

DATASHEET

The progression of MFA: How Yubico and key partners work together to provide impactful solutions

In 2023, the average cost of a data breach jumped from \$4.45 million to \$4.88 million.¹ Since the majority of breaches (74%²) come from human-managed vulnerabilities, including stolen credentials and phishing, enterprises are under tremendous pressure to adopt phishing-resistant multi-factor authentication (MFA).

Yet, despite MFA investments, organizations remain susceptible to phishing attacks. 83% of organizations who experienced a phishing attack in 2023 had a form of MFA in place that cyber criminals bypassed.³ 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%.⁴

\$4.88
million usd

average cost of
a data breach

74%
of breaches

stem from human-managed
vulnerabilities

83%
of organizations

targeted by phishing
attacks in 2023 had only
legacy MFA in place

10-24%
of legacy MFA

methods are compromised
by phishing and advanced
cyberattacks



Threats are more
sophisticated, but
so is protection

The YubiKey is a hardware security key that supports phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimized user experience—and is proven to reduce risk against phishing attacks and account takeovers by 99.9%.⁵

As part of Yubico's mission to make the internet safer for everyone, it partners with leading organizations—including Microsoft, Beyond Trust, Axia, Okta, and Intercede—to develop solutions that counteract ever-evolving threats.



As a leading provider of nearly a quarter (23%) of global cloud infrastructure services,⁶ Microsoft is committed to ensuring the highest levels of security through its Secure Future Initiative which, amongst other deliverables, mandates multi-factor authentication (MFA) protection for all Microsoft portal administrators.

To support this, the YubiKey integrates seamlessly with Entra ID, offering a powerful hardware-based authentication solution that provides an additional layer of protection for Azure, Microsoft 365, and remote desktop environments. This ensures that sensitive data and critical systems are safeguarded against unauthorized access.



As one of the global leaders in the identity space, Okta provides seamless and secure access, authentication, and authorization. Yubico and Okta have partnered together over the years to provide the strongest level of identity assurance and defense against phishing and man-in-the-middle attacks while also delivering a simple and seamless user experience—all with just the touch of the YubiKey.

The YubiKey protects critical assets with Okta Adaptive MFA and gives users complete control over identity and access. In 2024, Okta was the first partner to adopt and rollout [Yubico's FIDO Pre-reg](#) service as part of the Yubi Enrollment Suite to over 6000 of their employees globally, which enabled them to create phishing-resistant users and as a result, a phishing-resistant enterprise.



As a global leader in privileged access management (PAM), BeyondTrust is at the forefront of securing the most targeted users through a comprehensive Zero Trust strategy. This strategy mandates the use of FIDO2-certified authenticators, such as the YubiKey, to ensure secure on- and off-site logins for employees, vendors, and end users.

By integrating the YubiKey, BeyondTrust enhances its security framework, providing robust protection against unauthorized access and reinforcing its commitment to safeguarding critical systems and sensitive data.



Axiad excels in providing comprehensive authentication life-cycle management across computers, networks, and online services for both IT professionals and end users. By integrating the YubiKey, Axiad streamlines critical processes such as provisioning, account recovery, and credential renewals.

This integration not only eliminates the risk of account takeovers but also supports multiple authentication protocols and achieves FIPS 140-2 compliance. Through this partnership, Axiad ensures robust security and seamless user experiences, reinforcing its commitment to protecting digital identities.



Intercede's MyID serves as both a FIDO authentication server and a PKI credential management system, providing robust security solutions for enterprises. By partnering with Yubico, Intercede offers even stronger protection through the seamless integration of the YubiKey by enabling organizations to deploy PKI certificates to YubiKeys through MyID. Intercede and Yubico together provide strong hardware-backed protection at scale.

This integration works effortlessly across existing infrastructure via REST APIs, Microsoft ADFS adaptor, or OpenID Connect / OAuth 2.0, as well as leading web browsers. Together, MyID and YubiKey deliver comprehensive security, ensuring that enterprises can protect their digital assets with confidence.

“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.”



Jason Rucker
Director of IT | City of Southgate, MI



“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

“The nice thing about Okta and the YubiKey combination is the flexible configuration options it provides. We started small, requiring FIDO2 on only a few applications, but very quickly we expanded to all applications for employees in critical risk functions.”



Devdatta Akhawe

Head of Security | Figma

Future-proof protection

As human attackers bolster their efforts with AI and machine learning, Yubico and its partners give enterprises the highest-assurance protection while ensuring a seamless user experience that drives high productivity and business continuity.

Phishing-resistant users create phishing-resistant enterprises

Yubico makes it easy to create phishing-resistant users—ensuring that every user within the organization has phishing-resistant authentication that moves with them no matter how they work, across devices, platforms, and systems. With the YubiKey, enterprises can confidently protect their digital environments, providing seamless and secure access for all users, ensuring that authentication is not only secure but also user-friendly, enhancing productivity and security simultaneously.



YubiKeys deployed in:

9 of the top 10
global technology
companies

4 of the top 10
U.S. banks

5 of the top 10
global retailers



Contact us
yubi.co/contact



Find integrations
yubi.co/wwwyk

¹ IBM, *Cost of a Data Breach Report 2024*

² Verizon, *2024 Data Breach Investigations Report*, (June 6, 2023)

³ Egress, *Must-know phishing statistics for 2024*, (January 19, 2024)

⁴ Kurt Thomas and Angelika Moscicki, *New research: how effective is basic account hygiene at preventing hijacking*, (May 17, 2019)

⁵ Forrester, *The Total Economic Impact of Yubico YubiKeys*, (September 2022)

⁶ Egress, *Cloud Market Growth Stays Strong in Q2 While Amazon, Google and Oracle Nudge Higher*, (August 1, 2024)