Securing federal systems integrators and the defense industrial base with modern authentication

Stay one step ahead with Zero Trust and phishing-resistant MFA

Cyber attacks are on the rise

While the federal government is making strides in mandating the use of phishing-resistant multi-factor authentication (MFA) across the executive branches, progress is unclear with federal system integrators (FSIs) and the Defense Industrial Base (DIB), which serve as an extension of the government. In fact, between 2015 and 2022, breaches against the DIB **more than doubled**.

Attacks to FSIs and DIBs can have large consequences

FSIs have access to critical systems and hold large volumes of sensitive and Controlled Unclassified Information (CUI), making them targets of sophisticated attacks that combine malware, phishing, and/or hacking. A major challenge for both government and FSIs is that integrators may not have the same level of security as the agencies they serve—providing adversaries with an alternative attack point to compromise the integrity of products being delivered or the security and privacy of the data or code being exchanged.

79%

of DOD contractors lack comprehensive MFA (Source)

72%

of the top 100 defense contractors leaked at least one credential in a 90 day span (Source)

\$2.6 billion

The average cost of a public sector cyber attack in 2023, a 25% increase from 2022 (Source)

yubico

Not all MFA is created equal

Any MFA is better than a password, but not all MFA is created equal. Legacy authentication technologies—such as SMS, one-time passcodes (OTP), and push notification apps—remain highly susceptible to account takeovers from phishing, social engineering and attacker-in-the-middle incidents.

Hardware security keys such as the YubiKey are the only technology that offer phishing-resistant multi-factor and passwordless authentication at scale, helping organizations jump start their Zero Trust journey. Below are the benefits of the YubiKey:

AAL3

FIPS 140-2 validated and CMMC compliant: Meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B (Certificate #3914)

99%

Reduces risk by 99.9% and stops account takeovers with strongest phishing resistance

fido™

Bridge to modern FIDO **passwordless authentication**

Portable root of trust with multiple authentication protocols on a single key: PIV/CAC, FIDO U2F, FIDO2/WebAuthn, OTP, OpenPGP

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.

Yubico also offers the YubiHSM 2 FIPS that offers low cost hardware cryptographic security for servers, applications and computing devices in an innovative ‘nano’ form-factor that allows flexible deployment. The YubiHSM 2 FIPS can be applied to any process where secrets and the authenticity of components needs to be managed. It can be easily deployed to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices.

yubico

WHITE PAPER

Protecting Federal Systems Integrators against modern cyber threats with highest-assurance security

Win more contracts, stop account takeovers, and meet CMMC and FedRAMP requirements with phishing-resistant MFA

Discover how to meet these mandates and address emerging use cases in our whitepaper, Protecting Federal Systems Integrators against modern cyber threats with highest-assurance security.

Contact us
yubi.co/contact

Learn more
yubi.co/fsi

yubico