

# Protect manufacturers from modern cyber threats

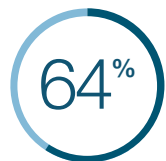
Safeguard your production and profits with reliable and robust MFA and hardware-backed security

## Cyber attacks are on the rise

Manufacturers are integral to society such that they create products and services we rely on, strengthen infrastructure, and provide technological advancements. Remote access, smart technology and the Industrial Internet of Things (IIoT) introduce new cybersecurity vulnerabilities in an industry already ripe with compromised credentials from phishing that lead to more widespread attacks like ransomware. Since information technology (IT) and operational technology (OT) are increasingly intertwined, cyber attacks can cause production outages, equipment damage, lost revenue and further impact end consumers.



of all cyber attacks in 2023 were carried out against manufacturers<sup>1</sup>



of manufacturing cyber attacks caused by compromised credentials, malicious emails, or phishing<sup>2</sup>



of manufacturers lost business-critical data/IP due to cyber attack<sup>3</sup>



of OT intrusions caused outages that affected productivity<sup>4</sup>

## A true Zero Trust approach to mitigate risk

For manufacturers of all kinds it's critical that no user or device is allowed into your network unless explicitly verified. Multi-factor authentication (MFA) should be the first-line defense of any cybersecurity strategy for manufacturers of all kinds. While any MFA is better than a password, not all MFA is created equal.

Legacy MFA such as mobile-based (SMS codes, one-time passcodes, push notifications) is susceptible to phishing, attacker-in-the-middle attacks and fails altogether in mobile-restricted or low connectivity areas.

Manufacturers need modern MFA that protects existing infrastructure while enabling the move to stronger phishing-resistant methods such as Smart Card/PIV and FIDO—both of which protect across industrial environments, factory floors, corporate offices and beyond.



high-tech  
silicon & semi-  
conductor



retail



machinery



medical



energy



transportation  
aerospace &  
automotive

<sup>1</sup> IBM, X-Force Threat Intelligence Index 2024, (February 2024)

<sup>2</sup> Sophos, The State of Ransomware in Manufacturing and Production 2024 (May 2024)

<sup>3</sup> Fortinet, 2024 State of Operational Technology and Cybersecurity Report, (June 2024)

<sup>4</sup> Ibid.

# Accelerate Zero Trust, build cyber resilience, and protect your supply chain with Yubico



“By leveraging the YubiKey and the YubiHSM, a small form factor and powerful hardware security module, we increase the security of our supply chain at Schneider Electric.”



Chad Lloyd  
Director of Cybersecurity  
Architecture for Energy Management  
[Read our case study](#)  
[yubi.co/SchneiderElectric](https://yubi.co/SchneiderElectric)



“YubiKeys are fast, robust and best-in-class: a best-in-class device and best-in-class security. It’s very smooth, and saves time compared to the people who have to enter the TOTP because you need to type six numbers, for every account. It’s much faster just to touch a key.”



Ángel Uruñuela  
Chief Information Security Officer  
[Read our case study](#)  
[yubi.co/Fluidra](https://yubi.co/Fluidra)

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](https://www.yubico.com).

## Secure user access with the YubiKey

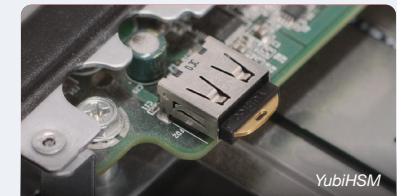
A modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication.

- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 203% ROI<sup>5</sup>
- Embrace multi-protocol support on a single key: Smart Card/PIV, FIDO U2F, FIDO2/WebAuthn (passkeys), OTP and OpenPGP
- Deploy the most secure passkey strategy: device-bound that is purpose-built for security and Authenticator Assurance Level 3 (AAL3) compliant
- Secure user access at scale on any device, to legacy and modern applications, shared workstations, IT and OT systems including industrial control systems (ICS) like SCADA
- Bridge to modern FIDO2 passwordless authentication
- Does not need battery or cellular connectivity to function

## Protect devices, servers and more with the YubiHSM

A hardware security module (HSM), that ensures enterprise-grade high cryptographic security and operations.

- Safeguard intellectual property, corporate secrets and secures manufacturing assembly lines
- Can be applied to any process where secrets and the authenticity of components needs to be managed
- Ultra-portable nano form factor allows for flexible deployment to any USB slot on servers, databases, robotic assembly lines, applications, and IoT devices



**Yubico has you covered.** IP68 certified and FIPS 140-2 validated solutions to protect any environment from industrial or corporate to highly regulated.

<sup>5</sup> Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)



Contact us  
[yubi.co/contact](https://yubi.co/contact)



Learn more  
[yubi.co/mfg-wp](https://yubi.co/mfg-wp)

**yubico**