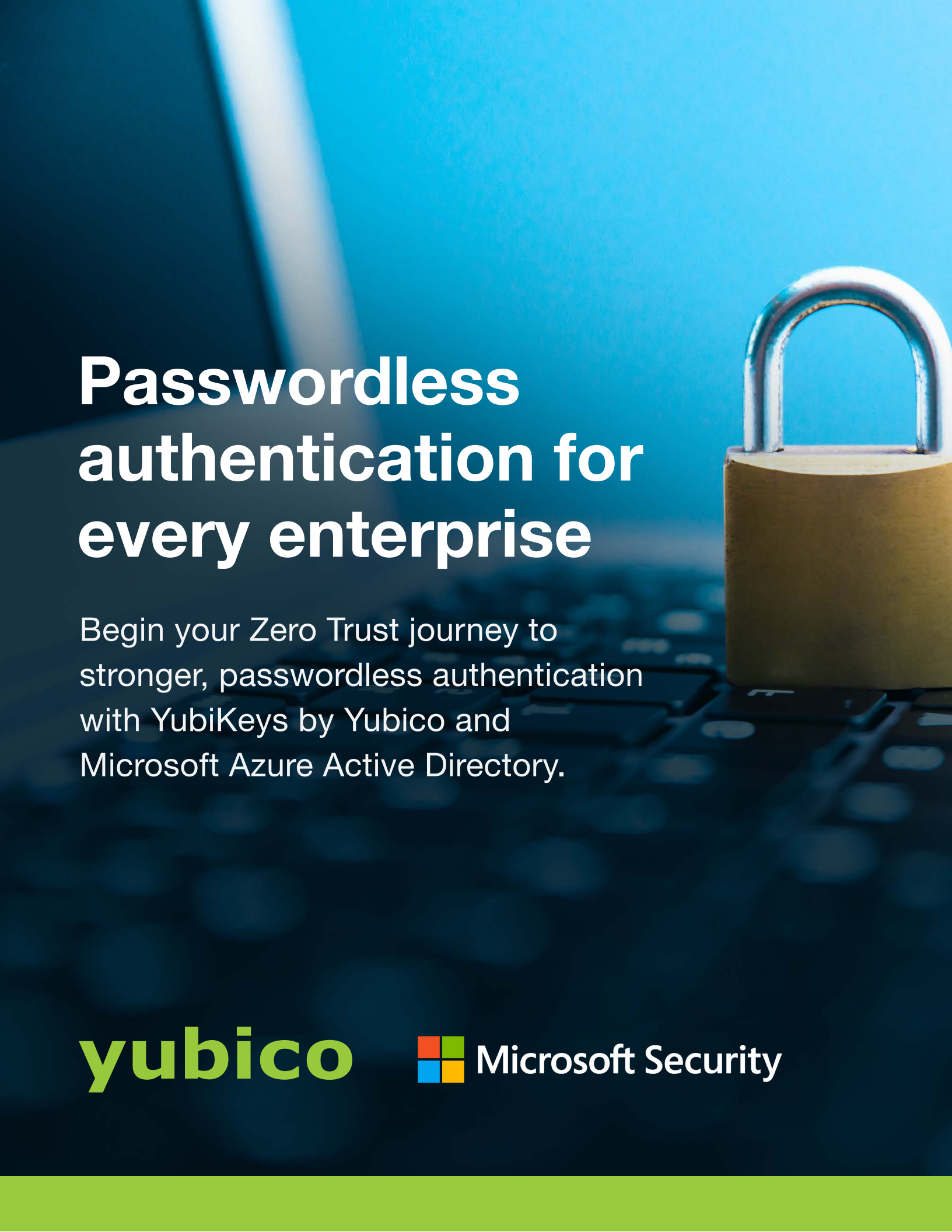


Passwordless authentication for every enterprise

Begin your Zero Trust journey to stronger, passwordless authentication with YubiKeys by Yubico and Microsoft Azure Active Directory.

yubico

Microsoft Security

Contents

How do you validate who is accessing your corporate network?.....3
Secure modern and legacy systems.....4
Enable seamless authentication anywhere.....6
Block remote phishing and MITM attacks.....7
Case study: Nunavut Northern Territories.....8
Start your Zero Trust journey and identity protection with passwordless authentication.....9

How do you validate who is accessing your corporate network?

Large-scale data breaches and credential theft are putting your user accounts at risk.

Today's organizations are embracing the Zero Trust security model to effectively adapt to the complexity of the modern environment, embrace the hybrid workplace, and protect people, devices, apps, and data wherever they're located. With the explosion of apps, devices, and users across and outside of the corporate network, it is difficult to validate identities for not only employees, but also external partners, suppliers, distributors, and end consumers. Organizations are constantly faced with the lurking possibility of a large-scale data breach and credential theft.

The global shift to remote work has only increased the security risk as more workers require access to corporate resources from outside the office. This puts pressure on IT to enable flexible and productive experiences for their distributed workforces while still securing user access and remaining compliant with changing regulations. How, then, can enterprises protect their organization from cyberattacks while adapting to changing business needs? The solution: go passwordless. Removing passwords and using strong authentication is the first step on the Zero Trust journey.

80% *of data breaches are caused by compromised, weak, and reused passwords.*[1]

$70 *is the average estimated cost of a single password reset.*[2]

37 billion *records were compromised in 2020, adding to the growing number of credentials cybercriminals use as source material.*[3]

Stop account takeovers at scale with strong authentication for traditional and passwordless environments.

Together, Microsoft and Yubico have paved the way for a passwordless future for organizations of all sizes. With FIDO2/WebAuthn, organizations can now benefit from a frictionless user experience while strengthening security with phishing-resistant, hardware-based, security key authentication. Whether your environment is on Microsoft Azure Active Directory or on-premises with Microsoft Active Directory, the YubiKey by Yubico offers a solution that supports you on your journey to passwordless authentication.

Secure modern and legacy systems

Enable multiple authentication options with a single key.

Implementing the Zero Trust methodology and going passwordless doesn't need to happen all at once. Passwords are common, entrenched in the enterprise, and cannot be replaced immediately. Though it may not be possible for many organizations, applications, and scenarios to immediately support passwordless sign-in, IT can begin the Zero Trust journey by planning ahead to enable the YubiKey to support the following implementations.

Consider modernizing with FIDO2.

Whether you have on-premises or cloud environments, FIDO2 can be leveraged to solve password concerns by allowing organizations to go passwordless in the way that makes the most sense for them. FIDO2 is an open standard, co-developed by Yubico, Microsoft, and other members of the FIDO Alliance. It was designed to support both passwordless and two-factor authentication options so that organizations can choose what's right for their identity and authentication strategy.

Implement change with MFA.

Passwords are the weakest link in a security chain and a single point of failure without any additional verification. If organizations can only do one thing, they should implement modern MFA – which can prevent 99.9% of identity attacks.[4] MFA enables a smoother passwordless transition once the full set of capabilities is in place and passwords can finally be eliminated. This gives organizations the time they need to slowly implement changes to modernize their infrastructure and business.

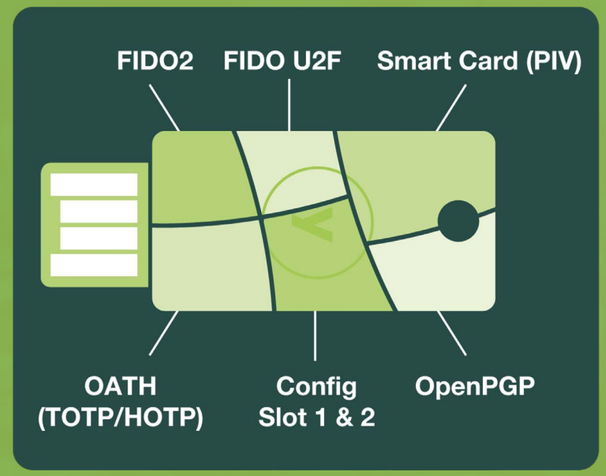
Provide multi-protocol authentication support.

The YubiKey supports multiple methods for authentication, enabling the same device to be used across platforms, services, and applications.

Smart Card/PIV The YubiKey supports out-of-the-box integration on Microsoft Windows Server 2008 R2 and later servers, and Windows 7 and later clients.

FIDO2/WebAuthn and Universal 2nd Factor (U2F) FIDO2 is an extension of FIDO U2F and is based on public key cryptography. FIDO2 offers expanded support for strong passwordless, two-factor, and multi-factor authentication.

One-Time Password (OTP) A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for a single transaction or login session.



Enable seamless authentication anywhere

Discover faster login flows and eliminate password hassles.

Say goodbye to forgotten passwords and expensive password reset scenarios. With FIDO2, organizations can now remove the inconvenience related to passwords, and accelerate business without compromising security. YubiKeys are a seamless fit with Microsoft Azure AD environments and can complement or be used in parallel with Windows Hello for Business and the Microsoft Authenticator app with supporting browsers, including Microsoft Edge and Google Chrome.

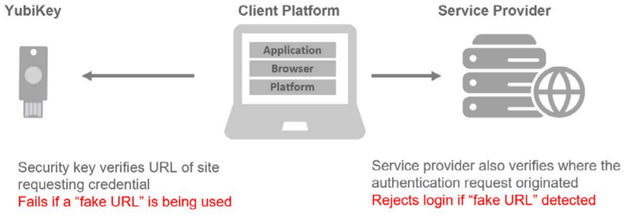
Discover a frictionless user experience.

Organizations can improve usability by authenticating with a simple tap or touch using YubiKeys. Simply touch the YubiKey while plugged into a USB port or tap with contactless near-field communication (NFC) for quick and easy sign-on. Yubico offers enterprise services such as YubiEnterprise Subscription and YubiEnterprise Delivery for flexible purchasing options and distribution of YubiKeys to remote workforces.

How does passwordless authentication with a YubiKey work?

Passwordless authentication is made possible by the new FIDO2 open authentication standard co-authored by Yubico and Microsoft, along with members of the FIDO Alliance. As YubiKeys support multiple security protocols, organizations can use Yubico's strong authentication in their existing environments and allow the YubiKey to serve as their bridge to passwordless security, in addition to adopting Microsoft Azure AD.

FIDO2 Phishing Resistant by Design



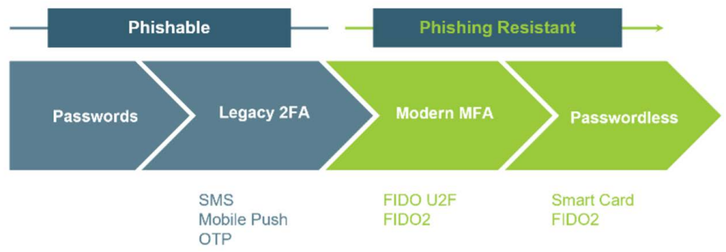
Block remote phishing and MITM attacks

Stop account takeovers by going passwordless.

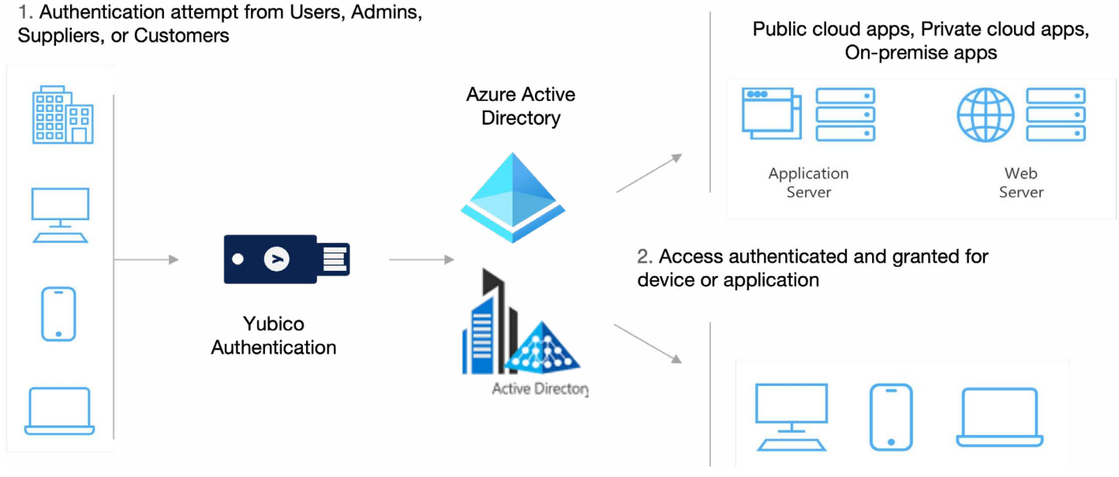
Phishing continues to be a primary method for stealing credentials from employees, vendors, and customers. In fact, 91% of cyberattacks begin with a phishing email.[5] Basic two-factor authentications (2FA) such as email, OTP, and SMS are still susceptible to attacks as they do not have high-security assurance. YubiKeys provide the highest resistance to phishing and enhance the security of existing IAM solutions. The YubiKey helps organizations achieve the highest level of security and usability, at any scale. Unlike other MFA solutions, the YubiKey is purpose-built for security and highly resistant to phishing attacks as the keys do not store any personal data and do not require network connection, battery, or client software.

The Journey to Passwordless

Strong Authentication Step by Step



Solution Integration with Microsoft



Case study: Nunavut Northern Territories

Challenge

In November 2019, the Government of Nunavut was the victim of a sophisticated spear phishing attack, which ultimately led to ransomware that took down critical servers, phone lines, and applications.

Solution

Due to inconsistent cellular networks across Nunavut communities and the constant threat of phishing attacks, the Microsoft Detection and Response (DART) security team recommended the YubiKey.

Results

Azure AD and the YubiKey's multi-protocol functionality allowed government employees to increase their security posture and use a single YubiKey for authenticating in their existing systems as a smart card as well as for passwordless authentication into modern cloud-based architectures through FIDO2.

Start your Zero Trust journey and identity protection with passwordless authentication

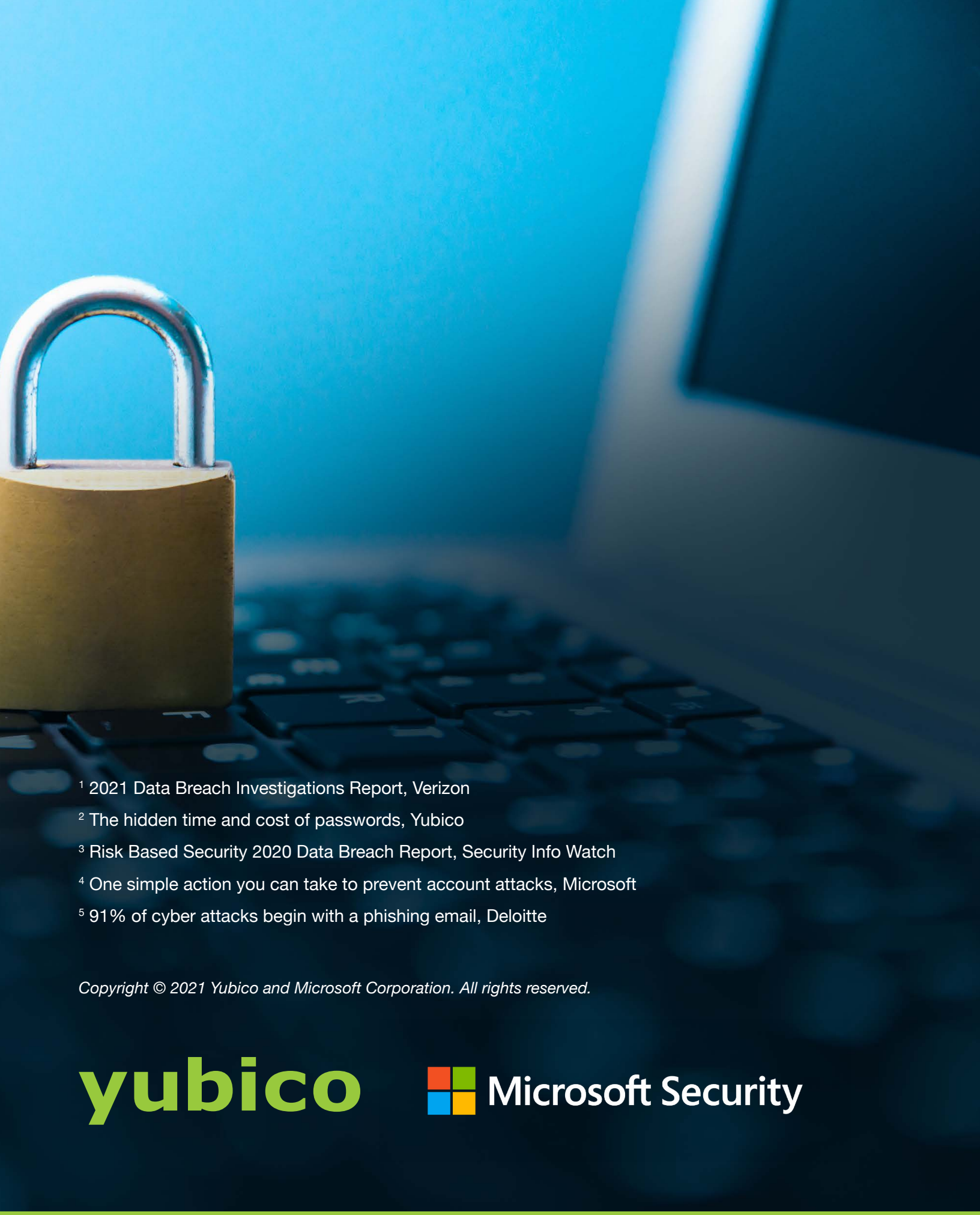
Yubico is a leading contributor to both the FIDO2 and FIDO U2F open authentication standards and the company's technology is deployed and loved by 9 out of the top 10 internet brands and by millions of users in over 160 countries.

Yubico is also a member of the Microsoft Intelligent Security Association (MISA) and is closely aligned with Microsoft to deliver strong hardware protection with a simple touch across any number of IT systems and online services.

With YubiKey, organizations can benefit from:

- Zero account takeovers.
- 92% support reduction.
- 4x faster logins.

>> Learn more today.



[1] 2021 Data Breach Investigations Report, Verizon

[2] The hidden time and cost of passwords, Yubico

[3] Risk Based Security 2020 Data Breach Report, Security Info Watch

[4] One simple action you can take to prevent account attacks, Microsoft

[5] 91% of cyber attacks begin with a phishing email, Deloitte

yubico

Microsoft Security