yubico

WHITE PAPER

Securing the world's critical infrastructure against modern cyber threats

Safeguard IT/OT systems and the supply chain with Zero Trust using phishing-resistant MFA and hardware-backed security

Contents

The pressing need to secure critical infrastructure

Across the globe, an increasing number of malicious actors are targeting critical infrastructure[1] and the supply chain with the intention to **disrupt operations**. Nation-state targeting of critical infrastructure has doubled, accounting for 40% of targeted attacks from July 2021 to June 2022.[2] Across discrete manufacturing, process industries and critical infrastructure, there has been a 150% global increase in attacks impacting operational technology (OT) resulting in production outages, equipment damage and the potential for **impact to human lives**.[3]

Attacks against critical infrastructure can be costly ($4.88M USD global average data breach cost[4]), but of primary concern is the debilitating impact these attacks can have on a **nation's security, economic security, public health and/or safety which can pose a physical threat to human lives**.[5]

40%

of targeted attacks are towards critical infrastructure[2]

150%

global increase in attacks impacting operational technologies (OT)[3]

$4.88 million

global average data breach cost[4]

Vital sectors and their impact

Chemical

Banking and Financial Services

Food and Agriculture

Information Technology

Healthcare and Public Health

Government Facilities
National, federal, state, local, tribunal

Commercial Facilities

Communications

Nuclear Reactors, Materials, and Waste

Energy

Transportation Systems

Water and Waste Systems

Emergency Services

Defense Industrial Base
Companies and subtractors supply materials, services and facilities to national militaries

Dams
Critical water retention and control services

Critical Manufacturing
Primary metals, machinery, electrical equipment, transportation

Although definitions of critical infrastructure can vary across countries and regions, the sectors listed are all considered vital to the continuity of society, even if they are not specifically called out by local law or regulation.

45%

of fuel distribution for the East Coast of the United States shut down from **Colonial Pipeline attack of 2021**[6]

Attacks have...

- targeted a medical holding group in the US, knocking out health systems across four states,[11]
- disrupted air travel,[12]
- wiped out four months of government emails in Sri Lanka,[13]
- shut down meat plants across the US and Australia,[14]
- targeted a port operator in Australia,[18]
- taken the Polish stock exchange offline,[16] and
- attempted to poison the water supply in Florida.[17]

Attacks against OT are not just costly, they **directly impact national security and human lives**.

Critical infrastructure organizations face mounting pressure **to reduce risk and to adopt a Zero Trust strategy** that sets identity as the new perimeter.

Following the high-profile Colonial Pipeline attack of 2021, an attack that **shut down 45% of fuel distribution** for the East Coast of the United States,[6] recent notable attacks on the energy sector include attacks against gas stations in Canada[7] and Germany[8] and attacks against Ukraine's energy grid.[9] In addition, attacks on Ukraine's law enforcement agencies[10] have demonstrated how traditional warfare and cyberwarfare can be combined.

Threat actors are increasingly targeting **OT systems and Internet of Things (IoT) devices**[18], leveraging both ransomware[19] and credential stealing campaigns.[20] In fact, 74% of data breaches can be traced back to the human element including the use of **stolen credentials**, privilege misuse and phishing. [21]

Threat actors also seek to **exploit supply chains**—all the products, services, software and code that an organization relies upon. Gartner predicts that by 2025, 45% of organizations will experience an attack on their software supply chains, a three-fold increase over 2021.[22] Just recently, the exploit of a MOVEit zero-day vulnerability caused a cascade breach to 140 other organizations, including 16 in the public sector.[23]

While critical infrastructure sectors function in very different ways, all face the same reality: **perimeter-based security is no longer effective**. Further, critical infrastructure organizations are often uniquely vulnerable, with highly complex infrastructure, legacy systems and convergence of information technology (IT) and OT systems. As a result, critical infrastructure organizations face mounting pressure to reduce risk and to adopt a **Zero Trust strategy that sets identity as the new perimeter** in order to combat the cascading and devastating impact that attacks can have on vital business operations.

In this whitepaper, we'll demonstrate how to accelerate the journey to Zero Trust with modern, phishing-resistant multi-factor authentication (MFA) to secure identities and corporate secrets, and modern cryptographic protection to secure servers, applications and computing devices.

> “It is important to note that not all MFA solutions provide equal protection against authentication attacks, and there are critical implementation details that can impact the security and usability of an MFA deployment.”
>
> **Recommended Best Practices for Administrators: Identity and Access Management, Enduring Security Framework**[24]

10-24%

attack penetration rate for mobile authentication[25]

94%

of organizations have been **victims of phishing**[26]

$1 million

per year **cost for password resets** alone[27]

Not all MFA is created equal

There is no question that cyber attacks are accelerating both in scope and intensity. As a result, critical infrastructure organizations need to evaluate which forms of MFA provide the greatest protection from attack.

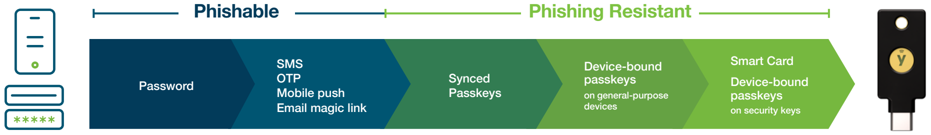
Legacy forms of MFA such as SMS, mobile authentication and one-time passcodes (OTP) are susceptible to account takeovers from phishing, attacker-in-the-middle attacks, account takeovers and SIM swaps at a penetration rate of 10-24%.[28] In fact, the risk of SMS interception is so high that the US National Institute of Standards and Technology (NIST) called for SMS to be deprecated as a method of authentication.[29]

Further, the **MFA strategy you choose can deliver a vastly different ROI** in terms of cost, user experience and coverage. In truth, legacy authentication carries many hidden governance and support costs around setting and managing password policies at scale, productivity costs associated with forgotten passwords, account lockouts and time-consuming workflows to generate and enter OTP/TOTP/push app codes, and of course additional costs associated with risk. Moreover, there are always gaps where mobile authentication does not work or is not an option—where users lack devices, where availability or mobile-restrictions may apply, as well as spark environments, among other scenarios.

MFA investments must provide organizations with protection that evolves alongside risk and compliance requirements. To be future-proofed, the MFA investment should reflect the growing regulatory requirement for phishing-resistant MFA, the need to implement Zero Trust, and modern login flows such as passwordless.

What is phishing-resistant MFA?

Globally recognized for promoting equitable standards, NIST defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4[30] as “the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an impostor relying party without reliance on the vigilance of the subscriber.”



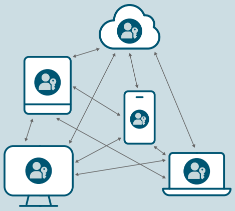
Phishing-resistant MFA processes rely on cryptographic verification between devices or between the device and a domain, making them immune to attempts to compromise or subvert the authentication process. Currently, two forms of authentication meet the mark for phishing-resistant MFA: **PIV/Smart Card** and the modern **FIDO2/WebAuthn** authentication standard.

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

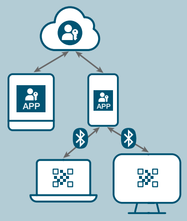
Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

Synced passkeys



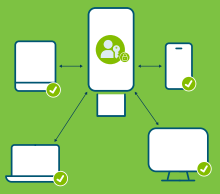
- Lives on a smartphone, tablet, etc.
- Copyable/shareable
- Consumer grade; lower security and compliance assurance

App-managed passkeys



- Lives in the authenticator app which can decide where the credential is shared; cross-device sign-in via bluetooth using a QR code
- Middle ground option for enterprises; but less secure than hardware-bound

Hardware-bound passkeys



- Lives on a security key or other hardware separate from everyday devices
- Best option for enterprises; meet higher security and compliance assurance
- Only passkeys that meet Authenticator Assurance Level 3 (AAL3)

What is high-assurance authentication?

This whitepaper has posited that not all MFA is created equal, and NIST SP 800-63[31] articulates this through the creation of authentication assurance levels (AALs), which classify the relative strength of authenticators.

While AALs are a fundamental concept for US federal agencies and the companies that work with them, other countries rely on similar maturity levels, including Australia's Essential Eight Maturity Model (E8MM)[32] and the EU's electronic Identification, Authentication and Trust Services Regulation (eIDAS),[33] a set of baseline mitigation strategies provided for organizations to mitigate the potential impact of cyber security incidents.

While any form of MFA will provide greater security than a password (AAL1), an authenticator at AAL3 provides very high confidence that someone logging onto your system can prove, by possession, who they are claiming to be, reducing the threat of compromise and attack from phishing.

AAL1	AAL2	AAL3
Single-factor authentication e.g., username and password	**Two-step authentication** e.g., 2FA, synced passkeys, device-bound passkeys on general purpose devices	**Hardware-based multi-factor authentication** e.g., device-bound passkeys on hardware security keys
• Low security assurance • Highly vulnerable to phishing • Puts enterprises at risk	• Phishing-resistant 2FA/MFA • Stronger security than a password but vulnerable to attacks • More enterprise-ready but leaves gaps in operational efficiency and audit/compliance requirements	• Phishing-resistant MFA • Strongest security and highest assurance • Addresses enterprise security, operational efficiency and audit/compliance requirements • Supports FIDO and Smart Card/PIV • FIPS 140-2 validated

Plan for a passwordless future

Passwordless authentication is any form of authentication that doesn't require the user to provide a password, and includes Smart Card/PIV and FIDO2/WebAuthn, two methods generally acknowledged as meeting the ideals of Zero Trust.

Traditional Smart Cards/PIV do offer high security, but generally require high capital expenditure (CapEx) for Smart Card readers and physical cards, in addition to backend management platforms. Further, many organizations that deploy PIV face challenges around authentication where **PIV is not available or practical**—access to cloud services, mobile devices, air-gapped/isolated networks, contractors, partners and third-parties, just to name a few.

79%

of critical infrastructure organizations lack a Zero Trust strategy[34]

Cultivating phishing-resistant users

The only effective approach to remove phishing from an organization's threat landscape is to ensure that every user within the organization becomes phishing-resistant—and that resistance must move with the users no matter how they work, across devices, platforms and systems. Deploying phishing-resistant authentication across the entire user lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

Due to this, many industries are moving toward a passwordless login flow leveraging modern authentication standards such as FIDO2/WebAuthn that work well with the cloud but don't necessitate a backend management system, ultimately resulting in lower ongoing costs even as enterprises scale up.

FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.

Accelerate Zero Trust with phishing-resistant MFA

Globally, critical infrastructure organizations recognize the insufficiency of traditional perimeter-based security models in reducing risk or supporting business resiliency and continuity. Best practice security is shifting to Zero Trust, a strategy that removes 'implicit trust' to better protect sensitive data, systems or intellectual property.

A Zero Trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be verified and authenticated before access is granted. A Zero Trust strategy considers five distinct pillars: identity, devices, networks, applications and workloads, and data.[35]

Identity is a core building block of Zero Trust, laying the groundwork for a user trust framework and the ideal starting point to jumpstart the journey toward a workable, effective strategy.

Identity will include considerations for:

Authentication support	Access management	Risk assessments	Identity stores
Phishing-resistant MFA, attestation and passwordless flow by the authenticator	Phishing-resistant MFA, attestation and passwordless flow by the authenticator	Use real-time signals for continuous risk assessments, e.g. to support step-up authentication	Use integrated identity stores to manage identity information across cloud and on-premise environments

The Zero Trust Maturity Model (ZTMM)[36] developed by CISA, building on the global NIST guidance,[37] recognizes that not all forms of MFA are created equal, requiring stronger forms of MFA be adopted for each subsequent stage, progressing toward the exclusive use of phishing-resistant MFA.

Global regulations reinforce the need for Zero Trust and phishing-resistant MFA

Critical infrastructure sectors around the world are subject to an ever-expanding set of regulatory requirements that support the shift to Zero Trust and phishing-resistant MFA.

Globally

The **Payment Card Industry Data Security Standard** (PCI DSS v4.0) has issued new requirements for phishing-resistant MFA for access to the card-holder data environment.[38]

Joint guidance on **Identifying and Mitigating Living Off the Land Techniques** was co-authored by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), U.S. Department of Energy (DOE), U.S. Environmental Protection Agency (EPA), U.S. Transportation Security Administration (TSA), Australian Signals Directorate's (ASD's), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE), United Kingdom National Cyber Security Centre (NCSC-UK), and New Zealand National Cyber Security Centre (NCSC-NZ) regarding common gaps in cyber defense capabilities. One of the recommendations is to enable phishing-resistant MFA by default to protect critical infrastructure and software manufacturers.[39]

US

The White House laid the groundwork for Zero Trust in 2021 with **Executive Order (EO) 14028**, "Improving the Nation's Cybersecurity,"[40] Office of Management and Budget Memo 22-09,[41] and **National Security Memorandum (NSM)-8**[42] for the Department of Defense (DoD). As organizations working across the public/private divide, critical infrastructure sectors will be held to account for adopting phishing-resistant MFA internally as part of any collaborations with joint venture, upstream, midstream or down-stream partners.

The Cyber Safety Review Board (CSRB), established as part of EO 14028 to make recommendations across the public and private sectors, recommends "organizations urgently implement improved access controls and authentication methods and transition away from voice and SMS-based MFA; those methods are particularly vulnerable. Instead, organizations should adopt easy-to-use, secure-by-default, passwordless solutions such as Fast IDentity Online (FIDO)2-compliant, phishing-resistant MFA methods."[43]

For critical infrastructure providers in the US, Department of Homeland Security's Transportation Security Administration (TSA) Security Directives 2021-01[44] and 2021-02[45] place new requirements on the **pipeline sector**, including the requirement for a Zero Trust policy and Security Directive 2022-01, which eliminates domain trust between IT and OT systems and requires the use of MFA for **rail operators**.[46] The North American Electric Reliability Corporation Critical Infrastructure Protection **(NERC CIP)** also creates enforceable standards, including the need to use MFA for all remote access sessions.[47] For OT-dependent organizations, Zero Trust can help simplify the implementation of standards such as **ISA/IEC-62443**[48] and **ISO 27001**.[49]

The Ensuring Security Framework (ESF), a public-private partnership designed to address risks against critical infrastructure, further advocates the use of phishing-resistant MFA.[50] US **FTC standards**, which govern almost every area of commerce, also require phishing-resistant MFA for all employees, contractors and affiliates.[51]

EU

The revised Network and Information Security (NIS) 2 Directive provides an expanded scope of requirements to a significantly expanded number of critical infrastructure providers,[52] including the adoption of "cyber hygiene practices, such as zero-trust principles" and risk-management measures that must include MFA.[53] Member States have until October 2024 to transpose these measures into national law.

Australia

The Security of Critical Infrastructure Act (SOCI Act) requires entities to minimize or eliminate cyber risks to digital systems, computers, datasets or networks that underpin critical infrastructure systems, including improper access.[54] Although guidance in the SOCI Act is not specific, the Essential Eight Maturity Model (E8MM) guidelines referenced by various critical infrastructure sector frameworks,[55] mandates the use of phishing-resistant MFA at maturity level two and three and excludes all legacy forms of MFA. The Australian Energy Sector Cyber Security Framework (AESCSF)[56] leverages the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and speaks to the importance of Zero Trust.[57] The Australian government continues to lead on cybersecurity efforts toward phishing-resistance for all citizens and businesses.[58]

Germany

The IT Security Act 2.0 and the new **BSI Ordinance Determining Critical Infrastructures** (BSI-KritisV) ordinance expands covered entities, requires "state of the art" protection measures,[59] and requires operators to obtain a declaration that ensures the authenticity of critical components.[60] In critical infrastructure, this represents a regulatory push for both modern MFA as well as the need to protect the supply chain, which will be addressed later in this whitepaper.

Japan and Singapore

In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) created **Common Standards for Cybersecurity Measures for Government Agencies**, suggesting choosing authentication based on an assessment of risk.[21] For critical infrastructure, guidance also suggests the use of MFA.[62] The NISC guideline steers toward the use of stronger authentication, specifically mentioning FIDO2/WebAuthn.[63]

In Singapore, regulations supporting Zero Trust and MFA are evolving, currently a requirement for critical infrastructure under the **Cybersecurity Act 2018.**[64] In October 2023, The Monetary Authority of Singapore's (MAS) Cyber Security Advisory Panel (CSAP) issued support for consumer use of MFA and passwordless authentication.[65]

Protecting all users in the enterprise

The YubiKey is uniquely designed to support all use cases in critical infrastructure, including:

- Privileged access
- Mobile restricted
- Shared workstation
- Remote workforce
- Office workers
- 3rd party access
- End customers

YubiKey offers high-assurance, phishing-resistant MFA

Cultivate phishing-resistant users

Yubico offers the YubiKey, a hardware security key that offers highest-assurance, phishing-resistant MFA supporting both FIDO2/WebAuthn and Smart Card/PIV authentication to ensure the highest protection against phishing-driven credential-based attacks.

The YubiKey is designed to meet you where you are on your authentication journey, offering multi-protocol support that also extends to FIDO U2F, OTP/TOTP and OpenPGP. For the most regulated industries in the US, the YubiKey FIPS Series is 140-2 validated, DOD-approved[66] and meets the highest AAL3 level.

Hardware security keys such as the YubiKey are an ideal option for **IT, OT and ICS access** because they don't require additional hardware, software, external power, batteries or a network connection—a single key secures hundreds of products, services and applications, including leading identity and access management (IAM) platforms, privileged access management (PAM) solutions and cloud services, with secrets never shared between services.

As a portable hardware root of trust, the YubiKey is proven to **reduce risk against phishing attacks and account takeovers by 99.9%**[67] and serves as a user-friendly, cost-effective enabler of a Zero Trust security architecture. When you're ready, the YubiKey can also help bridge to modern login flows such as passwordless.

Strong security	Fast	Reduce costs	High return	Durable
Reduce risk by	Decrease time to authenticate by	Reduce support tickets by	Experience ROI of	IP68 certified, dust-proof, crush-resistant and water-resistant
99.9%	>4x	75%	203%	

By simply plugging a YubiKey into a laptop or tapping it against a smartphone to authenticate, YubiKeys help organizations create phishing-resistant users by using the highest-assurance passkeys in the market. The passkeys that reside in YubiKeys can be used to register the user and secure the other passkeys they use across devices and services. In other words, YubiKeys can be used to secure other forms of phishing-resistant MFA used within organizations to create phishing-resistant users, who then ultimately create phishing-resistance that can't be circumvented.

Protect the supply chain with hardware-backed security

Every critical infrastructure organization relies on a supply chain—inputs into manufacturing, hardware and IoT devices, software, code that someone else has developed, or services used. Supply chain risks include compromised third-party access or compromised software, hardware or physical inputs, counterfeit inputs, embedded malware, breached intellectual property (IP) or poor supplier practices that interrupt business operations.[68]

The **supply chain is essential to the delivery of business operations**—if disrupted, it can have an impact on a nation's security, economic security, public health and/or safety.

With digital transformation, data and resources are no longer protected behind a network perimeter. Further, the supply chain disruptions of the past several years have resulted in larger supply chain networks to create greater resiliency and flexibility to withstand potential impacts. Altogether, these changes have increased risks to IT, OT and ICS systems—risks that are being exploited at an increased pace.

> “Nation state targeting of IT service providers might enable the threat actors to exploit other organizations of interest by taking advantage of trust and access granted to these supply chain providers.”
>
> **Microsoft Digital Defense Report 2020[69]**

The software supply chain gained attention in 2020 when hackers exploited a breach in the SolarWinds code signing system which allowed them to inject and distribute malicious code disguised as legitimate updates to more than 18,000 installations of the SolarWinds Orion product across the world.[70] This example was just one impetus behind the increased focus on software supply chain security as part of EO 14028 and NSM-8.

The most important thing security professionals can do to secure any environment is to know what they have, where it is, how it’s configured, and what it depends upon. In short, it is imperative to have an inventory and a **dependency map for your systems and services**. While this won’t stop an attacker, it is required to understand what you’re protecting, who and what can access it, and when something does go wrong, what the “blast radius” is.

To protect the integrity, availability and business continuity of inputs, IP and systems in the supply chain, it is integral that organizations identify and verify every user, device, application and transaction before access is granted—in essence, to apply **Zero Trust principles across the supply chain**. Securing the supply chain is about making explicit trust decisions for each of these products, services and interactions, including:

Third-party access to systems, code or IP	Software supply chain	IP and product integrity
YubiKey	YubiKey + YubiHSM 2	YubiHSM 2

When it comes to ensuring the **integrity of IP and product parts**, there is often a gap in security along the supply chain. Closing the gap requires creating a common channel of secure “communication” between organizations and their supply chain partners—communication that leverages cryptographic keypairs, certificates and digital signatures. A hardware security module (HSM) enables this “communication” between devices, servers and applications by storing critical cryptographic artifacts securely on its trusted platform module (TPM), that can then be used in subsequent operations to securely exchange data, code or other information.

HSM use cases include ensuring only certified programming stations can interface with the intended components, by writing digital signatures onto each component and later validating to ensure authenticity, and to protect the signing keys and certificates in any code signing software system. Traditional methods of storing cryptographic keys in software are highly vulnerable to a variety of attack vectors that are not possible or much more difficult to perpetrate against hardware-based storage.

The **YubiHSM 2** is an ultra-small, affordable solution to securely generate, store and protect both cryptographic keypairs and X.509 certificates on secure, purpose-built hardware. The YubiHSM 2 is also available as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution with the same capabilities. Both solutions ensure uncompromised cryptographic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

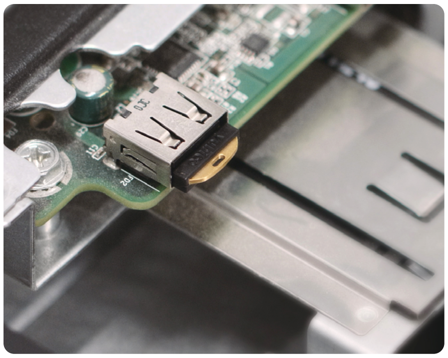
The YubiHSM 2 FIPS can be applied to any process where secrets and the authenticity of components needs to be managed, and where tampering needs to be prevented, in accordance with NSA guidance on how to harden on-premise systems.[71] Further, the YubiHSM 2 can be deployed to support Public Key Infrastructure (PKI) environments to support the **code signing process** and protect against SolarWinds-type supply chain attacks.

The YubiKey

provides secure, phishing-resistant MFA for **third-party access** and **secure code signing capabilities** to protect the software supply chain. To support code signing, and to ensure the integrity of IP and product parts, this involves the use of digital cryptographic signing keys and encryption.

The YubiHSM 2

is an ultra-small, affordable solution to securely generate, store and protect both cryptographic keypairs and X.509 certificates on secure, purpose-built hardware.



The YubiHSM 2 can be easily deployed to any USB slot on servers, databases, robotic assembly lines, applications and IoT devices.

YubiHSM 2 can protect and be easily deployed to any:				
USB slot on servers	Databases	Robotic assembly lines	Applications	IoT devices in the field

Deploy highest-assurance security at scale

To protect against the growing number of cyber threats and shifting requirements and regulations, critical infrastructure organizations need a modern solution to provide phishing-resistant MFA at scale and across a wide variety of complex authentication scenarios.

Yubico solutions are designed to meet you where you are on your cybersecurity journey, paving the way to a modern authentication infrastructure and jumpstarting your journey to Zero Trust.

We have made it easy to safeguard your IT and OT systems with the YubiKey and YubiHSM 2. We offer a simple 6 Step Best Practice Deployment Guide to get started with phishing-resistant MFA for Zero Trust.

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

To remove all the guesswork out of planning, purchasing and delivery, Yubico offers YubiKey as a Service, a service-based and affordable model to simplify how organizations procure, upgrade and support YubiKeys, as well as streamlined global distribution to remote and in-office locations through YubiEnterprise Delivery and trusted channel partners.

If you want a closer partnership on any of the six steps of this plan, Yubico's Professional Services team is here to help.

Safeguard your IT and OT ecosystem with Yubico

YubiKey and YubiHSM 2 in action

These are real stories of global critical infrastructure organizations and how they've addressed security at scale with the help of Yubico solutions.

Schneider Electric enhances global supply chain security with YubiHSM 2

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.

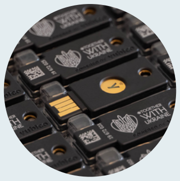
Lloyd was tasked with a challenge to integrate multi-factor authentication (MFA) on an isolated system—without the use of the Internet or traditional methods such as SMS. With the YubiKey, Schneider Electric is able to meet its requirement for MFA and to ensure only authenticated users can gain access 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 third-party 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.

> “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 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

READ CASE STUDY yubi.co/SchneiderElectric



> “The YubiKeys significantly increased the security and also made access across many IT systems faster and easier, which has been a tremendous relief to our employees. We believe YubiKeys are as important for our cyber defense as the bullet proof vests that are protecting the soldiers and others that are on the front lines of the ground war.”
>
> **Anonymous** | Ukraine energy plant

Protecting critical infrastructure in Ukraine

The Russian invasion of Ukraine is a battle in both the physical and the digital world. On both sides, cyberwarfare plays a more critical role than in any other war in human history, with the biggest attack vector and threat being weak login credentials.

In March 2022, Yubico got a request from authentication partner Hideez to help to protect critical infrastructure in Ukraine. When the war started, much of the Hideez team decided to stay in Ukraine to lend their expertise, products and services to the most targeted Ukraine entities and IT systems. With a donation of 20,000 YubiKeys, a dozen government agencies and critical infrastructure providers were able to quickly secure themselves against rising rates of attacks.

“Since the war began, we have experienced a massive increase in phishing attacks. To mitigate this risk, our organization required us to change passwords every day, which did not provide sufficient security and was time consuming as well as an added stress to employees working in a war zone. We needed something that was not only more secure, but that also worked seamlessly across a range of systems and devices. We also needed a tool that worked from locations where internet and cell phone connectivity are not stable. Additionally, because of the advanced types of phishing, and man-in-the-middle attacks, we simply could not rely on legacy or mobile-based authentication.

One of the critical infrastructure organizations who benefited from the deployment was Naftogaz, a government-owned group of oil and gas companies. Naftogaz-Bezreka, the security group responsible for securing Naftogaz, was already keen to deploy the YubiKey, but it was not until the invasion and Yubico’s donation that the deployment could be accelerated. The keys are used to secure authentication for logging into Windows, workstations and other applications like Microsoft Office 365. The YubiKeys offer enhanced protection for users who require privileged access, as well as enabling safe login for remote workplaces.

> “The YubiKeys significantly increased the security and also made access across many IT systems faster and easier, which has been a tremendous relief to our employees. We believe YubiKeys are as important for our cyber defense as the bullet proof vests that are protecting the soldiers and others that are on the front lines of the ground war.”

> **Oleksandr Tarasov** | Head of Security Controls | Security Operation Center, Naftogaz-Bezreka

READ CASE STUDY yubi.co/Naftogaz

> 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

Securing critical infrastructure at an Asia-Pacific energy company

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 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—Smart Cards—which require specific drivers and Smart Card 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 relies, the organization chose the YubiKey to secure all users who access the operational environment—offering a balance of security. Further, the flexibility of YubiEnterprise Subscription helps guarantee the highest level of protection into the future.

> In our world, critical infrastructure is a high priority target for many nation states, so there will always be malicious actors looking to get in. In a worst case scenario, there could be a catastrophic failure of the primary plant. Some of those things can take years to replace."
>
> **OT Security Specialist** | Anonymous State-Owned Energy Company

READ CASE STUDY yubi.co/EnergyCo

> “I When it comes to security, Yubico is a no brainer.”
>
> **Alexandre Hamez** |
> Tech Lead | EasyMile

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 US, 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

Contact us
yubi.co/contact

Learn more
yubi.co/bpg-zerotrust

Sources

[1] OECD, State of play in the governance of critical infrastructure resilience, (Accessed Oct 24, 2023)

[2] Microsoft, Microsoft Digital Defense Report 2022, (Nov 2, 2022)

[3] Waterfall, 2023 Threat report - OT Cyberattacks with Physical Consequences, (May 4, 2023)

[4] IBM, 2024 Cost of Data Breach Report, (July 2024)

[5] CISA, Critical Infrastructure Sectors, (Accessed Oct 24, 2023)

[6] Stephanie Kelly and Jessica Resnick-ault, One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators, (June 9, 2021)

[7] Graham Cluley, Over 1500 gas stations disrupted in Canada, after energy giant hacked, (June 29, 2023)

[8] Bill Toulas, German petrol supply firm Oiltanking paralyzed by cyber attack, (February 1, 2022)

[9] CISA, Cyber-Attack Against Ukrainian Critical Infrastructure, (July 20, 2021)

[10] Tom Balmforth and James Pearson, Exclusive: Russian hackers seek war crimes evidence, Ukraine cyber chief says, (September 22, 2023)

[11] Steve Zurier, Rhysida claims responsibility for ransomware attacks on Prospect Medical Holdings, (August 28, 2023)

[12] The Canadian Press, Sunwing technical issue continues to disrupt travel plans for thousands of passengers, (April 19, 2022)

[13] Daryna Antoniuk, Sri Lankan government loses months of data following ransomware attack, (September 11, 2023)

[14] Kevin Collier, Meat supplier JBS paid ransomware hackers $11 million, (June 9, 2021)

[15] Australian Associated Press, DP World hack: port operator gradually restarting operations around Australia after cyber-attack, (November 12, 2023)

[16] Stefanie Schappert, Polish stock exchange, banks knocked offline by pro-Russian hackers, (August 29, 2023)

[17] BBC, Hacker tries to poison water supply of Florida City, (February 8, 2021)

[18] Microsoft, Microsoft Digital Defense Report 2022, (Nov 2, 2022)

[19] Microsoft, Microsoft Digital Defense Report 2022, (Nov 2, 2022)

[20] Google, Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape, (February 2023)

[21] Verizon, 2023 Data Breach Investigations Report, (June 6, 2023)

[22] Susan Moore, 7 Top Trends in Cybersecurity for 2022, (April 13, 2022)

[23] Carly Page, Millions affected by MOVEit mass-hacks as lists of casualties continues to grow, (June 29, 2023)

[24] CISA and the NSA, Recommended Best Practices for Administrators: Identity and Access Management, (March 2023)

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

[26] Egress, Email Security Risk Report 2024, (March 8, 2024)

[27] Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (March 2, 2020)

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

[29] Rob Lemos, The state of two-factor authentication by text: What security pros need to know, (Accessed Sept 14, 2021)

[30] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (Dec 2022)

[31] NIST, NIST SP 800-63-4 Digital Identity Guidelines, (Dec 2022)

[32] Australian Signals Directorate, Essential Eight Maturity Model, (November 24, 2022)

[33] European Commission, eIDAS Levels of Assurance (LoA), (2014)

[34] IBM, 2022 Cost of Data Breach Report, (July 27, 2022)

[35] CISA, Zero Trust Maturity Model v 2.0, (April 2023)

[36] CISA, Zero Trust Maturity Model v 2.0, (April 2023)

[37] NIST, SP 800-207 Zero Trust Architecture, (August 2020)

[38] PCI, PCI DSS: v4.0, (March 2022)

[39] CISA, Identifying and Mitigating Living Off the Land Techniques, (February 2024)

[40] The White House, Executive Order on Improving the Nation's Cybersecurity, (May 12, 2021)

[41] OMB, M-22-09, (January 26, 2022)

[42] White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 2022)

[43] Cyber Safety Review Board, Review of the Attacks Associated with Lapsus$ and Related Threat Groups, (July 24, 2023)

[44] Department of Homeland Security, DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators, (May 27, 2021)

[45] TSA, Security Directive Pipeline-2021-02C, (July 21, 2022)

[46] TSA, Security Directive 1580/82-2022-01, (October 24, 2022)

[47] NERC, CIP-005-7, (Accessed October 23, 2023)

[48] IEC, IEC 62443-4-2:2019, (February 27, 2019)

[49] ISMS, ISO 27001:2022 Annex A Control 8.27, (Accessed October 24, 2023)

[50] CISA and the NSA, Enduring Security Framework (Accessed October 23, 2023)

[51] James Dempsey, The FTC's rapidly evolving standards for MFA, (November 8, 2022)

[52] European Parliament, The NIS2 Directive, (February 2023)

[53] European Parliament, Directive (EU) 2022/2555 of the European Parliament and of the Council, (December 14, 2022)

[54] Cyber and Infrastructure Security Centre, Critical Infrastructure Risk Management Program, (Accessed October 23, 2023)

[55] Australian Signals Directorate, Essential Eight Maturity Model, (November 2023)

[56] AEMO, Australian Energy Sector Cyber Security Framework, (Accessed October 26, 2023)

[57] AEMO, AESCSF framework and resources (Accessed October 23, 2023)

[58] Yubico, Australian government leading on cybersecurity efforts toward phishing-resistance for all citizens and businesses, (December 2023)

[59] Enisa, IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the art", (2023)

[60] Federal Office for Information Security, FAQs on the 2nd Amendment to the BSI Ordinance Determining Critical Infrastructures, (Accessed October 23, 2023)

[61] NISC, Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies, (FY2021)

[62] NISC, Guidelines for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition), (April 4, 2018)

[63] NISC, The Guidance on Operations of Cybersecurity Measures of Government Agencies and Related Agencies, 2023 (Japanese)

[64] Cyber Security Agency of Singapore, Cybersecurity Code of Practice for Critical Information Infrastructure - Second Edition (Accessed October 30, 2023)

[65] MAS, MAS' Cyber Security Advisory Panel Proposes Ways to Tackle Mobile Malware Scams and Generative AI Risks for the Financial Sector, (October 30, 2023)

[66] DOD OCIO, Memo, (December 20, 2019)

[67] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

[68] NIST, Best Practices in Cyber Supply Chain Risk Management, (Accessed April 18, 2022)

[69] Microsoft, Microsoft Digital Defense Report 2022, (Nov 2, 2022)

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

[71] NSA, Detecting Abuse of Authentication Mechanisms, (December 2020)

yubico

About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, 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.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.