yubico

WHITE PAPER

Best practices for biometric authentication

Delivering on the promise of secure login with a new user experience

Contents

Introduction

61%

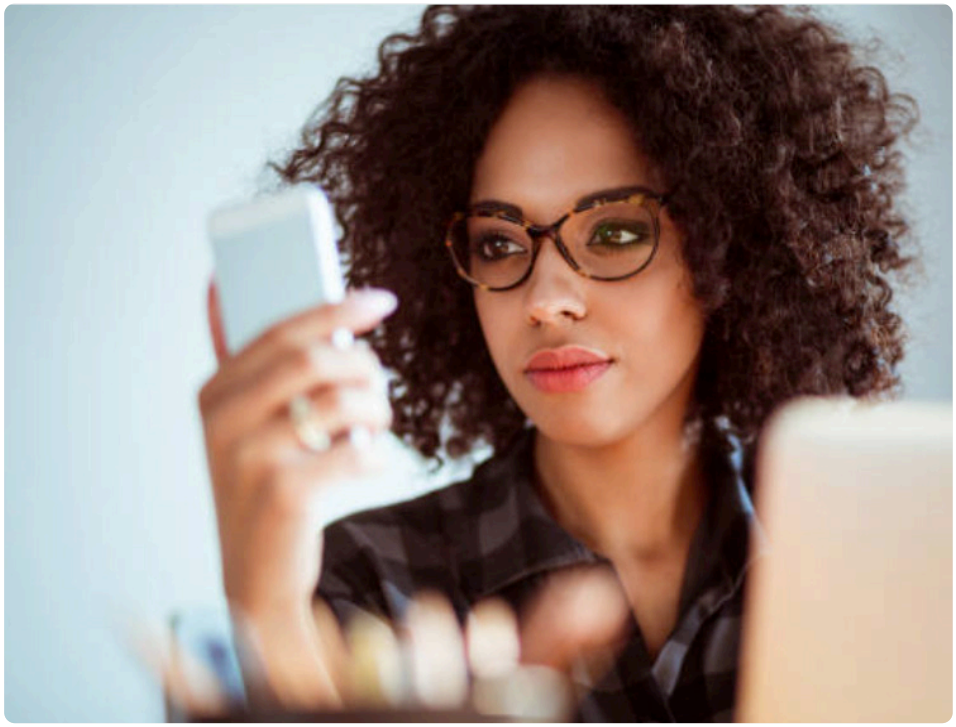
of breaches attributed to leveraged credentials[1]

It's no secret that the digital threat landscape has changed dramatically in recent years—and it continues to evolve rapidly. Highly targeted phishing attacks are on the rise, and have become extremely adept at stealing vulnerable passwords from even the most security-conscious enterprise users. In fact, according to the Verizon 2021 Data Breach Investigations Report, compromised credentials are the number one way bad actors break into an organization, with 61 percent of breaches attributed to leveraged credentials.[1]

The COVID-19 pandemic has also contributed to the spread of cyber attacks. Almost overnight, millions of people completely shifted to remote work and online classes. Today, staying productive often means accessing cloud apps and data from home networks and personal devices, such as the family laptop or a spouse's tablet. All too often, they are secured by little more than weak passwords and accessed by multiple users. What's more, the era of remote and hybrid workforces isn't likely to change anytime soon. In fact, the percentage of people working from home is expected to double to 34.4% through the rest of 2021 and beyond.[2]

It's time to move beyond passwords

To better protect access to corporate apps and data, companies need a fast and easy way to replace passwords with a more secure yet simple solution anyone can use. For this reason, biometric authentication has quickly emerged across every kind of industry to support a number of authentication use cases. This is mainly due to the convenience, speed, and security biometric-based authentication offers to users.



What is biometric authentication?

Modern devices have included biometric authentication, such as Touch ID, for the past few years. Other biometric factors, such as Face ID and voice recognition are also becoming more common as organizations and users look for easier ways to replace password-based authentication.

Biometric factors make it easy to support multi-factor authentication (MFA) on all types of devices and apps. The combination of factors used to authenticate with FIDO2 are a biometric or a PIN and the authenticator.

It's clear that biometric authentication offers a convenient, passwordless login experience that can support multiple use cases, such as shared workstation environments and research labs, where multiple users must securely authenticate several times a day, as well as mobile-restricted environments where mobile authentication is simply not an option. However, it's important to consider some of the current issues that should be addressed before deploying biometric authentication across the enterprise.

Gaps in biometric authentication today

Most modern devices like laptops and smartphones include built-in authenticators, so many consumers and enterprise users are already familiar with how to set up and use them. Although these authenticators are becoming more standard, they aren't optimized for enterprise security and user convenience. Here's why:

Single point of failure

Biometric authenticators built into the device are convenient, but can become unusable if the device or mechanism itself is damaged or otherwise compromised. If the authenticator breaks, the user (or company) will likely have to replace the entire device instead of just the mechanism itself.

Lack of portability

Built-in authenticators only work for that device, which means users need to set up their biometric profile on every device they access, which can be time-consuming for both the user and IT. In addition, a built-in biometric authenticator does not allow the user to seamlessly access their accounts regardless of which platform the user accesses or on shared workstations. For example, Apple's move to tie authenticators to iCloud accounts will allow iPhone users to transfer access between hardware platforms, but it won't help them log in to sites on a Windows device, or on shared workstations. And finally, a built-in authenticator restricts access to only that particular device, so if that device faces a loss of battery charge, or is compromised in any other way, users have limited fallback options to authenticate.

Slow account recovery

Services like Google may delay account recovery if any activity appears suspicious. While delayed recovery is intended to protect user account information, delays can take anywhere from a few hours to a few days, especially for users who have MFA set up on their accounts.[3] In addition to frustration and lack of productivity, slow account recovery can in itself pose a security and business risk if users can't access critical information, such as medical or financial records. Furthermore, while built-in biometric authenticators work well on devices such as smartphones or modern desktops/laptops, the user can lose access if the device is ever compromised, broken, lost, or stolen. In that case, the user (or his or her employer) would immediately have to purchase a new smartphone. Otherwise, they are locked out of any accounts they have registered, especially those with stringent account recovery options. What's more, once a new device is purchased, the user has to go through the very time-consuming process of reestablishing the new smartphone or desktop as a trusted device for each individual service.

Not only are these issues challenging to manage, they can be costly as well. Organizations need to take all of these factors into consideration to ensure that they can truly deliver the key advantages of biometric authentication—user convenience. If using passwords or single failure mechanisms users are routinely locked out, how much do those setbacks cost the business in the long run?

More importantly, are there simpler and more cost-effective alternatives to built-in biometric authenticators?

Not only are these issues caused by existing gaps challenging to manage, they can be costly as well. Organizations need to take all of these factors into consideration to ensure that they can truly deliver the key advantages of biometric authentication—user convenience.

Essential best practices for biometric authentication

The best way to avoid some of the pitfalls of built-in biometric authentication is to understand and implement these best practices.

The private key and any information about the authentication method—such as fingerprint, face, voice, or iris scans—never leave the local device. This allows the user to leverage a portable yet highly secure biometric authentication method to easily authenticate to online services in both mobile and desktop environments.

Use modern FIDO protocols in a portable form factor

FIDO protocols provide strong, modern authentication through the use of standard public key cryptography. These protocols are designed from the ground up to protect user privacy, and can work across desktop and mobile devices to provide ultimate portability.

The user first chooses a FIDO authenticator to register with an online service, and then uses the biometric touch to create the FIDO credentials to authenticate to the service using the newly-created credentials. This then creates a new and unique public/private key pair for the online service, and the user's account. The user can then unlock the device or account with a simple and secure action such as presenting a finger, entering a PIN, or pressing a button.

Most importantly, the private key and any information about the authentication method—such as fingerprint, face, voice, or iris scans—never leave the local device. This allows the user to leverage a portable yet highly secure biometric authentication method to easily authenticate to online services in both mobile and desktop environments.

Identify all use cases that require secure authentication

Consider specific business scenarios that can most benefit from simple and secure biometric authentication. This could include shared workstation environments like research labs, retail environments, and healthcare kiosks. It may also include mobile-restricted environments that prohibit MFA using a mobile device, such as call centers or manufacturing floors.

Look for a form factor with proven durability

Any portable solution will undoubtedly be subjected to all kinds of wear and tear—including constant handling as well as possible contaminants such as dust, liquids, etc. As with built-in authenticators, if the mechanism breaks, the user risks losing account access for a significant period of time. The ability to withstand environmental pressures over the long term is critical to any biometric authentication solution.

Have at least two FIDO authenticators registered with each service

The recommended best practice is to have at least two FIDO authenticators registered with each service, and if the user so chooses, they can register a portable FIDO authenticator with their services as well as register the built-in authenticator that ships with their laptop or smartphone. In this manner the user has two FIDO authenticators registered with each service for a better overall experience.

YubiKey Bio Series - FIDO Edition

Delivers the gold standard of biometric authentication

As part of Yubico's long-standing commitment to combining strong hardware security with greater user convenience, the YubiKey Bio Series allows users to authenticate with the same key across different desktop devices, operating systems, and applications.

With the introduction of the YubiKey Bio Series - FIDO Edition, Yubico continues to build on its legacy of strong security and a fast and easy user experience. The YubiKey Bio Series, built for desktops, is a FIDO-only lineup of biometric keys that delivers passwordless multi-factor authentication and strong second factor authentication. It is ideally suited for cloud-first environments and for shared workstation and mobile-restricted business scenarios. As part of Yubico's long-standing commitment to combining strong hardware security with greater user convenience, the YubiKey Bio Series allows users to authenticate with the same key across different desktop devices, operating systems, and applications.

The YubiKey Bio Series carries on Yubico's industry leadership from the YubiKey 5 Series—a range of multi-protocol, enterprise-ready security keys designed for organizations of all types with both legacy and modern environments. The YubiKey Bio Series features a unique security key design with a three-chip architecture that:

- Isolates fingerprint matching to a separate and dedicated secure element
- Encrypts traffic between the secure elements
- Treats the fingerprint sensor as not trusted and is therefore designed to be resilient to external attacks
- Mitigates the risk of fingerprint template material leaving the key

The FIDO-only YubiKey Bio Series comes in USB-A and USB-C form factors. If your organization is looking for more form factors, protocols, and NFC support, the industry-leading YubiKey 5 Series is recommended to address the broadest set of business scenarios.

What sets the YubiKey Bio Series apart

Contingency plan

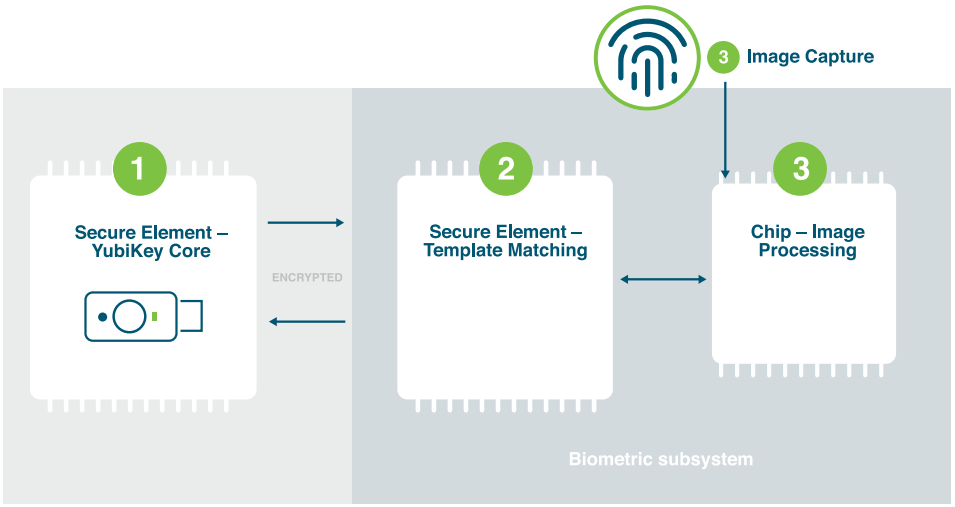
To minimize the risk of fingerprint spoofing, the YubiKey Bio Series has been thoroughly tested to ensure it delivers robust biometric authentication. To achieve user convenience, the YubiKey Bio Series offers fingerprint matching for authentication, with a PIN fallback if the user has failed to perform a fingerprint match.

Yubico hallmark design and durability

The hardware design of the YubiKey Bio Series carries forward all of the elements that users know and love about YubiKeys, including the sleek industrial design and same compact size as a regular YubiKey. Not only does the physical design and durability help prevent physical access to secure elements, it also ensures that the YubiKey Bio Series is just as secure and reliable as a regular YubiKey. The result is one of the industry's toughest and most secure biometric security keys.

Industry-first biometric subsystem

The YubiKey Bio Series has been designed with security, usability, and privacy in mind. The lineup is designed with a three-chip architecture that separates the biometric subsystem from the key's core functionality.



The YubiKey Bio Series stores enrolled fingerprint templates and performs biometric matching in a dedicated secure element to help protect it from both digital and physical attacks. Encryption is used to protect the communication between the biometric secure element and the one used for the core YubiKey software.

To minimize the risk of fingerprint spoofing, the security key lineup has been thoroughly tested to ensure it delivers robust biometric authentication. To achieve user convenience, the YubiKey Bio Series offers fingerprint matching for authentication, with a PIN fallback if the user has failed to perform a fingerprint match.

To ensure control and visibility through the manufacturing process, the YubiKey Bio Series is manufactured in the same secure facilities in Sweden and the US as other YubiKeys.

Highly customizable

To meet specific security requirements, organizations can custom order specific settings on the YubiKey Bio Series. For instance, a customer can limit the number of biometric attempts to any number less than 10 before requiring a PIN to authenticate. It is important to note that by default the user has three biometric attempts before a fallback to PIN. And finally, the minimum PIN length can also be custom ordered, with four alphanumeric characters as the default.

Easy enrollment and self-service

Working with the FIDO Alliance and key industry leaders, the YubiKey Bio Series has native platform support for fingerprint enrollment and management on Windows 10. On macOS, Chrome OS and Linux the same type of support is available via Chrome and Chromium-based browsers. We continue to work hard to integrate YubiKeys with browsers and operating systems to minimize software that needs to be deployed and managed. Native support on leading platforms and companion app options make it easy for users to enroll fingerprints, manage their PIN, and display key status. And for enterprises, it also helps to reduce IT support tickets and costs. It should be noted that fingerprint enrollment and management is also offered from Yubico via the Yubico Authenticator for Desktop on all previously mentioned Operating Systems.

Highly secure supply chain

To ensure control and visibility through the manufacturing process, the YubiKey Bio Series is manufactured in the same secure facilities in Sweden and the US as other YubiKeys.

Working with the FIDO Alliance and key industry leaders, the YubiKey Bio Series has native platform support for fingerprint enrollment and management on a range of leading platforms.

Top Five Benefits of the YubiKey Bio Series

The YubiKey Bio Series offers hallmark YubiKey security, with the same level of protection as all other YubiKeys, with added biometric user convenience. The top five benefits include:

1. Consistent reliable design

The YubiKey Bio Series leverages the same sleek and simple keychain design as other YubiKeys, including durability and water-resistant features. In lieu of the classic gold contact on other YubiKeys that establishes user presence, the fingerprint sensor on the YubiKey Bio authenticates the user using fingerprint recognition.

2. Passwordless authentication

Organizations increasingly need to eliminate the security risk and hassle of managing passwords. YubiKeys enable this today with a single PIN. The YubiKey Bio Series, which supports FIDO2/WebAuthn and U2F, makes this even more convenient by allowing fingerprint authentication in place of the PIN.

3. High security

To ensure protection of user biometric information, templates of the fingerprints are derived from the fingerprints presented to the key, and those fingerprint templates are stored and matched on a separate secure element that helps protect against physical attacks. The benefit of using templates is that it is not possible to reverse engineer a fingerprint from a template.

4. Enhanced user experience, portability, and a frictionless account login

With FIDO protocol support, the YubiKey Bio Series enables secure second factor and passwordless MFA login experiences that enhance the user experience with simplified authentication flows. This also increases productivity in scenarios such as shared workstation environments and mobile-restricted environments where phone-based authentication is not an option.

5. Portable authenticator purpose-built for security

The YubiKey Bio Series, together with all other YubiKeys, are designed to provide strong security. This reduces the risk of compromised passwords and account takeovers. Additionally, if a phone or computer is hacked, lost, or damaged, the portable YubiKey can enable faster account recovery.

The YubiKey Bio Series builds on Yubico's industry leadership with a highly secure, portable, and reliable solution for biometric authentication.

Biometric authentication is here—and so is the key to do it right

With the YubiKey Bio Series, fast, secure, and portable biometric authentication couldn't be easier. It really is as simple as inserting the key into the desktop, and placing a finger on the fingerprint sensor on the key and the user is in. As soon as the fingerprint matches the information on the YubiKey Bio, the user is authenticated to their Azure AD joined computer, or to their FIDO2/WebAuthn supported apps and services. And this process removes the need to remember, change or manage passwords.

The YubiKey Bio Series enables biometric login with all applications and services that support FIDO2/WebAuthn/U2F. It works right out of the box with leading services such as Citrix Workspace, Duo, GitHub, IBM Security Verify, Microsoft Azure Active Directory and Microsoft 365, Outlook.com, Okta, and Ping. Plus, with YubiEnterprise Premium Subscription customers can upgrade their current YubiKeys to the YubiKey Bio Series at any time.

The YubiKey, in all its form factors, was designed to support the evolutionary path toward passwordless with strong authentication across legacy and modern devices. The YubiKey Bio Series builds on that industry leadership with a highly secure, portable, and reliable solution for biometric authentication. To learn more, please visit www.yubico.com.

Sources

[1] Verizon, 2021 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

[2] Reuters, Permanently Remote Workers Seen Doubling in 2021 Due to Pandemic Productivity: Survey, (October 20, 2020), https://www.reuters.com/article/us-health-coronavirus-technology/permanently-remote-workers-seen-doubling-in-2021-due-to-pandemic-productivity-survey-idUSKBN2772P0

[3] Google Account Help, Why your account recovery request is delayed, https://support.google.com/accounts/answer/9412469?hl=en

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.