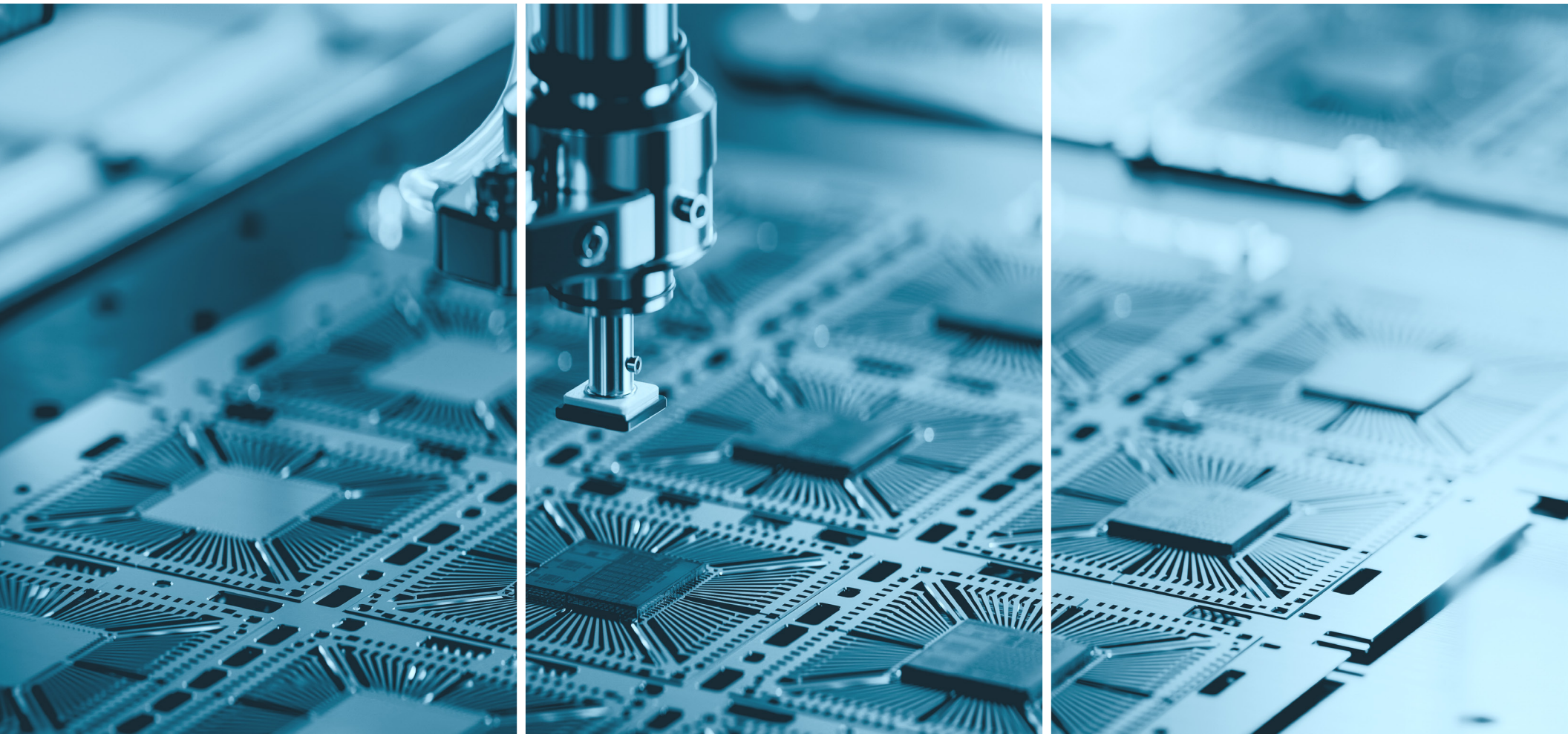
yubico

HOW THE YUBIKEY SOLVES HIGH-TECH MANUFACTURING MODERNIZATION USE CASES WITH PHISHING-RESISTANT MFA

Modern authentication for high-tech manufacturers

Safeguard critical IT and OT systems, sensitive IP, and the supply chain



A subsector in the manufacturing industry

integrated circuits

semiconductors

computers

smart phones

networking gear

High-tech manufacturers are a prime target of cyber attacks

Due to the information rich nature of high-tech manufacturers, safeguarding their intellectual property (IP) and R&D investments is of the utmost importance as they continue to be prime targets for cyber attacks. Malicious actors range in sophistication and persistence. These attacks can range from theft of the aforementioned IP for financial extortion or corporate espionage to nation-state actors leveraging stolen code and designs for malicious purposes.

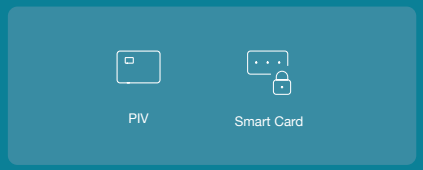
Most breaches (68%) originate from stolen credentials and human error as users click phishing emails;[1] continuing to be the most common way attackers gain entry to a victim's critical systems and data. Securing user access to both critical information technology (IT) and operational technology (OT) environments is integral for a strong cybersecurity strategy. However, attacks on OT in particular, tend to have larger negative impacts as they can have physical consequences like shutdowns, outages, leaks and explosions impacting operations.[2] Practitioners in high-tech manufacturing should prioritize implementing strong multi-factor authentication (MFA) as a first-line defense to secure access to protect critical data, IT and OT environments.

[1] Verizon, 2024 Data Breach Investigations Report, (May 1, 2024)

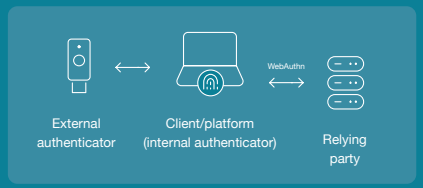
[2] McKinsey & Company, How to enhance the cybersecurity of operational technology environments, (March 23, 2023),

What qualifies as phishing-resistant MFA?

Channel binding PIV/Smart Card



Verifier name binding FIDO2/WebAuthn



[3] McKinsey & Company, How to enhance the cybersecurity of operational technology environments, (March 23, 2023)

Overcoming challenges to prioritize stronger MFA

Modernizing existing IT and OT systems is challenging and complex. Barriers to change include legacy technology that often does not support modern security controls, diverse industrial and restrictive production floor environments, over reliance on local and traditional on-prem access compared to the cloud, third-party remote connections to control OT devices connected to an internal network becoming more difficult to manage, and a shift in mindset from risk awareness and risk tolerance to one of proactivity.[3] All of these factors lead to competing business priorities and combine to create greater difficulty in achieving a more technologically modern state.

Not all MFA is created equal

There is a growing need for cost-effective, turnkey solutions to address the needs of today and future-proof against the authentication needs of tomorrow, leading to secure digital transformation and modernization of infrastructure. Securing identities, data, applications and computing devices using modern cryptography is integral.

Usernames and passwords are easily hacked, and legacy mobile-based authentication such as OTP, SMS and push notification apps are not phishing-resistant nor are they possible in mobile-restricted environments such as on factory floors. Accounts using MFA that are not based on phishing-resistant protocols are susceptible to cyber attacks.

Phishing-resistance: The draft National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-4), outlines the technical requirements for phishing-resistant authentication, recognizing two methods as being phishing-resistant: channel binding such as using a PKI-based Smart Card and verifier name binding such as using a Fast Identity Online (FIDO)-based credential and authenticator.

What is Fast Identity Online (FIDO)? FIDO2 is an open authentication standard, created by the FIDO Alliance, that consists of the W3C Web Authentication specification (WebAuthn API), and the Client to Authentication Protocol (CTAP). CTAP is an application layer protocol used for communication between a client (browser) or a platform (operating system) with an external authenticator such as a hardware security key. FIDO2 authentication options include strong single factor (passwordless), two-factor, and multi-factor authentication. Yubico is a core contributor to the FIDO2 open authentication protocol.

Ensure the confidentiality, integrity, and availability of your critical systems with the YubiKey.

To support your internally developed software, Yubico provides open source SDKs for integration to support YubiKeys anywhere.

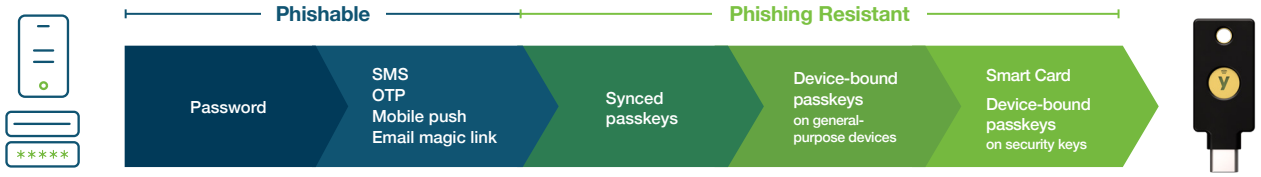
AAL3

For government contracts, the YubiKey FIPS Series enables manufacturers to meet the AAL3 requirements.

The YubiKey offers IP68 certified phishing-resistant MFA

Yubico created the YubiKey, a hardware security key that supports phishing-resistant MFA and passwordless authentication at scale with an optimized user experience. It provides the highest-assurance authentication to protect user access and accelerates the adoption of Zero Trust. With the YubiKey, deploy the most secure passkey strategy: device-bound that is purpose-built for security, FIPS 140-2 validated and is Authenticator Assurance Level 3 (AAL3) compliant.

The YubiKey is a multi-protocol hardware security key, supporting both PIV and FIDO2/WebAuthn standards, in addition to OTP and OpenPGP. Due to what is technically feasible in certain environments, the support for multiple protocols is crucial for helping high tech manufacturers bridge to a passwordless future, and integrate into both legacy/air gapped and network or cloud environments. The multi-protocol support enables you to meet the needs of the infrastructure while also strengthening your cyber posture.



As a result of Executive Order 14028 and OMB Memo M-22-09, phishing-resistant MFA is now required for all manufacturers with government contracts. It is also actively being recommended by CISA and the NSA (see 2023 publication Best Practices in Identity and Access Management) for all critical infrastructure sectors, including manufacturing. The YubiKey provides the highest level of device-bound, phishing-resistant MFA available on the market.

Bolster compliance strategy with YubiKeys
Learn more

The YubiKey 5 FIPS Series–from left to right: YubiKey 5C NFC FIPS, YubiKey 5 NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS, YubiKey 5C Nano FIPS

Securing hybrid and remote workers

> Everyday when I got to the IT department or I got to the physical areas, I see employees have their YubiKey hanging around their neck, it's part of their day-to-day life and day-to-day operations, and how they connect to systems. I don't think they even think about it"
>
> **Angel Urunuela** |
> CISO for Fluidra Group

As a high-tech manufacturer, your workforce is most likely distributed and global, further necessitating the importance of securing user access across the board. To meet the needs of the on-prem, hybrid and remote workforce, the YubiKey delivers a simple authentication experience no matter the computing device used. Moreover, the YubiKey works with leading Identity and Access Management (IAM) and Identity Provider (IdP) solutions, cloud services and thousands of applications, to enable phishing-resistant access for all employees without the need for peripheral or other supporting devices. Whether your employees rotate between an industrial environment or corporate office, the YubiKey is able to meet the demands of your employees' movements, providing a convenient solution that is portable, like they are. The purpose-built hardware on the YubiKey, including a touch sensor, provides a mechanism that can verify that the person logging in is a real human, and not a trojan or remote hacker.

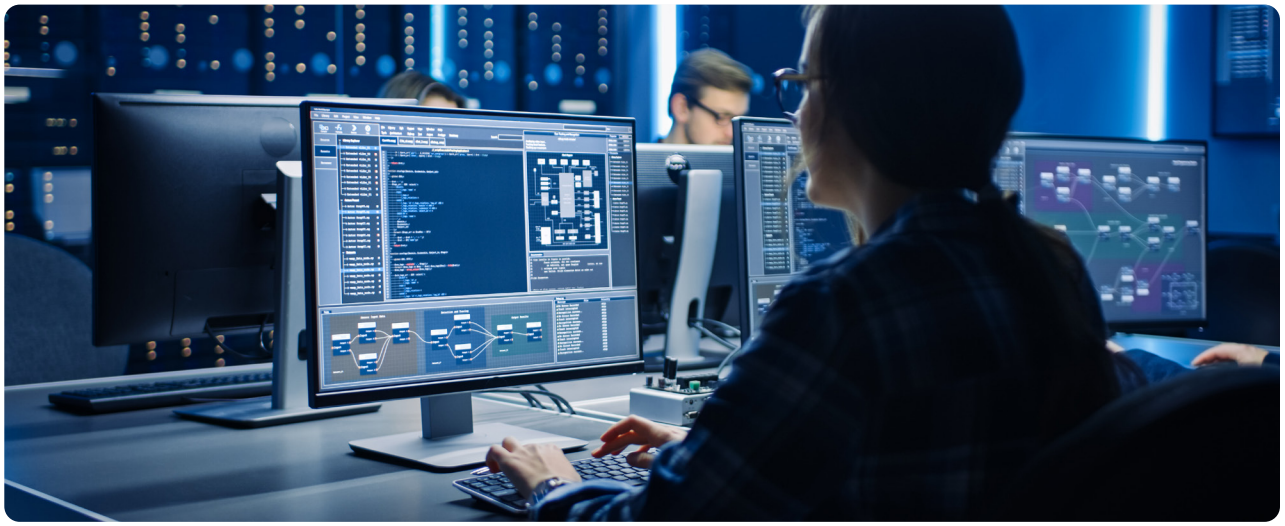
Securing privileged users and access

> “You can already see the extremely low probability of phishing attacks within Naftogaz-Bezreka. It is through using YubiKeys and Microsoft Azure, where we link our keys, that users no longer need to use passwords. In my opinion, we are the most secure company in our group.”
>
> **Oleksandr Tarasov** |
> Head of Security Controls
> at Security Operation Center
> Naftogaz-Bezreka

In today’s digital world, the idea of “privileged users” has expanded beyond the traditional IT functions, and now includes any business users who possess access to exploitable systems, IP or valuable data such as that associated with customer, HR, finance, legal or sales. As a high-tech manufacturer, you likely have a wide range of roles, so not only do you need to control who can view or have access to different types of information, but also the actions or ‘privileges’ an individual has to execute certain commands. As an example, in order to create printed circuit boards (PCBs), you may need to regulate access so that certain privileges are maintained only at the highest levels for read and write, so the IP remains protected amongst employees with special clearance. Authentication is a mission-critical service, and if employees can’t log into the apps or portals they need to use, they can’t do their job.

With the YubiKey, you can secure user access with phishing-resistant authentication to critical IP and personal information. The YubiKey offers the highest-assurance security that can be used to authenticate privileged users to both legacy and modern applications and secure access to devices. Further the YubiKey supports multiple protocols, enables public key cryptography and URL binding, stores authentication secrets on a secure hardware chip, and restricts data from being copied or exported—all of which amounts to best in class security for authenticating privileged users across the enterprise. As an example, Microsoft Entra ID now supports the enrollment of YubiKey as a FIDO2 authenticator. With this feature, admins are able to quickly enroll YubiKeys on behalf of their privileged user roles, to solidify enterprise security and meet phishing-resistant authentication requirements.

A user can use a single YubiKey to secure hundreds of applications and services with the secrets never shared between services.

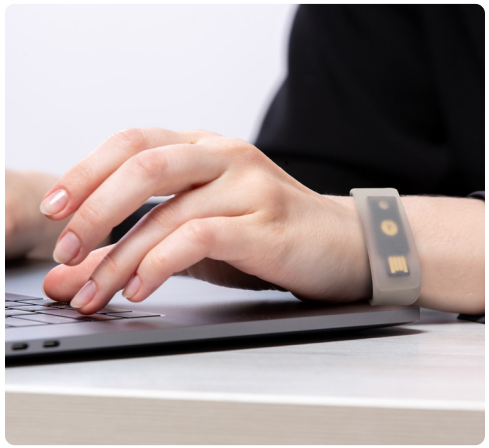


Securing industrial and restrictive factory floors with shared workstations & devices

Shared workstation environments and industrial and restrictive production floors are common in high-tech manufacturing. These systems are often using customized operating systems that have minimal corporate controls and a lack of defined access privileges. Typically, it is one shared user account used to access a workstation that may be air gapped. Therefore, several individuals will be using a common log-in to access the system. At times a supervisor may be responsible for an entire area, encompassing several different workstations, and for managing all access for users within the team. High-tech manufacturing workers that use shared workstations and devices can benefit from using the YubiKey as a portable root of trust for secure authentication for the following reasons:

- A single YubiKey works across multiple shared devices including desktops, laptops, mobile, tablets, and notebooks, enabling a user to utilize the same key as they navigate across devices
- It comes in a variety of different form factors with some fitting on a keyring, whilst offering USB-A, USB-C, and lightning connectors, in addition to NFC support
- YubiKeys are also easily re-programmed, making them suitable for rotating-shift and temporary users across these environments
- This process allows an operator to come on shift, authenticate quickly, and be able to take actions when appropriate, without any system interruptions. The YubiKey ensures only authenticated users with physical possession can gain access to operate the system
- There may be cases where you would like to warrant supervisory functions, and to utilize YubiKeys as a means to attest to proper authorization needed to make certain changes

A variety of YubiKey based solutions exist for securing access to sensitive data on tablets and mobile devices depending on the operating system, ranging from capabilities built into the operating system or application to remote desktop and application virtualization technologies. As an example, the YubiKey can be used for any managed devices that control access to the network, apps, and more. Further, you don't need to worry about mobile-based authentication solutions in places such as OT environments, which aren't always reliable where cell coverage is spotty or non-existent.



The YubiKey doesn't require a battery or internet connection, and is highly durable, dust proof, crush- and water resistant (IP68 certified) and is reliable to protect users and secure user access across:

- Factory floors
- Assembly lines
- Industrial control systems (ICS systems)
- Supervisory Control and Data Acquisition (SCADA) systems

Additionally, given the sensitive and complex nature of these systems, you rely on custom-built software and not commercial off-the-shelf software. As an example on the factory floor, it is common to see custom-built Debian GNU/Linux based on SCADA. Fortunately, Linux supports a variety of capabilities found on the YubiKey. Clean suits and gloves are frequently found in these environments, plus there is always a looming risk of foreign object debris (FOD) being introduced into these environments. With the YubiKey, using the NFC interface, it is possible to utilize wearables like rubber bracelets or gloves with a slot, so users can authenticate with a simple touch or tap, without having to remove protective clothing.

Securing local and traditional on-prem access, air-gapped networks, and cloud

> “As part of our IEC SL2 certification, we included MFA in our power operation system, well positioning us to meet SL3 requirements in the future. This is a point of differentiation for Schneider Electric.”
>
> **Chad Lloyd** |
> Director of Cybersecurity
> Architecture for Energy Management
> Schneider Electric

Availability and uptime are critical for this sector, which means in many cases there is no reliance on cloud infrastructure. There is a need to run services independently on local and traditional on-prem access, even if there are some cases where cloud infrastructure is used. Additionally, air-gapped networks and clean rooms are closed off from the outside, making it difficult to authenticate users using data sent over a network.

Many air-apped and SCADA systems still use a username and password, or a combination of passwords and a digital identity. YubiKeys ensure that local and traditional on-prem, air-gapped networks, and hybrid cloud networks stay secured against breaches, by providing highest-assurance authentication. YubiKeys works well in isolated network and mobile-restricted environments, as they don’t need any network connectivity, cellular connection, or batteries to work.

The multi-protocol capabilities of the YubiKey enables you to use MFA when and where you technically are able to, and in situations on the manufacturing floor where systems do not support phishing-resistant protocols, you can leverage YubiKey Static Password support for stronger security measures.

Securing the supply chain and third party access

> Proactively securing our global supply chain was an important step as properly tested and approved products are counted on by our customers who buy and deploy them”

Chad Lloyd |
Director of Cybersecurity
Architecture for Energy Management
Schneider Electric

The primary challenge for high tech manufacturers, including the semiconductor industry, is that protecting downstream supply chains is not easy given the hundreds (if not thousands) of entry points that need to be monitored along the way. When it comes to third-party remote connections to control OT devices connected to an internal network it is essential to safeguard that access. As there is a network of suppliers and partners ranging from the raw materials to make the devices and chips, to generating the designs–there is an urgent need to ensure that the right steps are taken from a security perspective.

High-tech manufacturing organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain. The YubiKey provides modern phishing-resistant authentication at scale across the supply chain, helping high-tech manufacturers and their suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical IP handoffs. Combined with YubiKey as a Service, you can offer an inexpensive and easy solution to improve supply chain security.

Protecting IP, device and product integrity

High-tech manufacturers know 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. As a result, there must always be a solution in place to protect the integrity and intellectual property of all components from production and assembly, to repair and replacement.

With the YubiKey, secure access to critical systems by verifying every user or device, including between IT and OT systems. Further protect code access and implement trusted code-signing with PKI keys and certificates to ensure product authenticity and protect corporate IP.

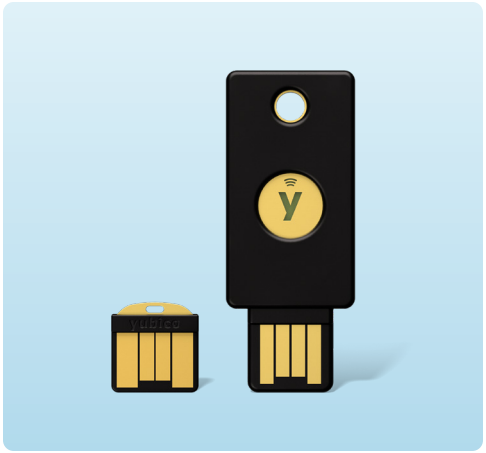
> By leveraging the YubiKey and the YubiHSM, a small formfactor and powerful hardware security module, we increase the security of our supply chain at Schneider Electric."
>
> **Chad Lloyd** |
> Director of Cybersecurity
> Architecture for Energy Management
> Schneider Electric

YubiHSM 2 protects corporate secrets and OT environments

The YubiKey helps secure authentication from external sources and between IT and OT systems, while the YubiHSM 2 (hardware security module) and YubiHSM FIPS enable secure key storage and operations on a physical device. The YubiHSM & YubiHSM FIPS provides the same philosophy of low-cost, high security and simplicity to cryptographic protection for servers, applications, assembly lines as well as IoT devices both for internal production and along the supply chain.

The small format YubiHSM 2 can be integrated into any process where secrets need to be managed, and the authenticity of components guaranteed or tampering needs to be avoided. The YubiHSM 2 can be easily deployed to a USB slot on servers, databases, robotic assembly lines and IoT devices.

The YuibHSM is ultra-portable with an innovative 'nano' form-factor that allows for flexible deployment. Further it is cost-effective by ensuring enterprise-grade high cryptographic security and operations without the traditional HSM price tag. It functions self contained into that server and it is not cloud dependent.



Products from left to right: YubiHSM and YubiKey 5 NFC

Making the business case

Moving to a passwordless and a phishing-resistant future is a journey due to managing older infrastructure, it will not happen overnight. It's important to embrace mindset shifts from risk awareness and risk tolerance which can lead to competing business priorities.

Most organizations have IT systems that will continue to require support for legacy authentication protocols for some time. However with YubiKey's multi-protocol support that combines the range of old and modern authentication protocols on the same key, it is now possible to move towards a brighter future in steps. Yubico's technical partners provide a variety of on-premise and cloud solutions to support manufacturing environments as well.

Ready to get started?

When you choose YubiKey as a Service, you make decisions as you go with our insight and help, simplifying the process of scaling YubiKeys to wider circles of use cases and leveraging the insight.

We have created a six step deployment process to plan for and accelerate adoption of phishing-resistant MFA at scale.

Plan

Ensure readiness by clarifying use cases and user populations

Validate

Confirm the process with a small group of users before broader rollout

Integrate

Ensure key apps and services are YubiKey-ready

Launch

Distribute keys to users with turnkey delivery services or channel partners

Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact

Once ready to purchase, Yubico is focused on helping easily access security products and services in a flexible and cost effective way to heighten security:

You purchase YubiKeys via a one-time perpetual purchasing model or can opt for greater flexibility with a subscription model. With YubiKey as a Service, receive a service-based and affordable model for purchasing YubiKeys in a way that meets their technology and budget requirements. This service also provides priority customer support, ease of form factor selection, backup key discounts, and replacement stock benefits.

With YubiEnterprise Delivery, IT teams have powerful capabilities to manage the delivery of hardware security keys to users globally and accelerates the adoption of strong authentication. Distribute keys to users with turnkey delivery services or through channel partners, even automate the process and integrate it with a ServiceNow portal.

Yubico's Professional Services team can help you with a successful implementation. Yubico offers a wide variety of advisory services in support of your YubiKey implementation and deployment, including best practices workshops, technical implementation packages, on-demand consulting resources and custom engagements. Our Professional Services team is composed of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sectors. From standard implementations to complex enterprise rollouts, Professional Services has the skills and expertise to help guide you through all facets of your YubiKey implementation and deployment.

Contact us
yubi.co/contact

Learn more
yubi.co/manufacturing

yubico
The key to trust

Yubico (Nasdaq 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.**