yubico

FINANCIAL SERVICES WHITE PAPER | OCTOBER 2021

Strong authentication to support hybrid and remote work in financial services with the YubiKey

Increased cyber threats due to COVID-19

Financial institutions such as banks and insurance providers, are reporting significantly increased threat levels from COVID-related cyber crime according to the COVID-19 Crime Index 2021. According to the index, which surveyed 902 organizations in the financial services sector, 74% have experienced a rise in cyber crime since the pandemic began, with 42% of banks and insurers revealing the remote working model has made them less secure[1]. 44% were also concerned that this has led to less visibility of potential holes in their network or infrastructure[2]. On the other hand, IT security, cyber crime, fraud or risk department budgets have been cut by 26% in the past 12 months[3].

Long term hybrid and remote work security challenges

Hybrid and remote work have changed how businesses operate, and exposed unanticipated security challenges. Many employees are using personal devices to access business applications and data, sharing devices between family members, and may be accessing corporate networks via unsecured wifi connections. While COVID-19 made remote work a necessity, some financial services organizations are now considering having employees return to the office. Other businesses are planning to offer employees long-term hybrid and remote work opportunities based on their job functions. In the June 2020 PwC US CFO Pulse Survey, 61% of financial services chief financial officers said that they plan to make remote work permanent for roles that allow it[4]. The distributed security perimeter of 2020 will continue into the future.

COVID-19 also accelerated enterprise adoption of SaaS collaboration tools and other cloud-based applications to ensure business continuity. According to predictions in the IDC FutureScape 2021 report, by the end of 2021, the lessons learned from the COVID-19 pandemic will lead 80% of enterprises to put mechanisms in place to shift to cloud-centric infrastructure and applications twice as fast as before the pandemic[5].

IT security and cyber risk departments will need to ensure continued management of secure access to distributed data from distributed locations and endpoints, in addition to protecting their employees from increasing cyber threats such as phishing attacks and account takeovers.

The need for strong authentication

The financial services industry is an attractive target for cyber criminals because of its vast store of customer and financial information, as well as the potential for large payouts. Additionally, financial services employees typically work in a variety of environments such as call centers, retail locations, trading desks etc, and access information through multiple devices including shared workstations/kiosks.

Financial institutions also experience a level of security requirements and regulatory burden that few other industries have to contend with. There are many compliance requirements, and critical laws and regulations that financial institutions need to meet such as Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI DSS), that include information security elements such as robust access controls.

In such a complex environmental and regulatory landscape, regardless of in-person, hybrid, or remote work, strong authentication is an essential requirement.

[1] COVID Crime Index 2021

[2] Ibid

[3] Ibid

[4] June 2020 PwC US CFO Pulse Survey

[5] IDC FutureScape 2021

What is strong authentication?

Strong authentication has two key features:

- It does not rely solely on a shared secrets process or protocol (symmetric keys), such as passwords, OTP, SMS codes, or recovery questions.
- It robustly prevents credential phishing, MitM attacks, and impersonation. Strong authentication assumes some attacks will reach the end user and that the authentication mechanism will prevent the attack from being successful.

Among the varied authentication methods and protocols, only smart cards, modern FIDO U2F, and FIDO2/WebAuthn provide strong authentication. In addition to security, it's also important to consider usability, portability, and scalability. Poor user experiences, low portability, and lack of scalability of authentication solutions can result in low adoption and drive up costs.

Why mobile-based authentication isn't strong authentication

Financial institutions were early adopters of two-factor authentication (2FA) and multi-factor authentication (MFA) using mobile-based authentication such as SMS codes, OTP, and push notifications. However, mobile-based authentication does not protect against modern cyber criminal tactics and can be breached by malware, SIM swapping, and man-in-the-middle attacks, and lead to enterprise-wide identity phishing and account takeovers.

A recent VICE article, "A Hacker Got All My Texts for $16," showcased how a white-hat hacker—an employee at a security vendor—was able to redirect text messages and then break into online accounts that rely on texts for authentication for just $16.

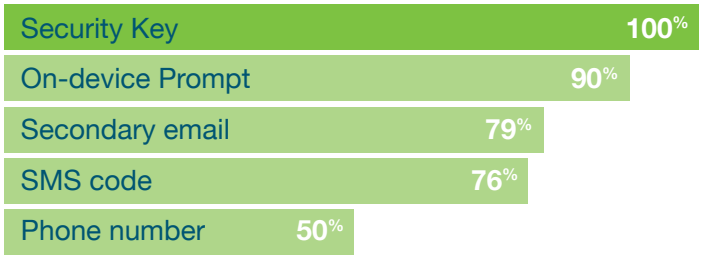
Strong authentication for hybrid and remote workers with the YubiKey

Yubico offers the YubiKey, for affordable and easy-to-use two-factor, multi-factor, and passwordless authentication. YubiKeys ensure the strongest security against phishing attacks and account takeovers as noted in independent research.

YubiKeys also provide an easy user experience. To authenticate, users simply tap/touch their security key.

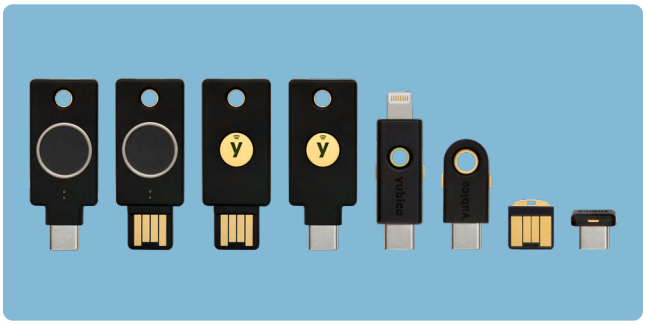
YubiKeys support modern protocols including FIDO2 and WebAuthn, as well as OTP, SmartCard (PIV), OpenPGP, earlier FIDO versions, and more. A single key supports multiple applications, allowing YubiKeys to work with current applications and authentication methods, and advanced and emerging protocols at the same time.

Account Takeover Prevention Rates



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

The YubiKey comes in multiple form factors to support both legacy and modern devices. Customers also receive a choice of FIPS 140-2 validated YubiKeys. Yubico also offers the YubiKey Bio Series - FIDO Edition, the gold standard for biometric authentication.



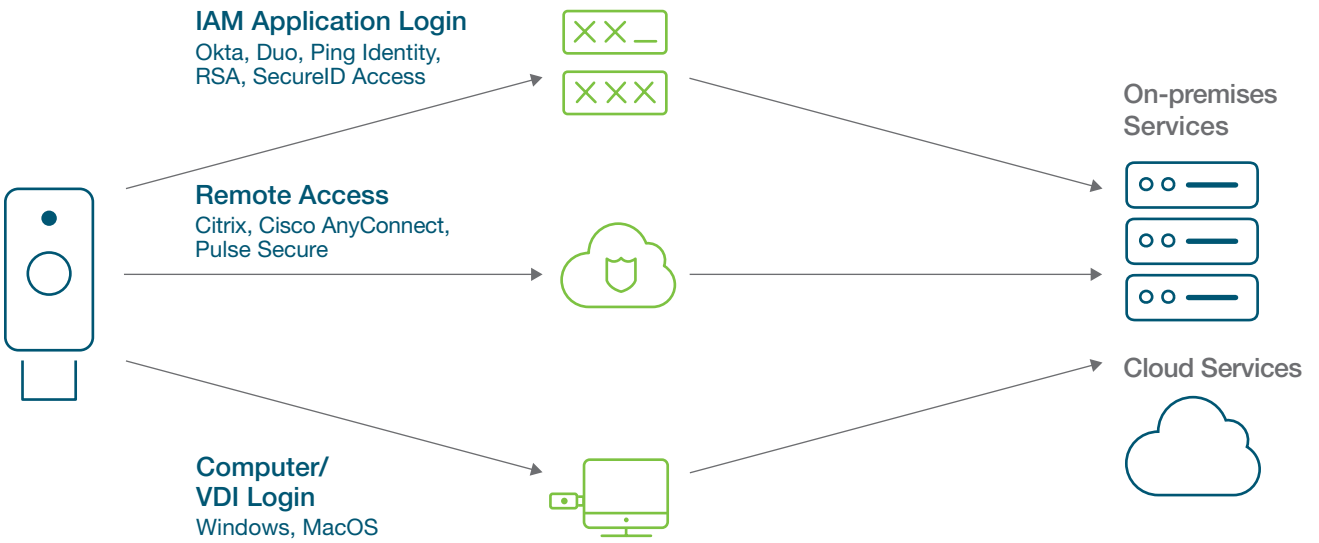
With the YubiKey, financial institutions can:

- Secure hybrid and remote workers against account takeovers and identity phishing with superior hardware cryptographic security
- Provide unmatched simplicity for users with 4x faster logins that ensure proof of presence and possession
- Comply with existing and emerging regulations such as SOX, PSD2, PCI, FIPS, and GDPR
- Reduce IT support costs related to password resets
- Deliver trust to users and gain peace of mind with a trusted solution from an industry leader pioneering global authentication standards

Best practices for strong authentication with the YubiKey

YubiKeys can be used to protect your employees—no matter where they work—against phishing attacks and account takeovers.

How the YubiKey helps secure hybrid and remote workers



1. Enable MFA for identity access management (IAM) systems and identity providers (IdPs)

The best cloud and hybrid environments leverage IAM solutions to enable employees to work without the hassle of multiple usernames and passwords. Many of the leading IAM vendors offer native YubiKey support, including Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, PingID, RSA SecurID®Suite, and others. Financial services organizations can immediately improve security by implementing MFA with YubiKeys. IAM vendors and IdPs can also be used for Single Single On (SSO) to other business-critical messaging or video conferencing apps such as Microsoft Teams, Google Hangouts, and Zoom.

2. Implement MFA for computer login

Whether employees are using a Mac or Windows machine, there are several options for securing computer logins with the YubiKey. One of the most effective ways is to leverage the smart card functionality of the YubiKey, and use the key in addition to a PIN, to lock down access to a computer. Employees can also experience a FIDO-based passwordless login experience for Microsoft Azure Active Directory, with native YubiKey support.

3. Secure VPN access with MFA

With the increase in hybrid and remote work comes an increase in the number of people utilizing a VPN to access the corporate network. Pulse Secure and Cisco AnyConnect, can be configured to work with a YubiKey as a smartcard (PIV) for remote access. Other VPN applications that offer native support for YubiKeys use the one-time password (OTP) capabilities.

4. Secure password managers with MFA

A recent Ponemon Institute report showed employees manage passwords with sticky notes and human memory. Regardless of whether employees are in the office or remote, they need a simple and safe way to create, store, and manage passwords. The YubiKey integrates with several enterprise-grade password managers including 1Password, Dashlane, Keeper Security, LastPass, and more.

5. Replace less secure one-time passcode applications

Many of the services or applications being used across financial services organizations may support time-based one-time passcodes (OTPs)—such as Google Authenticator or Authy—as a two-factor authentication method. The Yubico Authenticator application and a YubiKey can replace those authenticator apps. Instead of the one-time passcodes being stored within a mobile device or computer, secrets are stored securely on the YubiKey. This allows users to generate OTP codes within the app by inserting or tapping the YubiKey to a device. Yubico authenticator is compatible with iOS, Android, Windows, and Mac.

Easily procure and distribute YubiKeys to enable authentication at scale

Yubico offers YubiEnterprise Services, consisting of YubiEnterprise Subscription and YubiEnterprise Delivery, to help organizations simplify procurement and provide turnkey delivery of YubiKeys to corporate and residential addresses.

YubiEnterprise Subscription offers flexible purchasing options to easily buy and upgrade to the latest YubiKeys. Key benefits include predictable spending, lower entry cost, free buffer stock, upgrades, backup key discount, technical support, and extended warranty. The subscription model is especially beneficial for environments experiencing frequent employee turnover, such as call centers.

With YubiEnterprise Delivery, organizations receive turnkey service with shipping, tracking, and returns processing of Yubico products managed by logistics experts. This allows organizations to focus on what matters—securing internal and customer assets. With YubiEnterprise Delivery, YubiKeys can be mailed directly to residential addresses across more than 30 countries, enabling rapid deployment and adoption of strong authentication.

Trusted authentication leader

Yubico is the principal inventor of the WebAuthn/FIDO2 and U2F authentication standards adopted by the FIDO alliance and is the first company to produce the U2F security key and a multiprotocol FIDO2 authenticator.

YubiKeys are produced in the USA and Sweden, maintaining security and quality control over the entire manufacturing process.

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.