



Cyber risk management guide for authentication in manufacturing

How to identify, mitigate and future-proof authentication risk
with the multi-protocol YubiKey



Contents



Executive summary

While the value of digital transformation in the manufacturing sector is well-established, in addition to improving productivity, quality and agility, **70% of manufacturers agree that cybersecurity is one of the greatest risks.**¹ For three years, manufacturing has been the most attacked industry, representing **28% of global incidents** and **54% in Asia-Pacific** specifically.² If not managed, these cyber threats place intellectual property (IP) at risk and could lead to system downtime, equipment damage, or unwanted effects that could impact human lives.

Phishing, malware and credential theft remain the most prevalent vectors for cyber attacks in manufacturing, increasing the urgency to address authentication risk. In this guide, we will outline how to identify, assess, and prioritize risk mitigation strategies that respect the constraints of today while also creating a bridge to modern, phishing-resistant multi-factor authentication (MFA) and passwordless.

Cyber risk in manufacturing

Manufacturing is the #1 most attacked sector³



high-tech
silicon & semi-conductor



retail



machinery



medical



energy



transportation
aerospace & automotive

Threat actors don't hack in, they log in

Digital transformation has increased the attack surface, introducing more connected hardware (e.g. smart sensors) and greater connectivity between information technology (IT) and operational technology (OT) environments, eroding the protections of traditional air-gapped networks.



55%

of breaches employ phishing⁴



45%

of attacks employ malware⁵



35%

of breaches involve ransomware⁶



25%

of breaches involve stolen credentials⁷



22%

of attacks abuse remote services⁸



15%

of global cross-industry breaches involve a 3rd party creating supply chain issues⁹

Risks of unmanaged cyber threats

There is a wide range of cyber threats targeting the manufacturing sector. As a cybersecurity leader, or someone who cares about securing critical systems and data within manufacturing, it is important to weigh the risk of what unmanaged cyber threats can cause. The impact of a cyber attack can have far-reaching implications including but not limited to:



Downtime

In 2023, there was a 150% increase in OT cyber attacks with physical consequences, including production outages, equipment damage and the disabling of safety systems.¹⁰



Intellectual property (IP) theft

Exfiltration of IP can result in copycats that erode market position or result in financial losses.



Upstream & downstream impact

Attacks and outages can have a cascading impact across the supply chain, to critical infrastructure sectors, or to downstream consumers.



Reputation

Negative attention can impact stock price, undermine shareholder confidence, and impact future contracts.



Obstacles to modern authentication

To protect against cyber attacks, manufacturers need authentication solutions to help protect against risk. In order to overcome common obstacles, solutions need to meet manufacturers where they are on their journey to modern authentication.



Legacy systems

Across manufacturing, legacy OT and ICS systems may not support modern authentication, may rely on unsupported systems (25%) or have known vulnerabilities (78%).¹¹



Downtime intolerance

The cost of unplanned downtime in manufacturing is estimated at **\$50 billion** per year¹², increasing risk aversion related to technology integration and process change.



Fragmentation

There can be a cultural disconnect between enterprise and production environments as well as fragmented governance over IT and OT systems, limiting organization-wide efforts.¹³



Skills gap

As cybersecurity becomes more complex, skill shortages have emerged. Cybersecurity is the #1 skill manufacturers are seeking.¹⁴

Manufacturers need a strong authentication foundation—one that meets them where they are today and helps bridge to the smart factory of the future.



Risk management frameworks for manufacturing

Globally, industry associations continuously publish industry-sector guides for risk management and cybersecurity best practices. The National Institute for Standards and Technology (NIST), globally recognized for promoting equitable standards, has been continuously updating Risk Management Framework (RMF) and Cybersecurity Framework (CSF), including a specific guide for manufacturing.¹⁵ Further, the ISO/IEC 27001¹⁶ and ISA/IEC 62443¹⁷ standards provide a framework for security and authentication requirements for IT and OT systems.

Risk management strategies in authentication

While some manufacturing organizations selling to the government have been subject to strict regulations and standards, the urgent need to improve cyber defenses within manufacturers is being met by global regulators, across ISO standards and within industry associations.

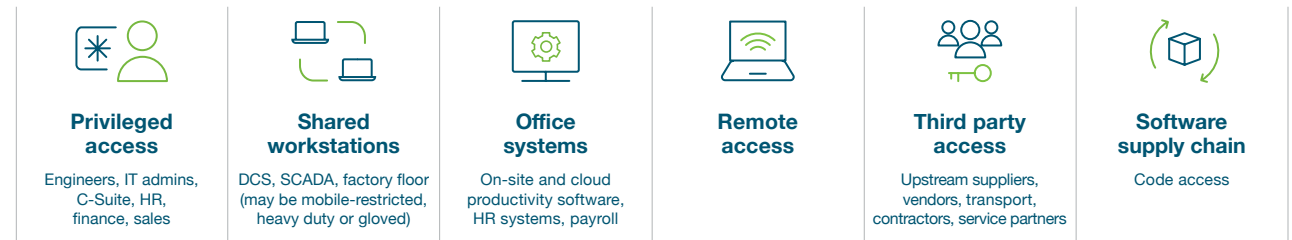
In some countries, manufacturers are categorized among critical infrastructure sectors, introducing regulatory requirements such as the National Security Memorandum/NSM-22 in the U.S.¹⁸ and the Cyber Resilience Act/CRA in the E.U.¹⁹ In other countries, federal bodies are closely collaborating with manufacturers to suggest best practices for cybersecurity and risk management, such as the Action Plan for Critical Infrastructure in Canada.²⁰

Although there are variations in guidance, all risk management frameworks consist of common practices to identify, assess, and mitigate risk, with a feedback loop to monitor and improve over time. The remainder of this guide will outline how to use risk management processes to identify and evaluate authentication risk and how to prioritize mitigation opportunities to avoid, reduce or transfer risk toward the target state of eliminating authentication risk altogether.



Step 1: Identify authentication risk

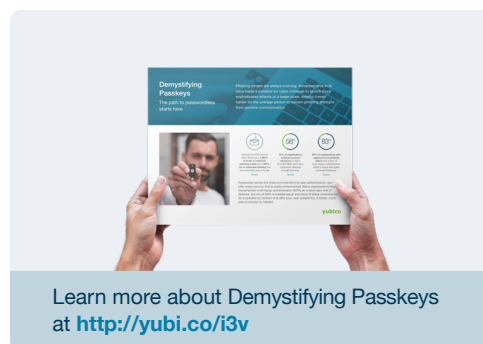
The first step in managing risk is to identify current authentication processes across users, devices, and environments (IT and OT), which for most manufacturers will include:






Historically, the manufacturing sector has relied on a mix of individual and shared passwords, one-time passcodes (OTP) and Personal Identity Verification (PIV) Smart Cards for most authentication scenarios across IT and OT systems. All users in the organization require access to core office systems (e.g. payroll), while only some users will have access to OT and ICS systems.

While historically shared passwords, TOTP tokens and PIV cards have satisfied authentication requirements within air-gapped networks, digital transformation has driven traditionally air-gapped systems online, opening the door to remote attacks. Air-gapped systems prevent remote access by being physically disconnected. Due to the workforce shortage, growth of IoT monitoring devices with automated feedback and the need to simplify workflows has caused the drop of traditional air-gapped philosophy. This leads to increased cyber risk. For example, Mitsubishi Electric recently announced a vulnerability that exposes its factory automation products to a risk of remote authentication bypass, if remote authentication is not replay-resistant.²¹





In order to properly assess risk, it is critical to recognize that while passwords offer the weakest protection against attacks, not all MFA is created equal. The strength of authenticators can be described with authentication assurance levels (AALs), standards used by NIST²², in Australia's Essential Eight Maturity Model (E8MM)²³ and the EU's electronic Identification, Authentication and Trust Services Regulation (eIDAS).²⁴

AAL1	AAL2	AAL3
Single-factor authentication e.g., username and password	Two-step authentication e.g., 2FA, synced passkeys, device-bound passkeys on general purpose devices	Hardware-based multi-factor authentication e.g., device-bound passkeys on hardware security keys
 <ul style="list-style-type: none"> • Low security assurance • Highly vulnerable to phishing • Puts enterprises at risk 	 <ul style="list-style-type: none"> • Phishing-resistant 2FA/MFA • Stronger security than a password but vulnerable to attacks • More enterprise-ready but leaves gaps in operational efficiency and audit/compliance requirements 	 <ul style="list-style-type: none"> • Phishing-resistant MFA • Strongest security and highest assurance • Addresses enterprise security, operational efficiency and audit/compliance requirements • Supports FIDO and Smart Card/PIV • FIPS 140-2 validated

In the next step, you can use this understanding of AALs to quantify risk across your authentication scenarios.

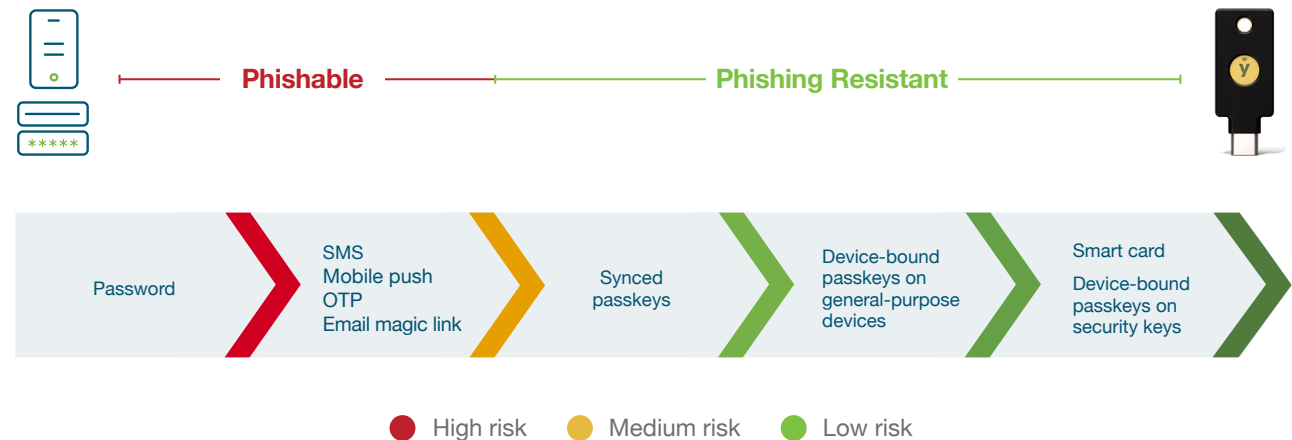
What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

- **Synced passkeys** live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.
- **Device-bound passkeys** offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security.

Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach, enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements.

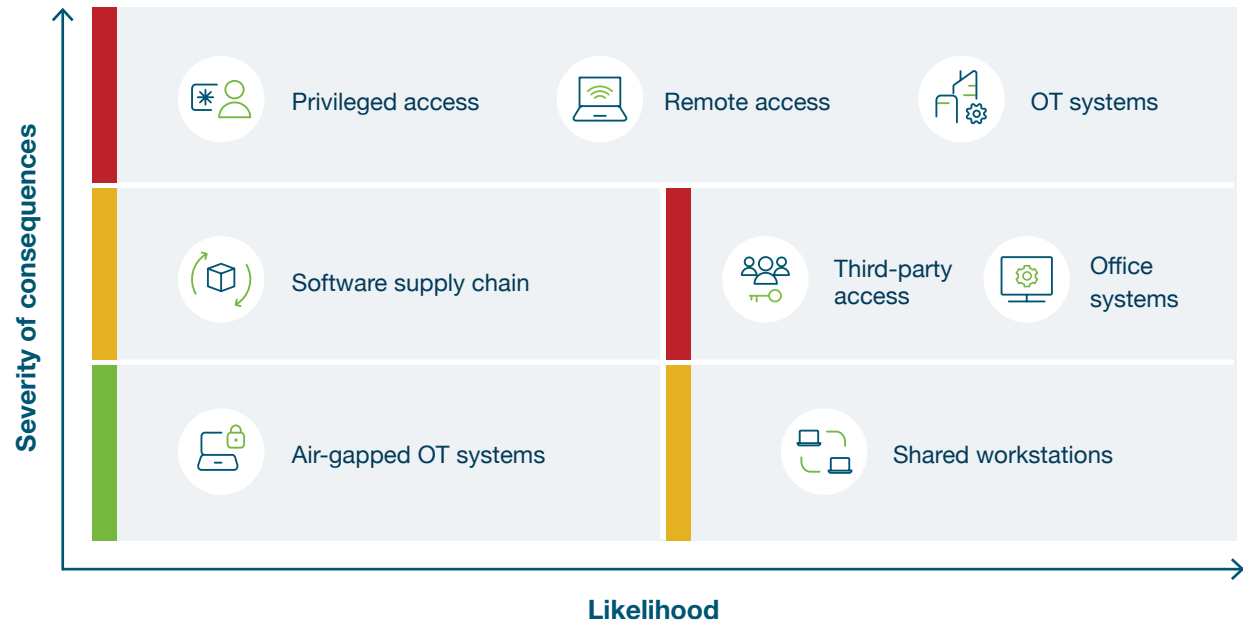
With reference to NIST's AAL guidance, any form of MFA will provide greater security than a password (AAL1), but an authenticator at AAL3 provides very high confidence that someone logging onto your system can prove, by possession, who they are claiming to be, reducing the threat of compromise and attack from phishing. According to NIST Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and FIDO2/WebAuthn (passkeys)²⁵, although passkeys can be further differentiated as synced (AAL2) or device-bound (AAL3).



Step 2: Assess authentication risk

There are many risk assessment methodologies, but generally speaking, you can quantify risk based on a combination of the likelihood of a risk (a combination of threat level and vulnerability) and the severity of consequences. In this stage, you will rank your IT and OT authentication use cases and user populations based on risk:

● High
Elevated access or risk of exposure is high. The consequences are severe or catastrophic, resulting in a major financial loss, physical harm, extended downtime, or loss of system capability
● Medium
Privilege is lower and/or the consequences are serious, but systems can be restored or repaired, financial losses are manageable, harm does not result in loss of life
● Low
The chance of compromise is low or there are limited adverse effects






For example, it is common to see a manufacturer create a matrix that looks something like the above.

In an ideal world, manufacturers would use this matrix as a guide to prioritize deployment of an authenticator at AAL3 to all “High” risk scenarios to provide the highest level protection against phishing attacks, with the gradual goal of also incorporating all “Medium” and “Low” scenarios. Unfortunately, manufacturers face technical constraints (e.g. legacy systems) that make it difficult or impossible to deploy an authenticator at AAL3.

In the next section, we will discuss risk mitigation strategies and how they line up with specific MFA implementations and strategies, and how to future-proof your risk management efforts with a single multi-protocol solution.

Step 3: Implement risk mitigation strategies

Manufacturers can approach identified risks with three primary strategies: Avoid, Reduce, Accept & Transfer.

Mitigation strategy and implementation details		
		
<p>Avoid</p> <p>Avoid risk by implementing device-bound passkeys on hardware security keys</p>	<p>Reduce</p> <p>Reduce the probability and impact of risk with synced passkeys and strong MFA practices</p>	<p>Accept & transfer</p> <p>Accept risks and the constraints that limit the use of controls, transfer risk to insurance</p>





Avoid

Avoid risk by implementing device-bound passkeys



Secure access to IT systems and applications

Privileged access, remote access, third-party access, office systems



At risk level “High,” you have the lowest tolerance for risk. The goal for these scenarios (e.g. privileged access) is to avoid identity-based attack risk by deploying the highest phishing-resistant protection available, closing off initial entry points that could expose IP or could migrate to OT systems.

With most IT systems and applications having wide support for FIDO authentication, the highest protection available is a device-bound passkey on modern FIDO hardware security keys. Device-bound passkeys are stored in dedicated hardware that have an AAL3 rating. Device-bound passkeys also support non-repudiation, binding specific users to sessions with a strong identity factor to know who logged into a device or application.

Since many attacks get into IT networks at lower levels, we recommend a phased deployment of device-bound passkeys that targets high value, high risk users first, then iterates across all “Medium” risk scenarios such as everyday workers (office and production floor) and third-party partners. Given the variability in technical knowledge, it is critical to choose an authentication solution that is easy to set up and use.



Eliminate risk with user presence

Shared workstations, OT and ICS systems (e.g. SCADA)

In the production environment, it is common to access shared workstations using shared accounts and shared passwords. Although passwords are inherently weak, you can reduce the threat of remote attack by using a device-bound passkey on modern hardware security keys. Unlike passwords or SMS codes, which can be intercepted, a device-bound passkey requires user presence to complete the login prompt. As mobile devices are often prohibited within production environments, device-bound passkeys on hardware security keys are the ideal solution.



Eliminate risk with MFA and a HSM

Software supply chain

The software supply chain creates a door into IT and OT environments, making it critical to reduce risk. CISA and the FBI recently prepared advice on how organizations can vet their software, including whether the software enables MFA or phishing-resistant forms of authentication such as passkeys by default.²⁶ To support secure code signing, manufacturers can additionally deploy a hardware security module (HSM) to protect against software supply chain attacks. A HSM can also be leveraged to protect the integrity of IP and product parts.





Reduce

Reduce the probability and impact of risk with synced passkeys and strong MFA practices



Strengthen legacy MFA

OT systems, Third-party access

Where the risk is “low” or where technical limitations prevent stronger authentication, the goal should be to reduce risk only to an acceptable level and instead focus on resilience and recovery planning that will minimize the negative consequences of a cybersecurity event. Proactive risk reduction activities include:



Add controls to synced passkeys

For any scenarios where you may choose to deploy synced passkeys rather than device-bound passkeys, it is critical to ensure you don't downgrade your security, but instead add compensating controls (such as a device-bound passkey for IT admins) to ensure synced passkeys are protected in the cloud.



Replace OTP with a hardware security key

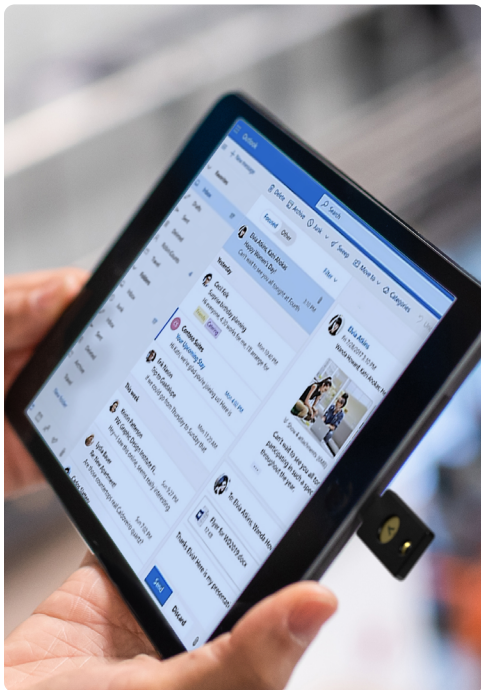
The risk landscape and concerns related to manufacturing origin for OTP hardware tokens has prompted many manufacturers to seek out alternative OTP solutions. With mobile-restrictions in place in OT environments, for safety and security, a hardware security key that supports OTP is a strong alternative that also provides a bridge to more modern authentication protocols.



Secure the seed exchange for the OTP process

To increase the security around OTP, you or your key provider can seed your hardware security key with a shared secret that will match up with your identity provider (e.g. Okta, Duo), creating an encrypted file with all the shared secrets that then is uploaded to the identity provider.

In addition to the above risk reduction measures, it is critical to develop and implement plans for resilience and to restore capabilities seamlessly and quickly.



Accept & transfer

Accept risks and the constraints that limit the use of controls, transfer risk to insurance



Transfer risk to insurance

Legacy systems

While some legacy systems support phishing-resistant PIV smart cards, which can be supported on the same hardware security key as device-bound passkeys, manufacturers have a clear path to 'Avoid' risk. However, other legacy systems represent a significant vulnerability where increased connectivity hinges on legacy authentication methods such as passwords and OTP.

Where risk is unavoidable, manufacturers can either accept that level of risk or transfer all or a portion of that risk with a cyber insurance policy. While cyber insurers will have some acceptance of risk associated with OT systems, most cyber insurers are hedging their own risk by requiring MFA and evidence of ongoing cyber risk mitigation efforts. In this case, cyber insurers may deny future coverage, or introduce new sub-limits or exclusions, if efforts are not made over time to reduce the level of risk.

Step 4: Evolve over time

The goal of any risk management program is to create a feedback loop that iterates improvements and reduces risk over time. For example, while in the short term there may be constraints that make replacement of legacy systems either too costly or not in the best interest of the manufacturer, over time, the benefits of digital transformation will outweigh the costs.

To help you evolve over time, choose an authentication solution that meets you where you are today, with support for OTP protocols as well as phishing-resistant Smart Card and FIDO2 (passkey) to help support a seamless journey into the future.

Key business outcomes from investing in stronger authentication



Reduced exposure to risk



Increased user productivity



Reduced IT support costs



Operational cost savings



Ability to win contracts



Compliance



Yubico has you covered

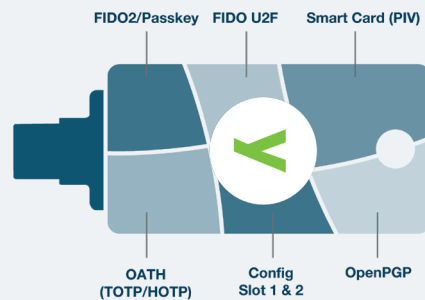
- IP68 certified, AAL3 compliant, and FIPS 140-2 validated solutions to protect any environment from industrial or corporate to highly regulated.
- A single key secures hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with the secrets never shared between services.
- YubiKeys help organizations on the journey to deploying phishing-resistant authentication across the entire user lifecycle, including registration, authentication and recovery processes, to create phishing-resistant users.



YubiKey 5C NFC

YubiKey is the bridge to modern authentication

Upgrading authentication across complex IT and OT manufacturing scenarios is a journey that mirrors the evolution toward the smart factory.



To support this journey, Yubico offers the YubiKey, a hardware security key that contains the highest assurance passkeys and helps manufacturers bridge to phishing-resistance and passwordless. The YubiKey's multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn (passkeys), FIDO U2F, OTP and OpenPGP helps meet you where you are on your risk management journey. For each scenario, choose the strongest possible form of MFA available to you, knowing you're creating a path to future improvements, all on a single YubiKey.

The YubiKey provides authentication that moves with users, no matter how they work across devices, to legacy and modern applications, shared workstations, IT and OT systems including ICS systems like SCADA, all from a single key. The YubiKey does not require external power or batteries or a network connection, making it an ideal solution for mobile-restricted environments. The YubiKey is proven to **reduce risk by 99.9%** and provide significant value at scale, delivering an ROI of 203%²⁷, all while enabling a frictionless user experience, letting users quickly and securely log in with a single tap or touch.



More value

Reduce support tickets by

75%



High return

Experience ROI of

203%



Strongest security

Reduce risk by

99.9%



Faster

Decrease time to authenticate by

>4x

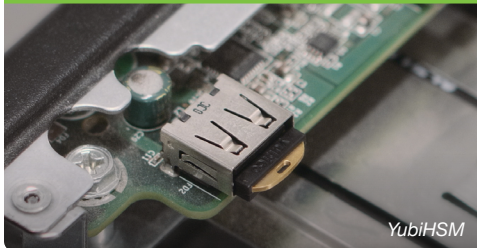


Durable

IP68 rated,
crush-resistant,
no battery required,
no moving parts

Yubico also offers an hardware security module (HSM), YubiHSM:

- Ensures enterprise-grade high cryptographic security and operations that protects servers, applications, and computing devices
- Safeguards intellectual property, corporate secrets and secures manufacturing assembly lines
- Ultra-portable nano form factor that allows for flexible deployment



Read our case study
yubi.co/SchneiderElectric

With Yubico you secure:



Privileged access



Remote access



OT systems



Software supply chain



Third-party access



Office systems



Air-gapped OT systems



Shared workstations

When you are FIDO ready and capable

In those cases where you are able to go to FIDO right off the bat, Yubico accelerates the ability to create phishing-resistant users with out-of-the-box FIDO authentication. **The Yubico FIDO Pre-Reg service eliminates manual user registration**, enabling users to receive YubiKeys that are pre-registered with the organization's Identity Provider (IdP)—so organizations can seamlessly get started on the most secure form of passkey authentication for new and existing users, while reducing the burden on IT departments.



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.”



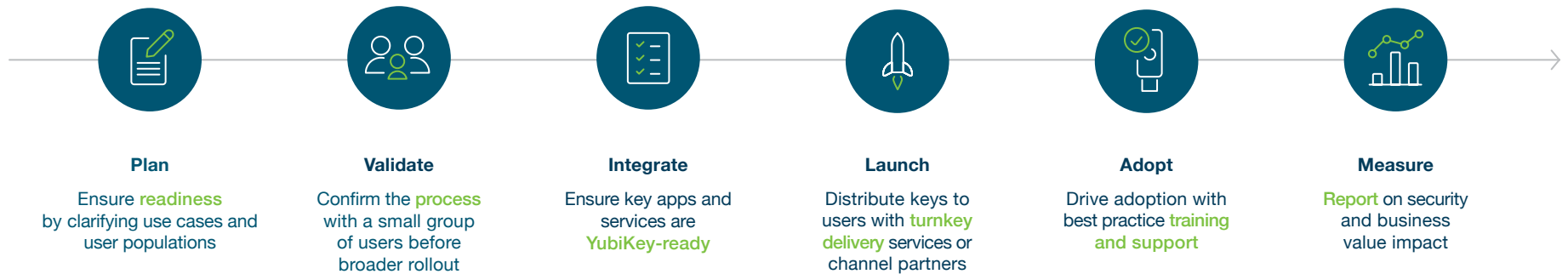
Chad Lloyd

Director of Cybersecurity Architecture for Energy Management
Schneider Electric

Manage and future-proof risk at scale

To protect against the growing number of cyber threats, manufacturers need an authentication solution that supports risk mitigation efforts across the spectrum of authentication scenarios. Yubico solutions are designed to meet you where you are on your cybersecurity journey, paving the way to smart factories and highest-assurance device-bound passkeys.

We have made it easy to safeguard your organization with the YubiKey. We offer a simple guide that details the six deployment best practices to accelerate adoption at scale, [How to get started with the YubiKey to secure manufacturing](#).



Yubico Professional Services



[Read the solution brief yubi.co/6fu](https://yubi.co/6fu)

To remove all the guesswork out of planning, purchasing and delivery, Yubico offers YubiKey as a Service, a service-based and affordable model to simplify how organizations procure, upgrade and support YubiKeys, as well as streamlined global distribution to remote and in-office locations through YubiEnterprise Delivery and trusted channel partners. Our professional services team also meets you where you are, taking over the process of securing the seed exchange before delivery, when supporting legacy OTP and TOTP processes.

If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help.



Contact us
yubi.co/contact



Learn more
yubi.co/manufacturing

Sources

- ¹ Deloitte, [Deloitte and MLC Industrial Metaverse Study](#), (September 2023)
- ² IBM, [2024 X-Force Threat Intelligence Index 2024](#), (February 21, 2024)
- ³ IBM, [2024 X-Force Threat Intelligence Index 2024](#), (February 21, 2024)
- ⁴ Verizon, [2024 Data Breach Investigations Report](#), (May 1, 2024)
- ⁵ IBM, [2024 X-Force Threat Intelligence Index 2024](#), (February 21, 2024)
- ⁶ Verizon, [2024 Data Breach Investigations Report](#), (May 1, 2024)
- ⁷ Verizon, [2024 Data Breach Investigations Report](#), (May 1, 2024)
- ⁸ IBM, [2024 X-Force Threat Intelligence Index 2024](#), (February 21, 2024)
- ⁹ Verizon, [2024 Data Breach Investigations Report](#), (May 1, 2024)
- ¹⁰ Waterfall, [2023 Threat report - OT Cyberattacks with Physical Consequences](#), (May 4, 2023)
- ¹¹ Microsoft, [Microsoft Digital Defense Report 2023](#), (November 8, 2023)
- ¹² Emerson, [How Manufacturers Can Achieve Top Quartile Performance](#), (Accessed January 31, 2022)
- ¹³ World Economic Forum, [Building a Culture of Cyber Resilience in Manufacturing](#), (April 29, 2024)
- ¹⁴ Rockwell Automation, [State of Smart Manufacturing Report](#), (March 26, 2024)
- ¹⁵ NIST, [Cybersecurity Framework Version 1.1 Manufacturing Profile](#), (October 2020)
- ¹⁶ ISO, [ISO/IEC 27001](#), (2022)
- ¹⁷ ISA, [ISA/IEC 62553 Series of Standards](#), (Accessed July 24, 2024)
- ¹⁸ The White House, [NSM-8](#), (April 30, 2024)
- ¹⁹ European Commission, [Annexes to the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation \(EU\) 2019/1020](#), (Sept 2022)
- ²⁰ Government of Canada, [National Cross Sector Forum 2012-2023 Action Plan for Critical Infrastructure](#), (2021)
- ²¹ Eduard Kovacs, [Mitsubishi Electric Factor Automation Flaws Expose Engineering Workstations](#), (February 5, 2024)
- ²² NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (December 2022)
- ²³ Australian Signals Directorate, [Essential Eight Maturity Model](#), (November 23, 2023)
- ²⁴ European Commission, [eIDAS Levels of Assurance \(LoA\)](#), (2014)
- ²⁵ NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (December 2022)
- ²⁶ CISA, [Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem](#), (2024)
- ²⁷ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)



About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

For more information, please visit: www.yubico.com.