

A small icon of a folded piece of paper with a blue arrow pointing upwards from the top left corner.

WHITE PAPER

Modernizing authentication to support cyber resilience and business continuity

Reduce cyber risk, accelerate digital transformation and keep your business running smoothly by creating a phishing-resistant enterprise



Table of contents

Executive summary	3
The link between your authentication strategy and business continuity	4
How to identify authentication risk	5
Address authentication vulnerabilities with device-bound passkeys	7
What is phishing-resistant MFA?	8
Passkey approach	8
Account lifecycle management	8
From phishing-resistant MFA to phishing-resistant users	9
The breadth of deployment	9
Protect authentication availability with phishing-resistant users	9
Support contingency plans with a portable root of trust	6
Emergency break glass accounts	7
Bootstrapping	8
Backup authenticator	8
Protect cyber resilience and business continuity with the YubiKey	10
Support alternate site recovery and multi-cloud security sharing with the YubiHSM 2	12
Client highlights	10
Schneider Electric boosts supply chain resiliency with Yubico	8
Herning Kommune uses the YubiKey to ensure continuous access to health systems	8
Future-proof your business continuity plans at scale	17



Executive Summary

Organizations face a growing number of threats that can impact their operations. While cyber attacks represent the most prevalent threat—59% of organizations have reported a cyber attack that resulted in data loss or unplanned system downtime—external threats account for 90% of data loss or downtime, including hardware or software failure, cloud errors, loss of power or natural disaster¹. Data loss or downtime can have a significant impact, including lost productivity, missed opportunities, decreased revenue, diminished shareholder value, damaged trust and confidence, and unplanned legal and compliance fees.

While most organizations have a variety of plans to prepare for, respond to, and recover from threats, most cyber resilience and business continuity plans make assumptions about multi-factor authentication (MFA) coverage and reliability that result in increased risk or prolonged business disruptions.

In this paper we will examine the most commonly overlooked authentication vulnerabilities that increase cyber risk, how to mitigate these risks, and what contingency measures can be put in place to maintain or restore access in the event of disruption.

61.8%



of organizations have a business continuity plan²

Global regulations that require continuity, disaster recovery or contingency plans:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule,³
- Sarbanes-Oxley Act (SOX) under SOC 2 controls⁴
- Federal Information Security Management Act (FISMA)⁵
- Digital Operational Resilience Act (DORA)⁶
- and more...

The link between your authentication strategy and business continuity

A business continuity plan (BCP) is central to ensuring an organization's resilience to unexpected events such as cyber attacks (cyber resilience) and natural disasters. The plan includes a combination of proactive activities to prevent or minimize threats to business operations and reactive activities to respond to adverse events and restore operations as quickly as possible.



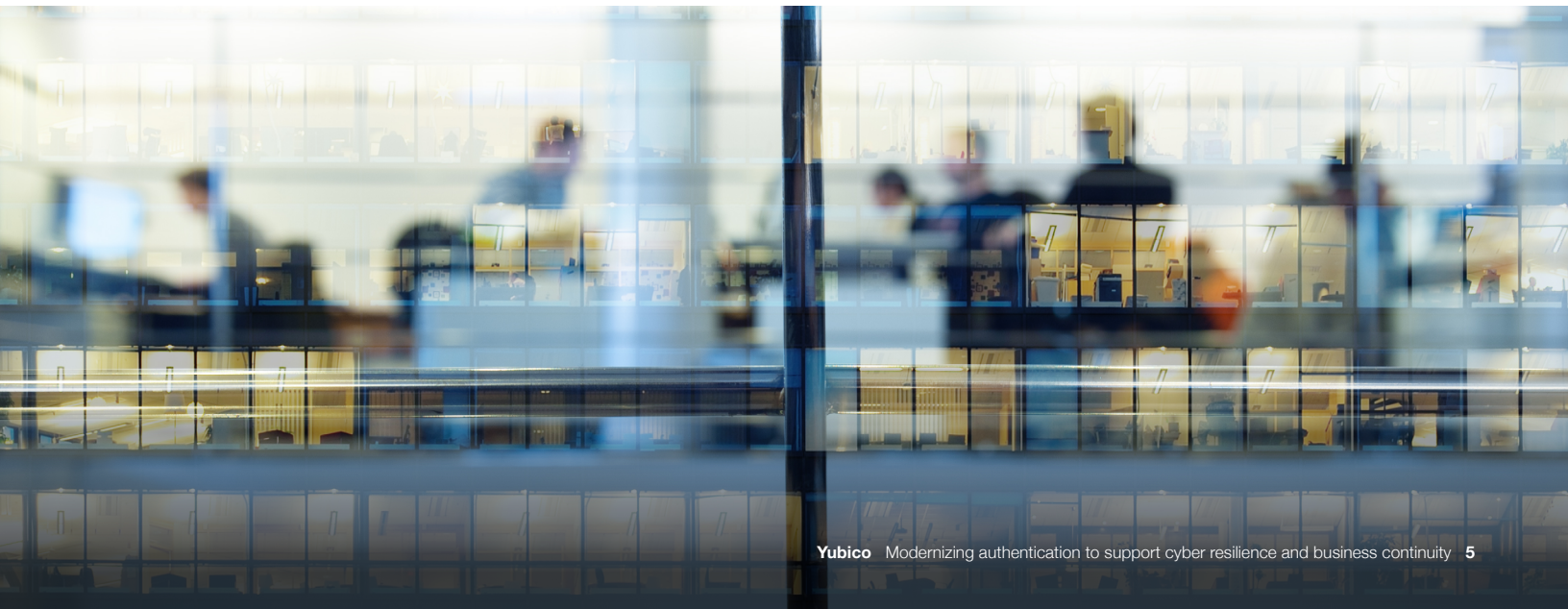


While adoption of BCPs is growing, the majority of business continuity managers (61%) report to business executives rather than to a CIO or CISO.⁷ Further, IT security and privacy pros report that a lack of executive support is the top barrier to security resilience.⁸ Combined, these insights suggest a lack of input from IT teams into continuity plans—a disconnect that could result in under-estimating authentication vulnerabilities and cyber risk as well as gaps in contingency plans that could result in unplanned delays in restoring access following adverse events.

For example, the American Hospital Association recently warned members of a service desk social engineering scam that allowed threat actors to enroll a new device and gain access to corporate systems.⁹ This scam exposes a gap in the authentication user lifecycle that falls back on shared secrets to verify user identity for account recovery to bypass phishing-resistant MFA. When shared secrets such as passwords are used for account recovery, it's all too easy for attackers to gain access—just ask MGM Resorts, who suffered 10 days of downtime and \$100 million in lost revenue when hackers exploited this vulnerability.¹⁰

In the remainder of this white paper, we will examine the most commonly overlooked authentication vulnerabilities that increase cyber risk, how to mitigate these risks, and what contingency measures can be put in place to help minimize unplanned downtime.

Mitigate				Contingency		
Identify and mitigate points in time when an enterprise user falls out of phishing-resistance or where there are gaps in coverage				Implement capabilities to maintain and securely recover access		
Account lifecycle management			Coverage Passkey approach deployment breadth	Emergency break glass accounts	Bootstrapping	Backup authenticator
Onboarding	Device registration	Account recovery				



Nearly two-thirds of organizations

experience major security incidents that jeopardize business operations¹¹

\$2 million per hour

cost of downtime in production sectors¹²

\$256 million per year

average cost of IT downtime for US companies¹³

How to identify authentication risk

The first step in business continuity planning is identifying risk—that combination of vulnerabilities and threats that have the potential to cause a disruption through the compromise or failure of systems or operations. Common threats to business continuity that could directly involve authentication include:



Direct cyber attacks

Systems are offline due to or to contain an attack



Supply chain attacks

Third-party credentials or software compromise your systems



Non-cyber production loss

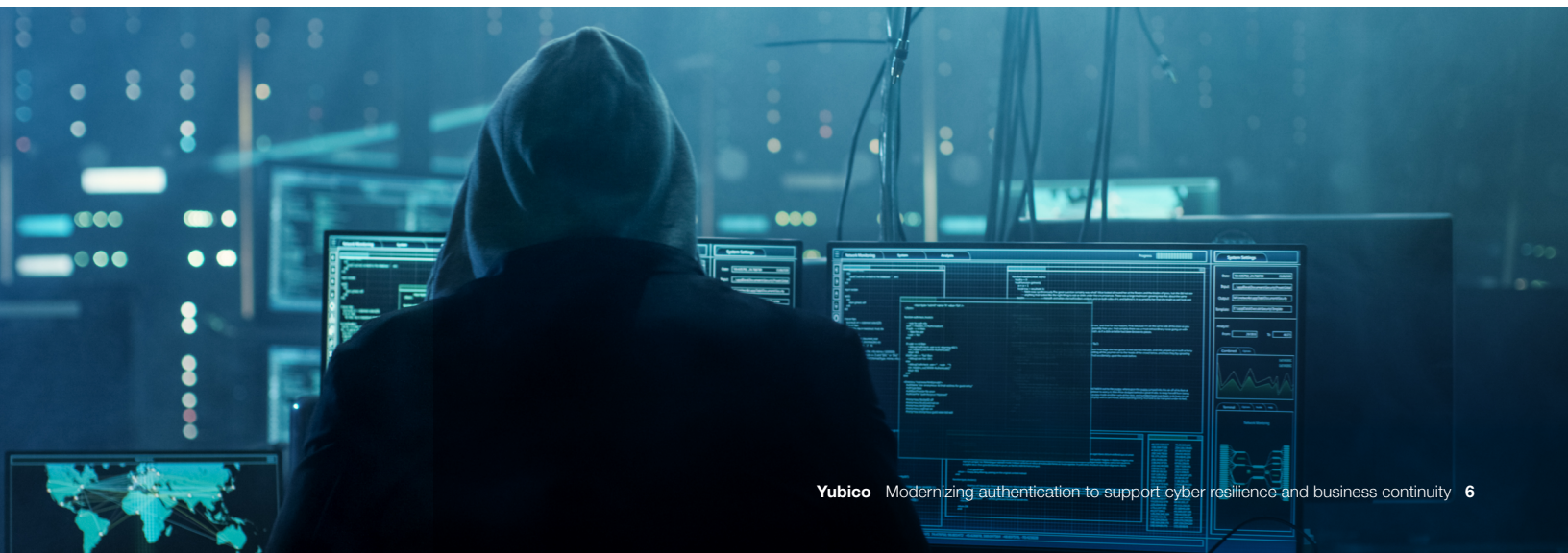
Mobile device has no signal/battery or is lost

In the following sections, we'll detail the specific authentication vulnerabilities that can be exploited by cyber attackers or lead to unplanned downtime and productivity loss.

Address authentication vulnerabilities with device-bound passkeys

Malicious actors don't break in, they log in. 90% of all cyberattacks leverage social engineering,¹⁴ with compromised credentials and phishing representing the most common initial attack vectors in successful cyber attacks.¹⁵ Through risk assessments, organizations know that while passwords offer the weakest protection against attacks, not all MFA is created equal.

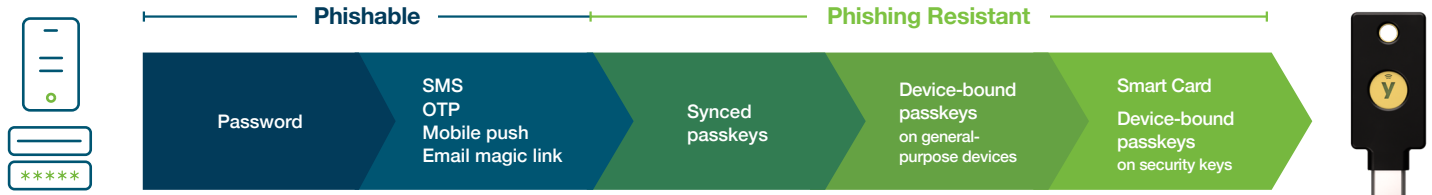
Legacy MFA such as SMS, mobile authentication, email 'magic links,' and one-time passcodes (OTP) can be easily bypassed by malicious actors, making them vulnerable to account takeovers (e.g. phishing) at a rate 10-24%.¹⁶ In the move away from problematic passwords and phishable MFA, organizations are adopting phishing-resistant MFA such as Smart Card/PIV and FIDO2/WebAuthn (passkeys).



What is phishing-resistant MFA?

National Institute of Standards and Technology (NIST), globally recognized for promoting equitable standards, defines phishing-resistance in Special Publication (SP) 800-63 and Draft 800-63-4¹⁷ 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.



Phishing-resistant MFA offers the lowest level of risk, reducing the threat of compromise and attack from phishing, but critical choices you make during deployment can contribute to gaps in coverage:



1. Passkey approach:
synced or device-bound

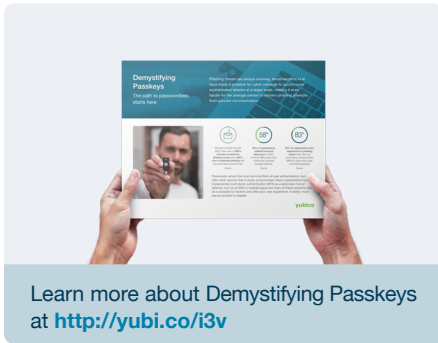


2. Account lifecycle management:
whether or not fall-back passwords and legacy MFA are used for onboarding, device registration and account recovery



3. The breadth of deployment:
whether deployed organization-wide or only for high-risk users and scenarios

These four areas represent blind spots in many risk management, cyber resilience and business continuity plans, reducing an organization’s ability to mitigate cyber attacks.



Learn more about Demystifying Passkeys at <http://yubi.co/i3v>

Passkey approach

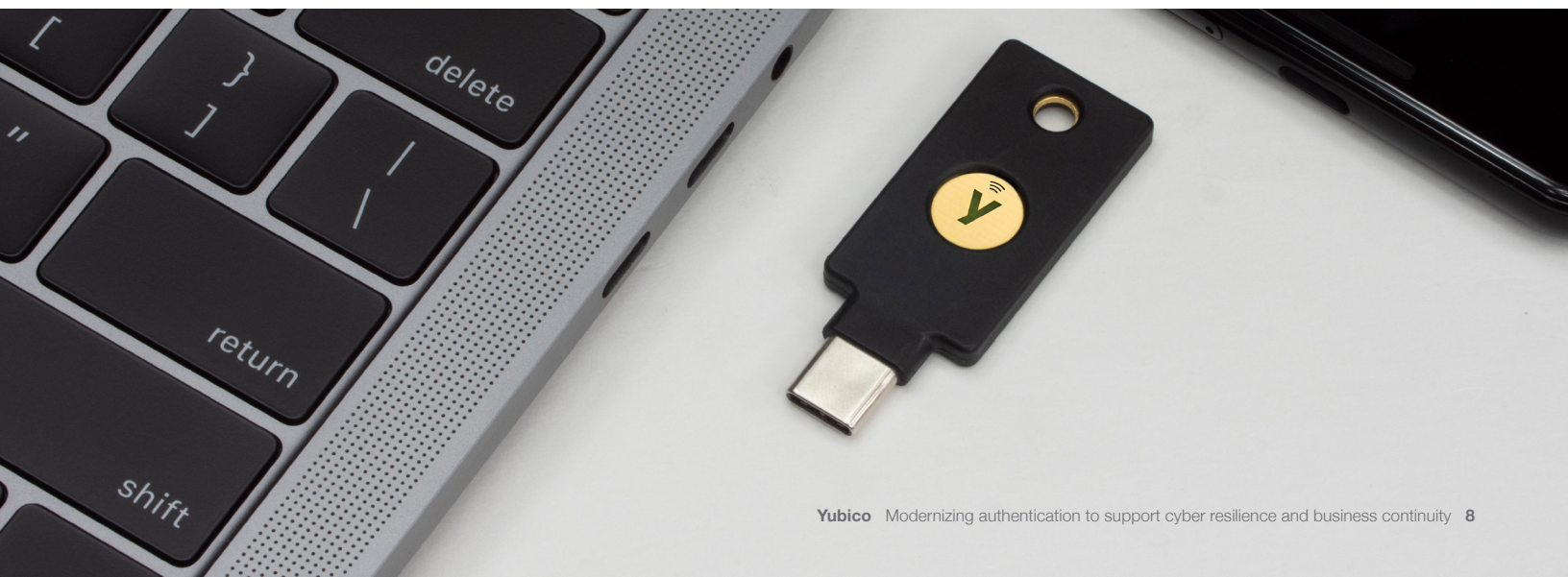
Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

- **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

Passkeys are based on public/private key pairs. Whoever or whatever has access to the private key has access to whatever the passkey is protecting. As cyber threat actors continue to seek out and exploit new vulnerabilities, syncable passkeys present a new vulnerability.

Syncable passkeys are considered lower assurance since the passkey can be copied across accounts and devices—a vulnerability that can be exploited by phishing if the passkey is shared to a personal cloud account or if the passkey is exposed by a breach of a third-party passkey provider service.

To have the highest level of assurance, to know that the user who is controlling the device is the one who is supposed to be using the passkey, the passkey needs to be stored in hardware-based secure elements such as security keys. A security key is a surefire way to block phishing attacks from succeeding or to limit the degree of impact in an environment, protecting you from privilege escalation.



Account lifecycle management

The overall strength of any form authentication is only as strong as its weakest step. Most MFA implementations (even the strongest phishing-resistant MFA) focus on the user experience of authentication—that moment in time when the user authenticates to a facility, device, or app. In doing so, organizations could leave the account lifecycle process vulnerable to attack.

Points in time when existing MFA processes fall down or are open to abuse



Onboarding



Device registration



Account recovery

All phishing-resistant MFA solutions require organizations to establish a relationship that registers the Smart Card or passkey to establish trust that the user is who they say they are. Most organizations establish Smart Card relationships in-person, but this is more challenging for passkeys, which typically rely on self-service registration. Many implementations will fall back on passwords or legacy MFA for this stage of the authentication lifecycle, bypassing the intended security of phishing-resistant MFA solutions.

The prevalence of phishing attacks using tactics like the aforementioned social engineering calls to the helpdesk (among many other methods) can not only hijack the user registration process, but also ongoing authentication and account recovery processes in the event of a lost or stolen device.

This piecemeal approach to authentication exacerbates the challenge for enterprises in consistently safeguarding their systems and data, posing a threat to cyber resilience, business continuity, and even compliance.



What is a root of trust?

A root of trust, such as a hardware security key, offers a physical and cryptographic guarantee of possession of a unique hardware device to support account recovery or bootstrapping a new device. The private key material or “secret” cannot be extracted as the external authenticator cannot be cloned or tampered with, and the privacy secrets cannot be revealed.

From phishing-resistant MFA to phishing-resistant users

For authentication policies to be effective, organizations must ensure that users have the right type of authenticators, credentials, and processes for every stage of the account lifecycle. Put another way, phishing-resistant authentication is only effective when it moves effortlessly with the user:

Across platforms



Across devices



Across business scenarios



This shift—from **phishing-resistant authentication** to **phishing-resistant users**—helps close these gaps in the account lifecycle and ensures that for every authentication task, the user will use a phishing-resistant MFA solution.

To achieve this state of continuous phishing-resistant protection, organizations need to elevate the processes for issuing credentials, registering devices, signing into passkey providers, and recovery processes. This starts with deploying the highest-assurance hardware security keys as a portable root of trust.

1. Equip all users with hardware security keys as the primary authenticator
2. Make hardware security keys the foundation for registration and recovery procedures for all users
3. Employ technology-driven solutions that minimize the reliance on user education, while also providing essential education on the principles and benefits of phishing-resistant MFA for both corporate and personal use.





The breadth of deployment

Organizations know they need to move away from passwords and legacy MFA to protect against the growing number of cyber threats, but there are many realistic obstacles to full deployment—legacy systems, shortage of IT staff, budget. In an ideal world, cyber resiliency and continuity would demand that the one obstacle we eliminate is breadth of deployment.

Although privileged users with elevated access to systems and data have credentials with the greatest risk of causing catastrophic harm to the business, the idea of privileged users is itself outdated. Any business user who possesses access to exploitable systems or IP are targets of attack, giving cyber criminals the opportunity to move laterally to other systems (IT or OT) and gain additional privileges, as was the case with the SolarWinds attack.¹⁸

If traditional privileged users are secured with phishing-resistant MFA but the rest of the business still relies on passwords and legacy MFA, this leaves vulnerable gaps in the cybersecurity infrastructure. Think of it as locking the front door of the house, but leaving the back door wide open. The safest defense? Treat every user like a privileged user.

An enterprise is truly a phishing-resistant enterprise if all users are considered “privileged users” and protected with phishing-resistant authentication across the entire user lifecycle.



Privileged users

Engineers, IT and security admins, C-Suite, HR, finance, and sales



Shared workstation environments



Remote staff, office workers, & field technicians



OT and mobile-restricted environments



Users across supply chain

Contractors, contract service workers, secondees and joint ventures



Customer accounts



Beyond downtime, organizations should also consider the complexity and cost of supporting mobile authenticators. It is estimated that the average organization spends \$1 million annually on password resets, with passwords representing one factor in many mobile authentication workflows.²⁰ Mobile connectivity is also a consideration for organizations deploying syncable passkeys or device-bound passkeys on general purpose mobile devices, making them unsuitable for mobile-restricted environments, air-gapped or isolated networks and shared workstations.

Protect authentication availability with phishing-resistant users

Although we've established that not all MFA is created equal, mobile authentication further introduces risk and threatens business continuity. Cyber risk is not the only risk to consider—a lack of authenticator availability can also be a contributing factor to production loss. This can include:



Loss of cellular service



Loss of possession
Device lost | stolen



Battery life

In all scenarios, the lack of authenticator availability can result in employees unable to access facilities, devices or apps, negatively impacting productivity. In the case of critical IT users, this could result in unplanned system downtime.

A recent attack on mobile device management (MDM) firm Mobile Guardian recently wiped thousands of devices.¹⁹ Although many articles speak to the impact this had on student access to their personal learning devices, an attack of this nature in the corporate environment could wipe out authentication availability unless contingency plans included a backup authentication method.









Support contingency plans with a portable root of trust

Continuity planning considers both proactive and reactive capabilities to mitigate adverse events. Up until this point, we have detailed authentication vulnerabilities that can expose organizations to unanticipated levels of risk, but authentication also plays a role in contingency planning.

Resuming access to a system is a critical component of recovery activities, yet very few organizations take the time to document what recovering access looks like. NIST suggests the use of “alternative security mechanisms to support system resiliency, contingency planning, and continuity of operations,” advice which can and should be applied to authentication to support both system and account recovery and as a secure backup if primary authentication fails.²¹

Emergency break glass accounts

Break glass accounts are crucial accounts that provide access to critical systems during a variety of emergencies, including:

			
Network or service outage	Failure of federation/identity provider (IdP) services Service disruption or breach	Privileged role member unavailable or has left the company	Privileged access management (PAM) unavailability Service disruption or maintenance

As established earlier when speaking to account lifecycle management, the overall strength of any form authentication is only as strong as its weakest step. It is critical to ensure that break glass accounts do not fall back on passwords or legacy MFA. In fact, Microsoft recently announced that it is updating best practice guidance to use FIDO2 security keys instead of long-passwords alone on break glass accounts for signing into Entra.²²

It is critical to have a secure, traceable authenticator for break glass accounts. Device-bound passkeys on hardware security keys are an easy way to achieve high assurance authentication.

Best practices for setting up security keys for break glass accounts:



1. Create a security group

Start by creating a security group specifically for your break glass accounts. Assign the Global Administrator role to this group.



2. Use cloud-only accounts

Create accounts native to identity and service provider platforms ensuring they aren't federated or synchronized.



3. Register two keys

Each break glass account should have two security keys registered to ensure redundancy, with one stored in a secure, separate location.



4. Policy exclusions

Make sure your policies do not block access to break glass accounts so that you have unimpeded access during an emergency.

It is critical to consistently monitor activities related to break glass accounts and set up alerts for any changes or usage. Periodically review who has access to ensure that only authorized personnel can use these accounts. This helps maintain the security and integrity of your emergency access procedures.



What are authentication assurance levels (AALs)?

Authentication assurance levels (AALs), or Levels of Assurance (LOAs), classify the relative strength of authenticators, from password (AAL1) to standard MFA and synced passkeys (AAL2) to Smart Cards and device-bound passkeys (AAL3). 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.

Points in time when existing MFA processes fall down or are open to abuse



Onboarding



Device registration



Account recovery

Bootstrapping

Should an authorized workstation or device be lost or corrupted, it may need to be wiped. In the case of a wiped machine, or in the event an employee receives a new device, you need a secure way to “bootstrap” or redeploy workstations or laptops to users.

Security keys act as a portable root of trust, enabling rapid bootstrapping on new devices, in addition to the ability to recover accounts quickly.

Backup authenticator

The availability of an alternate authenticator helps support the availability of access to systems in the event of account lockouts or authenticator availability issues—which also applies to synced passkeys, due to their reliance on cellular connectivity.



Account lockouts

biometric and other
MFA failure



Authenticator availability

Loss of cell signal,
possession, or battery

Like a backup generator, having a backup authenticator provides redundancy to the system, helping reduce the time it takes to get back online. This is particularly acute if an account lockout occurs during the stress of an emergency situation. A hardware security key provides that portable root of trust for critical users to bypass a lockout and regain access to systems. NIST further encourages the use of multiple authenticators to a subscriber account and when binding an authenticator to the account that it requires authentication at either the maximum AAL currently available or the maximum AAL at which the new authenticator will be used.²³





The YubiKey has you covered.

- ✓ IP68 certified, AAL3 compliant, and FIPS 140-2 validated solutions to protect any environment from industrial or corporate to highly regulated.
- ✓ 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 the secrets never shared between services.
- ✓ The YubiKey does not require external power or batteries or a network connection, making it an ideal solution for mobile-restricted environments.

Protect business continuity and enhance cyber resilience with the YubiKey

Provide continuous secure access with the YubiKey

Organizations looking to proactively enhance cyber resilience and safeguard continuity are fostering phishing-resistant users and a phishing-resistant enterprise built on deploying the highest-assurance hardware security keys for all users across the entire organization.

Yubico offers the YubiKey, a hardware security key that contains the highest assurance passkeys and is the essential starting and ending point on the journey to business continuity and resilience.

The YubiKey provides authentication that moves with users, no matter how or where they work. YubiKeys help organizations deploy phishing-resistant authentication across the entire credential user lifecycle, including registration, authentication and recovery processes, to create phishing-resistant users.

The YubiKey as the primary way to authenticate

The only way to remove phishing from the enterprise



The YubiKey 5 Series

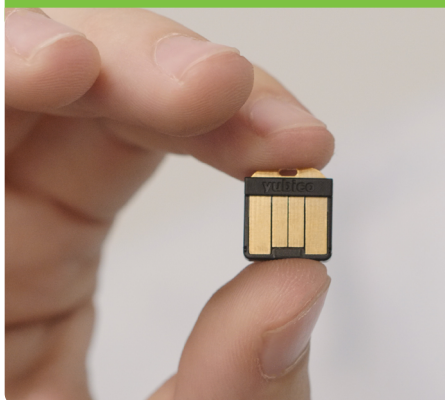
From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano

The YubiKey is proven to reduce risk by 99.9% and provide significant value at scale, delivering an ROI of 203%²⁴, all while enabling a frictionless user experience, letting users quickly and securely log in with a single tap or touch.

				
More value	High return	Strongest security	Faster	Durable
Reduce support tickets by	Experience ROI of	Reduce risk by	Decrease time to authenticate by	IP68 rated, crush-resistant, no battery required, no moving parts
75%	203%	99.9%	>4x	

The YubiHSM 2 has you covered:

- ✓ Ensures enterprise-grade high cryptographic security and operations that protects servers, applications, and computing devices
- ✓ Safeguards intellectual property, corporate secrets and secures manufacturing assembly lines
- ✓ Ultra-portable nano form factor that allows for flexible deployment



Support alternate site recovery and multi-cloud security sharing with the YubiHSM 2

As part of continuity planning, some threats or disruptions require a business to relocate operations to another site. For federal agencies required to comply with the Federal Information Security Management Act (FISMA), the NIST Contingency Planning Guide for Federal Information Systems suggests the implementation of technical security controls including the need for cryptographic key management.²⁵ The YubiHSM 2 enables organizations of all sizes to enhance cryptographic key security throughout the entire lifecycle and to provide continuity across multi-cloud environments.

The YubiHSM 2 makes it easy to transfer a root secret key pair from one environment to another, making it possible to spin up production in an alternate facility. The YubiHSM 2 also helps you simplify your security stack by using the same set of keys in multi-cloud environments, allowing you to push code and updates without needing to switch between individual key pairs for each cloud environment.





Read our case study
yubi.co/SchneiderElectric

“By leveraging the YubiKey and the YubiHSM, a small form factor and powerful hardware security module, we increase the security of our supply chain at Schneider Electric.”



Chad Lloyd
Director of Cybersecurity
Architecture for Energy
Management

Client highlights

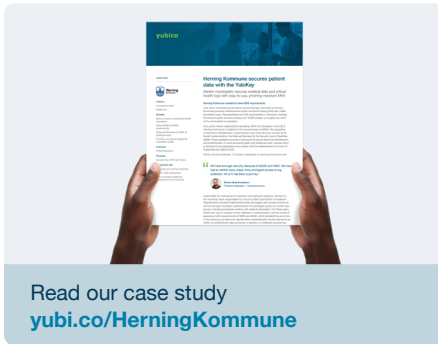
Schneider Electric boosts supply chain resiliency with Yubico

Schneider Electric Energy Management, one of the two businesses of Schneider Electric, is built around providing safe and reliable products and power management systems for critical infrastructures. These include data-centers, large office buildings, hospitals, and oil and gas drilling operations, among others.

Schneider Electric introduced YubiKeys in their power operation SCADA system to increase security, supporting secure transitions during shift change and ensuring there is always a trusted way to authenticate users quickly when quick actions are needed.

To proactively increase security within their supply chain, the company has taken measures to protect its supply chain from compromise. Deploying the YubiHSM within Schneider Electric and across key vendors, Schneider Electric has enabled a dual encryption process that confers confidence that products with the Schneider Electric brand are indeed authentic based on encrypted keys that are embedded by both companies during manufacturing.





Read our case study
yubi.co/HerningKommune

“ We are taking care of people
24 hours a day, 365 days a year.
It's critical that we have a reliable
method to access healthcare
systems anytime, anywhere.
The YubiKey provides that for us.”



Jonas Philipsen
IT Consultant,
Herning Kommune

Herning Kommune uses the YubiKey to ensure continuous access to health systems

As a public sector organisation providing comprehensive public services including child care, health and elderly care, Herning Kommune needs to ensure that access to Health and Senior service systems would be both reliable and secure.

Prior to the implementation, Herning Kommune only relied on single-factor username and password for authentication to all government systems, including those that stored sensitive personal or medical information. With the need to meet the new compliance requirements of eIDAS and NSIS and the need to eliminate the unsafe practice of password sharing, Herning Kommune selected the YubiKey.

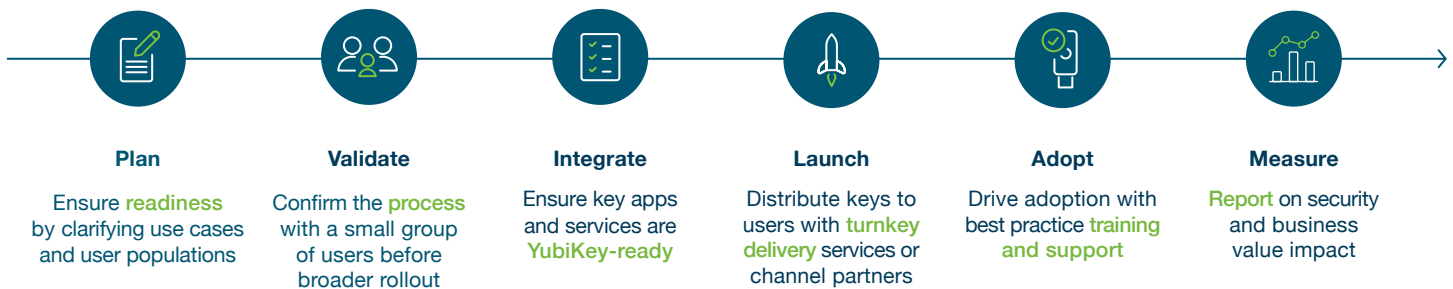
The YubiKey gives every employee a secure, reliable connection to health systems to ensure seamless care delivery, including for those care providers who may be working off-network or remotely. devices, in addition to the ability to recover accounts quickly.

Future-proof your business continuity plans at scale

To protect against the growing number of threats to business operations, organizations need an authentication solution that reflects the risk environment and provides phishing-resistant MFA at scale and across a wide variety of authentication scenarios.

Modern organizations are thinking past phishing-resistant authentication as a technology and instead are focused on creating phishing-resistant users to support more resilient, phishing-resistant enterprises—enterprises more resilient to attack and armed with detailed contingency plans to restore access in times of need.

Because Yubico solutions are designed to meet you where you are on your journey to enterprise resilience, we have made it easy to close gaps in your business continuity plans with the YubiKey. We offer a simple guide that details the six deployment best practices to accelerate adoption at scale, [How to get started with phishing-resistant MFA](#).



Contact us yubi.co/contact

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. Our Professional Services team is composed of trained and accredited security professionals with experience gained from hundreds of customer implementations across a wide range of industries and the government sector to meet you where you are and integrate YubiKeys into your business processes.

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



Sources

- ¹ DELL Technologies, [Global Data Protection Index](#), (October 2023)
- ² Avidxchange, [Critical Gaps in Business Continuity Plans](#), (Accessed September 26, 2024)
- ³ US Department of Health and Human Services Office for Civil Rights, [HIPAA 164.310 Physical safeguards](#), (March 2013)
- ⁴ Imperva, [SOC 2 Compliance](#), (Accessed 2024)
- ⁵ NIST, [NIST SP 800-53 R.5 Security and Privacy Controls for Information Systems and Organizations](#), (September 2020)
- ⁶ DORA, [Article 6 ICT Risk Management Framework](#), (Accessed April 16, 2024)
- ⁷ Demartine, [Amy reporting on Forrester Research, The State of Business Continuity Preparedness 2023](#), (February 16, 2023)
- ⁸ Cisco, [Security Outcomes Report Volume 3](#), (March 20, 2023)
- ⁹ AHA, [Cyber schemers continue to target hospital IT help desks](#), (April 3, 2024)
- ¹⁰ White, M., [MGM Resorts: How attackers hit the jackpot with service desk social engineering](#), (September 27, 2024),
- ¹¹ Cisco, [Security Outcomes Report Volume 3](#), (March 20, 2023)
- ¹² Siemens, [The True Cost of Downtime 2022](#), (2022),
- ¹³ Splunk, [Splunk Report Shows Downtime Costs Global 2000 Companies \\$400B Annually](#), (June 11, 2024),
- ¹⁴ Avast, [Avast Threat Report Q1 2024](#), (May 14, 2024),
- ¹⁵ IBM, [2024 Cost of Data Breach Report](#), (July 30, 2023)
- ¹⁶ Kurt Thomas and Angelika Moscicki, [New research: how effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ¹⁷ NIST, [NIST SP 800-63-4 Digital Identity Guidelines](#), (December 2022)
- ¹⁸ Harrell, C., [Lessons from the SolarWinds incident](#), (December 23, 2020),
- ¹⁹ Paganini, P., [Hackers breached MDM firm Mobile Guardian and wiped thousands of devices](#), (August 7, 2024)
- ²⁰ Forrester Research, Inc, [Optimize User Experience With Passwordless Authentication](#), (March 2, 2020)
- ²¹ NIST, [NIST SP 800-53 R.5 Security and Privacy Controls for Information Systems and Organizations](#), (September 2020)
- ²² Shahid, N., [Update on MFA requirements for Azure sign-in](#), (June 27, 2024)
- ²³ NIST, [NIST SP 800-63B-4, R2 Digital Identity Guidelines: Authentication and Authenticator Management](#), (August 2024)
- ²⁴ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- ²⁵ NIST, [Contingency Planning Guide for Federal Information Systems](#), (May 2010)



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.