yubico

Accelerate your Zero Trust strategy with modern phishing-resistant MFA

What is Zero Trust?

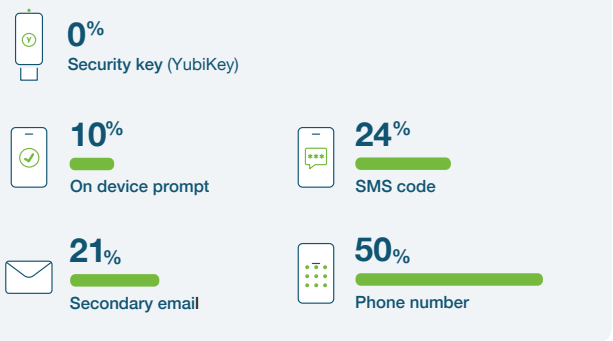
A Zero Trust framework implies that an organization should trust no individual or thing unless properly verified, before being given access to the network and data. Zero Trust means you can trust no one and no thing—not the user, not the computer, and not the communication.

Authentication is a core component of Zero Trust

In a Zero Trust approach, mitigating known vulnerabilities that expose sensitive data is critical. Given that user access is a fundamental risk to protecting sensitive data, it is critical that a Zero Trust framework should include strong authentication measures, to ensure a strong level of trust in the authentication mechanisms of every user. Adopting strong multi-factor authentication (MFA) as a core part of your Zero Trust strategy will jumpstart the security posture of your organization.

Authentication best practices to accelerate Zero Trust

- **Deploy phishing-resistant MFA:** Despite the growing tide and sophistication of cyber attacks based on credential compromise, many organizations continue to rely on legacy authentication such as usernames and passwords, and mobile-based authenticators. Usernames and passwords are easily hacked, and while any form of MFA offers better security than legacy username and password based authentication, not all forms of MFA are created equal. In fact, mobile-based MFA such as SMS, OTP, and push notifications are highly susceptible to phishing attacks, man-in-the-middle (MiTM) attacks, malware, SIM swapping, and account takeovers. According to NIST, only two authentication protocols are currently considered to be phishing resistant: Smart Card and FIDO2.



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

> "The YubiKey complements our Zero Trust architecture and helps get us closer to Zero Trust."
>
> **Morey J. Haber** | Chief Security Officer, BeyondTrust

BeyondTrust

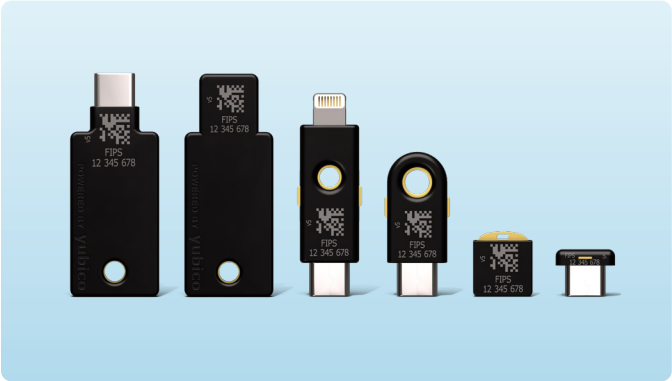
- **Ensure attestation is factored into Zero Trust:** In a Zero Trust model, you cannot have implicit trust in the authenticator. Strong authentication is very important but you still need to validate the hardware device itself, to ensure that it is coming from a known source and that it is not compromised. Attestation enables validation that the authenticator hardware is from a trusted manufacturer and the credentials generated on the device have not been cloned.
- **Establish strong authentication for all access points:** Most organizations use Identity and Access Management (IAM) platforms as core components of their Zero Trust framework. These solutions can grant access rights, provide single sign-on (SSO) from any device, enhance security with MFA, enable user lifecycle management, protect privileged accounts, and more. When considering MFA, it is a prudent architectural approach to decouple the authenticator from the IAM platform. This allows for an authenticator that can work with a wide array of IAM solutions.

- **Introduce strong authentication for non-user accounts:** Similar to user accounts, accounts that are used to run services are also vulnerable to compromise. Service accounts need to be heavily protected, monitored, and properly scoped as well. Too often these types of accounts have been protected with static passwords which can be easily hacked. It is imperative to deploy phishing-resistant MFA for these types of accounts.
- **Sign to prove it is a verified user over time:** Strong authentication is critical to a Zero Trust approach but it is also important to know that an authenticated person did the work, and it is possible for the work to be attested to over time.

- **Implement risk-based authentication:** A Zero Trust framework involves implementing real time risk-based access policies based on signals and risk scores. A trusted strong authentication approach allows for step-up authentication based on risk, protecting the user and the organization while increasing productivity.
- **Plan for a passwordless future:** Passwords are a burden—they don't offer good security or even good user experience, and while modern, phishing-resistant MFA is a good step toward Zero Trust, eliminating passwords should be the end goal. Organizations can choose between smart card passwordless, FIDO2/WebAuthn passwordless or a hybrid passwordless approach depending on business scenarios and infrastructure elements. For organizations looking to go passwordless with FIDO2/passkey-based strategy, security keys that contain hardware-bound passkeys offer the highest security assurance with a frictionless experience for users.

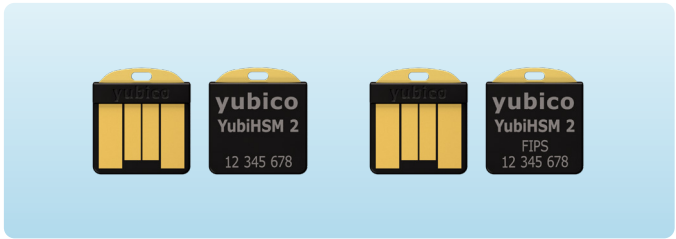
Yubico's YubiKey and YubiHSM create a strong baseline of trust in a Zero Trust world

Yubico's phishing-resistant hardware security solution—the YubiKey, supports the 'Trust nothing, verify everything' Zero Trust approach with strong user identity and device authentication. YubiKeys are purpose-built for security and designed to stop phishing and other forms of account takeovers in their tracks, delivering strong authentication at great scale. Leveraging Smart Card/PIV and the modern FIDO2/WebAuthn authentication standards, YubiKeys work seamlessly across on-premises or cloud environments, do not rely on shared secrets between registered services, store no data and require no cellular connectivity. YubiKeys are also FIPS 140-2 validated to meet the most stringent Authenticator Assurance Level 3 (AAL3) requirements.



The YubiKey 5 FIPS Series–from left to right: YubiKey 5C NFC FIPS, YubiKey 5 NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS

The YubiHSM 2 is available as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution, and provides uncompromised cryptographic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.



The YubiHSM 2 and YubiHSM 2 FIPS

Contact us
yubi.co/contact

Learn more
yubi.co/zero-trust

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.