yubico

A YUBICO WHITE PAPER
NOVEMBER 2018

Going Passwordless

with FIDO2 and WebAuthn

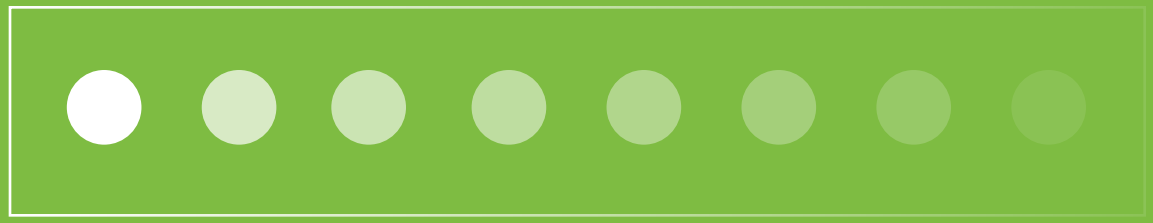


Table of Contents

Executive Summary

Imagine a world where users no longer need to set, reset, forget and reset again multiple passwords. Passwords are known as the weakest link for enterprise security and are an obstacle to streamlined customer journeys and internal processes. The world is about to change with the introduction of passwordless authentication.

The new FIDO2/WebAuthn authentication standards offer the opportunity for organizations to solve the problems inherent in password-based security. FIDO2 is an open standard, co-developed by Yubico, Microsoft, and other members of the FIDO Alliance that enables expanded options for strong authentication including the flexibility to now offer passwordless single factor or multi-factor strong authentication to users, in addition to supporting the existing scenario of two factor authentication.

Passwordless authentication offers the opportunity to transform enterprise security and user experiences in every industry, including healthcare, manufacturing, and retail, as well as for office workers, partners, and suppliers. It can simplify user onboarding and given that password resets currently represent the #1 IT support cost, passwordless login promises to significantly reduce workloads in IT call centers where agents today spend considerable time setting and resetting user passwords.

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 business and IT leaders should be asking now.

This whitepaper provides the background on passwordless authentication and considerations for enterprise deployment.

The Time and Cost of Passwords

Businesses today are looking for ways to leverage the cloud and mobile technology in order to deliver improved products and services faster and more efficiently. However businesses pursuing ambitious plans for streamlining customer and workforce journeys, soon find themselves running into security challenges.

Security technologies and controls are put in place to protect the enterprise, 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[1], while business users are estimated to be responsible for memorizing and using an even greater number of passwords, as many as 191.[2] 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.[3]

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.

About 63% of data breaches involved a weak password, according to the 2017 Verizon Data Breach Investigations Report (DBIR).[4] Incredibly, after years of highly publicized data breaches, the two most commonly used passwords remain '123456' and 'password'.[5]

63% of data breaches involve a weak password.[4]

Verizon Data Breach Investigations Breach

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]

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

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 at other organizations where consumers have used the same username-password pair. For example, when hackers stole 1 billion Yahoo! login credentials in 2016, they gained access to all the other accounts accessible with the same email address-password pairs. 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. Today nine out of ten login attempts on popular retail and banking sites are actually bot-driven attacks.[10]

As long as enterprise IT has to rely on passwords for authentication, costly support requirements, weak security, and frustrating customer experiences are inevitable. Forgotten and stolen passwords degrade customer experiences, reduce brand loyalty, and contribute to lost revenue.

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.

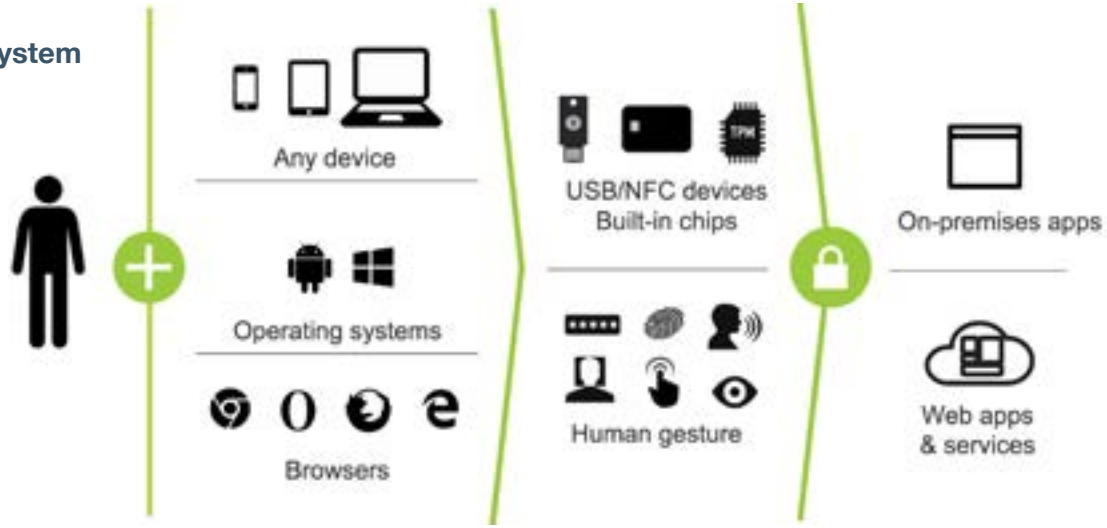
These benefits of passwordless authentication can now be achieved with the new FIDO2/WebAuthn open authentication standards.

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 400 million Windows 10 devices worldwide with an upgrade to Windows 10 Redstone 4.

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, business people 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 Windows 10 Redstone 4 or later, making FIDO2 available on over 400 million devices around the world,[11] in addition to being available for billions of Azure AD accounts. Also as of November 2018, Microsoft Accounts now 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 enterprises the expense of having to invest in the development and maintenance of custom security models to address the problems of passwords. Now enterprises in every industry 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.[12]

"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 Enterprise 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%

Source: McKinsey ClickFox survey[14]

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. For example, in the interest of providing the fastest possible service to customers, a retail sales associate could be allowed to authenticate simply by setting their key on an NFC pad, instantly unlocking a computer system. 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 sales associate steps away.[13] Because FIDO2 radically alters the process for authenticating users, businesses 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 new FIDO2 certified security keys such as the YubiKey 5 Series and the Security Key by Yubico.

New Use Cases with Passwordless Logins

Employees

When onboarding new employees, companies 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.

Retail

Sales associates, floor leaders, team leaders, cashiers and other retail employees need fast, easy access to IT systems. Passwordless logins streamline onboarding and access while providing rigorous authentication as a guard against fraud.

Retailers often hire seasonal staff. For example, at least one well-known North American retailer typically hires 30,000 temporary workers for the holiday season. Traditionally all those workers would have required usernames and passwords. With FIDO2, they can simply be issued security keys. Authorized services can be centrally disabled through a directory service such as Azure AD when the seasonal activity concludes.

FIDO2 saves the IT department the trouble of creating, resetting, and rescinding passwords. If employees are rehired, their security keys can simply be reactivated and reassigned for access to in-store services.

Finance

Making fast, hassle-free passwordless authentication available improves brand experiences, streamlines ecommerce and customer support interactions, and even supports the creation of new products and services. A bank, credit union, or other financial institution offering security keys and passwordless authentication to customers, reduces the risk of account take-over while simplifying life for account-holders.

Manufacturing

Like retailers, manufacturers have multiple shifts of workers. FIDO2 simplifies managing access for this ever-changing workforce. Because workers don't have to type in passwords but can still uniquely authenticate themselves, FIDO2 streamlines access to IT systems while supporting internal security and identity management policies. At the same time, it eliminates the risk of password management policies (such as periodic password cycling) from introducing delays or other problems in operations.

The U.S. Department of Homeland Security has warned that manufacturing remains a prominent target for phishing attacks, in part because hackers are interested in stealing intellectual property.[15] By replacing phishable passwords with the FIDO2 security keys, manufacturers can help close the door on this type of attack, by providing strong authentication which defends against phishing.

Healthcare

Healthcare organizations (HCOs) are vulnerable to data breaches of various kinds. Patient Health Information, including patient history and payer information, is ten times more valuable on the black market than credit card data.[16] Why? Because medical fraud, including the filing of false insurance claims, pays off.

HCOs are also susceptible to ransomware attacks, many of which are launched through phishing. By replacing passwords with security keys, HCOs and their business associates can greatly reduce their vulnerability to these types of attacks.

FIDO2 can also help HCOs ensure that Personal Health Information (PHI) is accessed only by authorized users in compliance with HIPAA regulations. A recent healthcare industry survey found that 76% of U.S. doctors have accessed PHI using a password from a colleague.[17] Simplifying login processes encourages doctors to use only their own credentials for accessing PHI and other protected data and services, and to stop sharing credentials. At the very least it limits them to sharing access only with other people who are physically present. In contrast, shared passwords allow access from any location.

FIDO2 provides another important benefit for the healthcare industry: fast, easy authentication. Doctors and nurses have to login dozens of times per day as they move from patient to patient, room to room, and device to device. Now access can be immediate and more secure with passwordless logins. Caregivers can focus on giving care instead of fumbling with cumbersome login procedures.

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 enterprise through its partner portal.

In addition, FIDO2 does not require a business to manage all the identities of its suppliers. Instead, a business 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.

Conclusion

For too long, passwords have hampered end users, security teams, and IT teams. By enabling passwordless security, FIDO2 opens a new era in enterprise IT, 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 profitable services enabled by fast, convenient, and ubiquitous trust. Passwordless login offers:

- **Improved usability** With passwordless login users 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.

FIDO2 is a solution that is available now for hundreds of millions of Windows 10 devices with an upgrade to Windows 10 RS4. It is a solution that IT vendors and enterprise IT departments can begin working with to address not only internal IT security needs, but also those of customers.

How might customer journeys be streamlined with passwordless 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 business and IT 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 business 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 business and IT 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. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
2. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
3. 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/
4. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/2017_dbir.pdf
5. Ehrenkranz, Melanie. “The 25 Most Popular Passwords of 2017: You Sweet, Misguided Fools”. Gizmodo.com. https://gizmodo.com/the-25-most-popular-passwords-of-2017-you-sweet-misgu-1821425092
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. Verizon, ibid.
10. Ward, Kelsey. “Credential stuffing rules the day as 90% of login attempts no longer made by humans”. Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
11. “Windows 10 Hits 500 Million Active Devices”. Engadget. https://www.engadget.com/2017/05/10/windows-10-500-million-users/
12. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
13. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
14. McKinsey, ibid.
15. “Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business”. Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-of-us-industries-under-cyber-attack-says-homeland-security-report
16. “Your Medical Record Is Worth More To Hackers Than Your Credit Card”. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
17. “Do Doctors Share Electronic Health Record Passwords?” The Millennium Alliance. https://mill-all.com/blog/2017/10/04/do-doctors-share-electronic-health-record-passwords/

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.**

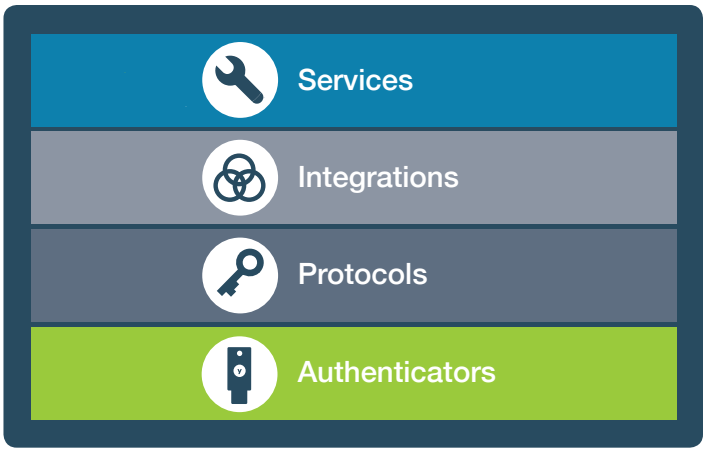
Yubico AB
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

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

yubico

The Yubi Platform

Enabling rapid deployment of strong authentication



Username and Passwords Put Enterprise Data at Risk

Catastrophic security breaches top world headlines every day, and for good reason. A single corporate security breach costs an average of $3.86M, and 81% of breaches are caused by stolen or weak passwords. As a result, IT organizations cannot rely exclusively on passwords to protect access to corporate data. They have to adopt stronger employee and customer authentication—or risk becoming the next target.

The Yubi Platform–

A Full Stack Foundation for Strong Security

The Yubi Platform delivers a strong foundation that enables organizations to introduce modern authentication into their environment. The Yubi Platform is comprised of four key layers that enable rapid and effective deployment of strong authentication.

Authenticators

Hardware Security Keys Eliminate Account Takeovers

Hardware based authenticators provide superior defense against phishing, prevent man-in-the-middle attacks and enable compliance for strong authentication. Any software downloaded on a computer or phone is vulnerable to malware and hackers. The YubiKey is based on hardware with the authentication secret stored on a separate secure chip built into the YubiKey, so it cannot be copied or stolen. Hardware authenticators help organizations eliminate account takeovers and reduce risk from remote attacks and other breaches.

The YubiKey supports multiple protocols and offers expanded authentication options such as passwordless, strong two-factor authentication (2FA) and strong multi-factor authentication (MFA), and also enables encryption. And it is available in a choice of form factors that enable users to connect via USB, NFC and coming soon—Lightning connector.

Protocols

A Future-Proofed Solution Delivers Strong Authentication at Scale

The YubiKey multi-protocol support streamlines authentication for existing systems while paving the way forward to a passwordless future. Centralized servers with stored credentials such as passwords can be breached. With the YubiKey, the data is encrypted with strong public key cryptography where only the public key is stored on the server, eliminating risks.

Organizations can leverage modern authentication protocols such as FIDO Universal 2nd Factor (U2F), and WebAuthn/FIDO2 and U2F to enhance security and the user experience. THe Yubikey also works with legacy Personal Identity Verification-compatible (PIV) Smart Card, and OpenPGP smart card, providing a path for organizations to bridget from existing enterprise systems to a passwordless future The YubiKey also supports the YubiKey OATH and Time-based OTP (TOTP) and Hash-based OTP (HOTP) protocols.

The YubiHSM enables organizations to enjoy strong security for servers and computing devices with the world's smallest hardware security module. The YubiHSM enables the secure generation, storage and management of digital keys, and supports a wide range of existing and emerging use cases.

YubiKeys deployed in:

9 of the top 10 global technology companies

4 of the top 10 U.S. banks

2 of the top 3 global retailers

Integration

A Broad Ecosystem Enabled Through Rapid Integration of Strong Authentication

Yubico provides free and open source software to rapidly integrate YubiKey strong two-factor, multi-factor and passwordless authentication into any software or service. With the use of open source code and servers, and a wide array of developer tools such as SDKs, libraries and APIs, developers can quickly and easily integrate Yubico solutions with their services across Windows, macOS, Linux, iOS and Android. And, organizations can control their own cryptographic secrets. No passwords, keys, or PINS are shared with Yubico.

The YubiKey works with hundreds of services to secure user login, and makes it easy for only the rightful user to access their accounts.

With a single YubiKey a user can securely login to all of the needed business IT systems such as computers, VPN, single-sign-on systems, password managers, privileged access software, online services, developer tools, and card/credential management systems, and hundreds of services a user needs to access at work or at home.

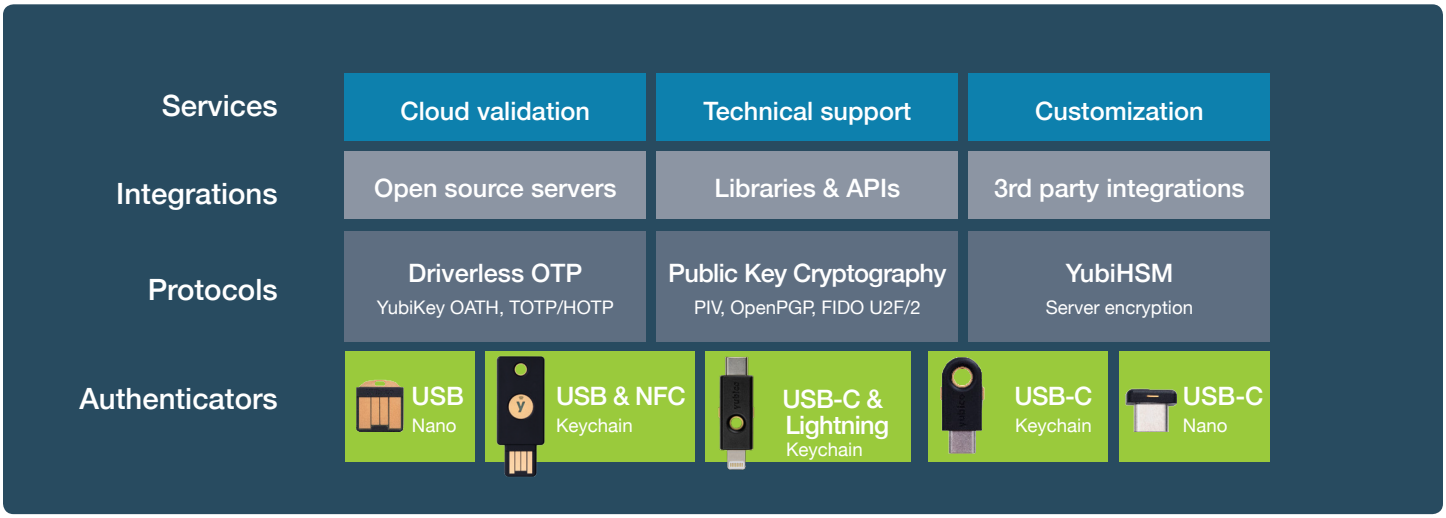
Services

Technical Support and Customization Services Deliver Modern Authentication

Organizations embarking on the journey to implementing modern and more secure approaches to authentication can rely on support and customization resources to optimize effectiveness and speed of deployment. The Works with YubiKey program also ensures that the YubiKey can work with hundreds of services right out of the box speeding up your journey to modern authentication.

Proven Security Leadership

The Yubi Platform delivers authentication capabilities that offers a superior user experience while maintaining strong security. Working across major operating systems including Microsoft Windows, macOS, iOS, Android, and Linux, as well as leading browsers, the Yubi Platform ensures support for the full range of modern devices and services users love to use for work and life. With a proven modern approach, organizations are now able to deliver strong authentication that is fast, easy and simple all while significantly reducing IT costs and eliminating account takeovers. The internet just got safer for everyone.



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
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

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