Protecting the supply chain with modern security

Phishing-resistant authentication for users, servers, and machines

Cyberattacks and a shifting regulatory environment

Organizations are facing an unprecedented level of disruption to supply chains, from the global pandemic and the economic recession, to port disruptions and record high freight costs. Hackers now specifically target third-party systems, software, code or IP. In fact, up to 97% of organizations have had a cybersecurity breach as the result of a weakness in the supply chain.[1] Disruptions to the supply chain can compromise the integrity of the products or services being delivered or the security and privacy of the data or code being exchanged which can lead to delays in business operations and reduced bottom lines across all industries.

In response to increased threats to the supply chain and critical infrastructure sectors, the White House Executive Order (EO) 14028 and Office of Management and Budget (OMB) Memo M-22-09 introduced new expectations and guidelines for Zero Trust and phishing-resistant multi-factor authentication (MFA) for federal agencies and enterprises—as well as their suppliers and partners.[2]

Organizations can begin their journey to reducing risk across the supply chain at all levels, by identifying and mitigating risk in three key areas:

Key areas to identify and mitigate risk

- Third-party access
- IP and product integrity
- Software supply chain

Securing supply chain access with modern, phishing-resistant MFA

Organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain. One of the top recommendations in the updated NIST 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations, is to employ multi-factor authentication to safeguard remote and third-party access to the network.[3] However, not all MFA is created equal, nor is all MFA considered phishing-resistant. OMB M-22-09 defines phishing-resistant MFA as an authentication process that is immune to attackers intercepting or even tricking users into revealing access information.

Phishing-resistant MFA

- Federal Government's Personal Identity Verification (PIV) standard
- FIDO2/WebAuthn

Not phishing-resistant MFA

- Passwords
- Security questions
- SMS and other one-time passwords (OTP)
- Mobile push apps

The YubiKey from Yubico provides phishing-resistant multi-factor and passwordless authentication at scale across the supply chain, helping organizations and their suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical IP handoffs.

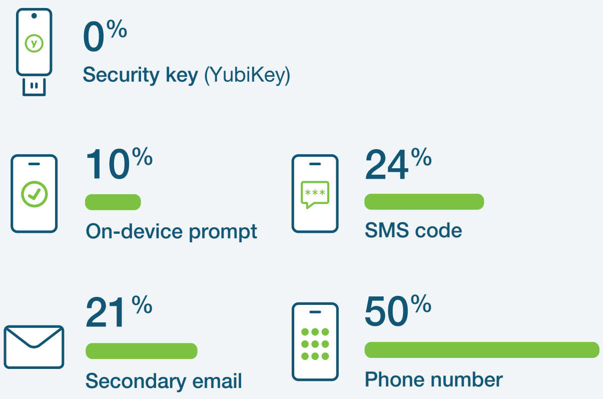
[1] BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021

[2] The White House, Executive order on Improving the Nation's Cybersecurity, (May 12, 2021)

[3] NIST, NIST SP 800-161 Rev. 1

The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.[4] Further, the YubiKey offers an unparalleled user experience, a tap-and-go passwordless experience that is 4x faster than SMS and offers a 92% reduction in support calls. YubiKeys are also available in FIPS 140-2 validated form factors.

Risk of account takeovers



Securing supply chain integrity

One of the risks inherent in supply chain security is the possibility of compromise to the integrity, quality, or reliability of the product, software or service being delivered. It is crucial to ensure that all components involved in an end-to-end process are authentic, to avoid unsolicited replication and theft, but also for quality assurance, since a manufacturing assembly line should only consist of genuinely sourced products. Further, it is crucial to ensure the integrity of the software supply chain, to ensure that any code, software, frameworks or libraries from external sources is subject to secure code-signing and is protected from unauthorized access and tampering.

The traditional approach to ensuring the integrity of IP, to prevent counterfeiting and to safeguard code signing involves the use of cryptographic signing keys and encryption, stored either in software—highly vulnerable to attack—or a hardware security module (HSM).

Safeguarding product integrity, IP and code management with YubiHSM2

Yubico created the ultra-portable and low-cost YubiHSM 2, the world's smallest HSM that comes in a nano form factor. The YubiHSM 2 enables secure, tamper-resistant key storage and operations, by preventing the copying and distribution of cryptographic keys, and preventing remote theft of keys stored in software. The YubiHSM 2 can be applied to any process where secrets and the authenticity of components needs to be managed, where tampering needs to be prevented, or to protect PKI infrastructure and its network of cryptographic keys.

The YubiHSM 2 is ideally suited to safeguard the signing keys and certificates for both signing code and creating digital signatures, helping support the secrets being shared within the supply chain. For organizations that need to meet the FIPS 140-2 requirements, there is also the option of the FIPS 140-2, Level 3 validated YubiHSM 2 FIPS to ensure the highest levels of data protection in addition to strict levels of compliance.

[4] Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019)

The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

The YubiHSM 2 and YubiHSM 2 FIPS

From left to right: YubiHSM 2 and YubiHSM 2 FIPS

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

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