yubico

PARTNER WITH YUBICO TO SECURE YOUR END-TO-END SUPPLY CHAIN

Manufacturers across the globe are investing in modern authentication

75%

of cyber attacks result in a **production outage**.[1]

$50 million

is estimated cost in unplanned **downtime**.[2]

In 2022

Ransomware groups targeted the **manufacturing industry** more than any other industrial sector.[3]

Manufacturing was the **top attacked** industry, accounting for 24.8% of all attacks and 58% of OT incidents.[4]

[1] Trend Micro: The State of Industrial Cybersecurity, (February 2, 2022)

[2] Emerson: How Manufacturers Can Achieve Top Quartile Performance, (May 4, 2023)

[3] Dragos ICS/OT Cybersecurity Year in Review 2022 (May 4, 2023)

[4] IBM Security X-Force Threat Intelligence Index 2023 (July 14, 2023)

The urgency to harden cybersecurity defenses in manufacturing

The manufacturing industry is vital to everyday life and it impacts an array of sectors critical to daily operations.

- high-tech (silicon & semiconductor)
- retail
- machinery
- medical
- energy
- transportation (aerospace & automotive)

Industries, such as manufacturing, that are part of critical infrastructure are often prime targets for cyberattacks. Stolen credentials gained through phishing or weak, legacy authentication processes pose as an entry point. Today's attackers don't hack in, they just log in.

Despite barriers to change, including legacy infrastructure, complex industrial and restrictive production floor environments, and the high cost of operational disruption, manufacturers face an imperative to move beyond passwords and are now considering modern authentication solutions to secure identities and modern cryptographic protection to secure servers, applications and computing devices.

Multi-factor authentication (MFA) should be a first-line defense of any cybersecurity strategy to protect critical data, information technology (IT), and operational technology (OT) environments. And while any MFA is better than passwords, not all forms of MFA offer the same level of security or frictionless user experience.

Not all MFA is created equal

Protect your critical infrastructure, stop phishing attacks and account takeovers before they start with modern, phishing-resistant multi-factor authentication (MFA). Stay ahead of evolving cyber threats and regulatory requirements with a proven solution which cannot be bypassed by malicious actors, unlike basic forms of MFA such as SMS, one-time passcodes and mobile authentication.

What is phishing-resistant MFA?

Phishing-resistant MFA processes rely on cryptographic verification directly between devices or between the device and a domain, making them highly secured against attempts to compromise or subvert the authentication process. A minimum standard met only by PIV/Smart Card and MFA based upon the FIDO2/WebAuthn standard.

Protecting all users in the enterprise

Start by addressing key user populations. Expand to broader set of stakeholders.

Priviliged access
Secure priviliged account users

Mobile restricted
Secure call centers for mobile restriced users

Shared workstation
Protect shared workstation users

Remote workforce
Enable remote workforce

Office workers
Improve UX and security for office workers

3rd party access
Protect corporate system access by 3rd parties

End customers
Safeguard Yubico customers and consumers

Safeguard your IT and OT ecosystem with Yubico

Yubico solutions meet you where you are on your cybersecurity journey, while paving the way to a modern authentication infrastructure, and jumpstarting your plans to implement a zero trust framework. A worthwhile investment to feel confident in knowing that your data and intellectual property are secure and that you can maintain product integrity.

The YubiKey

A pioneer in modern, hardware-based authentication and Yubico's flagship product, the YubiKey is designed to meet you where you are on your authentication journey by supporting a broad range of authentication protocols, including FIDO U2F, WebAuthn/FIDO2 (passkeys), OTP/TOTP, OpenPGP and Smart Card/PIV.

yubi.co/key

Yubico Hardware Security Module (HSM)

The world's smallest HSM, YubiHSM 2, packs a lot of power, and offers game changing cryptographic protection for servers, applications and computing devices. Secure your public key infrastructure (PKI) environments, encrypt your files and databases and securely sign code or any digital artifact to raise the bar for security for your OT and IT systems.

yubi.co/hsm

YubiEnterprise Subscription

Get peace of mind in an uncertain world with a YubiKey subscription service that makes supporting new hires, tackling employee turnover and securing remote/hybrid workers fast, flexible and future-proofed—all with a lower cost to entry.

yubi.co/subscription

YubiEnterprise Delivery

Accelerate your journey to phishing-resistant MFA with an end-to-end domestic and international YubiKey delivery service. Let Yubico and our global partners worry about the logistics so you can focus on bigger business issues.

yubi.co/delivery

These are real stories of global manufacturers and other leading brands and how they've changed the game for modern enterprise security with the help of Yubico solutions.

Schneider Electric enhances global supply chain security with Yubico

> “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

As leaders in the digital transformation of energy management and the manufacturing of electric products, Schneider Electric worked closely with Yubico to deploy phishing-resistant YubiKeys to increase security with MFA in its power operation Supervisory Control and Data Acquisition (SCADA) system, a system common in manufacturing.

“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

Lloyd was tasked with a challenge to integrate multi-factor authentication (MFA) on an isolated system—without the use of the Internet or traditional methods such as SMS. With the YubiKey, Schneider Electric is able to meet its requirement for MFA and to ensure only authenticated users can gain access to operate the SCADA system. Further, the YubiKey has helped reduce system interruptions during shift changes or when step-up authentication is needed for certain operations.

After positive results from the initial deployment of YubiKeys, Schneider Electric then expanded to solve additional use cases in managing its supply chain. Schneider Electric deployed the YubiHSM 2 with key vendors to proactively increase security within their supply chain. Creating a dual encryption process allows both the vendor and Schneider Electric to have confidence that products with the Schneider Electric brand are indeed authentic based on encrypted keys that are embedded by both companies during manufacturing.

READ CASE STUDY →
yubi.co/SchneiderElectric

FLUIDRA

Fluidra enhances its global workforce security with YubiKeys

> “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**
> CISO for Fluidra Group

The Fluidra Group is a multinational conglomerate of companies that develops, manufactures and distributes products for the pool market, operating in more than 45 countries with over 7,000 employees. Fluidra decided to deploy phishing-resistant YubiKeys to privileged users, namely those with elevated access to back-end systems or infrastructure. The YubiKey integrated seamlessly with existing infrastructure, supported by onboarding materials to streamline adoption.

As is the case for most organizations, Fluidra Group needed an authentication solution that would satisfy multiple use cases and extend beyond the core group of privileged users. After measuring the success of its first launch, Fluidra expanded deployment of YubiKeys to all employees for use at work and at home to support secure, anywhere access to cloud-based services including Google Workspace and the many other products, services and applications supported by the YubiKey.

Every employee has a YubiKey on a lanyard which is used to authenticate to OT systems and other cloud systems in the environment. The deployment also helped the organization obtain a higher score for cyber insurance, helping reduce premium costs.

READ CASE STUDY →
yubi.co/Fluidra

Genetec eliminates passwords with the YubiKey

Genetec is an innovative technology company with a broad portfolio developing physical security hardware and software solutions. As a manufacturer of security products, and working with an extensive network of resellers, integrators, partners and consultants, Genetec wanted to create a security program that was based on identity strength. After smart cards proved challenging due to high costs and complex infrastructure requirements, Yubico worked with Genetec to pilot the lower cost YubiKey with embedded PIV/smart card features.

After a successful pilot, all 1200+ employees now use YubiKeys in their daily activities. To expand upon its security goals, Genetec then began distributing YubiKeys in much larger quantities to its partner ecosystem and to customers to log into and authenticate to various portals.

> Strong identity is the cornerstone of any security program and passwords are fundamentally dead."
>
> **Christian Morin**
> Genetec CSO and Vice President of Integrations and Cloud Services

> The YubiKey is now used to log on and authenticate to our product, that's part of what we mean by implementing stronger identity for our customers and partners. This will start with our cloud services and will make its way also into our various products as well."
>
> **Christian Morin**
> Genetec CSO and Vice President of Integrations and Cloud Services

READ CASE STUDY →
yubi.co/Genetec

EasyMile is safeguarding their software supply chain

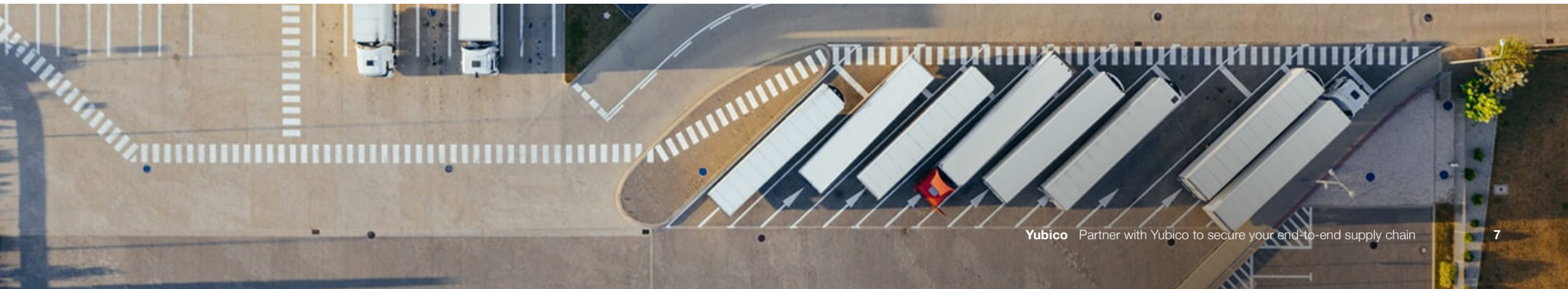
EasyMile develops software solutions for autonomous vehicles, mainly for vehicles used to transport people and goods. Founded in 2014, EasyMile is headquartered in Toulouse, France, and has an international presence, principally in the USA, Japan, and Australia.

To protect its fleet of autonomous vehicles, developed with the assistance of suppliers and other original equipment manufacturers (OEMs), EasyMile uses a Public Key Infrastructure (PKI) based on X.509 certificates to authenticate different assets and components to ensure the integrity of the software deployed. Practices focus on the authentication of differing assets and components, the integrity of the software deployed, and more.

Already users of YubiKeys for privileged accounts, EasyMile embarked on a project to harden its PKI infrastructure with the YubiHSM 2, which offers enhanced protection to safeguard cryptographic keys and certificates. With rapid returns on investment in both the YubiKey and YubiHSM 2, EasyMile continues to work with Yubico Professional Services to explore expanded use cases, focusing on both internal and external uses.

READ CASE STUDY →
yubi.co/EasyMile

> "When it comes to security, Yubico is a no brainer."
>
> **Alexandre Hamez**
> Tech Lead at EasyMile



ENERGY

Securing critical infrastructure at an Asia-Pacific energy company

Energy systems, like manufacturing, are a growing target for cyber criminals. For this leader in electricity distribution in Asia-Pacific, serving millions of customers, much of the responsibility for protecting operations from cyberattacks falls to the OT Security Specialist, a job which sits at the border between IT and OT.

During the procurement process of an authentication solution, the Anonymous Energy Company had to balance multiple requirements. It was important that the product would also integrate easily with existing infrastructure, without requiring additional software. This ruled out one possible solution—smartcards—which require specific drivers and smartcard readers to function. The OT Security Specialist was also keen to find a solution that was user-friendly.

The OT Security Specialist was most attracted by how YubiKeys balanced security and usability: "if you've got to physically touch the button, you know a user is physically there using it. We could set up one YubiKey as MFA for all a user's accounts, so they don't need six different TOTPs."

To protect the hardware and live equipment upon which distribution lies, the organization chose the YubiKey to secure all users who access the operational environment—offering a balance of security and usability and the ability to deploy it without additional software. Further, the flexibility of YubiEnterprise Subscription helps guarantee the highest level of protection into the future.

READ CASE STUDY →
yubi.co/EnergyCo

> "My personal opinion is that they're more convenient to use than a token off your phone, especially when your YubiKey is next to you. I don't like having to grab my phone and look for an app to get a token out of it or unlock it to approve a request. It's a lot quicker to just hit a button on the USB stick."

OT Security Specialist
Anonymous State-Owned Energy Company

The path forward to phishing-resistant MFA at scale

No matter where you are on your MFA journey, we'll meet you there. You can accelerate your zero trust approach and gain a bridge to a passwordless future. With a tried and true process that hundreds of organizations have followed already—and with a 'YubiKey as a Service' model—it's not a matter of if you'll be successful but when you'll be successful in raising your bar for security with modern, hardware-based security keys.

A worthwhile investment that not only shows that you care about the safety of employee authentication experiences, and cybersecurity across your supply chain, but will drive competitive differentiation and bolster you as a thought leader.

Plan

Ensure readiness and alignment ahead of execution

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

Contact us
yubi.co/contact

Learn more
yubi.co/bpg-mfg

yubico
The key to trust

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services. Yubico has a presence around the globe and offices in Santa Clara, San Francisco, Seattle area, and Stockholm. For more information, please visit: **www.yubico.com.**

© 2023 Yubico