yubico | Microsoft

WHITE PAPER

Strengthen cyber resilience in your Microsoft ecosystem with phishing-resistant MFA

Counter modern cyber threats and eliminate legacy security limitations with phishing-resistant MFA from Yubico

Table of contents

99.9%

of compromised accounts do not have MFA, leaving them vulnerable to phishing, password spray and password reuse[1]

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

10-24%

attack penetration rate for mobile authentication

94%

organizations were victims of phishing

$1M

per year cost for password resets alone

The critical need for phishing-resistant MFA in your Microsoft environment

Powering most modern work environments is a mix of on-premises solutions alongside a suite of cloud, intelligence and emerging technologies. Globally, Microsoft provides 25% of cloud infrastructure services, and advancing digital capabilities with Microsoft's cloud solutions has become an imperative for organizations that want to empower their teams with the most modern tools and capabilities. This imperative is particularly strong for remote and hybrid workforces, which continue to grow. In fact, the number of what the World Economic Forum calls "global digital jobs"—jobs where all of the component tasks can be completed remotely—is expected to rise 25%, for a total of 92 million, by 2030.

This ongoing transition to remote work creates a larger threat surface as 62% of organizations can partially attribute a data breach to remote work. Further, the combination of digital transformation and remote work have introduced new elements of risk by making traditional perimeter-based security models ineffective—82% of breaches involve data stored in the cloud.

No matter where your employees work, though, data breaches are costly in a number of ways. First, financially, as the average data breach costs $9.48M in the US and $4.45M globally. Cyber attacks can also create severe and long-lasting consequences for organizations including damage to physical assets, customer trust and brand reputation, increased cyber insurance premiums and potential loss of intellectual property.

As a pioneer and established leader in modern cybersecurity practices, Microsoft has provided trusted solutions for enterprise organizations, government agencies and other high-security environments such as support for certificate-based authentication (CBA) and other high-security features. In 2023, Microsoft launched its Secure Future Initiative (SFI) which prioritizes "cyber safety above all else" in the way it designs, builds, and tests its products and services. An expansion to the SFI followed a few months later, in part to address recommendations from the Cyber Safety Review Board.

At the same time, the threat landscape is growing and evolving rapidly. Cyber criminals are launching increasingly-sophisticated attacks, nation states are becoming more aggressive and Microsoft detects nearly 4,000 password-based attacks against its customers every second of every day. Furthermore, attacks against identity are pervasive; 68% of data breaches can be traced back to the human element including situations such as stolen credentials and phishing.

Combatting this myriad of threats requires a two-pronged approach. While Microsoft has created a security-first culture, its customers must also adopt more stringent cybersecurity measures. One measure is non-negotiable—in keeping with a major SFI goal to protect identities and secrets, Microsoft mandated the use of multi-factor authentication (MFA) for all Azure users.

Adopting more secure authentication is a crucial step towards cyber resilience. To help create maximum cyber resilience across your Microsoft ecosystem, this whitepaper will outline key considerations when choosing authenticators, provide specific Microsoft use cases that can be supported by phishing-resistant MFA, and explore how the most modern organizations are expanding beyond phishing-resistant MFA to create phishing-resistant users.

Drivers for adoption of phishing-resistant MFA

External | Internal

Cyber threats	Compliance software
Privileged access devices	Cyber insurance requirements access
Support complexity teleworkers	Remote access
User convenience	
Zero Trust and passwordless initiatives	

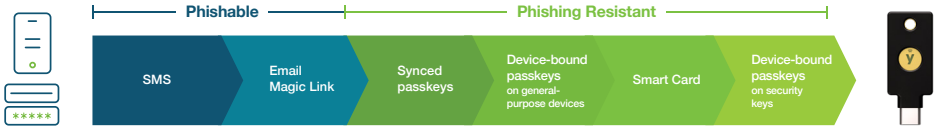
Not all MFA is created equal

While any form of MFA is better than a password, not all MFA is created equal. 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%. In fact, the risk of SMS interception is so high that NIST called for SMS to be deprecated as a method of authentication. Further, Microsoft examined commercial accounts where a known password leak occurred and found SMS was 40.8% less effective than its Authenticator app in preventing attacks and that MFA prevented 98.6% of attacks.

What qualifies as phishing-resistant MFA?

Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intention to initiate through deliberate action.

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



Organizations are turning to MFA to protect against cyber attacks—for example, Microsoft detects 345 million cyber attacks against its customers every day. However, there are additional reasons why organizations leverage MFA: to support remote access (34%), support privileged access (26%), improve user convenience (24%), support Zero Trust initiatives (25%) and meet compliance requirements (21%).

MFA is the requirement for Azure users, but phishing-resistant MFA is the standard for many global cybersecurity regulations and is a growing requirement for organizations to either qualify for cyber insurance or eliminate costly increases in premiums, sub-limits or exclusions. With such a wide array of benefits, it is understandable why the Cybersecurity & Infrastructure Security Agency (CISA) called phishing-resistant MFA "key to peace of mind."

What about passkeys

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

Phishing-resistant MFA in your Microsoft environment

In the Microsoft ecosystem, phishing-resistant MFA (PIV/Smart Cards) has long been supported for desktop systems on Windows and macOS leveraging certificate-based authentication (CBA), a process that uses a digital certificate derived from cryptography to identify a user, device or machine before access is granted. While PIV/Smart Card met the needs for traditional perimeter-based authentication requirements, the modernization of IT and growth of remote work requires an alternative high assurance authentication solution. The modern FIDO2 authentication standard enables phishing-resistant two-factor, multi-factor and passwordless authentication to easily authenticate to online services in mobile and desktop environments.

Synced or device-bound: What's the difference?

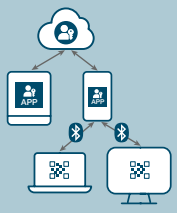
There are three different types of passkey implementations that you can roll out across your organization.

Synced passkeys

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

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.

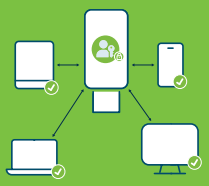
Device-bound passkeys on general purpose devices



- Lives in general purpose devices such as smartphones and tablets. For example using an authenticator app
- Middle ground option for enterprises; but less secure than device-bound passkeys on hardware security keys

Device-bound passkeys on general purpose devices such as smartphones, laptops and tablets offer enterprises greater control of their FIDO credentials compared to synced passkeys but are still backed by a password and offer weak security.

Device-bound passkeys on modern FIDO hardware security keys



- Lives on 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)

Device-bound passkeys on modern FIDO hardware security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach, organizations 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 regulated industries.

The YubiKey is the only:

- external device that supports CBA on Android and iOS
- FIPS-certified phishing-resistant solution available for Entra ID on mobile

Create cyber resilience with Yubico and Microsoft

Modern, passwordless phishing-resistant authentication with the YubiKey

Yubico is proud to play a key role in helping Microsoft customers realize the goals behind the SFI. Microsoft and Yubico are FIDO Alliance members, helping to deliver strong phishing-resistant authentication solutions based on FIDO2 and CBA standards. These solutions, coupled with Microsoft's Conditional Access policies, help organizations create stronger cyber resilience, and can support organizations that want to further advance their strategy with a Zero Trust model.

Yubico created the YubiKey, a hardware security key that delivers an optimized user experience and supports phishing-resistant two-factor, MFA and passwordless authentication at scale across Microsoft environments. The YubiKey is a multi-protocol key, supporting both PIV/Smart Card and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy and modern environments, helping organizations bridge to a passwordless future.

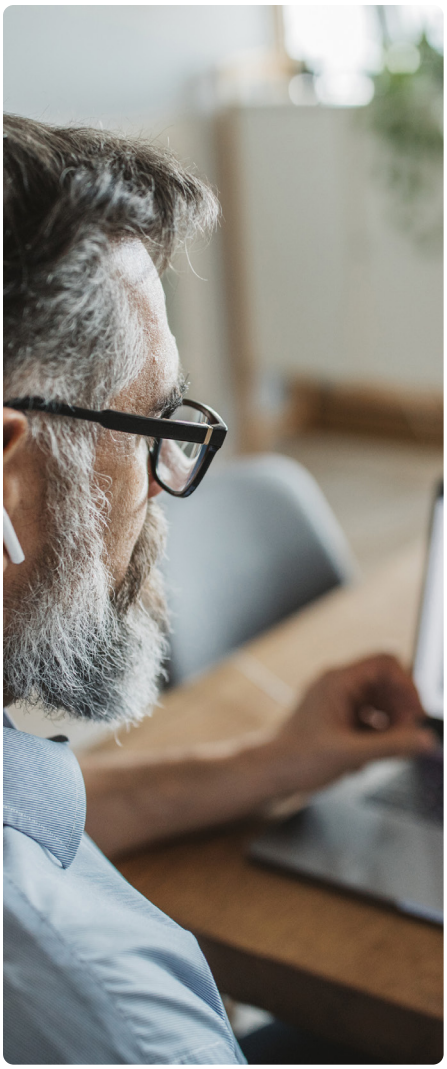
By leveraging the YubiKey's robust hardware-based authentication, organizations can significantly reduce the risk of credential theft and unauthorized access. YubiKeys use public key cryptography to ensure that authentication sessions are only between the registered authenticator and the relying party, making them highly resistant to phishing attacks. This collaboration not only strengthens cybersecurity and cyber resilience in Microsoft ecosystems, but it also helps organizations comply with security standards and regulations such as PCI DSS, HIPAA, GDPR, and NIST.

A user can use a single YubiKey for secure access to Windows Hello for Business (WHfB) and Microsoft Entra ID protected workstations, applications and services, as well as over 1,000 other products, services and applications, with the secrets never shared between services.

The YubiKey is proven to reduce risk of account takeovers by 99.9% while delivering a great user experience, letting users securely log in with a single tap or touch. The total economic impact of YubiKeys includes:

The total economic impact of YubiKeys[41]:

Strongest Security	High Return	More Value	Faster
Reduce risk by	Experience ROI of	Reduce support tickets by	Decrease time to authenticate by
99.9%	**203%**	**75%**	**>4x**



YubiKeys are the foundation for phishing-resistant users across your Microsoft ecosystem

Modern organizations are moving towards the most effective phishing-resistant MFA strategy: phishing-resistant users. After all, attackers target users, and authentication starts and ends with the user.

Despite investments in MFA and the implementation of phishing-resistant authentication, organizations remain susceptible to phishing attacks.

Organization susceptibility

User carelessness

"User carelessness" was the most common cause of sensitive information loss in worldwide organizations in 2023

MFA bypass

83% of organizations that experienced a phishing attack in 2023 had a form of MFA in place that cyber criminals bypassed

Compromise factors

Over 60% of compromise factors come from gaps in users' credential lifecycle that attackers can exploit with relative ease

For example, malicious actors can easily target enterprise users through the IT helpdesk, request a password reset and divert legitimate MFA codes to fraudulent devices such as smartphones and then access a user's email and other accounts. From there, they can infiltrate the corporate network and even install malware, setting the organization up for a ransomware attack. In this manner, even phishing-resistant MFA can be circumvented, and the organization falls out of phishing-resistance.

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, and thus, a phishing-resistant Microsoft ecosystem.

Authentication scenarios supported by Microsoft and the YubiKey

The YubiKey can be deployed alongside Entra ID to protect Azure, Microsoft 365 and remote desktop environments. Deployment can be supported by identifying the highest priority use cases and user populations based on risk and business impact:

Top scenarios for phishing-resistant MFA

Privileged access

Targeted employees who have elevated access to systems or data.

Shared workstation

Employees who need access to shared computers and devices (e.g. customer facing environments and call centers).

Hybrid and remote work

Employees who require remote access to VPN, IAP, IAM, & IDP platforms.

Mobile-restricted

Sensitive environments where mobile devices are not allowed (e.g. call centers, manufacturing environments, server rooms).

High security

Federal and tightly regulated organizations who require a FIPS 140-2 validated solution.

User groups

Office workers

Office workers who can be targets of elaborate credential phishing schemes.

Shared workstation

Shared kiosks, point-of-sale (POS) terminals, and grab-and-go devices can put company and customer data at risk of being hacked.

End customers

Customer accounts are susceptible to attacks & fraud; build loyalty and trust.

Microsoft support for phishing-resistant authentication:

	Privileged access	Shared workstations	Hybrid and remote work	Mobile-restricted	High security	Office workers	Third party	End customers
CBA	✓	✓	✓	✓	✓	✓	✓	
CBA on mobile	✓		✓		✓	✓	✓	
FIDO2 Password-less	✓	✓	✓	✓	✓	✓	✓	✓
WHfB			✓	✓		✓		

MFA Mandate

Microsoft's MFA mandate for Azure users creates a security baseline at the tenant level—a critical protection layer especially considering Microsoft research found that MFA can block more than 99.2% of account compromise attacks. Yubico applauds the move to require stronger authentication for end users and encourages organizations to not only satisfy the mandate, but to also move past all phishable MFA solutions. The YubiKey is designed to be scalable and user-friendly across the Microsoft ecosystem, and Yubico is ready to help organizations meet this mandate.

Also included in the mandate are break glass accounts that provide access to critical systems during a variety of emergencies. Because YubiKeys are phishing-resistant hardware that do not require batteries or an external power source, and can be stored offsite when not in use, they are an ideal break glass account solution.

> “At Microsoft, we are committed to providing the highest levels of protection for our customers. Phishing-resistant multi-factor authentication (MFA) is a critical component to a healthy and secure cybersecurity practice for any organization. Through our FIDO2 Provisioning API integration with Yubico solution, our enterprise customers can quickly implement YubiKey, enhancing employee protection more efficiently. Together, we are empowering our customers to safeguard their digital identities and protect their data against ever-evolving threats.”
>
> **Natee Pretikul** | Principal Product Management Lead | Microsoft Security division

Provisioning APIs

A variety of entities, particularly government agencies, wanted the ability to provision hardware security keys, like the YubiKey, on behalf of their users. As a result, Yubico and Microsoft partnered to create Entra ID FIDO2 provisioning APIs, which give organizations the option to develop or leverage alternative administrator-led provisioning. Before, organizations had to depend on users to register their own security keys—leaving gaps for those that wanted to advance their phishing-resistant journey.

Certificate-based authentication

Certificate-based authentication (CBA) enables organizations with existing smart card and public-key infrastructure (PKI) deployments to authenticate to Entra ID for workstation, application and browser sign-in.

CBA has been a staple of government agencies and other high-security environments for decades due to its reliability and effectiveness in physical environments. Microsoft added cloud-managed support for CBA to eliminate the need for an on-premises federated server to host Active Directory Federation Services (AD FS), allowing users the ability to authenticate using the YubiKey as a smart card without the need for a third-party IAM product.

CBA on iOS and Android

CBA on iOS and Android provides users with the same convenient smart card authentication method using Microsoft Entra ID on mobile devices that they have on their desktops. Leveraging the YubiKey and Entra ID, users can sign in to Microsoft applications as well as third-party and web applications.

Currently the YubiKey is the only external device that supports CBA on Android and iOS, and is also the only FIPS-certified, phishing-resistant solution available for Entra ID on mobile.

Conditional Access

Microsoft Entra allows organizations to create Conditional Access policies—specific user authentication policies—that restrict authentication to defined requirements. For example, policies can be set up to enforce the use of MFA, require minimum authenticator strength (e.g. blocking legacy authentication), or to develop more granular access policies for external customer and partner identities.

Microsoft also offers Conditional Access Policy Authentication Strengths to allow customers the flexibility to require CBA or FIDO2 everywhere except edge-cases where protocols may not yet be supported. This helps move organizations toward the ideal modern passwordless end-state where end-users are no longer allowed to use phishable authentication methods when accessing applications. These out-of-the-box policies can require phishing-resistant MFA via YubiKeys (FIDO2 and CBA), CBA or Windows Hello for Business (WHfB), as well as custom policies to enforce specific YubiKey use (e.g. YubiKey 5 FIPS series).

Azure Virtual Desktop and Remote Desktop

Azure Virtual Desktop (AVD, formerly Windows Virtual Desktop) and Microsoft Remote Desktop Services (RDS) support remote access to Windows 11 and Windows 10 desktops, Windows Server and Microsoft 365 applications from both desktop and mobile devices. Since AVD and RDS rely on Entra ID for authentication, you can support users with a virtual desktop with the same security and work experience no matter where they are.

AVD and RDS enable users to use their YubiKey (using FIDO2 passwordless and CBA) to sign into the remote desktop or an application inside the virtual desktop.

Entra ID-protected iOS and iPadOS native apps also support passwordless logins via the YubiKey. As a result, users can connect their iPhone or iPad to Azure Virtual Desktop, Windows 365, admin-provided virtual apps and desktops and remote PCs. Lightning and USB users can insert their YubiKey, while NFC users can simply tap the top of their iPhone with their YubiKey.

Passwordless authentication

In addition to support for smart card/PIV, Microsoft has continued to implement FIDO2 passwordless authentication across its ecosystem while extending this directive to Microsoft partners to eliminate the risks associated with passwords and deliver a seamless user experience.

YubiKeys work together with both Windows Hello for Business (WHfB) and Microsoft Entra to provide a phishing-resistant passwordless login flow to Windows 11 and Windows 10 workstations, native apps, web applications and remote desktops.

Windows Hello for Business (WHfB)

WHfB replaces passwords with strong phishing-resistant authentication for Windows via platform authentication where the credentials are protected on a TPM and unlocked with PIN or biometrics. WHfB is leveraged for dedicated Windows workstations and for hybrid and cloud-only environments with Entra ID.

The YubiKey can be used in combination with platform authenticators to add portability and high assurance, extending to additional use cases that lack TPM or biometric support, to mobile devices and to support shared workstations that would require re-registering the WHfB. The YubiKey can also be used as a back-up to support account recovery or to bootstrap WHfB to other devices.

Getting started is easy

With Microsoft and the YubiKey, public and private organizations receive phishing-resistant, strong hardware-backed authentication that is simple to deploy across multiple applications as well as modern devices with single sign-on (SSO) capabilities for a smooth user experience when accessing apps and services.

We have made it easy to deploy the YubiKey to your Microsoft ecosystem and workforce—including remote workers. We offer a simple 6 Step Best Practice Deployment Guide to help accelerate modern MFA adoption at scale.

Plan

Ensure readiness clarify 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

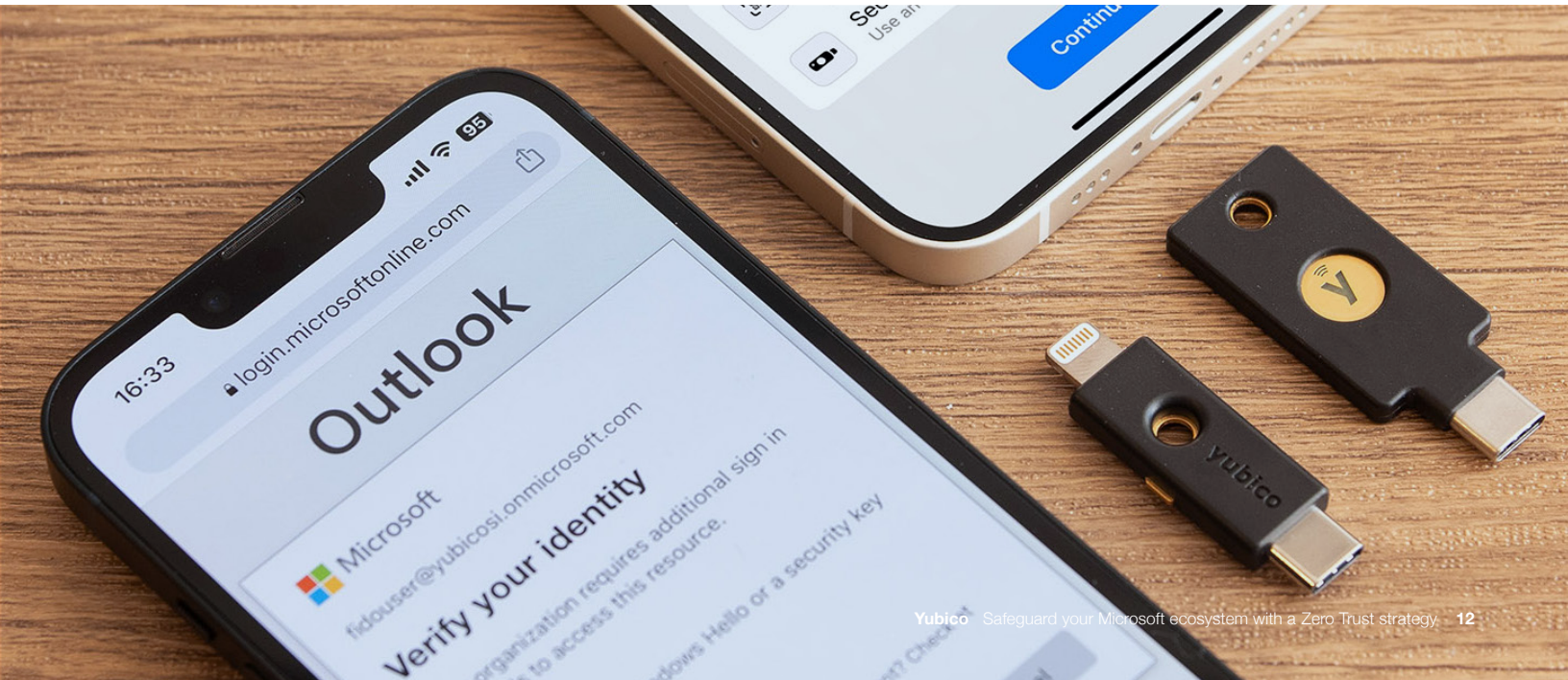
Adopt

Drive adoption with best practice training and support

Measure

Report on security and business value impact

Yubico also offers **YubiKeys as a Service** and **YubiEnterprise Delivery**, to help simplify procurement and distribution of YubiKeys. If you want a closer partnership on any of the six steps of this plan, Yubico's Professional Services team is here to help.



> The fact that I can ensure identity with a physical YubiKey, even for remote workers, is very beneficial for my efforts to reduce risk at Afni.
>
> **Brent Deterding** | CISO | Afni

Microsoft and YubiKey in action

Real-world success stories

Afni strengthens cybersecurity with YubiKey and Microsoft Conditional Access

Afni provides comprehensive inbound, outbound, and digital channel services around the world. In this business, targeted phishing attacks are a big problem, despite having MFA deployed to almost all of its 10,000 global employees—it's too easy for users to be conditioned to hit 'approve' for every request to authenticate (MFA fatigue) or to fall prey to a phishing attack. However, the fault for these lies not with the user, but with legacy authentication.

Already a Microsoft customer, Afni took advantage of the native support for the YubiKey, a phishing-resistant hardware security key that could be used to enable easy and secure access to OneDrive, SharePoint and Office365 for all non-production office workers and to provide remote access for VPN remote workers. Afni took advantage of Microsoft Entra ID (previously Azure AD) Conditional Access features to enforce YubiKey usage for all required applications and leveraged Microsoft Intune for endpoint management. As part of its cybersecurity efforts, the combination of the YubiKey with Microsoft solutions helped Afni demonstrate a comprehensive reduction in risk to cyber insurers—to the tune of a 30% price reduction.

> The biggest benefit that Hyatt is going to receive from deploying YubiKeys is to be able to get rid of passwords in our environment. You can't compromise what you don't have. I think we're going to have a great big party once we turn that button off and there's no more passwords anywhere in the environment."

Art Chernobrov | Director of Identity, Access, and Endpoints | Hyatt Hotels Corporation

Yubico and Microsoft deliver strong identity, endpoint and access controls to Hyatt Hotels

Hyatt Hotels Corporation is one of the world's most well-recognized and respected hospitality brands with approximately 1,500 hotel and all-inclusive properties spanning across 70 countries. With so many properties and employees spread out across the globe, it is a daunting task to keep them all safe from an ever growing list of cyber risks.

Hyatt has worked closely with Microsoft for the past decade, onboarding products such as Office 365 and Microsoft Entra ID. While the latter was ticking all the boxes for provisioning access and managing identity, Hyatt's implementation of MFA was a source of user friction (passwords + OTP) and risk—in fact, every compromise at Hyatt could be traced back to an inadvertently approved MFA request.

Microsoft introduced Hyatt to the YubiKey to provide both a phishing-resistant and passwordless authentication experience for all front-of-house, call center and loyalty program colleagues as well as to supply chain partners. To use a YubiKey in any scenario, colleagues simply insert the key and either tap or enter a PIN to authenticate to Entra ID resources. The long-term goal is to ensure every new application has SSO under Entra ID to entirely eliminate passwords.

The City of Southgate, Michigan leads the way in public sector security with Yubico and Microsoft

Southgate, Michigan has a population of over 30,000 residents and is a growing business community that's a part of the Downriver fellowship of communities south of Detroit. While all municipalities have a responsibility to keep citizens secure, the City of Southgate extends its duty beyond police, fire and public works to defend critical infrastructure and citizen data against cyber threats.

Recognizing that 49% of ransomware attacks in SLTT governments begin with phishing and the use of compromised credentials, Southgate's Director of IT knew the city needed a solution that would support the highest assurance security and varied authentication scenarios, while also working seamlessly across Microsoft's cloud infrastructure and Entra ID.

Southgate combined Yubico's hardware-based authentication and Microsoft Entra CBA to achieve a compliance level that exceeds federal mandates such as CJIS and EO 14028. Southgate is now on the forefront of the country for public sector security posture and is firmly on the path to Zero Trust.

"Our team uses mobile phones, tablets, and other devices. Through Yubico, I need to partner indirectly with Microsoft to understand what they have, what they offer, and how it works with the YubiKey. The YubiKey works to replace one-time passwords, it works as multi-factor authentication, it factors all that into one easy-to-use device. I was able to implement it with my forward thinking methods. I feel like it's put me in the top 1% of public sector for implementing this using certificate-based authentication that Microsoft provides. I am freed up to focus on servicing the people in my city."

Jason Rucker | Director of Information Technology City of Southgate, Michigan

Sources

[1] PwC, Global Digital Trust Insights 2023, (Accessed April 6, 2023)

[2] Synergy Research Group, Cloud Provider Market Share Trend Q2 2023, (August 3, 2023),

[3] IBM, 2023 Cost of Data Breach Report, (July 24, 2023)

[4] Fortinet, 2023 Work-from-Anywhere Global Study, (March 7, 2023)

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

[6] IBM, 2023 Cost of Data Breach Report, (July 24, 2023)

[7] Microsoft, Zero Trust Business Plan, (Accessed September 12, 2023)

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

[9] Lucas Augusto Meyer, et. al., How effective is multifactor authentication at deterring cyberattacks, (May 1, 2023)

[10] S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, (2023)

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

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

[13] The White House, Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, (January 19, 2020),

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

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

yubico

About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, 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.

For more information, please visit: www.yubico.com.