



PARTNER WITH YUBICO TO CULTIVATE PHISHING-RESISTANT USERS

Modernizing authentication across global critical infrastructure

Around the world, critical infrastructure organizations are deploying modern authentication with hardware-backed passkeys



70%



of cyberattacks in 2024–2025 targeted critical infrastructure sectors¹

146%



global increase in sites impacted by cyber attacks with physical consequences²

72%



of attacks targeting OT systems from IT at the entry point³

56%



of organizations believe that GenAI will provide an overall advantage to attackers within the next two years⁴

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and the modern FIDO2/ WebAuthn authentication standard.

¹ IBM X-Force 2026 Threat Intelligence

² Waterfall, 2025 Threat report - OT Cyberattacks with Physical Consequences

³ ABI Research and Palo Alto Networks, The State of OT Security

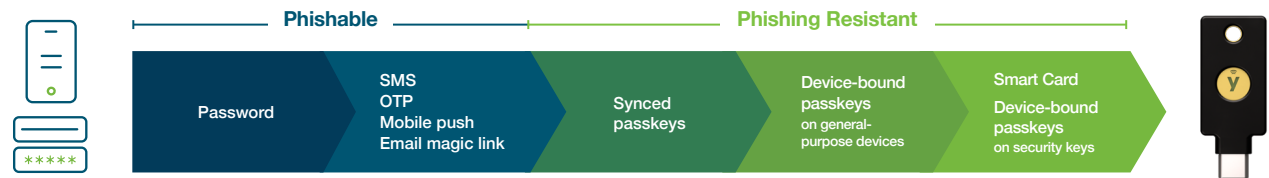
⁴ Accenture, Prioritizing Security for Success: Analyzing Organizational Security Structures 2024

Cyberattacks target critical infrastructure necessitating stronger protections

Globally there is an increasing number of malicious actors trying to cause mass disruption to public life and safety by targeting critical infrastructure and disrupting supply chains with cyberattacks. The rise of AI also enables malicious actors to craft convincing attacks at scale amplifying the attack surface. 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. 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

Not all MFA is created equal

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



Usernames and passwords are easily hacked. Legacy mobile-based authentication OTP codes, and push notifications are highly susceptible to phishing attacks, malware, SIM swaps, and attacker-in-the-middle attacks. Mobile-based MFA can also be costly as organizations may be liable for mobile-related service costs. MFA investments must provide critical infrastructure 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.

Protecting all users in the enterprise

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



Privileged access
Secure privileged account users



Mobile restricted
Secure call centers for mobile restricted users



Shared workstation
Protect shared workstation users



Remote workforce
Enable remote workforce



Office workers
Improve UX and security for office workers



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



End customers
Safeguard Yubico's customers' end-customers

Safeguard your IT and OT ecosystem with Yubico

Yubico solutions meet you where you are on your cybersecurity journey, while paving the way to a modern authentication infrastructure, and jumpstarting your plans to implement a Zero Trust framework. With Yubico solutions, you can be confident that your data and intellectual property are secured, and product integrity is always ensured.



The YubiKey

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

yubi.co/key



Yubico Hardware Security Module (HSM)

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

yubi.co/hsm



YubiKeys as a Service

An industry-first cybersecurity service that fast tracks organizations to strong phishing resistance and passwordless at scale. Receive exclusive access to turnkey **Enrollment** and **Delivery** services that help IT get users quickly onboarded with YubiKeys. YubiKey as a Service offers a choice of form factors, replacement stock, and priority customer support.

yubi.co/yubikeyasaservice

Discover how global critical infrastructure leaders are revolutionizing enterprise security and hardening critical IT and OT environments with phishing-resistant Yubico solutions.

“ YubiKeys continue to be an important element of how we approach cyber protection.”

Jeff Simon |
Chief Security Officer |
T-Mobile

Yubico and T-Mobile deployment of phishing-resistant YubiKeys across its operations enhances Un-carrier's work systems security

Yubico, the leading provider of hardware authentication security keys, has been working with [T-Mobile U.S.](#) and Yubico highlighted the partnership in a press release on their deployment of FIDO2 YubiKeys across its teams including employees, vendors and authorized retail partners. The passwordless, device-bound passkeys replaced legacy authentication to further secure the Un-carrier's work systems and information amidst the growing escalation of cyber threats, stopping unauthorized credential use by bad actors.

With Yubico's FIDO2 security keys, T-Mobile's teams no longer have to change or remember their passwords, or type in OTP codes that could be intercepted by bad actors; they use their YubiKey to passwordlessly authenticate and verify their identity to gain access to the resources they need.

“T-Mobile took a critical step forward to further reduce credential phishing by deploying the stronger, device-bound passkey solution that Yubico offers,” said Jeff Simon, Chief Security Officer, T-Mobile. “Once we had our YubiKeys in hand we were able to get them up and running across the company in less than three months, and we've seen the positive results after just one year of having them. That progress is even more important in today's environment where bad actors continue to wage sophisticated campaigns to attempt to infiltrate telecommunication networks. YubiKeys continue to be an important element of how we approach cyber protection.”

READ THE YUBICO & T-MOBILE PRESS RELEASE

[Learn more](#)

“ We are definitely more secure. We are really fond of the YubiKey for strong authentication. It’s much more reliable and secure than any non-Smart-Card-based factor.”

Matthias Wagner |
IT Architect & Director |
Cybersecurity Center |
City of Munich

⁵ Cyberattacks in Germany are increasing significantly, with education and telecommunications particularly affected

City of Munich protects itself from cyber attacks with YubiKeys

Public sector organizations, such as the City of Munich, face many of the same cyber threats as those in the private sphere, but can be even more enticing targets for cyber criminals who want to disrupt crucial public services or cause financial harm. In January 2026, German companies were exposed to an average of 1,314 cyberattacks per week.⁵

The city’s IT leadership began market research back in 2017 to a new MFA strategy aligned with their multifaceted setup: an identity management system in the backend, a Windows domain with Active Directory and an SSO endpoint. While mobile authentication methods were considered, IT Architect Matthias Wagner and team were keen to have a separate factor, and so they began investigating the vendor landscape for FIDO2 hardware security keys. They considered different vendors, and ultimately opted to purchase the YubiKey 5 Series, with contactless NFC capability, in both USB-A and USB-C models. In addition to Yubico’s proven and innovative authentication solution, that the company was European, with headquarters in Stockholm, Sweden was also a key consideration.

By implementing YubiKeys, the City of Munich is a pioneer in ensuring business continuity and cyber resiliency against modern AI-based cyber attacks that are increasingly sophisticated. They successfully rolled out to the full range of employees city-wide with an IT account. This meant over 30,000 employees, in a broad selection of departments ranging from HR and finance, to waste management and education. Reflecting on their deployment, the City of Munich is pleased with the decision to implement FIDO authentication across the organization. “We are definitely more secure,” says Wagner.

READ THE CASE STUDY

yubi.co/CityofMunich



“ Our aim was to eliminate account takeovers by adopting stronger MFA. Adopting YubiKeys has made it easy for us to continuously move our authentication strategy forward. Our goal is to enable passwordless authentication for all users in the future.”

Mr. Okamoto |
IT Platform Division |
Mitsubishi Electric Digital Innovation

Mitsubishi Electric strengthens global cybersecurity with the YubiKey

Mitsubishi Electric is a global leader in product innovation and the manufacturer of electrical and electronic products and systems, for consumers, businesses and a wide range of critical infrastructure including energy, transportation and information and communication systems. Established in 1921, Mitsubishi Electric is headquartered in Tokyo, Japan and globally active in over 120 countries.

As a key supplier of electrical and electronics products and solutions to critical infrastructure sectors worldwide, and a major supplier of Japan's defense systems, it is paramount for Mitsubishi Electric to guard against persistent cyber attacks.

In order to guarantee that their investment in MFA was well suited, Mitsubishi Electric wanted to ensure that the solution met the standards set by the National Institute of Standards and Technology (NIST) Digital Identity Guidelines and the Authenticator Assurance Level (AAL), which are recognized worldwide as equitable standards for identity management. While implementing MFA at various divisions and affiliates, Mitsubishi Electric faced a variety of challenges including, frequently, mobile-restricted scenarios, as most production facilities limit the usage of any mobile devices.

The YubiKey emerged as an optimal solution for both IT and Operational Technology (OT), including access to industrial control systems (ICS), requiring no additional hardware, software, external power, batteries or network connections. Embracing Yubico solutions, such as the YubiKey, significantly raises the bar for security and establishes a robust foundation for Mitsubishi Electric to facilitate and safeguard its digital transformation by paving a path to secure authentication that does not require passwords.

READ THE CASE STUDY

[yubi.co/Mitsubishi Electric](https://yubi.co/Mitsubishi%20Electric)



“ 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.

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

Schneider Electric enhances global supply chain security

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.

READ THE 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

“ One of the greatest cybersecurity threats is the human factor, through phishing attacks when cybercriminals obtain passwords or credentials.”



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

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 received 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,” explains a cybersecurity executive at a Ukrainian energy plant. “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.

READ THE 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

“ 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

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 YubiKey as a Service helps guarantee the highest level of protection into the future.

READ THE CASE STUDY
yubi.co/EnergyCo

“ YubiKeys are a big enabler for digitization. They protect the identity of the end user and make their life easier. If a company moves towards digitization, you have to do it securely. It was different 15 years ago, but since more and more tools and functions are cloud based, it's essential to protect identities.”



Mathias Ignberg |
Service Manager: Identity
& Access Management
and Cloud

Boliden advances its reputation for innovation with YubiKeys

Boliden is one of Europe's leading metal mining companies. Based in Sweden, with presence around the Nordic region and beyond, Boliden produces a vast array of the metals required for modern life: zinc, copper, lead, nickel, gold, palladium, platinum and silver. Known for their commitment to sustainability, with a vision to be the most climate friendly metal provider in the world, Boliden operates at the forefront of innovation, utilizing cutting-edge technology to optimize and improve their operations.

Mathias Ignberg shared that the two big drivers are a Zero Trust philosophy and being on the journey to passwordless login. Since people are roaming around more and using more cloud services, it makes the protection of identities more important. From a security standpoint, passwords by their nature are bad. Going passwordless is a win-win.

They use the YubiKeys for FIDO2 authentication to Azure, Microsoft Office 365 and AWS, but also as Smart Cards, using certificates, to protect privileged accounts and server access on-prem. The same YubiKey can be used for everything. While the initial deployment was relatively small, Boliden plans to roll out FIDO2 authentication across the entire organization in phases. First, they want to roll out to all IT employees company wide and then offer YubiKeys to end users more widely. It all depends on the use case. They see big potential for using YubiKeys in our open-pit mines, where a big chunk of the workforce only has a mobile device.

Ignberg is delighted with the results so far and has advice for anyone else considering starting on a similar journey. “Start! Just start,” says Ignberg. “Start small, with your most important admin accounts. It's better to start even if you don't have the full picture or know exactly how you're going to do it. It's better to protect a few users rather than none. The more accounts and identities you protect, the better.”

READ THE CASE STUDY

yubi.co/Boliden



“ I’m always thinking about what comes next, what is going to be the future of cybersecurity and how those things may impact the press’ ability to do the work they do. The YubiKey puts us ahead of the curve.”



Harlo Holmes |
Chief Information Security
Officer and Director of
Digital Security, Freedom of
the Press Foundation

“ Many journalists don’t even use an office anymore, which changes the attack surface significantly,”



David Huerta |
Senior Digital
Security Trainer

Freedom of the Press Foundation protects press freedom with the YubiKey

The Freedom of the Press Foundation (FPF) is a 501(c)(3) non-profit organization founded in 2012 to fund and support free speech and freedom of the press. The organization’s main objective is to protect and defend adversarial journalism in the 21st century. FPF uses crowdfunding, digital security, and internet advocacy to support journalists and whistleblowers worldwide.

Due to the high profile nature of their work, journalists are a target for attacks that threaten their personal safety, the safety of their sources and which undermine the freedom and integrity of the press. Spyware, surveillance, malware, and phishing attacks may compromise systems, reveal sensitive data, or reveal personal information about journalists in order to discredit, harass or intimidate them from covering stories (doxing).

FPF was also an early adopter and strong advocate for multi-factor authentication (MFA) and the YubiKey. The YubiKey supports phishing-resistant MFA and passwordless authentication, offering the highest level protection for a journalist’s identity, accounts and devices. Without having physical access to the security key, a bad actor isn’t able to access an account. “Helping journalists adopt the most secure form of authentication available is important in supporting our goal,” shares Huerta. “Our ultimate goal is a free press that acts within the autonomy it gets when it doesn’t have to fear repercussions.”

It is one thing to recommend the YubiKey to journalists, it is quite another to be able to put a YubiKey directly in their hands. With the help of Yubico’s Secure it Forward program, FPF can now freely distribute YubiKeys to the journalists they work with.

Looking to the future, for FPF and the press, Holmes knows that cybersecurity is always changing, such as the use of artificial intelligence to boost the effectiveness of social engineering campaigns. The YubiKey doesn’t just stop run-of-the-mill phishing attacks, but also these emerging and threatening social engineering attacks.

READ THE CASE STUDY
yubi.co/FPF



“ With YubiKeys we have been able to speed up the login process from over 40 seconds down to less than 10 seconds, which means that healthcare personnel have more time to care for their clients.”



Matthias van Alphen |
CEO & Founder, Adapta

Adapta secures healthcare worker access to Google Cloud with YubiKeys

Adapta is an IT services and development company based in the Netherlands, specializing in the implementation and maintenance of enterprise architectures for healthcare institutions, with a particular focus on care for the elderly and those with disabilities. Their mission is to make the working lives of healthcare professionals easier and more enjoyable. Matthias van Alphen is the founder and CEO of Adapta, and is committed to offering innovative solutions for clients.

In healthcare, where the security of patient data is critical, any digital transformation must be secure by design. When Adapta began looking for multi-factor authentication (MFA) solutions to introduce to healthcare settings, popular legacy MFA solutions did not prove suitable. The most common method organizations choose,” says van Alphen, “is an authenticator app. However, in nursing homes staff need something like a laptop or tablet, not a cellphone. If you have to log in with a code from an app or by clicking a prompt, then you need two devices before you even start.”

Adapta have recently introduced YubiKeys to two care organizations in the Netherlands, Zorgcentra De Betuwe and BrabantZorg. Adapta chose the Security Key NFC by Yubico, which supports the FIDO U2F and FIDO2/passkey protocols, making it a perfect complement to newly-implemented Google Cloud architectures. The results of the implementation are clear: happier employees. The future is going to be ‘passwordless’ and with FIDO2 we will be able to offer a password-free workplace. From the perspective of caregivers or nurses, the powerful combination of Google and the YubiKey can be summarized in a single word: speed!”

The partnership between Adapta and Yubico is also about values, according to van Alphen. “Our mission is to make the working lives of healthcare professionals more enjoyable, easier and generally better,” he says. “Yubico’s mission is to make the internet more secure and user-friendly for everyone. That’s why we fit so well together.”

READ THE CASE STUDY

yubi.co/Adapta



“ It was important for us to design our ICT systems to be both secure and easy to use. The YubiKey has made the login process for our staff much simpler, allowing them to continue to focus on providing quality care.”



Thomas Pike |
ICT Innovation Lead,
Carers ACT

Carers ACT delivers quality carer interactions thanks to passwordless logins with the YubiKey

Operating from four locations across Canberra and Illawarra, Carers ACT has 65 full-time employees, with additional support workers in short term respite facilities and a disability services program. Providing safe and effective respite and services for family and friend carers requires timely access to sensitive health information about the individuals being cared for, including care plans, health conditions and consents.

“Account compromise is something which is hugely worrying for us,” says Pike. “We hold some of the most sensitive personal information you can and we take our responsibility in holding that information very seriously.” In the past several years, Pike has noticed increasingly sophisticated cyber threats, including spear phishing campaigns that target employees with malicious emails that appear to come from the CEO of Carers ACT. Threats also come from potentially insecure devices used by clients and other guests accessing guest WiFi systems while in their facilities. Pike decided to replace cumbersome passwords and complex two-factor and legacy multi-factor authentication (MFA), such as SMS codes, with a FIDO security key to enable a secure, user-friendly passwordless experience for its support workers.

Having used and worked with YubiKeys at a previous organization, choosing the YubiKey for Carers ACT was an “easy choice to make.” The YubiKey is a hardware security key that delivers phishing-resistant MFA and passwordless authentication, complying with Essential Eight Maturity Levels 2 & 3. Carers ACT began by rolling out the Security Key C NFC by Yubico which supports FIDO2/WebAuthn (device-bound passkeys) to all support staff to address cyber threats and enable a seamless and user-friendly login to shared devices. As an established Microsoft environment, Pike was able to take advantage of out-of-the-box support for the YubiKey to streamline implementation.

After first-hand experience with the drawbacks associated with passwords and legacy MFA, the YubiKey provides Carers ACT with a high-assurance and user-friendly passwordless experience for its support workers. Looking to the future, Carers ACT plans to extend the YubiKey deployment across other parts of the organization.

READ THE CASE STUDY

yubi.co/CarersACT

Cultivate phishing-resistant users with the YubiKey



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 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

The YubiKey is the most secure and user-friendly option for protecting all users across business units; providing authentication that moves with users no matter how they work across devices, platforms and systems. Also stay ahead of evolving cyber threats and regulatory requirements (PCI DSS v4.0.1, PSD2, NIS2 and more).

YubiKeys work with leading IDPs, IAM, and PAM solutions and secure user access across 1,000+ of applications and services. Some partners we collaborate with as part of our Works with YubiKey (WWYK) catalog:



Learn more at yubi.co/WWYK



The path forward to cultivate phishing-resistant users

No matter where you are on your MFA journey, we'll meet you there. You can accelerate your zero trust approach and gain a bridge to a passwordless future. With a tried and true process that many organizations have followed already—and with services to help deploy phishing-resistant and passwordless at scale—it's not a matter of if you'll be successful but when you'll be successful in raising your bar for security with modern, hardware-backed passkeys such as the YubiKey.



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



Yubico (Nasdaq Stockholm: YUBICO) is a modern cybersecurity company on a mission to make the internet safer for everyone. As the inventor of the YubiKey, we set the gold standard for modern phishing-resistant, hardware-backed authentication, stopping account takeovers and making secure login simple. Since 2007, we've helped shape global authentication standards, co-created FIDO2, WebAuthn, and FIDO U2F, and introduced the original passkey. Today, our passkey technology secures people and organizations in over 160 countries—transforming how digital identity is protected from onboarding to account recovery. Trusted by the world's most security-conscious brands, governments, and institutions, YubiKeys work out of the

box with hundreds of apps and services, delivering fast, passwordless access without friction or compromise. We believe strong security should never be out of reach. Through our philanthropic initiative, Secure it Forward, we donate YubiKeys to nonprofits supporting at-risk communities. Dual-headquartered in Stockholm, Sweden and Santa Clara, California, Yubico is proud to be recognized as one of TIME's 100 Most Influential Companies and Fast Company's Most Innovative Companies. Learn more at www.yubico.com.

© 2026 Yubico



Contact us
yubi.co/contact



Learn more
yubi.co/criticalinfrastructure