yubico

WHITE PAPER

Protecting manufacturing with highest-assurance security

Go passwordless, ensure product integrity, secure your supply chain, and avoid downtime

Contents

2 Table of contents

3 The critical need for security and efficiency across the manufacturing ecosystem

6 Modernize MFA and go passwordless for secure user access to critical systems and data

- 5 Key considerations for authentication across IT and OT environments
- 8 Drawbacks of legacy authentication
- 9 The future is passwordless
- 10 Modern, phishing-resistant authentication and passwordless with the YubiKey

12 Securing the manufacturing supply chain

- 12 Safeguarding third-party access
- 12 Ensuring the highest integrity of your product parts
- 13 Securing external code and data
- 13 Safeguarding IP and product integrity with YubiHSM
- 14 Supporting Public Key Infrastructure (PKI) environments

15 Case study: Securing the systems and supply chain at Schneider Electric

15 Case study: A portable root of trust for EasyMile to secure autonomous vehicles

16 Yubico offers simple procurement and distribution of phishing-resistant security at scale

17 Summary

The critical need for security and efficiency across the manufacturing ecosystem

75%

of cyber attacks result in production outage[1]

50 billion/yr

cost of unplanned downtime in manufacturing[2]

$4.47 million

cost of data breach in manufacturing[3]

10%

of every day spent on non-productive tasks[4]

The manufacturing industry has been an emerging target for cyber attacks, including sophisticated malware, phishing, and Man-in-the-Middle (MiTM) attacks. Manufacturing organizations face not only data breach costs—an average of $4.47 million, but also risk loss of production time, intellectual property, and/or product integrity.[5] The 2021 Colonial Pipeline attack reinforced the need for higher security across the manufacturing industry to improve operational resilience, and ensure product integrity and visibility across the supply chain.

In the Colonial Pipeline attack, a phishing attack introduced malware that shut down the gas pipeline responsible for 45% of the fuel for the east coast of the United States. After two days, and with uncertainty over the extent of the attack, CEO Joseph Blount agreed to pay a $4.4 million ransom.[6] While a portion of this ransom was eventually recovered, the attack underscored the widespread impact of prolonged shutdown. Though no mention has been made of internal costs, unplanned downtime in manufacturing is estimated to cost $50 billion per year.[7] A recent manufacturing survey revealed that 75% of cyber attacks result in a production outage; in 43% of the outage cases, production stopped for more than four days.[8]

While some manufacturing organizations selling to the government have been subject to strict regulations and standards such as FIPS, DFARS, and ISO 9001, recent attacks have led to more wide-reaching regulatory requirements. The Colonial Pipeline attack resulted in two new TSA Security Directives[9] and the release of Executive Order (EO) 14028, which tightens the security standards for software sold to the government and requires the use of impersonation-resistant multi-factor authentication (MFA).[10] The Biden Administration also announced an upcoming new National Institute of Standards and Technology (NIST) framework for securing the technology supply chain; in collaboration, Apple announced plans that it would require all 9,000 of its suppliers to adopt MFA.[11]

Why the increased focus on MFA specifically? The answer is that current authentication and security solutions, including usernames and passwords and mobile-based authenticators, are no longer effective to protect organizations against modern cyber threats. Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based one-time-password (OTP) only blocked 76% of targeted attacks and a push app only blocked 90%.[12] That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of *if* you will be attacked—it's a matter of *when.*

Manufacturing organizations have identified the critical need to modernize authentication and security across Information Technology (IT) and Operational Technology (OT) environments, to ensure access to critical data and systems but also to protect the integrity and intellectual property of all components. However, a unique set of challenges in manufacturing have resulted in many manufacturers not keeping pace with the cybersecurity attack landscape:

Challenges faced in the manufacturing sector

Legacy infrastructure

Shared workstation environments

Heavy duty, gloved environments

Mobile-restricted areas

Supply chain management

Work disruption concerns

Product component integrity

Protecting manufacturing and design IP

Manufacturing operations often rely on legacy production equipment and applications, which may place constraints on the scalability and interoperability of security solutions. Further, the conventional separation of manufacturing systems from corporate IT systems and outside networks is no longer the reality of today's integrated manufacturing systems. Shared workstation environments are also common in manufacturing, often using unsupported operating systems with minimal corporate controls and a lack of defined access privileges.

According to recent research, the average manufacturing employee can access over 27,000 sensitive files (e.g. financial data, supply chain information, IP) on their first day of the job.[13] Authentication can be a first line of defense to protect against modern cyber threats, but reliance on legacy authentication methods such as username and password, and mobile-based authentication can put manufacturing organizations at greater risk of being breached.

61%

of data breaches can be traced back to credentials in some way.[14]

60%

of IT service desk interactions are related to password resets[16]

Compromised credentials continue to be the most common attack entry point—61% of data breaches can be traced back to credentials in some way.[14] Passwords can also rack up IT Help Desk costs related to password resets. The ideal state is to move to a passwordless future by eliminating passwords completely. The average employee has to use and remember 191 passwords, contributing to complexity and user frustration.[15] Currently, for the average company, 60% of IT service desk interactions are related to password resets.[16] Aside from the IT cost, the average company loses $5.2 million annually in productivity due to account lockouts.[17]

In the manufacturing industry, it is crucial to ensure authenticity of all components to avoid unsolicited replication and theft, but also for quality assurance, since an assembly line should only consist of genuinely sourced products, as the whole is always a sum of its parts. Production lines for various product components may come from different manufacturing plants as well as third-party manufacturing facilities around the world. Product integrity challenges can occur if component firmwares aren't digitally signed and certified to ensure component authenticity and integrity at the end of respective production lines. This is also important to ensure that only genuine components are used during service or replacement by a third-party reseller.

As a manufacturing organization, you need solutions that can offer modern security capabilities, helping transition to a more secure, passwordless workflow for a better user experience and overall efficiency. Further, you need solutions that can be quickly and easily deployed to support the quality, integrity, and intellectual property (IP) of all components in the end-to-end process—from production and assembly, to repair and replacement. To ensure that an assembly line only consists of genuinely sourced parts and products, there must be trusted solutions in place.

Modernize MFA and go passwordless for secure user access to critical systems and data

While considering authentication solutions to improve the security of IT and OT systems in manufacturing, it is important to consider how effective the solution is at protecting against external cyberattacks and insider threats, as well as how the solution affects user productivity and how reliable the solution is across varied environments.

Key considerations for authentication across IT and OT environments

To the left are the five critical authentication requirements that manufacturing organizations should take into consideration:

Security

Productivity

Reliability

Durability

Cost

Security

How do you make sure that only authorized users are accessing shared equipment?

How do you secure shared terminals and devices commonly found across the manufacturing floor, with multiple rotating users, making sure both the user accounts are secure and that the users are gaining access to only the applications, services and data they should have access to?

Currently, 44% of manufacturing organizations have 1000+ ‘ghost user’ accounts related to inactive user and service accounts.[18]

Admin accounts, or shared workstations with access to privileged information, should be protected with an authentication mechanism that is impersonation-resistant.

Shared workstations should rely heavily on user permissions and access controls (no shared, guest, or anonymous logins), and have restrictions that prevent password saving. Administrator accounts should also be individual, not shared, to support in-person or remote troubleshooting.

Further, it is important in a manufacturing context to ensure that the authentication solution does not introduce new security or safety challenges. For example, many manufacturing organizations have had to implement mobile device-related policies to keep phones off the assembly floor due to the disruptions to productivity and potential dangers of improper cell phone usage, which can cause inattention to the task at hand or the surroundings—both dangerous and costly in a manufacturing environment.

Productivity

How do you make sure the user is able to seamlessly authenticate across multiple devices and applications?

44%

of manufacturing organizations have 1000+ 'ghost user' accounts related to inactive user and service accounts[18]

54%

of employees think 2FA solutions such as OTP and push-codes disturb their day-to-day workflow[19]

Any authentication mechanism adopted should provide fast and easy authentication for employees, to avoid workflow disruption and prevent unapproved workarounds such as sharing passwords. Currently, 54% of employees think two-factor authentication (2FA) solutions such as OTP and push-codes disturb their day-to-day workflow.[19] Further, if systems are accessed infrequently, such as HR or payroll systems, the chance of forgotten passwords and account lockouts are high.

Not all forms of MFA offer the optimal balance of strong security with a fast and easy user experience that enables high productivity. Mobile authenticators increase the number of steps in the authentication process, requiring users to wait for OTP or push app codes or to remove gloves for interaction. Further, these processes are subject to the limitations of mobile-restricted environments and union rules.

Regardless of the scenario, consider how much time is appropriate for authentication and how many times a user may have to authenticate during the course of a shift or day. Consider also the size of the IT department and the average time to deal with account lockouts—all of which contributes to non-production time and direct labor costs. Where efficiency requirements are high, consider a passwordless authentication experience or the benefit of a tap-and-go NFC experience in conjunction with mobile devices where possible, especially with shared workstations.

Reliability

How do you ensure consistent authentication that always works, even in tough environments with varying points of failure?

Authentication is a mission-critical service, and if employees can't log into the apps or portals they use, they can't do their job. Any authentication solution has to be reliable for every user and not rely on common points of failure including connectivity, device battery, cell reception, or hard token battery. Authentication solutions should also have capabilities such as NFC that are suitable for environments such as industrial manufacturing, clean rooms, or no spark environments.

Consider that any authentication solution that relies on "something you know" (such as a password) is subject to human error—lost, forgotten, or mistyped details that add friction to the authentication experience, potentially locking users out of accounts. Additionally mobile-based authentication solutions aren't always reliable across shared workstation environments where cell coverage is spotty or non-existent in places such as OT environments, not to mention the reliance on the device battery in the case of mobile-based authentication.

Durability

How do you ensure that the product can withstand the rigors of the manufacturing floor?

Any authentication solution used in a manufacturing facility must be able to withstand the daily rigors of that environment. The use of moving and heavy equipment, hard surfaces, and thick gloves all combine to increase the risk of damage to authentication solutions that enter the workplace.

Consider whether your chosen authentication solution is highly durable, crush-resistant, and can withstand regular sanitization.

Cost

How do you reduce the number of authentication-related support tickets?

> "The average company loses $5.2 million annually in productivity due to account lockouts."
>
> –Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report

Any form of legacy authentication such as usernames and passwords, and mobile authentication applied and enforced at scale, will require ongoing policy enforcement, user training and IT support. Even the easiest forms of 2FA and MFA mobile authentication such as OTP for instance—creates a huge support burden if codes are delayed, users get locked out of their accounts, or users need to register new devices. Further, unions may require that organizations carry the full cost for the device, including hardware costs, recurring service costs, enterprise device management and security software, as well as phone replacement costs due to the inevitable breakage that could follow in production environments.

Any time a user struggles with mobile authentication, they are not being productive. The faster an employee can authenticate and do their job securely, or even perform a self-service password reset if required, the better the return on investment.

Drawbacks of legacy authentication

Low on reliability and security, high on friction and cost

It's important to note that while any form of 2FA or MFA offers more security than passwords alone, legacy authentication still relies on passwords as the first factor—still insecure, still inefficient, still a source of employee frustration. And that frustration only leads to unsafe workarounds such as password sharing, password reuse across multiple accounts, or passwords being saved to the browser or application where they may be vulnerable.

Further, in mobile-based MFA (SMS, OTP, and push app), the second factor is tied to the mobile device. This is a red flag, because of four aspects. (1) There can be availability challenges with mobile devices sending codes in a timely manner due to poor connectivity or unreliable services. (2) There is no real guarantee that the private key ends up on a secure element on the mobile device. (3) The OTP or private key could be intercepted in some way (such as via SIM swapping), and (4) It is impossible to ensure proof of possession—or in NIST terms—impossible to prove it is impersonation-resistant.

Risk of account takeover rates

0%
FIDO security key (YubiKey)

10%
On-device prompt

21%
Secondary

24%
SMS Code

50%
Phone number

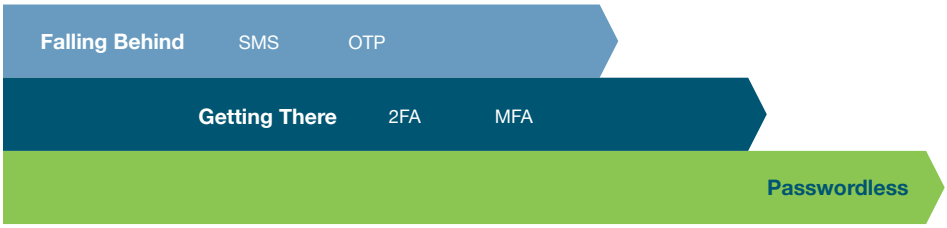
Google, How effective is basic account hygiene at preventing account takeovers

Legacy mobile authentication is susceptible to modern cyberattacks including phishing, brute force attack, MiTM attack, malware, and the previously mentioned SIM swapping. Beyond security, legacy mobile authentication carries with it many hidden costs associated with lost productivity, device costs, increased IT support, and friction in the user experience. In fact, 43% of organizations cite user experience as the top obstacle to using MFA.[20] For additional details, read our whitepaper: The Top 5 Mobile Authentication Misconceptions: Demystifying the myth versus reality of legacy MFA.

Replacing legacy single-factor authentication (username and password) with phishing-resistant multi-factor authentication (MFA) is the first step in improving security practices.

The future is passwordless

Moving from legacy MFA to phishing-resistant MFA is a key step forward in securing shared OT and IT environments in manufacturing. But the next step in modern MFA is introducing passwordless authentication. Because ultimately the actions of the user are the biggest weaknesses in legacy authentication, and multi-step authentication is a big contributor to user dissatisfaction, the global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.



Traditional smart cards are another form of passwordless that offer high security, but generally require high capital expenditure (CapEx) for smart card readers, cards, and backend management platforms. Smart card technology is primarily implemented in on-prem environments. Based on your needs, smart cards might be a suitable solution for you. The industry as a whole is moving toward a passwordless login flow leveraging modern authentication standards such as FIDO2/WebAuthn that work well with the cloud.

The FIDO (Fast IDentity Online) modern authentication standard enables strong two-factor, multi-factor, and passwordless authentication. The FIDO standard was created by the FIDO Alliance, an open industry association whose mission is to reduce the reliance on passwords. FIDO2/WebAuthn is the most recent FIDO standard and uses public key cryptography for high security, where the private keys never leave the authenticator. For manufacturing organizations that have legacy OT systems and a low tolerance for non-productive tasks, FIDO2 hardware security keys offer multi-factor and passwordless authentication with the high security and user experience that have thus far remained elusive. FIDO2-based hardware security keys can provide a portable root of trust that is highly appropriate for shared workstation as well as mobile-restricted environments.

Modern, phishing-resistant authentication and passwordless with the YubiKey

Yubico offers the YubiKey—a hardware security key built for highest-assurance security, usability and durability. With the YubiKey, manufacturing organizations can deploy phishing-resistant multi-factor and passwordless authentication at scale, with a fast and easy user experience that drives high productivity. YubiKeys are the only solution proven to stop account takeovers 100%[21]—organizations are ensured highest-assurance security with the hardware authenticator protecting the private secrets on a secure element that cannot be easily exfiltrated.

The YubiKey uses modern authentication protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential attacks. Additionally, YubiKeys also support SmartCard, OTP, and OpenPGP protocols, enabling the use of a single security key across a variety of modern and legacy IT and OT environments, and with a variety of 3rd party IAM solutions such as Microsoft, Okta, Duo and Ping, as well as authentication for hundreds of applications and services. The multi-protocol support allows organizations to leverage the YubiKey as a bridge to transition towards passwordless authentication.

YubiKeys are extremely portable and simple to use, supporting employee productivity. The YubiKey offers fast, tap-and-go passwordless login that is 4x faster than login with SMS—and a single YubiKey conveniently works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations. It comes in a variety of different form factors with some fitting on a keyring, whilst offering USB-A, USB-C, NFC, and lightning connectors.

YubiKeys provide robust security across manufacturing floors—YubiKeys don't require a battery or internet connection, and are highly durable, dust proof, crush- and water-resistant (IP68 certified), and suitable for no spark / low spark environments. No battery, software installation, or cellular connection required.

To further improve the user experience and speed of authentication, Yubico also offers the YubiKey Bio Series—FIDO Edition supporting FIDO U2F and FIDO2, which delivers the same hallmark security that all YubiKeys are known for, but with a new biometric-based passwordless experience.

> "We believe that by using this token we've raised the standard of security for our employees beyond what was commercially available. The device works with Google's Web browser Chrome, and works very seamlessly for people in their day-to-day workflow here at Google."
>
> –Mayank Upadhyay, Director of Security Engineering, Google Inc.

The YubiKey

is the **only** solution that is highly phishing resistant, and is proven to stop **100%** of account takeovers in independent research.

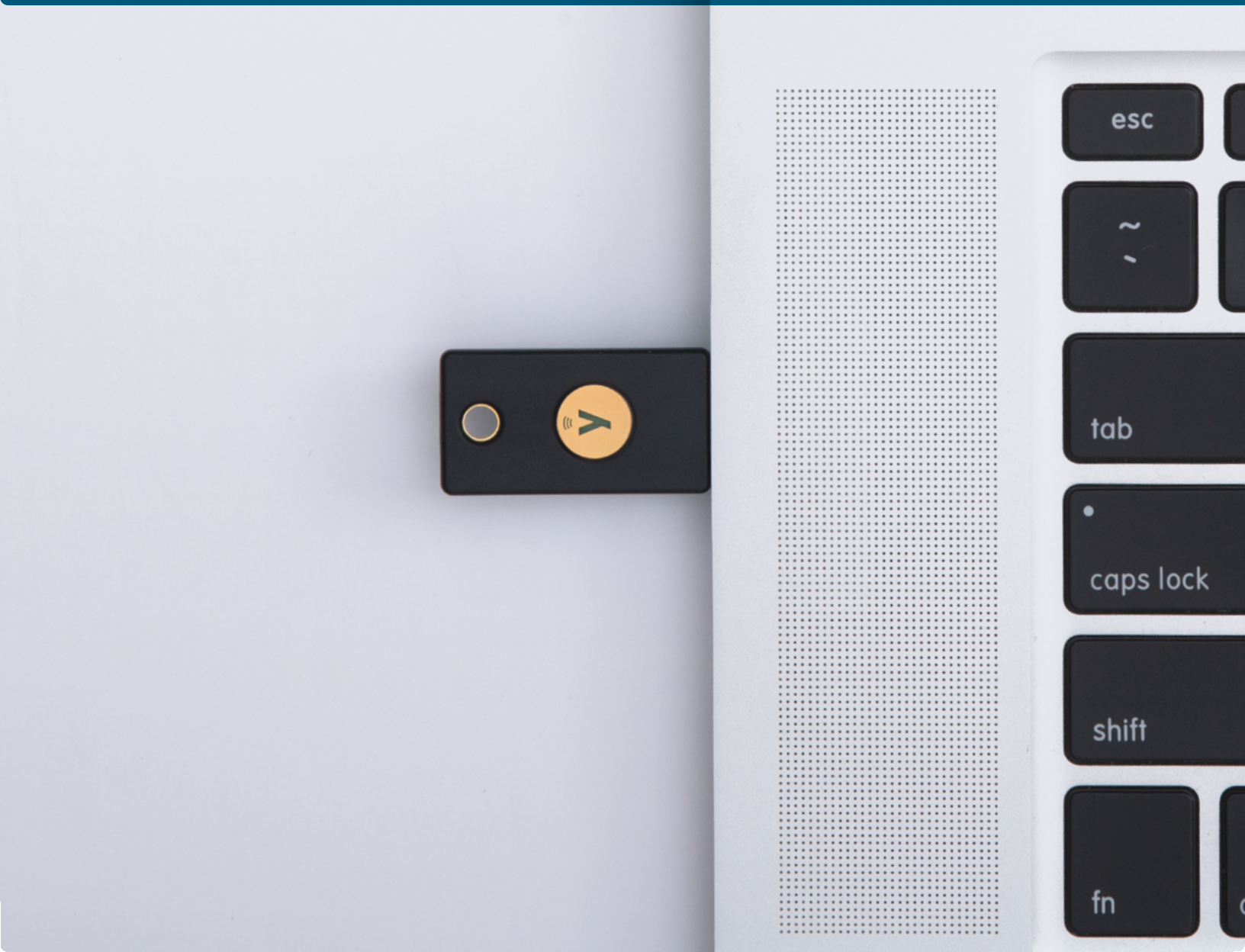
The YubiKey 5 Series
From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

The YubiKey 5 FIPS Series
From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS

YubiKey Bio Series - FIDO Edition
From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

> 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



Securing the manufacturing supply chain

Third-party access

IP and product integrity

Secure code signing

> "To proactively protect our supply chain, we work closely with key vendors to create dual encryption as both the vendor and Schneider Electric have YubiHSM modules built into the manufacturing process."
>
> –Chad Lloyd, Director of Cybersecurity Architecture for Energy Management, Schneider Electric

Manufacturing supply chains encompass the movement of physical goods and components from point to point, but also the other partnerships and business relationships that support the organization—including integrations often overlooked such as the use of third-party resources or code. When defined as such, an external supply chain covers *any* product or service that is used "as is" to develop a company's own product or service.

Securing the supply chain requires securing both the *access* and the *inputs* (physical component, software, or data) in the manufacturing process, to ensure the quality and integrity of the product and protect against loss of IP or production time.

Safeguarding third-party access

The Colonial Pipeline attack was just one in a long line of high profile supply chain breaches that have put manufacturers on edge. Shutdowns in production can be costly in many manufacturing scenarios, not to mention concerns over the loss of IP. A recent survey found that up to 97% of organizations have had a cybersecurity breach as the result of a weakness in the supply chain.[22] For example, stolen credentials from a third-party vendor are what ultimately caused the Target breach in 2013, which resulted in over $18.5 million in fines alone.[23]

The primary challenge for manufacturers 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. Manufacturing organizations must identify and authenticate every user who has access to inputs, IP, or to the systems involved in the supply chain. For example, KP Snacks' internal network was breached causing hackers to gain access to and hold sensitive files which escalated to supply chain disruptions.[24]

The YubiKey from Yubico provides modern phishing-resistant 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 IP handoffs.

Combined with YubiEnterprise Services (see below), you can offer an inexpensive and easy solution to improve supply chain security.

Ensuring the highest integrity of your product parts

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, since an assembly line should only consist of genuinely sourced products. 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.

The traditional approach to protect intellectual property (IP) and prevent counterfeiting in manufacturing involves the use of digital cryptographic keys and encryption. Cryptographic keys would be stored either in software, which is highly vulnerable, or a hardware security model (HSM). Unfortunately, traditional rack-mounted and card-based HSMs are large and expensive, making them impractical on the assembly floor, in caged data centers, or for IoT devices.

Securing external code and data

Manufacturing organizations that use software in their products, must have a method of secure code-signing for ingesting code or data from external sources. The need for secure code signing solutions has increased in the recent past, as demonstrated in the aftermath of the 2020 SolarWinds attack. In that attack, hackers exploited a breach in the SolarWinds code signing system, which allowed them to fraudulently distribute malicious code as legitimate updates to more than 18,000 installations of the SolarWinds Orion product across the world.[25]

Further, the strength of the cryptographic solution you're using is only as strong as your supply chain partner's attestation method. It's therefore vital that those partners can show a chain of custody for code that runs all the way back to the original developer's computer.

Safeguarding IP and product integrity with YubiHSM

As a result of having worked alongside several partners within the manufacturing sector responsible for large scale production of electronic components, Yubico has created the ultra-portable and low-cost YubiHSM 2, the world's smallest HSM that comes in a nano form factor. The YubiHSM 2 enables secure, tamper-resistant key storage and operations by preventing accidental copying and distribution of cryptographic keys, and preventing remote theft of keys stored in software. The YubiHSM 2 can be applied to any process where secrets and the authenticity of components needs to be managed, and where tampering needs to be prevented.

It can be easily deployed to a USB slot on servers, databases, robotic assembly lines, applications, and IoT devices.

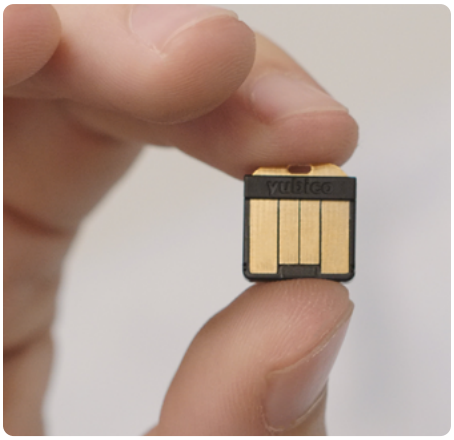
The YubiHSM 2 is being used to protect the manufacturing process by ensuring only certified programming stations can interface with the components, or to write digital signatures onto each component to ensure authenticity. In both scenarios, the added security of the YubiHSM 2 helps to maintain a company's reputation and gives them peace of mind that their products will work as expected even after they have left the manufacturing floor.

The YubiHSM 2 is ideally suited to safeguard the signing keys and certificates for signing code, helping support the secrets being shared within the supply chain. For organizations that need to meet the FIPS 140-2 requirements, they have the option of the FIPS 140-2, Level 3 validated YubiHSM 2 FIPS to ensure the highest levels of data protection.

It's important to note that the cryptographic key used to sign and/or certify components is never exposed outside of the YubiHSM 2 hardware, ensuring a high level of security. To illustrate this point with an example, even if a remote attacker is able to compromise a network or the computer connected to it, there are still no obvious attack vectors. On the other hand, if the same attacker is able to gain full underlying access to a software equivalent, they might be able to at least run analysis on the memory or local files for potential weaknesses or patterns.

The YubiHSM 2

enables secure, tamper-resistant key storage and operations by preventing accidental copying and distribution of cryptographic keys, and preventing remote theft of keys stored in software.

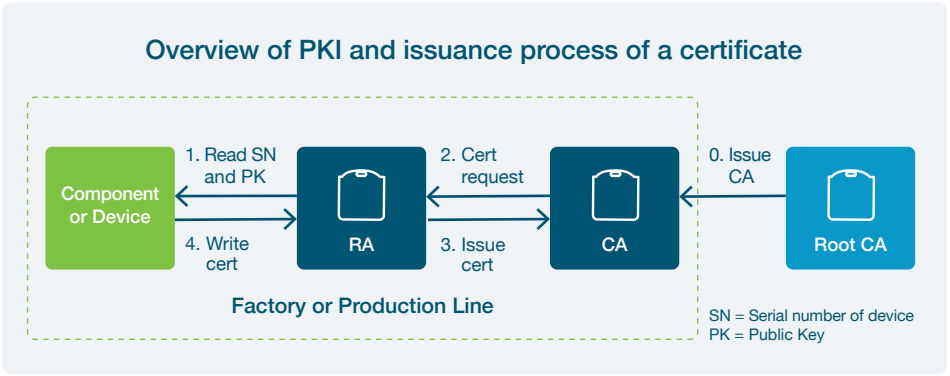


The YubiHSM 2

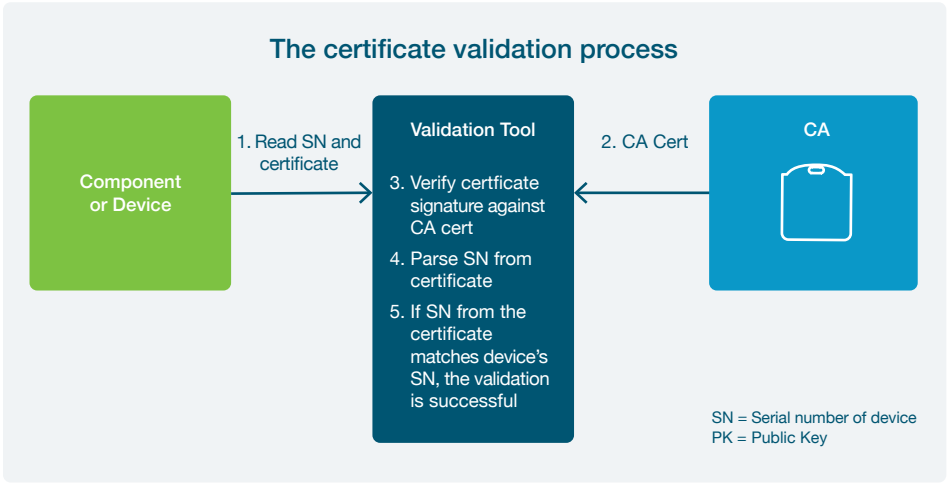
is being used to protect the manufacturing process by ensuring only certified programming stations can interface with the components, or to write digital signatures onto each component to ensure authenticity.

Supporting Public Key Infrastructure (PKI) environments

Since the YubiHSM 2 is designed to store cryptographic keys, it is ideally suited to protect PKI infrastructure and its network of cryptographic keys. The issuance process of certificates using a PKI based on the YubiHSM 2 for manufacturing is illustrated as follows:



In this diagram, the Root Certificate Authority (Root CA) uses a YubiHSM 2 to house its key-pair (i.e. both its Private and Public Keys) in addition to its certificate, either on-site or at an off-site data center. On the production line, a Certificate Authority (CA) can be deployed and configured with a certificate that has been signed by the Root CA as a delegate, and with this key-pair and certificate, all subsequent credentials may be signed and also protected by a YubiHSM 2. These additional credentials are issued by a Registration Authority (RA) that, in turn, has had its certificate signed by the CA. Ultimately, the component certificates can then be used to check the authenticity of each component, product or device being produced, as shown in the diagram below.



In practical application, this enables manufacturers to verify the authenticity of each component being produced. The collection of encrypted serial numbers to the electronic control unit (ECU) can also support testing and can be used for audit tracking.

CASE STUDIES

Securing the systems and supply chain at Schneider Electric

Schneider Electric is a leader in the digital transformation of energy management and automation, manufacturing electrical parts and power management systems, including a Supervisory Control and Data Acquisition (SCADA) system used for the remote management of critical infrastructure (e.g. data centers, hospitals, oil and gas).

The YubiKey enabled Schneider Electric to integrate MFA into an isolated system without the reliance on the Internet or less-secure SMS-based authentication, streamlining authentication for shift changes. The YubiKey is also being used in control situations where supervisory override actions are required. Modern MFA through YubiKeys was a part of the process to successfully achieve IEC-62443 SL2 certification.

“Safety and security are paramount at Schneider Electric and are reflected in everything we do,” notes Chad Lloyd, Director of Cybersecurity Architecture for Energy Management at Schneider Electric. “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 now a point of differentiation for Schneider Electric,” said Lloyd.

In addition to the integration of YubiKeys within its SCADA systems used by clients in critical infrastructure, Schneider Electric has taken steps to ensure the quality and integrity of its supply chain by leveraging the YubiHSM hardware security module to integrate with key suppliers in the manufacturing process. The high-security cryptographic hardware security of YubiHSM helps support the rigorous testing and manufacturing processes of all genuine Schneider Electric products.

The nano form factor of YubiHSM was critical to support flexible deployment and use across manufacturing floors, requiring only a simple USB port for connection.

A portable root of trust for EasyMile to secure autonomous vehicles

EasyMile develops software solutions for its fleet of autonomous vehicles (mainly those used to transport people and goods) to the maximum security standards. Already users of Yubico’s YubiKeys for securing administrator accounts, EasyMile turned to Yubico to help target-harden its PKI infrastructure. EasyMile quickly and easily rolled out YubiHSM 2 to secure the PKI X.509 CA infrastructure used to secure its ecosystem of autonomous vehicles. The result? A label of trust for its security certificate ecosystem.

YubiHSM also provides a portable root of trust in global manufacturing. For example, after developing its own internal PKI, a Fortune 500 company came to Yubico for a more cost effective solution to maintain product integrity. This brand leveraged YubiHSM to digitally sign and certify each component being manufactured across various facilities to ensure product authenticity and integrity at the end of the respective production lines.

Yubico offers simple procurement and distribution of 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.

YubiEnterprise Subscription

YubiEnterprise Delivery

With YubiEnterprise Subscription, organizations with 500 users or more can greatly simplify the acquisition and roll out of phishing-resistant authentication. Organizations can move authentication spend from CAPEX to a predictable OPEX model, and ensure security is always covered as business needs evolve, and experience benefits such as 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 automatically entitled to access the Console, a web-based interface that helps organizations easily view orders, shipments, inventory status and a wide range of other information that helps with enterprise planning, and 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 across 49 countries. Additionally, new YubiEnterprise offerings and additional enterprise capabilities will be designed explicitly for Subscription customers.

YubiHSM 2 Procurement

YubiHSM 2 is one of the smallest and most affordable HSMs on the market, ideally suited across a wide-range of use cases and all types of organizations and industries, making it simple and quick to purchase, procure, and deploy. With its small footprint, YubiHSM 2 provides an accessible solution to strong, phishing-resistant security for a variety of manufacturing and supply chain customers all across the globe.

Summary

Secure the supply chain and safeguard third-party access, IP, and product integrity by leveraging the YubiKey and YubiHSM 2 to ensure highest-assurance security.

Modern manufacturing organizations require modern solutions to drive security and efficiency, and to minimize costs. At the same time, such solutions must be durable and easy-to-use on the production floor—ideally, these solutions will also ease some of the current frustrations with legacy authentication that are contributors to costly non-productive overhead.

The cyber attacks of the recent past have underscored the need to secure the production line and the supply chain against disruption. As a result, leading manufacturing organizations are deploying passwordless authentication and ultra-small HSM to protect against modern cyber threats.

Being proactive and securing your data and products with the right security solution can help you mitigate attacks, minimize attack penetration rates, protect corporate secrets, and provide greater transparency and control over the inputs into the manufacturing process.

The YubiKey and YubiHSM 2 are secure, portable, easy-to-use solutions designed to meet manufacturing organizations where they are, helping to seamlessly support legacy infrastructure as well as modern, cloud-based systems.

Sources

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

[2] Emerson, How Manufacturers Can Achieve Top Quartile Performance, (Accessed January 31, 2022)

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

[4] Roger Johnson, Low Profit Margins—The Perils and Potential in Manufacturing, (July 20, 2018)

[5] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021)

[6] Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom, (May 19, 2021)

[7] Emerson, How Manufacturers Can Achieve Top Quartile Performance, (Accessed January 31, 2022)

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

[9] Department of Homeland Security, Ratification of Security Directive, (July 19, 2021); Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators (July 20, 2021)

[10] NIST, Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028, (July 19, 2021)

[11] Jonny Evans, Apple: It's time to bolster supply chain security, (August 26, 2021); The White House, FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity, (August 25, 2021)

[12] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[13] Varonis, 2021 Data Risk Report, Manufacturing, (Accessed February 1, 2022)

[14] IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021); Verizon, 2021 DBIR Master's Guide, (Accessed May 18, 2021)

[15] Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé, (November 1, 2017)

[16] Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests, (Aug 2019)

[17] Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (Accessed September 14, 2021)

[18] Varonis, 2021 Data Risk Report, Manufacturing, (Accessed February 1, 2022)

[19] Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020)

[20] 451 Research, 2021 Yubico and 451 Research Study, (April 2021)

[21] Kurt Thomas, Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking, (May 17, 2019)

[22] BlueVoyant, Managing Cyber Risk Across the Extended Vendor Ecosystem 2021, (Accessed February 2, 2021)

[23] Reuters, Target Settles 2013 Hacked Customer Data Breach for $18.5 Million, (May 24, 2017)

[24] Reuters, Hackers Hold Hula Hoops Hostage in cyber-raid on Britain's KP Snacks, (February 3, 2022)

[25] SEC, Form 8-K SolarWinds Corporation, (December 14, 2020)

yubico

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 is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.