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 $4.24 million. 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 2 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. 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 2 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.
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, 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 2 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.

Easily procure and distribute phishing-resistant security at scale
Yubico also offers services to help simplify procurement and distribution for employees at scale.

- **YubiEnterprise Subscription** provides a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support, and more. This is especially important for organizations experiencing frequent employee turnover.
- **YubiEnterprise Delivery** provides turnkey service with shipping, tracking, and returns handled by logistics experts, so organizations can focus on what matters—securing the workforce.

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.

---

2. Google defends against account takeovers and reduces IT costs
3. Google, Ibid.
5. Customers outside of North America should contact their local Yubico rep for details

---

**About Yubico**
As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: [www.yubico.com](http://www.yubico.com).

**Yubico AB**
Kungsagan 44
2nd floor
SE-111 35 Stockholm
Sweden

**Yubico Inc.**
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088

**YubiEnterprise Subscription** provides a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support, and more. This is especially important for organizations experiencing frequent employee turnover.

**YubiEnterprise Delivery** provides turnkey service with shipping, tracking, and returns handled by logistics experts, so organizations can focus on what matters—securing the workforce.

**Contact** the Yubico sales team today to be a cyber security leader in manufacturing.

---

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