



Modernize security across manufacturing

Protect people, data, and critical infrastructure with Yubico

The manufacturing industry is complex, with systems and technology to not only support the manufacturing of goods, but to support daily operations as well. This industry has been an emerging target for sophisticated malware, phishing, and Man-in-the-Middle (MiTM) attacks with the average data breach costing \$4.47 million.¹ The 2021 Colonial Pipeline attack reinforced the need for higher security across the industry in order to improve operational resilience.

To protect against evolving cyber threats, multi-factor authentication (MFA) can be a strong first-line of defense, however not all forms of MFA are created equal. Usernames and passwords are cumbersome to manage and drive up costs. Mobile authenticators (push notifications, OTP and SMS codes) are highly susceptible to cyber attacks and fail altogether in mobile-restricted or low connectivity areas. The continued reliance and support of these legacy authentication solutions can lead to lost productivity, delayed supply chains, increased operating expenses (OpEx), higher capital expenditure (CapEx) costs, and a greater risk of being breached.

Manufacturing environments need an easy-to-use, modern authentication solution. One that is scalable, can withstand the rigors of the manufacturing floor, and can be used to securely access systems and applications.

Yubico's security solutions for manufacturing

Yubico offers the [YubiKey](#) for modern phishing-resistant MFA and the [YubiHSM](#) for protecting servers, applications, and computing devices.

The YubiKey is a hardware security key that provides strong two-factor, multi-factor and passwordless authentication at scale. It is the only solution proven to stop account takeovers 100% in independent research.² With multi-protocol support, YubiKeys are future-proof investments by acting as a bridge to passwordless. The YubiKey meets and surpasses the Zero Trust and phishing-resistant MFA recommendations outlined in the [Office of Management and Budget \(OMB\) Memo M-22-09](#).

The YubiHSM ensures uncompromised cryptographic hardware security for servers, applications, and computing devices at a fraction of the cost and size of traditional HSMs. It is a FIPS 140-2 validated, Level 3 solution, and is also available as a non-FIPS solution—both with the same capabilities.



The YubiKey is:

- **Simple to use**—offers tap-and-go functionality that enables users to log-in 4 times faster than SMS.³
- **Cost-effective**—enables self-service password resets which reduces IT support costs by up to 90%.
- **Convenient**—provides easy, portable authentication across legacy and modern devices and applications without requiring a battery or internet connection.
- **IP68 certified**—ensures robust security across manufacturing floors and are highly durable, crush-resistant, and water-resistant.



We introduced YubiKeys in our power operation SCADA systems to increase security with MFA. This process allows an operator to come on shift, authenticate quickly, and to take actions when appropriate, without any system interruptions. MFA ensures only authenticated users can gain access to operate the system.”

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



The YubiHSM is:

- **Ultra-portable**—an innovative ‘nano’ form-factor that allows for flexible deployment.
- **Cost-effective**—ensures enterprise-grade high cryptographic security and operations without the traditional HSM price tag.
- **FIPS 140-2 validated**—robust hardware protection that ensures the highest levels of data protection and maintains compliance demands.

Leverage Yubico solutions to:

Reduce password reset costs

YubiKeys used for two-factor/multi-factor authentication dramatically reduce support costs related to password resets. YubiKeys enable self-service authentication without requiring users to wait for a manager or IT support in the event of an issue, thus lowering overhead costs related to password resets and lost productivity. This is especially important for applications/environments that are infrequently accessed by users and forgotten passwords are a common occurrence. According to Forrester, password resets cost the help desk over \$179 per employee per year,⁴ so an organization with 1,000 employees using YubiKeys for self-service can achieve average yearly savings of over \$179,000.

Secure web-based applications

Convenient and strong authentication is a necessity as adoption of cloud-based applications increases, such as for email, payroll and timekeeping systems. YubiKeys seamlessly integrate into existing and new environments—they work with hundreds of applications and services including leading Identity Access Management (IAM) solutions such as Microsoft, Okta, Ping, and Duo. The YubiKey in conjunction with IAM vendors and Identity Providers (IdPs) can also be used for Single Sign-on (SSO).

Secure shared workstations/kiosks

Plant floors typically have shared workstations/kiosks which need strict access controls. YubiKeys are extremely portable and simple to use across shared workstations, ensuring that only people who are authorized to access a system or application will be able to, helping eliminate any insider threats. A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations/kiosks.

Secure mobile-restricted environments

For manufacturing environments where mobile use is restricted, or when there is no cellular connection, YubiKeys offer simple and secure authentication. YubiKeys do not require a cellular connection to operate nor batteries or have any other external dependency. To authenticate, users simply tap or insert, then touch the YubiKey and, because the YubiKey arrives in a variety of form factors—including support for USB-A, USB-C, NFC, and Lightning—authenticating to the full gamut of modern devices is simple. Additionally, since YubiKeys have no cameras, microphones, or network connections, data confidentiality is ensured.

Secure the assembly line and supply chain

The YubiKey provides modern authentication at scale across the supply chain, helping manufacturing organizations and their suppliers implement robust, easy-to-use authentication for any user who has upstream access to the network or at critical intellectual property (IP) handoffs. The YubiHSM is suited to safeguard cryptographic keys and certificates used for signing code or components. It supports the secrets being shared within the supply chain, secure IoT devices, encrypt files and more.

Secure all users along the supply chain and safeguard third-party access with the YubiKey. Protect IP and product integrity with the YubiHSM. Yubico solutions ensure highest-assurance security.



Easily procure and distribute phishing-resistant security at scale

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With [YubiKey as a Service](#), organizations can benefit from a predictable OPEX model, the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to Deployment Services, Priority Support and a dedicated Customer Success Manager.

Subscription customers are also eligible to purchase additional services and product offerings, such as [YubiEnterprise Delivery](#), a global turnkey hardware key distribution service to residential and office locations in 199 locations (175 countries and 24 territories) around the world.

[Contact](#) the Yubico sales team today to be a cyber security leader in manufacturing.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator.

YubiKeys are produced in the USA, maintaining security and quality control over the entire manufacturing process.



The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops and mobile devices.

¹ IBM, [2022 Cost of Data Breach Report](#), (Accessed December 8, 2022)

² Google defends against account takeovers and reduces IT costs

³ Google, *Ibid.*

⁴ Sept 9, 2015 Forrester Report: [Benchmark Your Employee Password Policies And Practices](#)