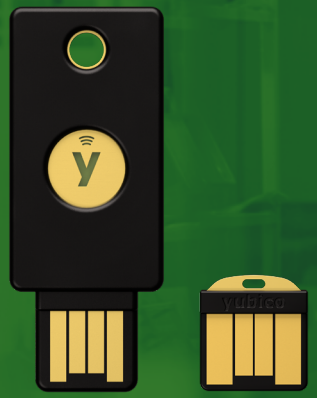

Build Cyber Resilience for Manufacturing in 2025

Manufacturing was once again the top attacked industry globally in 2024 for the fourth year in a row, representing 25.7% of incidents within the top 10 attacked industries.[1] Phishing, malware, and credential theft remain the most prevalent vectors for cyber attacks in manufacturing, increasing the urgency to address authentication risk. Cyber attacks threaten intellectual property (IP) and can lead to system downtime, equipment damage or risk to human life.

Here are our top recommendations:

Identify current authentication touchpoints

Not all forms of multi-factor authentication (MFA) are created equal in terms of usability or security and often may not be appropriate for mobile-restricted, heavy duty or gloved environments. Additionally legacy environments normally contain many disparate technologies. Evaluate your current users, devices, and environments (IT and OT) along with how they are interacting with your technology ecosystem. Some questions to consider:

- How do you make sure the user logging into the device is the legitimate person?
- How do you make sure the user is able to seamlessly authenticate across multiple devices and applications?
- How do you ensure consistent authentication that always works, even in tough environments with multiple points of failure?

[1] IBM Security, X-Force Threat Intelligence Index 2025

Pictured above from left to right: YubiKey 5 NFC and YubiHSM

yubico

Prioritize a cyber risk management strategy

Utilize and embrace industry guidance suggested by standards bodies (i.e. NIST 800-64, ISO/IEC 2700116 and ISA/IEC 6244317) and national requirements (e.g. ESF, NIS2) which provide guidelines to build a framework for security and authentication requirements for IT and OT systems. Evaluate authentication risk and prioritize mitigation opportunities to avoid, reduce or transfer risk toward the target state of eliminating authentication risk altogether.

With the YubiKey, a IP68 certified hardware security key–which contains the highest assurance passkeys–deploy phishing-resistant authentication and bridge to passwordless. The YubiKey's multi-protocol[2] capability and diverse form factor[3] support helps meet you where you are on your risk management journey, while driving productivity and compliance.

Protect your crown jewels: people, processes and IP

Attackers often start by targeting a user with relatively low access and then move laterally from there to disrupt systems and services. Avoid identity-based attack risk by deploying the highest phishing-resistant protection, such as the YubiKey, across your entire workforce, closing off initial entry points that could expose IP or could migrate to OT systems, and upholding the CIA triad (confidentiality, integrity, and availability for IT and AIC triad (availability, integrity, confidentiality for OT). When securing machine to machine authentication, leverage hardware-based secret stores with strong access control, like the YubiHSM, to prevent encryption and signing keys are not abused, and data at rest is protected.

[2] Supports a broad range of authentication protocols: FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart card/PIV, and enables you to bridge to passwordless.

[3] USB-A, USB-C, and lightning connectors, in addition to NFC support.

yubico

Secure IT and OT systems, including shared workstations

It's critical to protect access to IT and OT systems with phishing-resistant authentication where possible. The YubiKey is reliable and robust to secure your users wherever they work–corporate offices, factory floors, mobile restricted environments, out in-the-field or elsewhere. It is spark, crush, and water-resistant while also not relying on battery or network. YubiKeys provide a cost-efficient and effective way to secure access to shared workstations avoiding insecure practices, such as password sharing and also increases auditability.

Safeguard the supply chain

In this interconnected world, attacks and outages can have a cascading impact across the supply chain, to critical infrastructure sectors, or to downstream consumers.

Leverage the YubiKey to secure access for upstream supplies, vendors, contractors and service partners, ensuring that anyone who touches your systems takes advantage of the highest phishing-resistant protection available.

The YubiHSM provides another secure cryptographic solution to ensure component integrity as each part moves through the supply chain. Similar to a code signing evolution, the YubiHSM can be used to generate secure signatures in a produced component to prove integrity during shipping or at final assembly.

Combining the YubiKey for end-user authentication and the YubiHSM for product integrity and secure supply chain provides a complete secure solution for the manufacturing industry.

We Are Here For You

Yubico can partner with you to accelerate your Zero Trust approach, prioritize operational resilience, and build a cyber resilient authentication strategy.

Contact us
yubi.co/contact

Learn more
yubi.co/manufacturing

Yubico (Nasdaq 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 passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com

yubico