yubico

A YUBICO WHITE PAPER
JUNE 2020

Going Passwordless in the Public Sector

with FIDO2 and WebAuthn

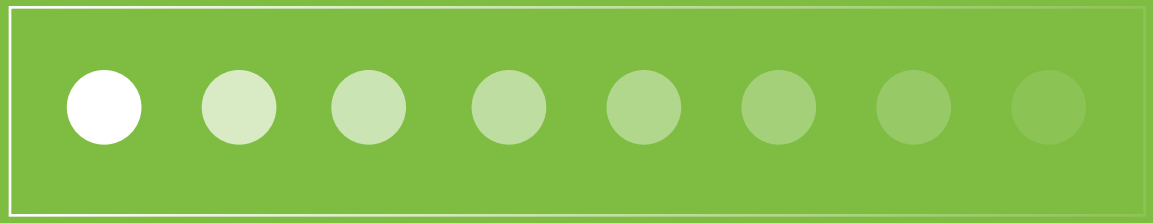


Table of Contents

Executive Summary

Cyber-espionage is rampant in the public sector, with state affiliated actors accounting for 79 percent of breaches involving external actors and privilege misuse and error by insiders account for 30 percent of breaches[1]. The widespread use of passwords to access applications and services internally by employees or contractors, and externally by citizens puts public sector entities at risk of being hacked and their data and systems compromised. In addition, forgotten passwords and account lockouts can stack on help desk costs and time.

Instead, imagine a world without passwords. The new FIDO2/WebAuthn authentication standards offer the opportunity for public sector entities to strengthen their security postures and go password-less. FIDO2 is an open standard co-developed by Yubico, Microsoft, and other members of the FIDO Alliance that builds on FIDO U2F to offer the flexibility of passwordless single factor or passwordless multi-factor strong authentication to all users - employees, contractors, vendors and suppliers and end-customers. Given that password resets currently represent the #1 IT support cost, password-less login promises to significantly reduce workloads in IT call centers while offering the opportunity to transform authentication security and user experiences.

How might customer and workforce journeys be streamlined with passwordless login? What new products and services become possible when passwords are no longer required? These are the questions that forward-thinking leaders should be asking now.

This whitepaper provides the background on passwordless authentication and considerations for deployment in the public sector.

The Time and Cost of Passwords

Security technologies and controls are put in place to protect the organization, however those same security controls can frustrate users. High on everyone's list of cumbersome, irritating security controls are passwords.

Passwords have been a fact of life since the 1950s for business users and consumers alike. Nearly every digital experience requires them—from social networks like Facebook, to banks and retailers like Chase and Macy's, to business applications like Salesforce and QuickBooks Online.

The average U.S. consumer tries to keep track of over 14 different passwords, which they use across all their web sites and services[2], while business users are estimated to be responsible for memorizing and using an even greater number of passwords, as many as 191.[3] With Millennials making up a growing share of the workforce, the results from an IBM study show they are less patient with memorizing all these secrets. They are more likely to reuse passwords, memorizing no more than eight, compromising security in the name of convenience.[4]

Password Fatigue Leads to Data Breaches

Users grow tired of creating new passwords for different services and having to change passwords every few months according to the dictates of security policies. To reduce memorization, many users end up relying on simplistic passwords which unfortunately are easy to crack or reuse passwords across multiple sites, where breach of one service, can open the door to many.

Most data breaches involve a weak password. NCSC's 2019 Cyber Survey security breach analysis found that 23.2 million victim accounts worldwide used 123456 as password.[5]

23.2 million victim accounts worldwide used 123456 as password.[5]

National Cyber Security Center
2019 Cyber Security Survey

In a single month in 2017, Microsoft had to reset 686,000 passwords for users, resulting in support expenses of over $12 million.

Forgotten Passwords Lead to High Support Costs

When users forget their passwords, they often end up calling help desks or support centers, consuming valuable time. Password-reset inquiries account for up to 6% of call center activities, costing large enterprises between $5 million and $20 million annually.[6] Gartner estimates that these password reset inquiries are even more frequent and costly, comprising 20% to 50% of all help desk calls.[7]

Microsoft estimates that password management costs (including password recovery, lockout, and changing passwords) constitute the largest single IT support expense. In a single month in 2017, Microsoft had to reset 686,000 passwords for users, resulting in support expenses of over $12 million.[8]

Phishing Attacks Target Credential Theft

Phishing continues to be a massive security problem as attack techniques continue to evolve. Fake email messages urging users to re-enter their credentials can be used for harvesting credentials to be used for account takeovers. About 30% of phishing emails are opened by their recipients, and over 7% of email recipients were persuaded to open an attachment or click on a link, which often is a login link. Most phishing attacks then lead to the installation of malware leveraged to help perpetrate a breach.[9] Even if users set up complex passwords, hackers can gain access to them through phishing and penetrate user accounts.

Stolen Credential Lists Available for Sale

When hackers break into an organization and steal credentials, they gain access not only to that organization's accounts but also accounts and services where users have used the same username-password pair. Billions of stolen credentials are available for sale on the Dark Web and cyber criminals are now launching automated login attempts with this trove of stolen passwords.

As long as IT has to rely on passwords for authentication, costly support requirements, weak security, and frustrating experiences are inevitable.

Solving the Password Problem with FIDO2

Imagine offering fast, convenient, and secure services of all kinds to users, whether customers or employees, without requiring passwords, and without incurring the operational overhead of password management. Imagine customers, partners, and employees on desktops and mobile devices being able to instantly access content and services they want without having to conjure passwords from memory or call the support desk for help. Imagine new services that could be enabled if authentication were instantaneous and easy. Imagine IT organizations freeing themselves from the daily grind and expense of managing and resetting passwords.

FIDO2 is a new authentication standard that offers the option for passwordless authentication.

The Benefits of Passwordless Authentication

Improved Usability
Passwordless authentication frees users from having to remember and type passwords.

Improved Security
Passwordless authentication eliminates the security risks associated with stolen passwords and brute force attacks against login screens.

Improved Efficiency
Passwordless authentication eliminates the need for IT departments to manage passwords.

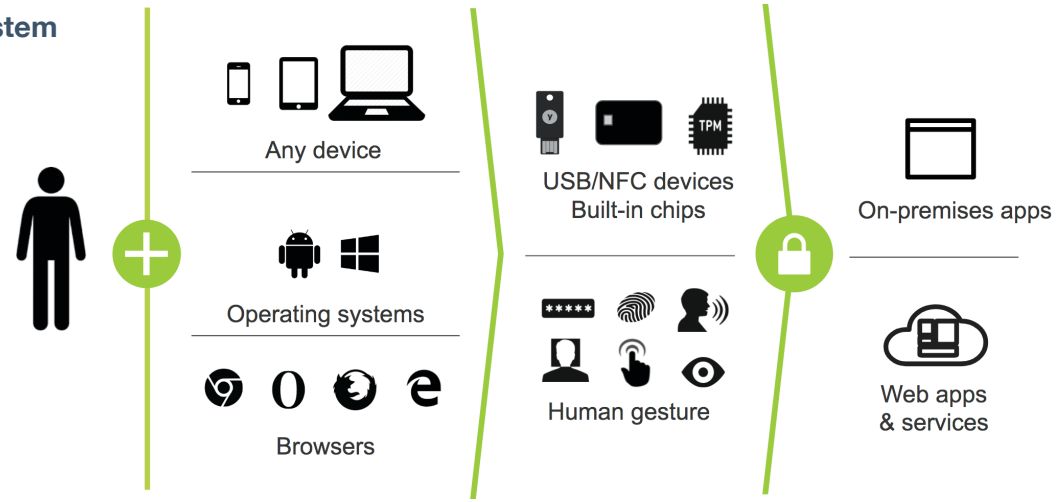
These benefits of passwordless authentication can now be achieved with the new FIDO2/WebAuthn open authentication standards.

Introducing Passwordless Authentication

FIDO2 is a new authentication standard co-authored by Yubico, Microsoft and members of the FIDO Alliance, in conjunction with the World Wide Web Consortium (W3C), supporting multiple use case scenarios and experiences.

FIDO2 is comprised of two standardized components, a web API (WebAuthn) and a Client to Authenticator Protocol (CTAP). The two work together and are required to achieve a passwordless experience for login. WebAuthn defines a standard web API that can be integrated into browsers and web platform infrastructure to give users new methods to securely authenticate on the web. CTAP enables an external authenticator, such as a security key, to communicate strong authentication credentials locally over USB, NFC, or Bluetooth to the user's PC or mobile phone.

FIDO2 Ecosystem



FIDO2 relies on an asymmetric (public/private) pair of cryptographic keys to authenticate users. The public key is stored on any service or computing device supporting FIDO2 authentication, while the private key is kept by the user and is protected on a physical security key, such as the YubiKey 5 Series and Security Key by Yubico. Authentication itself is fast and easy: by simply inserting or tapping the security key the authentication challenge is completed, and login is immediate.

With FIDO2, the security key can be used on its own or in conjunction with a PIN or gesture to provide strong passwordless authentication, in addition two factor authentication with a password continues to be a supported authentication mode.

World Wide Web Consortium (W3C) support for FIDO2

The Web Authentication (WebAuthn) API specification gives browser users new methods to securely authenticate on the web based on the FIDO2 specification. Microsoft Edge, Google Chrome and Mozilla browsers all support the WebAuthn API specification.

FIDO2/WebAuthn Authentication Choices

Single Factor (Passwordless)
Use of the security key on its own as a strong first factor of authentication, requiring only the possession of the device, allowing for a tap and go passwordless experience

Two Factor (Password + Authenticator)
Use of the security key as a second factor in a two-factor authentication solution

Multi-Factor (Passwordless + PIN or Biometric)
Use of the security key for multi-factor authentication requiring possession of the device AND a PIN or Biometric, to solve high assurance requirements

FIDO2 is supported on Windows 10 devices, including Windows desktop and mobile systems, running the latest release of Windows 10. This makes FIDO2 available on over 400 million devices around the world and billions of Azure AD accounts.

Benefits of Going Passwordless

Improved Usability

FIDO2 passwordless login makes authentication fast and easy, by eliminating the need for passwords.

FIDO2 passwordless login makes authentication fast and easy by eliminating the need for passwords. With FIDO2, a single hardware authenticator, such as a YubiKey, can be used to authenticate across all the services a user interacts with, including business applications and services at work, social media networks, and other consumer applications at home with no shared secrets.

At the same time, FIDO2 can be used to support multiple identities for a single user. The same YubiKey can be used for access to both business and consumer applications, websites, services, servers, and devices–ranging from buildings to vehicles–designed to support FIDO2.

With passwordless authentication, employees and contractors traveling on planes or subways lacking Wi-Fi or cellular access can still authenticate to their laptops and work productively and securely, even if their lack of network access prevents them from receiving SMS or OTP credentials for user authentication.

FIDO2 eliminates the need for network access (either cellular or internet-based) to receive second factors. In addition to strengthening IT security, FIDO2 makes it easier for users to access the devices they need for work anytime, anywhere.

FIDO2 is supported on Windows 10 devices, including Windows desktop and mobile systems, running the latest release of Windows 10. This makes FIDO2 available on over 400 million devices around the world and billions of Azure AD accounts. Microsoft Accounts support FIDO2 authentication, enabling passwordless login on many of the Microsoft services including: Outlook, Office, Skype, OneDrive, Xbox Live, Bing, MSN, Windows.

Because FIDO2 has been developed as an open industry standard and is being broadly championed by Microsoft and the World Wide Web Consortium (W3C) with support from Google and Mozilla, adoption does not depend on any single entity. FIDO2 saves organizations the expense of having to invest in the development and maintenance of custom security models to address the problems of passwords. Now public sector organizations can take advantage of an open industry authentication standard endorsed by industry leaders.

Improved Security

FIDO2 dramatically improves the security of user authentication and access management.

FIDO2 dramatically improves the security of user authentication and access management.

With passwordless login users cannot be tricked into unexpectedly divulging passwords, since passwords are no longer required. Users authenticate with a hardware authenticator such as a YubiKey, which at a high level works as follows:

- The YubiKey creates and manages the FIDO2 credential (a public/private key pair) including binding the credential to the specific service, known as the origin. Origin binding prevents Man in the Middle attacks.
- When presented with an authentication challenge by a service such as Azure AD, the private key is used to sign the response which is sent over the network and verified by the online service using the public key.

The FIDO2 credential, which is stored on a secure element chip within the YubiKey and which never leaves the device, is designed to prevent hackers from spoofing users logging in to sites.

FIDO2 reduces risk for applications, websites, services, servers, and devices by removing the centralized storage and management of sensitive credentials. FIDO2 accounts don't need a password; therefore there is no longer a trove of passwords to steal. Web sites and other services store only the public keys that users have registered, thus the secret (private key) is maintained securely on the hardware authenticator, and never sent over the network like a traditional password. Those public keys can validate signatures generated by the private keys, but they are useless on their own for initiating access to other resources. Only an end user with the FIDO2 private key can successfully authenticate to a service. Security improves, while also making login access quicker, easier, and more reliable for end users.

Authentication privileges can be granted in compliance with security policies specific to the organization or required by industry regulations, such as GLBA and HIPAA, or government regulations such as NIST SP800-63. By complying with NIST SP800-63, FIDO2 ensures compliance with a broad range of other regulations that build on NIST standards. IT administrators and compliance officers can be confident that users are not circumventing authentication controls by sharing passwords on post-it notes or by email. Each user is issued a unique key that authenticates them to registered services and applications.

Meeting NIST Authentication Standards

FIDO2 can be either a Single Factor Cryptographic Token or a Multi-Factor Cryptographic Token. According to NIST Special Publication 800-63, the Multi-Factor Cryptographic Token is categorized as Authentication Assurance Level 3, which is the highest assurance level declared by that standard. Using FIDO2 with a PIN therefore meets the highest authentication requirements in regulated markets where compliance with NIST SP800-63 is mandatory.[10]

"FIDO2 does not require a complex PKI environment to manage certificates"

Improved Efficiency

FIDO2 enables IT departments–including service desks and call centers—to be free from having to create, store, cycle, and reset passwords.

Passwordless login offers the opportunity for hassle-free employee and contractor onboarding, eliminating the support costs of issuing and managing passwords. Instead of issuing new employees and contractors temporary passwords that must be changed immediately and then changed again on a prescribed schedule, with FIDO2 authentication each user is simply issued a FIDO2 security key and the user optionally specifies a PIN at issuance. FIDO2 authentication privileges can be easily revoked when an employee or contractor finishes their service for the company.

Using the FIDO2 security key, users can authenticate themselves to a central service such as Azure AD, establishing their identities so that they can register new devices, such as smartphones. In organizations where computing devices are shared, each user can quickly and easily authenticate without having to remember and enter passwords. By simply inserting or tapping an NFC-enabled YubiKey, users can unlock their devices and gain access to their accounts.

In addition, FIDO2 does not require a complex PKI environment to manage certificates. IT department can redirect their time and efforts to more strategic and productive tasks.

Meeting Critical Requirements for User Authentication

FIDO2 meets all these critical requirements for user authentication:

- **Provides credentials that cannot be hacked or spoofed**
- **Provides an authentication method that prevents phishing**
- **Provides better end user experience than passwords**
- **Provides machine-bound authentication and authorization - authentication cannot be transferred among machines**
- **Supports varying strengths of authentication**
- **Supports multiple credentials**
- **Requires only a single user gesture such as a tap, or finger swipe for granting access**

Easy login increases usage of digital services by 10-20%

McKinsey ClickFox survey[12]

As Convenient as a Debit Card

To appreciate the convenience of a passwordless login using a YubiKey, consider the convenience of your debit card. You probably carry your debit card with you everywhere. You protect it; you don't just leave it lying out in public. To unlock it at an ATM, you enter a short PIN. The PIN is changed very rarely if at all, there's no password to remember, and no username, and yet your ATM access is very secure.

A passwordless YubiKey is similar. You carry it everywhere. To unlock a device—whether a desktop computer, a smartphone, a manufacturing control system, a healthcare portal, or some other device—you simply plug the YubiKey into a USB port or place the key near a NFC sensor. Then, when prompted, you tap the key and optionally enter a PIN or use a biometric control, depending on the application or service.

Like the PIN on your debit card, the FIDO2 PIN vouches for your access to the security key mechanism. The PIN unlocks your FIDO2 security key and enables it to initiate a key exchange with whatever it's authenticating to: the local device, a remote directory service, a web site, a social network, or some other IT service.

Optionally, services could be configured to authenticate users without requiring PINs or gestures. If the computer system is configured with a pressure pad that detects a user's presence, the system can automatically log the user out of the system when the authenticated employee steps away.[11] Because FIDO2 radically alters the process for authenticating users, public sector entities can reasonably afford its additional authentication measures, because FIDO2 user experiences are so simple and fast, improving productivity while simultaneously reducing support costs.

In all these scenarios, FIDO2 passwordless login provides an experience that is faster and more secure than usernames and passwords. Passwordless login transforms the user experience of logging into applications, websites, services, servers, and devices, into the familiar split-second convenience of accessing an ATM.

FIDO2 passwordless login requires use of a FIDO2 certified authenticator, such as the YubiKey 5 Series.

FIDO2, WebAuthn and FIDO U2F

How do FIDO2 and WebAuthn work with FIDO U2F?

U2F is an open authentication standard that enables hardware authenticators, mobile phones, and other devices to securely access any number of web-based services—instantly and with no drivers or client software needed. U2F was co-created by Google and Yubico, with contribution from NXP, and is today hosted by the open-authentication industry consortium, FIDO Alliance.

U2F is a strong authentication solution, but it is a two-factor solution, relying on usernames and passwords as the first factor. In fact, the 2F in its name refers to 2nd factor.

FIDO2 is a second generation of U2F. FIDO2 builds on U2F by adding the required elements so that a user can be identified and authenticated without the need for a password. FIDO2 authentication supports strong single-factor, two-factor and multi-factor authentication.

The WebAuthn component of FIDO2 is backwards-compatible with FIDO U2F authenticators. This means that all previously certified FIDO U2F Security Keys and YubiKeys will continue to work as a second-factor authentication login experience with web browsers and online services supporting WebAuthn.

To make use of the new FIDO2 passwordless experience will require the use of FIDO2 certified security keys such as the YubiKey 5 Series and the Security Key by Yubico.

Use Cases with Passwordless Logins

Employees and Contractors

When onboarding new employees and contractors, especially those that are not PIV/CAC eligible, public sector organizations no longer need to issue temporary passwords or passwords of any kind. Instead they can simply issue a hardware authenticator, such as the YubiKey. Using the YubiKey, a user can authenticate to Azure AD or other services with or without a short PIN, depending on the application. The YubiKey can also be used to register additional devices, such as smartphones or laptops, to also serve as authenticators.

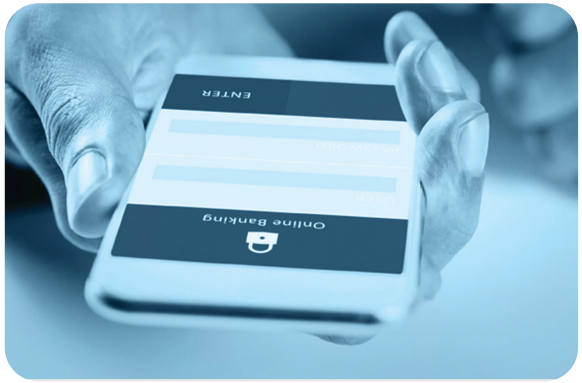
The authentication process can become remarkably quick and easy. For example, instead of sitting down and entering a username and password, an office worker can simply sit down, tap the YubiKey, and begin the work day.

Vendor and Supplier Networks

The Target data breach of 2013 remains a stark reminder of the security risks of vendor and supplier networks. That breach began when hackers infiltrated the network of an HVAC supplier. When that supplier connected to Target's partner portal, they eventually were able to make their way to the retailer's point-of-sale systems.

Strengthening partner portal authentication with FIDO2 security keys streamlines access for partners while eliminating the possibility of stolen passwords being used to infiltrate an organization through its partner portal.

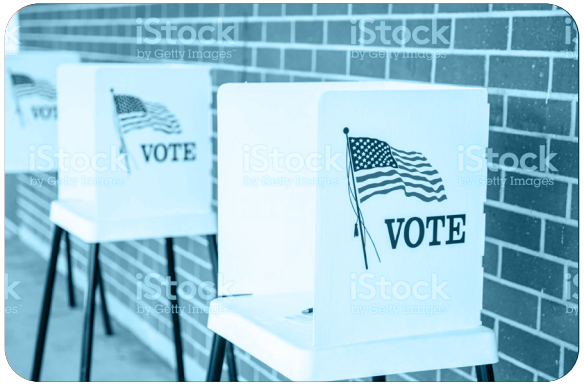
In addition, FIDO2 does not require an organization to manage all the identities of its suppliers. Instead, an organization can simply adopt a "no passwords" policy and require vendors to authenticate using a security key. Vendors can easily acquire FIDO2 security keys on their own. This sort of federation was not previously possible with other authentication technologies, which made securing vendor networks cost-prohibitive.



Citizens and Local Constituents

Local constituents need to seamlessly access citizen services without leaving open attack vectors, as these services may contain sensitive information like PII data including SSN numbers, addresses and drivers license information.

With passwordless, public sector entities no longer need to issue passwords of any kind. Instead citizens can chose a hardware authenticator, such as the YubiKey. Using the YubiKey, a user can authenticate to online government and citizen services with or without a short PIN via their laptops, desktops or mobiles.



Election Security

Voter registration systems, election networks and political campaigns are high risk targets for foreign hackers and nation-states looking to infiltrate the political system and gain access to voter information, campaign strategy, fundraising data, political candidate personal accounts and more. With the passwordless option, YubiKeys help protect against domestic and foreign threats by securing sensitive information and high-risk individuals across election networks and political campaigns without the use of passwords. They defend global democracy by ensuring email confidentiality, securing access to laptops, protecting voter databases and stopping candidate social account takeovers.

Education

Today, education faces the same security threats as commercial sectors, with sensitive data being compromised for staff, students, and researchers. As with the enterprise, the most common attack vector is a static password. With passwordless, school and college employees, teachers, professors and students will be able to easily and securely login to their laptops desktops and mobile devices, and any online services provided by the institution.

Conclusion

For too long, passwords have hampered end users, security teams, and IT teams. By enabling passwordless security, FIDO2 opens a new era in customer service, and human-machine interactions.

Using FIDO2 passwordless login, enterprises can strengthen network security, reduce IT expenses, improve productivity, and create a new class of services enabled by fast, convenient, and ubiquitous trust. Passwordless login offers:

- **Improved usability** With passwordless login public sector entities never have to pause to enter passwords or struggle to remember passwords. Access becomes fast and easy.
- **Improved security** Eliminating passwords eliminates security vulnerabilities from stolen passwords, passwords harvested by phishing, and brute force attacks on simple passwords.
- **Improved efficiency** A passwordless world liberates IT administrators from provisioning tens or hundreds of thousands of passwords. IT support load decreases, even while security and usability improves.

How might employee, contractor, partner and end-customer journeys be streamlined with password-less login? How might user experiences be reimagined without the need for passwords? What if accessing applications and services could be fast, easy, and secure everywhere?

What new products and services become possible when passwords are no longer required, when remote desktop and mobile devices can be easily provisioned and trusted, and when risks of data breaches and fraud–at long last–substantially decline?

These are the questions that forward-thinking leaders should now be asking.

FIDO2 passwordless login makes these questions not a speculative question for futurists, but rather a practical question–even a pressing question–for CISOs, product managers, UX designers, marketers, and other professionals dedicated to delivering the best possible products, services, and experiences while ensuring that authentication is always secure.

Recommendations

How should leaders, CIOs, CTOs, and other IT leaders prepare for a passwordless world? Yubico offers the following recommendations.

Stay Informed

Subscribe to updates from Yubico by visiting www.yubico.com/go-passwordless

Join the Yubico Developer Program

Developers should join the Yubico Developer Program to gain access to workshops, open source software and development support.

Upgrade Two Factor Authentication Options Today

To include support for FIDO2 security keys and be ready to go with passwordless login.

Develop a Strategy for Going Passwordless

Assemble a team of leaders within your organization to consider how to leverage passwordless authentication. To begin with, the team might want to:

- Develop a cost model for passwords. How many help desk and call center requests are tied to passwords? How long does each request typically take? How long does it take for administrators to assign passwords for new users? How much productivity is lost because of account lockouts? Benchmark the time and expenses of your current authentication practices so you can understand cost savings.
- Identify pilot projects that will allow your team to rollout passwordless login to a select user community. Focus on areas that require strong authentication where optimizing user experience would deliver big benefits. Monitor the progress of the rollout, and apply any lessons learned to future rollouts.

References

1. Verizon Data Breach Investigations Report 2019
2. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
3. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
4. Kessem, Limor. “Millennial Habits May Bring An End To The Password Era | SC Media”. SC Media. https://www.scmagazine.com/millennial-habits-may-bring-an-end-to-the-password-era/article/746144/
5. National Cyber Security Center, 2019 Cyber Security Survey
6. McKinsey, ibid.
7. “Password Management: Getting Down To Business”. Infosecurity Magazine. https://www.infosecurity-magazine.com/webinars/password-management-getting/
8. “Windows Hello For Business: What’s New In 2017”. Channel 9. https://channel9.msdn.com/events/Ignite/Microsoft-Ignite-Orlando-2017/BRK2076?ocid=cx-blog-mmpc
9. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
10. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
11. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
12. McKinsey, ibid.

yubico

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at **www.yubico.com.**

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088