verify identities beyond doubt while also creating a frictionless user experience.



Modern hardware-based phishing-resistant MFA, like the YubiKey:

- Provides passwordless authentication
- Reduces risk of credential theft by 99.9%[2] and stops account takeovers
- Deploy the most secure passkey strategy: device-bound that is Authenticator Assurance Level 3 (AAL3) compliant.

Legacy mobile-based MFA (SMS, one-time passwords, push authenticators)**:**

- Uses one-time passwords sent via SMS messages
- Creates MFA fatigue by forcing users to re-authenticate at random intervals account takeovers
- Unusable in mobile-restricted environments and dependent on network and battery

Start forging your own path to Zero Trust with six deployment best practices to accelerate the adoption of modern, phishing-resistant MFA at scale. It's all in our guide How to get started with phishing-resistant MFA for Zero Trust.

1. Office of Management and Budget (OMB), M-22-09, (January 2022)
2. Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

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.

Contact us
yubi.co/contact-us

yubico