



WHITE PAPER

# Securing shared workstations against modern cyber threats

Phishing-resistant MFA with exceptional UX



# Contents

- 3 Shared workstations are low-hanging cyberattack targets**
- 5 Common shared workstation scenarios and associated vulnerabilities**
  - 5 Shared kiosks
  - 5 Mobile-restricted
  - 6 Grab-and-go
  - 6 Point-of-sale (POS)
- 7 Four critical authentication requirements across shared workstations**
- 9 Drawbacks of legacy MFA**
- 11 Securing shared workstations with phishing-resistant MFA**
- 12 Industry use cases**
  - 12 Protect confidential personal and financial information in retail banking call centers
  - 12 Secure nurse workstations and tap-and-go devices in hospitals
  - 12 Supporting retail POS with convenience and security
- 13 Summary**
- 14 Sources**

# Shared workstations are low-hanging cyberattack targets

Organizations today face an evolving cyber threat landscape, involving elements such as artificial intelligence and machine learning, and a range of threat vectors such as phishing, SIM swaps, and Man-in-the-Middle (MiTM) attacks that continue to grow in sophistication. Many of these approaches are virtually indistinguishable to the end user, leaving both them and their organizations highly exposed. Compromised credentials continue to be the most common attack entry point—61% of data breaches can be traced back to credentials in some way.<sup>2</sup> Insecure practices around credentials, including the sanctioned and unsanctioned sharing of usernames and passwords, only compound data breach risks for organizations.

Shared workstations—common across industries such as healthcare, manufacturing, retail, hospitality, financial services, energy, utilities, oil and gas, and education—have environments with high employee shift rotations, seasonal employees, and high turnover, creating potential high security risks if strong protection measures aren't in place. Shared workstations amplify the insider threat, whether malicious or negligent, and present additional security risks when used in high-traffic areas. Insecure shared workstation practices such as password sharing and the use of sticky-notes for passwords are common in shared workstation and shared device scenarios used by shift workers, and an indication of systemic issues with authentication workflows that get in the way of essential tasks.

## Data breach cost by industry<sup>1</sup>



Healthcare

\$9.23M

Financial services

\$5.72M

Manufacturing

\$4.99M

Energy

\$4.65M

Education

\$3.79M

Retail

\$3.27M

Hospitality

\$3.03M

61%

\*\*\*\*\*

of data breaches traced back to **credentials**<sup>3</sup>

\$11.45M



total average cost of insider threats<sup>4</sup>

46%



of employees **share passwords** or accounts<sup>5</sup>

82%



of individuals **reuse passwords** across accounts<sup>6</sup>

41%



rely on **sticky notes** for password management<sup>7</sup>

## What is a shared workstation?

Shared workstations are devices that are used by multiple users, sometimes called ‘roving users’, with multiple people authenticating to the same workstation throughout the day, such as call centers, or retail point-of-sale kiosks, just to name a few. Shared workstations are commonly used in industries with staff who work different shifts, rotating positions throughout the day, or in industries that have hourly, temporary or seasonal workers.

Shared workstations, kiosks, and devices are critical to the day-to-day operations of businesses in a wide cross-section of industries. These systems often have a direct link to critical systems and data, including customer data, payment information, proprietary information, manufacturing or assembly lines, and even protected health information.

The very nature of shared workstations make them low-hanging targets for cyber criminals and insider attacks:



**Has multiple users**



**Used in high traffic areas**



**Access to critical systems or data**



**Traditionally prone to insecure security practices**



**May or may not be managed by the corporate entity**

Shared workstations amplify risks associated with devices, user access, authentication, or insider threats that lead to the theft or loss of credentials, mission critical data, or intellectual property. If a shared workstation is unavailable due to a cyberattack, this can lead to business downtime, and further repercussions related to revenue, brand reputation, and regulatory compliance penalties.



# Common shared workstation scenarios and associated vulnerabilities

## Shared kiosk industries



Front-of-house at retail and hospitality



Nursing station at hospital or clinic



Manufacturing or logistics station



## Shared kiosks

Shared kiosks are workstations providing a set of common applications shared by many different users in front-of-house scenarios (restaurant, hotel, bank, post office, retail), at the nurses' station, or in manufacturing and logistics scenarios. Shared kiosks can be both stationary or even portable, as is the case with mobile workstations in healthcare.

Shared kiosks often support multiple users in a single shift, increasing the prevalence of insecure practices around password sharing to cut down on logout/login time necessary to access shared resources. In healthcare, for example, password sharing among healthcare professionals remains prevalent (73.6%), where individual access levels are the same.<sup>8</sup>

## Mobile-restricted industries



Call centers



Clean rooms



Airgap environments



High-security sites



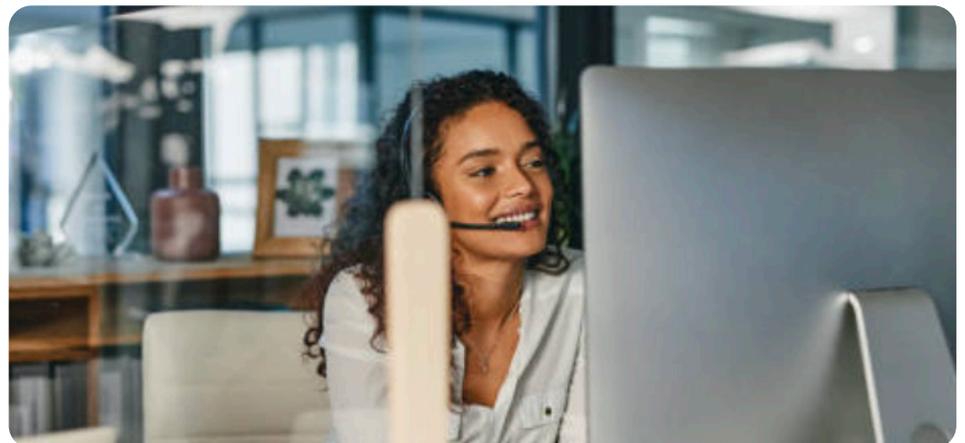
Industrial (no connection, oil rigs, etc)



## Mobile-restricted

A mobile-restricted environment is an environment where mobile devices cannot be used. These could be due to factors related to the environment itself, such as air-gapped or isolated networks, hard environments, offline or offshore locations, clean rooms or high-security sites. They could also be due to restrictions imposed by regulations, unions, or where mobile devices are simply discouraged by company policy. There may also be a subset of employees within an organization that do not wish to use personal mobile devices for work purposes, requiring a different authentication method.

Shared workstations and devices across mobile-restricted environments calls for authentication that is highly secure, compliant to industry regulations, and simple to use, to drive user adoption.



## Grab-and-go industries



Police and security workers



Healthcare and homecare



Visiting third parties



## Grab-and-go

A grab-and-go environment typically involves the use of a mobile cart of shared devices that can be picked up and used on-premise or in remote locations, and can be either a modern computing device such as a laptop, tablet or mobile phone, or even a device tied to a legacy system. The grab-and-go shared device is common in education and library settings, in law enforcement, and in healthcare. In each of these environments, a user only needs the device for a limited period of time.

Additionally, many industries have reacted to the post-pandemic realities of hybrid work by offering more grab-and-go opportunities to support employees who may have opted for fixed home configurations. Post-pandemic employees consider grab-and-go devices and “hoteling” a workspace in-office as a flexible and attractive work option.<sup>9</sup>

As no user is tied to the device, it is important to have controls that grant access to only those applications and services associated with the specific user credentials, and to authenticate quickly and reliably to support productivity.

## Point-of-sale industries



Retail



Grocery



Wholesale



## Point-of-sale (POS)

These specialized workstations used for customer-facing financial transactions in retail, grocery store, fast-food and restaurant industry, or wholesale environments, can be used by employees or even by customers (self-service kiosks). In order to optimize for the customer experience, special attention must be paid to speed and ease of authentication, avoiding potential account lockouts, and most importantly, ensuring the security of customer and payment information.

Due to the high risk to financial data at the point-of-sale, these workstations are highly regulated under PCI DSS (Payment Card Industry Data Security Standard). Card skimming is the most common risk with POS terminals, capturing data from payment infrastructure, overlays, malware or compromised software, or wireless / NFC interception. The high rate of employee turnover and the nature of seasonal work often create added pressure points around onboarding and offboarding employee access to POS systems.

A growing area of concern in POS is the use of smartphones, tablets, or other wireless devices in lieu of a standard POS terminal. By 2023, it is estimated that 1 in 4 POS transactions will be via mPOS (mobile point-of-sale), a process which increases the risk of Man-in-The-Middle (MiTM) attacks and introduces other mobile vulnerabilities.<sup>10</sup>



# Four critical authentication requirements across shared workstations

“ MFA is critical, but not all MFA methods are created equal. Twitter used application-based MFA, which sent a request for authentication to an employee’s smartphone. This is a common form of MFA, but it can be circumvented. During the Twitter Hack, the Hackers got past MFA by convincing the Twitter employees to authenticate the application-based MFA during the login. The most secure form of MFA is a physical security key, or hardware MFA, involving a USB key that is plugged into a computer to authenticate users. This type of hardware MFA would have stopped the Hackers, and Twitter is now implementing it in place of application-based MFA.

**–New York Department of Financial Services, Twitter Investigation Report, October 2020**



Security



Efficiency



Reliability



Cost

While considering authentication solutions for shared workstation environments, in addition to how effective the solution is in protecting against external cyberattacks and insider threats, organizations should also consider how the solution affects user productivity (account lockouts, log in times), how reliable the solution is across varied environments and use cases, external variables which may negatively impact performance, such as cell signal and batteries, and what the long-term total cost of ownership is.

Below are the four critical authentication requirements that organizations should take into consideration for any shared workstation environment:

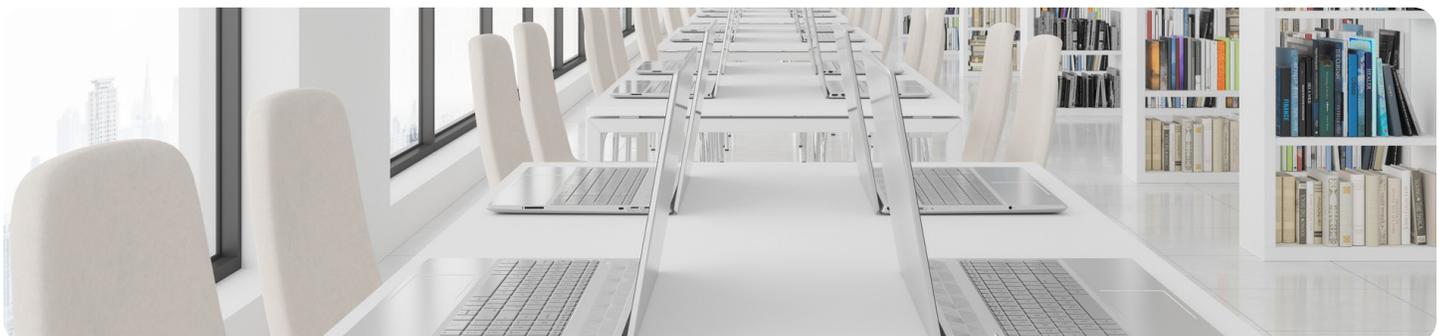
## Security

**How do you make sure the user logging into the device is the legitimate person?**

How do you secure shared devices and internal assets with multiple rotating users, making sure both the user accounts are secure and that the users are gaining access to only the applications, services and data they should have access to?

Admin accounts, or shared workstations with access to privileged information, should be protected with an authentication mechanism that is impersonation-resistant.

Shared workstations should rely heavily on user permissions and access controls (no shared, guest, or anonymous logins), and have restrictions that prevent password saving. Administrator accounts should also be individual, not shared, to support in-person or remote troubleshooting.



## Efficiency

### How do you make sure the user is able to authenticate quickly and seamlessly?

---

Consider how much time is appropriate for authentication and how many times a user may have to authenticate during the course of a shift or day.

---

Any authentication mechanism adopted for shared workstations should provide fast and easy authentication for employees, to avoid workflow disruption and unapproved workarounds. Currently, 54% of employees think two-factor authentication solutions such as OTP and push-codes disturb their day-to-day workflow.<sup>11</sup> Further, 34% of employees have experienced an inability to access critical work-related information due to not having access to a phone or authenticator app.<sup>12</sup>

As mentioned earlier, not all forms of multi-factor authentication (MFA) offer the optimal balance of strong security with a fast and easy user experience that enables high productivity. Some mobile authenticators may increase the number of steps in the authentication process, requiring users to wait for OTP or push app codes, or in case of pharmaceutical, healthcare and chemical organizations—to remove Personal Protective Equipment (PPE) for the authentication process. Regardless of the scenario, consider how much time is appropriate for authentication and how many times a user may have to authenticate during the course of a shift or day. Where efficiency requirements are high, consider a passwordless authentication experience.



## Reliability

### How do you ensure consistent authentication that always works, even in tough environments with varying degrees of connection?

Authentication is a mission-critical service, and if employees can't log into the apps or portals they use, they can't do their job. Any authentication solution has to be reliable for every user and not rely on common points of failure in connectivity, device battery, cell reception, or hard token battery. Authentication solutions should also have capabilities such as NFC that are suitable for environments such as labs, industrial manufacturing, clean rooms, and other types of environments with no spark requirements.

Consider that any authentication solution that relies on “something you know” (such as a password) is subject to human error—lost, forgotten, or mistyped details that add friction to the authentication experience—potentially locking users out of accounts. Mobile-based authentication solutions aren't always reliable across shared workstation environments where cell coverage is spotty or non-existent in places such as offshore rigs, operations technology (OT) environments, and remote geographic areas, or where users have to rely on device battery in the case of mobile-based authentication.

“ The average company loses \$5.2 million annually in productivity due to account lockouts

–Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report

## Cost

### How do you reduce the number of authentication-related support tickets?

Any form of legacy authentication such as usernames and passwords, and mobile authentication applied and enforced at scale, will require ongoing policy enforcement, user training and IT support. All forms of mobile-based authentication such as SMS, OTP, and push notifications can create a huge support burden if codes are delayed, users get locked out of their accounts, or users need to register new devices.

Any time a user struggles with mobile authentication, they are not being productive. The faster a user can authenticate and do their job securely, or even perform a self-service password reset if required, the better return on investment.

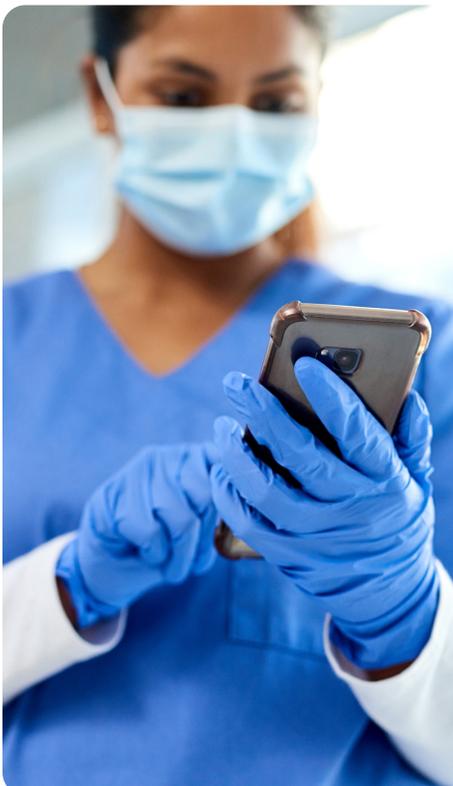
## Drawbacks of legacy MFA

### Low on security and reliability, high on cost and friction

Credentials remain one of the top targets for cyberattackers, and are connected to 61% of data breaches.<sup>13</sup> The average employee has to use and remember 191 passwords, contributing to complexity and user frustration.<sup>14</sup> Currently, for the average company, 60% of IT service desk interactions are related to password resets.<sup>15</sup> Aside from the IT cost, the average company loses \$5.2 million annually in productivity due to account lockouts.<sup>16</sup>

What is ongoing frustration with authentication most likely to lead to? Unsafe security workarounds—even by the most educated users. In fact, 49% of IT security professionals admit to password sharing.<sup>17</sup> We know that shared workstations are associated with higher rates of password sharing, password reuse across accounts, or passwords being saved to the browser or application—practices which are never safe, but amplify the risk in a shared workstation scenario.

However, it's important to note that while any form of two factor (2FA) or MFA offers more security than passwords alone, each still relies on passwords as the first factor. Further, with legacy MFA, such as mobile-based MFA, the second factor is tied to the mobile device. This is a red flag, because of three aspects: there is no real guarantee that the private key ends up on a secure element on the mobile device, the OTP code or private key could be intercepted in some way, and it is impossible to ensure proof of possession; or in National Institute of Standards and Technology (NIST) terms—impossible to prove it is impersonation resistant.



---

FIDO2 hardware security keys offer multi-factor and passwordless authentication with high security and an exceptional user experience. They also provide a portable root of trust that is highly appropriate for shared workstation environments.

---

Legacy mobile authentication is susceptible to modern cyberattacks including phishing, brute force attack, Man-in-The-Middle (MiTM) attack, malware, and SIM swapping. Beyond security, legacy mobile authentication carries with it many hidden costs associated with lost productivity, device costs, increased IT support, and friction in the user experience. In fact, 43% of organizations cite user experience as the top obstacle to using MFA.<sup>19</sup> For additional details, read our whitepaper: [The Top 5 Mobile Authentication Misconceptions: Demystifying the myth versus reality of legacy MFA](#).

Replacing legacy single-factor authentication (username and password) with phishing-resistant MFA, is the first step in improving security practices.

Because ultimately the actions of the user are the biggest weakness in legacy authentication, and multi-step authentication is a big contributor to user dissatisfaction, the global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

Moving from legacy MFA to phishing-resistant MFA is a key step forward in securing shared workstation environments. And the next step in modern MFA is introducing passwordless authentication. A SMS OTP is one form of passwordless authentication, but one considered weak from a security perspective. Traditional smart cards are another form of passwordless that offer high security, but generally require high Capex for smart card readers, cards, and backend management platforms, and don't offer the best user experience across modern devices such as smartphones and tablets. Because of this, the industry is moving toward a modern passwordless login flow leveraging FIDO2/WebAuthn.

FIDO (Fast IDentity Online) is a modern authentication standard that replaces traditional username and password with strong two-factor, multi-factor, and passwordless authentication. The FIDO standard was created by the FIDO Alliance, an open industry association whose mission is to reduce the reliance on passwords. FIDO2/WebAuthn is the most recent FIDO standard and uses public key cryptography for high security, where the private keys never leave the authenticator. FIDO2 hardware security keys offer multi-factor and passwordless authentication with high security and an exceptional user experience. They also provide a portable root of trust that is highly appropriate for shared workstation environments.



# Securing shared workstations with phishing-resistant MFA

The YubiKey delivers strong defense against phishing, portability, and an exceptional UX

Google: How effective is basic account hygiene at preventing hijacking



## The YubiKey 5 Series

From left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano



## The YubiKey 5 FIPS Series

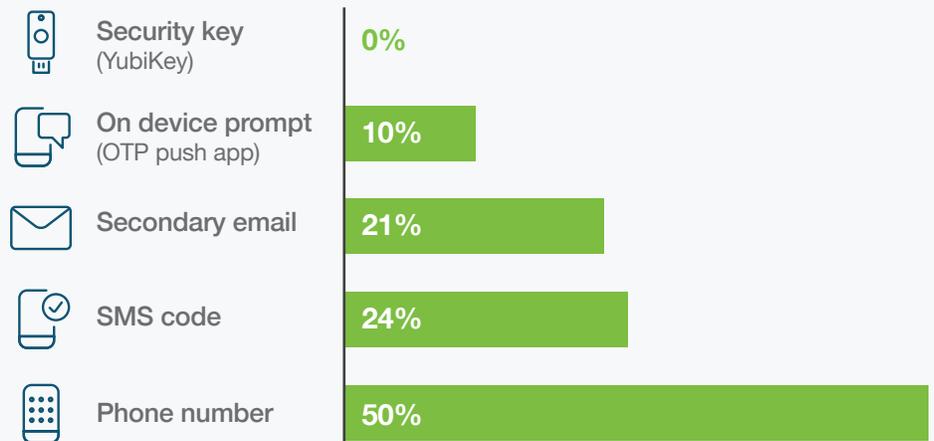
From left to right: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS and YubiKey 5C Nano FIPS



## YubiKey Bio Series - FIDO Edition

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition

## Account takeover prevention rates<sup>18</sup>



Yubico created the YubiKey, a hardware security key that offers phishing-resistant security and exceptional user experience in a portable USB and nano form factor. With the YubiKey, users can securely and easily authenticate to more than 700 applications and services across a variety of devices, with a simple tap or touch.

The YubiKey provides strong phishing-resistant two-factor, multi-factor, and passwordless authentication at scale, with the hardware authenticator protecting the private secrets on a secure element that cannot be easily exfiltrated. The YubiKey is the only solution that is proven to stop 100% of account takeovers in independent research.<sup>20</sup>

The YubiKey uses modern authentication protocols such as FIDO U2F and FIDO2 open authentication standards to help eliminate phishing-driven credential attacks. YubiKeys also support SmartCard, OTP, and OpenPGP protocols, enabling the use of a single security key across a variety of modern and legacy systems. The versatile YubiKey requires no software installation, battery, or cellular connection, making it ideal for shared workstation and mobile-restricted environments, including isolated areas. Users can benefit from a frictionless authentication workflow—a user plugs the YubiKey into a USB port and touches a button to authenticate, or simply taps the YubiKey using NFC against a device (highly suited for no spark environments).

YubiKeys also offer a bridge to passwordless authentication with support for multiple authentication protocols. To further improve the user experience and speed of authentication, Yubico also offers the YubiKey Bio Series—FIDO Edition supporting FIDO U2F and FIDO2, which delivers the hallmark security that all YubiKeys are known for with a new biometric-based passwordless experience.

# Industry Use Cases

## **Protect confidential personal and financial information in retail banking call centers**



In 2019, Aite Group interviewed 25 executives at 18 of the top 40 largest U.S. financial institutions, and found that 61% of fraud can be traced back to the contact center.<sup>21</sup> With high employee churn, seasonal peaks, and other challenging business dynamics, call center shared workstation environments need a secure, yet simple approach to verify agent identities before providing access to critical systems, and PII data.

Financial services call centers can deploy YubiKeys to deliver stronger security that can securely verify the identity of call center agents before they are given access to PII and other sensitive data, or make any changes to a customer account, such as raising a credit limit. In practice, the YubiKey has delivered a low TCO in call center environments, eliminating the need for frequent password refreshes, eliminating account lockouts and costly IT support, and streamlining employee productivity. For additional details, read the white paper: [Essentials for enabling strong authentication in financial services call centers](#).

## **Secure nurse workstations and tap-and-go devices in hospitals**

Healthcare organizations continue to be the top target for data theft, posing a challenge for securing point-of-care access to shared workstations and tap-and-go devices used for rounding.

While most hospitals have badge solutions for tap access to shared workstations and devices, in cases where elevated access is required (for admin access or for Electronic Prescriptions for Controlled Substances (EPCS) prescribing), these systems still rely on second-factor authentication with passwords, mobile authentication, or biometric data. In these scenarios, YubiKeys with a FIDO2-based passwordless experience can provide step-up authentication with a tap/touch and a PIN stored and verified locally on the key without the need of additional hardware drivers as would be needed with smart cards.

For additional details on using the YubiKey for phishing-resistant MFA across healthcare, read the white paper: [Best practices for strong authentication in healthcare using the YubiKey](#).

---

“ Instead of YubiKey being a highly recommended solution for our clients, we’re moving towards making it a required solution. We are building it into our hosting suite, and into our user fees.

– Retail Control Systems

---

## **Secure retail POS with convenience and security**

Retail Control Systems (RCS) markets and supports business management and point-of-sales (POS) systems to retailers and restaurants. Subject to increasingly strict PCI (Payment Card Industry) compliance requirements, RCS sought a solution that could be used internally by RCS to secure remote admin access to systems, but also externally to protect access to sensitive data.

Today, RCS authenticates over 11,000+ user logins with YubiKeys in a typical 48-hour period, helping protect devices as well as specific users and shared-user profiles.

# Summary

The YubiKey offers modern, phishing-resistant MFA, and enables a transition to passwordless for a better user experience and overall efficiency.

The YubiKey is an extremely robust and reliable solution (IP68 certified), offering high security and exceptional UX, replacing time-consuming and insecure second factors with a consistent tap-and-go experience that not only supports the user experience, but also reduces IT support costs.

To ensure strong security for your shared workstation environments, the YubiKey is uniquely designed to meet organizational and user needs, offering strong phishing resistance. It offers modern MFA capabilities, and even helps you make the transition to eliminating passwords altogether for a better user experience and overall efficiency. Stay ahead of the ever-evolving threat landscape with best-in-class security that sets you up for success not only now, but also into the future.

	Username & password	Mobile-based authenticators	YubiKey
 <b>Security</b>	Low, easily hacked	Medium, 10-15% account takeover rates <sup>22</sup>	High, 0% account takeover rate <sup>23</sup>
 <b>Efficiency</b>	Password fatigue, account lockouts	Users that can't, won't, don't use mobile MFA	Tap-and-go experience. 4x faster to login than OTP <sup>24</sup>
 <b>Reliability</b>	Prone to human error	Reliant on device battery and cellular network.  Not suited to mobile-restricted environments	Robust build, does not rely on cellular network
 <b>Cost</b>	No up-front cost. High IT support cost. High potential risk	\$1,840 is the true cost of enterprise mobility per owned device <sup>25</sup>	Low cost compared to mobile MFA, and 92% reduction in support tickets <sup>26</sup>

## Sources

- <sup>1</sup> IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), <https://www.ibm.com/security/data-breach>
- <sup>2</sup> IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), <https://www.ibm.com/security/data-breach>; Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- <sup>3</sup> Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- <sup>4</sup> IBM, Cost of Insider Threats: Global Report 2020, (Accessed November 12, 2021), <https://www.ibm.com/downloads/cas/LQZ4RONE>
- <sup>5</sup> Keeper, 4 Rules for Safe Password Sharing in the Workplace (April 2021), <https://www.keepersecurity.com/blog/2021/07/06/4-rules-for-safe-password-sharing-in-the-workplace/>
- <sup>6</sup> IBM, 2021 Cost of Data Breach Report, (Accessed September 14, 2021), <https://www.ibm.com/security/data-breach>
- <sup>7</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report>
- <sup>8</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report>; Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (July 2017), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5572521/>
- <sup>9</sup> Simon Constable, How Hot Desking Will Kill Your Company (June 20, 2019), <https://www.forbes.com/sites/simonconstable/2019/06/20/how-hot-desking-will-kill-your-company/?sh=16f55a8032e9>; Jessica Dickler, Post-pandemic, the office will now have a whole new look, (July 12, 2021), <https://www.cnbc.com/2021/07/12/post-pandemic-offices-have-a-new-look-as-employers-adopt-hoteling.html>
- <sup>10</sup> Juniper Research, POS & mPOS Terminals: Market Summary & Key Takeaways, (Accessed November 10, 2021), <https://www.juniperresearch.com/infographics/pos-mpos-terminals-market-summary-key-takeawa?ch=mpos>; Charlie Osborne, PayPal, Square vulnerabilities impact mobile point-of-sale machines (August 10, 2018), <https://www.zdnet.com/article/paypal-square-vulnerabilities-impact-mobile-point-of-sale-machines/>
- <sup>11</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report>; Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (July 2017), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5572521/>
- <sup>12</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report>; Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (July 2017), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5572521/>
- <sup>13</sup> Verizon, 2021 Data Breach Investigations Report, (Accessed May 18, 2021), <https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/>
- <sup>14</sup> Amber Steel, LastPass Reveals 8 Truths about Passwords in the New Password Exposé, (November 1, 2017), <https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose/>
- <sup>15</sup> Gartner, 3 Simple Ways IT Service Desks Should Handle Incidents and Requests, (Aug 2019)
- <sup>16</sup> Ponemon Institute, 2019 State of Password and Authentication Security Behaviors Report, (Accessed September 14, 2021), <https://pages.yubico.com/2019-password-and-authentication-report>
- <sup>17</sup> Ponemon Institute, 2020 State of Password and Authentication Security Behaviors Report, (February 2020), <https://pages.yubico.com/2020-password-and-authentication-report>; Ayal Hassidim, MD et. al., Prevalence of Sharing Access Credentials in Electronic Medical Records, Healthcare Informatics Research, (July 2017), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5572521/>
- <sup>18</sup> 451 Research, 2021 Yubico and 451 Research Study, (April 2021), <https://pages.yubico.com/work-from-home-policies-driving-mfa-adoption>
- <sup>19</sup> Kurt Thomas and Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (May 17, 2019), <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>
- <sup>20</sup> Aite Group for PinDrop, 61% of Fraud Traced Back to the Contact Center, (Accessed November 15, 2021), <https://www.pindrop.com/blog/61-of-fraud-traced-back-to-the-contact-center/>
- <sup>21</sup> <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>
- <sup>22</sup> Ibid.
- <sup>23</sup> Ibid.
- <sup>24</sup> Wander: Uncovering the true costs of enterprise mobility <https://www.clevermobile.it/risorse/file/wandera/tcowhitepaper.pdf>
- <sup>25</sup> <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>



## 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](http://www.yubico.com).