



WHITE PAPER

Protecting against modern cyber threats in retail and hospitality

Modernize MFA while improving customer experience



Contents

3	The critical need for security and efficiency across the retail and hospitality sectors
4	Meeting the customer experience demands of today
5	Evolving security regulations & cyber insurance requirements
6	Common authentication scenarios and their vulnerabilities
6	Employees and third-party workers
7	Privileged users
8	Customers
9	Corporate systems & eCommerce
9	Call centers
10	Cruise ships
10	Customer-facing retail stores or hospitality locations
10	Supply chain
11	Retail manufacturing
11	Shared workstations & POS
12	Inventory Scanner
13	Modernize MFA to address security, user and customer experience
14	The future is passwordless
14	Modern, phishing-resistant authentication with the YubiKey
16	Yubico offers simple procurement and distribution of phishing-resistant security at scale
18	Case Study: Supporting retail POS with convenience and security
19	Case Study: Hyatt Hotels leverages passwordless to reduce risk & elevate the guest experience
20	Summary
21	Source

The critical need for security and efficiency across the retail and hospitality sectors

Cost of data breach¹



Retail:

**\$3.48
Million**



Hospitality:

**\$3.82
Million**

The retail and hospitality sectors have been forced to evolve rapidly, replacing legacy systems, restructuring supply chains, expanding digital offerings and redesigning the customer experience. However, this digital transformation has increased the attack surface, exposing organizations to rising rates of sophisticated cyber attacks. A Trustwave investigation lists retail and hospitality industries among the top three most compromised industries.⁶

Credentials are the top data type compromised in both sectors, with 47% of retail attacks linked to a combination of compromised credentials and ransomware.⁷ Sophisticated attacks involving phishing and malware have both been on the rise, with retail named the top target of phishing attacks.⁸ Further, malware designed to exfiltrate data—almost always payment card data—is almost seven times higher in retail.⁹ Attacks in hospitality span across corporate networks (64%), eCommerce (18%) and point-of-sale (POS) systems (18%), with 36% of attacks involving ransomware.¹⁰

77%



of **retail** attacked by ransomware²

264%



increase in **ransomware attacks**³

Retail IT environments are often complex and large, spanning across the supply chain, from manufacturing and/or third-party risk to inventory, administration, brick-and-mortar POS, eCommerce and social or embedded commerce. Similarly, the hospitality sector covers a broad range of fields, from hotels and cruise ships to restaurants and travel and tourism organizations. As with retailers, hospitality organizations have a high reliance on partner reservation sites, shared workstation environments, and legacy POS and key card systems.

In both retail and hospitality, the high availability of both payment card information (PCI) and other sensitive personal information makes these organizations a lucrative target for cyber attacks. Data breaches in retail and hospitality can be costly, cause significant interruptions to operations, lead to significant regulatory non-compliance costs, as well as a loss in consumer confidence—a loss that ultimately damages both reputation and the bottom line.

90%



hospitality IT professionals
cite phishing as top concern⁴

68%



of data breaches tied to
the **human element**

social attacks, errors, misuse, credential theft⁵

Recent attacks in the news

In June 2022, Marriott International reported a social engineering attack, the third attack on the brand in four years, the most significant of which resulted in a £18.4m GDPR fine.¹¹ In 2021, a ransomware attack on Nordic Choice Hotels paralyzed most of its systems, including digital room key cards, and exposed employee data to the dark web.¹² 7-Eleven recently reported a similar store shutdown in Denmark that rendered checkouts and payment systems inoperable¹³ and Holiday Inn owner, Intercontinental Hotels Group (IHG) recently had their booking channels and other applications disrupted.¹⁴ These breaches can be costly, in terms of operations and settlements, as retailer Wawa recently discovered, having settled its 2019 credit card breach, which affected 34 million payment cards, for \$8 million.¹⁵

Organizations in retail and hospitality are facing mounting pressure to modernize authentication and security to protect sensitive customer and payment information as well as information technology (IT) and operational technology (OT) environments. Growing consumer pressure to prioritize privacy and security, coupled with requirements for MFA from active Salesforce CRM implementations¹⁶ and PCI DSS v4.0, are accelerating the shift to modern authentication standards.

Many retail and hospitality OT environments rely on legacy equipment and applications, placing constraints on the scalability and interoperability of security solutions. Organizations in the retail and hospitality space need an authentication solution that supports the transition to a more secure, tap-and-go workflow for better user experience, efficiency, and customer experience. Further, that solution must be quickly and easily deployed across a variety of IT and OT environments to support the complex needs of each authentication scenario and its vulnerabilities.

Meeting the customer experience demands of today

New battlegrounds on customer acquisition, relationship building, and retention are focusing on an understanding of consumer expectations and the customer experience (CX). Positive customer experiences minimize friction, establish trust and exceed customer expectations, helping boost loyalty and positive word of mouth. In contrast, increased levels of friction or other negative experiences can lead to poor conversion and ultimately customer churn. In fact, even when people love a company or product, 59% will walk away after several bad experiences—and 17% will walk away after just one bad experience.¹⁸

As the retail and hospitality sectors explore new technology to enhance the customer and guest experience, including contactless technology, apps and connected devices, it is critical to address security gaps in authentication that place data at risk. Further, customer-facing technology must be supported by efficient, unobtrusive authentication to allow front-desk staff and sales associates to provide a high level of attention. Imagine, for example, how a guest would feel if a front desk representative had to refer to their mobile phone during a customer interaction?

71%



of CMOs believe the biggest cost of a security incident is the loss of brand value.¹⁷



Guests are **29% more likely** to share positive reviews when hotel teams provide a high level of attention.²⁰

Even when people love a company or product, 59% will walk away after several bad experiences—and 17% will walk away after just one bad experience.¹⁹

Passwords and answers to security questions can be forgotten, and SMS/OTP codes can be delayed or missed. Mobile-based MFA could also be a source of delay and uncertainty in customer or guest interactions, when used by front-line staff, or a source of friction in the purchase experience for travel booking. Further, magnetic cards (mag stripe cards) do not offer the security of a smart card, as the information is not protected and the card is at risk for duplication.

For today's savvy consumers, strong multi-factor authentication is not just a nice-to-have element to prevent fraud or to convey trust, it is an essential part of the customer experience. In fact, security has emerged as a top environmental, social and governance (ESG) priority in hospitality to support employee retention and customer loyalty.²¹

Investing in strong authentication can replace the friction associated with passwords or mobile-based authentication, including the option for a tap-and-go passwordless experience with the highest levels of security protection and a seamless user experience, for customers and for employees.

Some of the regulations impacting global retail and hospitality organizations

PCI DSS	PSD2
GDPR	CCPA

What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

Evolving security regulations & cyber insurance requirements

Retail and hospitality organizations are subject to an increasing regulatory burden, most notably the Payment Card Industry Data Security Standard (PCI DSS) and EU Payment Services Directive 2 (PSD2) that provide the technical and operational requirements to protect payment data, as well as more broad reaching regulations including the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and other similar state privacy laws. Further, cyber insurance risk models have had to adapt to growing cyber attacks, with new minimum security requirements that require MFA.

The PCI DSS officially took a stand on requiring MFA in PCI DSS 3.2 and subsequent revisions.²² In response to growing cyber attacks, PCI DSS v4.0 takes a strong stand on multi-factor authentication, requiring the use of strong MFA for all accounts that have access to cardholder data, at every instance, with a three-year window to implement these new standards.

PCI DSS v4.0.1 expands the requirement to include MFA for all access into the cardholder data environment (CDE) consistent with NIST Special Publication 800-63, including POS accounts*, accounts with administrative capabilities, system and application accounts, and all third-party or vendor remote access.²³ Requirement 8.4.2, MFA will be required for all users at every attempt to access the CDE, with MFA expanded to all systems, environments, devices, and workstations. Further, Requirement 8.5 now requires MFA systems to be configured to prevent misuse and resist attack. In other words, PCI DSS v4.0.1 is placing emphasis on the use of phishing-resistant MFA. Just as importantly, Requirement 12, within PCI DSS v4.0, requires organizations establish a comprehensive information security policy to communicate security to relevant users inside and outside the organization as well as have security training to educate users on cyber risk and best practices.

What qualifies as phishing-resistant MFA?



Phishing-resistant MFA refers to an authentication process that is highly resistant to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intent to authenticate through deliberate action.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, two forms of authentication currently meet the mark for phishing-resistant MFA: the Federal Government's Personal Identity Verification (PIV)/Smart Card standard and the modern FIDO2/WebAuthn authentication standard, also known as passkeys. The FIDO (Fast Identity Online) modern authentication standard enables strong two-factor, multi-factor, and passwordless authentication.

Current authentication and security solutions, including usernames and passwords, security questions, and mobile-based authenticators such as SMS one-time-password (OTP) and push app are no longer effective to protect against modern cyber threats and do not meet the phishing-resistant standards required by PCI DSS v4.0.1.

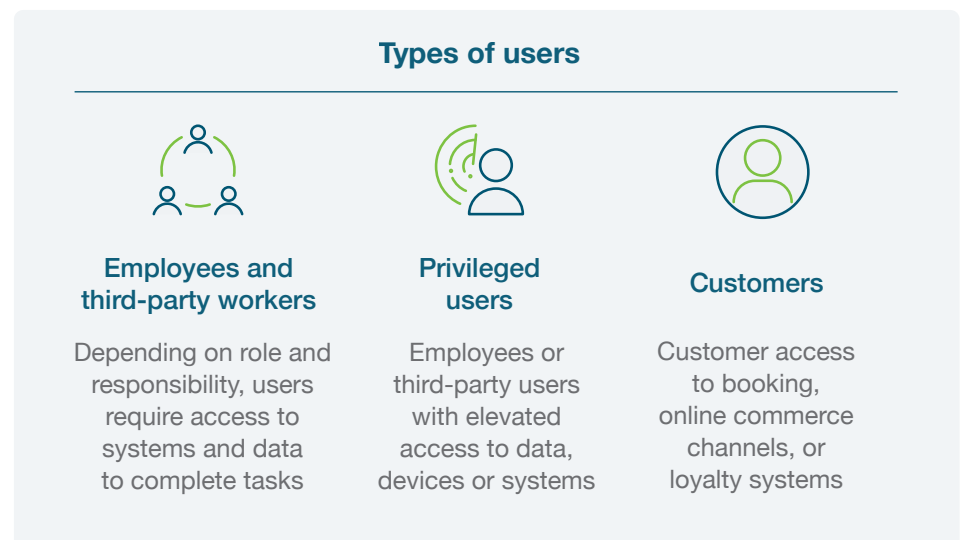
*PCI DSS 4.0 8.3.1 clarifies that the new requirement does not apply to user accounts on POS terminals that have access to only one card number at a time to facilitate a single transaction. The new requirement would apply to privileged access on POS terminals (e.g. managers).

Common authentication scenarios and their vulnerabilities



Across retail and hospitality, authentication can look quite different depending on the type of user, the anatomy of the retail & manufacturing organization, and even the type of shared device scenario. Each use case presents a wide range of factors to consider in order to best meet the authentication needs of the end user and the risk landscape, as well as the expectations of the customer.

As demonstrated below, this non-exhaustive list of scenarios can occur at any point in the organization and in isolation or combination with other scenarios. For example, a single authentication scenario can combine the vulnerabilities and challenges associated with privileged users, shared workstations, and cruise ships.



Employees and third-party workers

Retail and hospitality employees cross every area of the organization, from the administrative office to the warehouse, shipping, or customer-facing location. Employees may be full-time, part-time, contracted or hired as third-party workers. Organizations need a way to make user accounts secure and to ensure users have access to only the applications, services and data they should have access to based on their job responsibilities.

Privileged users

A privileged user or account is any user or login credential with elevated access to critical data or systems on the network, or to critical infrastructure. Privileged users and accounts should have different levels of access based on what they are required to see and do within these systems, ideally least privilege. The principle of least privilege means to provision the least possible access (who has access to what) and the least possible privilege (actions that someone can take) associated with that access. [According to research conducted by Ponemon Institute](#), an average of 23% of employees in an organization can be considered privileged users. [Learn more about the critical strong authentication need for privileged users.](#)

Types of privileged users



Sometimes users

Access to sensitive/confidential data or systems for contractors or for specific tasks



Privileged business user

Access to sensitive/confidential data C-suite, HR, finance, sales



Privileged IT user

Access to systems, software, and data IT admins, security admins, network admins, and database admins





Customers

Most online customer accounts and loyalty programs still use legacy username and password-based authentication, which doesn't keep customers safe against phishing attacks or account takeovers. Further, retailers are increasingly the target of fraud attempts to impersonate customers, particularly through call centers.²⁴

Drive competitive differentiation by investing in the safety and privacy of customer information internally, as well as at the point of use. By offering strong two-factor authentication or MFA for customers to access their online and mobile accounts, customers gain peace of mind that their accounts are protected against account takeovers. This same MFA protection also becomes a strong weapon against identity-based fraud.

Factors to consider for authentication



Corporate & eCommerce

Business, IT or corporate access to corporate systems, networks, eCommerce channels and systems, or data



Call center

Mobile-restricted environment, sometimes managed by a third-party vendor



Cruise ships

Independent infrastructure, disconnected from centralized network



Customer-facing retail stores or hospitality locations

Use shared devices that tie into the brand's corporate environment



Retail manufacturing

Potential for IP or product parts to be compromised in the manufacturing process



Supply chain

Third parties with physical or virtual access to information systems, code, inputs, or intellectual property

Corporate systems & eCommerce

With critical systems and PII data located across on-premises and the cloud, organizations need a simple yet effective way to ensure applications and data are protected against unauthorized access. Whether it's office workers, remote employees, contractors, or privileged users such as IT admins, strong authentication is the need of the hour, especially given a sharp increase in cybercrime.

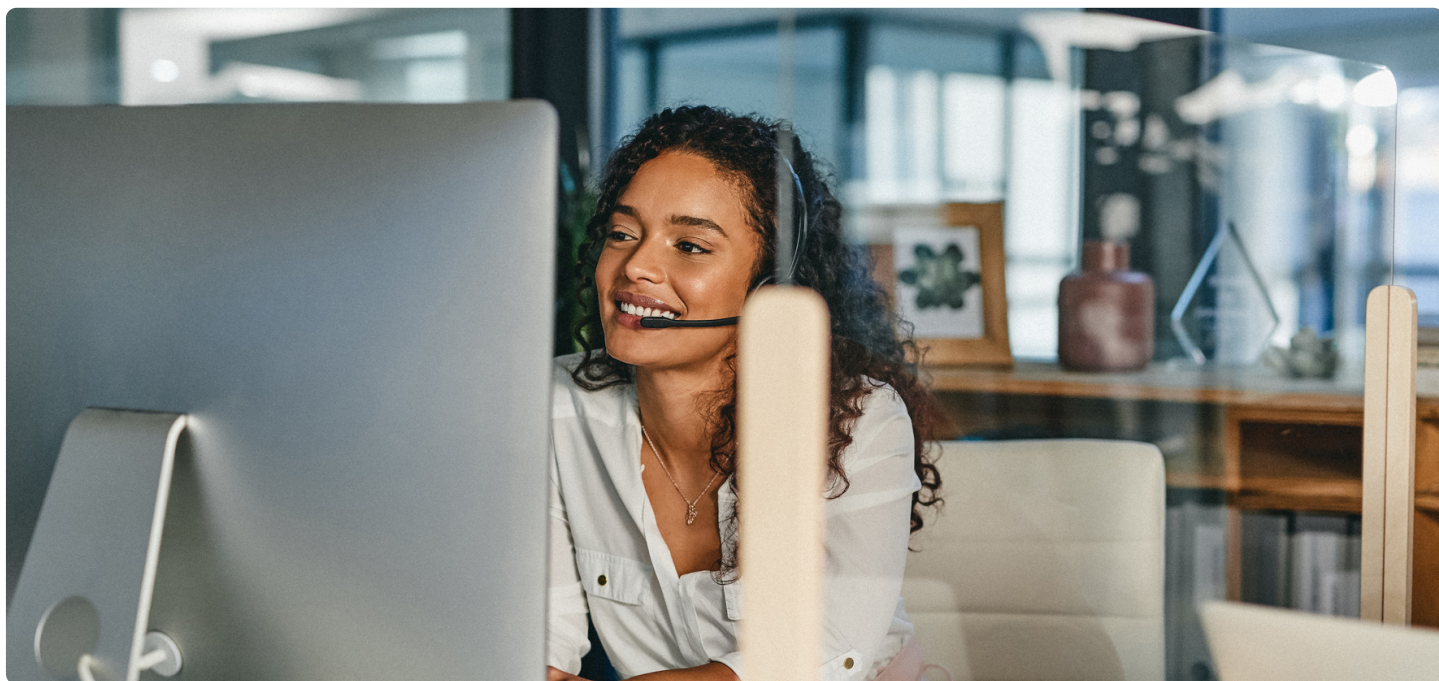
Even for other user groups outside the corporate office, access to corporate systems may be needed to support time clock activities or for access to corporate email, HR, or payroll systems. When systems or applications are used infrequently, this often leads to higher incidences of forgotten passwords and account lockouts, with impact on productivity and increasing IT support costs.

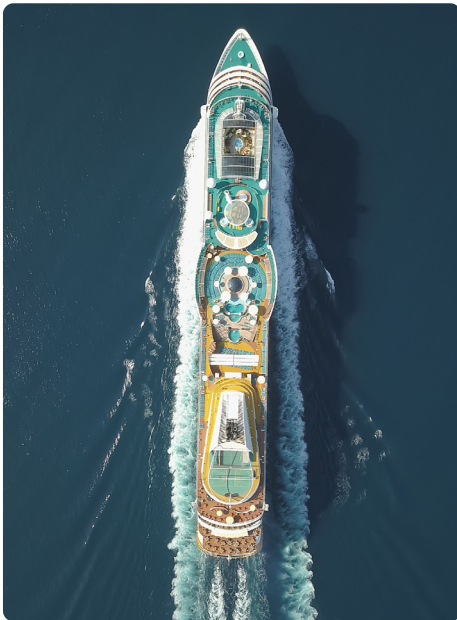
Beyond administration, as retailers and hoteliers expand their digital footprint across new channels including eCommerce and social, they need to address secure MFA to computers, servers and customer accounts, as well as create a system for secure code commits and code signing for the software being developed to support these commerce channels. As organizations leverage social media as a method to amplify their product or service offerings, strong MFA should be leveraged to secure these accounts.

Call centers

Call center agents have access to PII, PCI and other sensitive data to address customer concerns or assist in customer transactions, making it important to verify call center agent identity before such access is granted. At the same time, security controls around authentication need to support response time SLAs.

With most call centers now mobile-restricted by corporate policy, with mobile phones locked away in a secure environment, retail and hospitality organizations need a solution that will help secure a global workforce with a fast, seamless login to deliver efficient customer service.





Cruise ships

Cruise ship organizations collect and store vast amounts of personal, payment and health information, including COVID or other safety testing, making them lucrative targets for cyber criminals. In the span of one year, Carnival disclosed four data breaches across its brands, several related to ransomware, one of which was recently settled for \$1.25 million.²⁵ As part of the settlement, Carnival agreed to strengthen its MFA requirements for remote email access and general authentication requirements across the company.

In addition to the standard needs of any hospitality organization, cruise ships have unique security challenges and requirements. While at sea, cruise ships must support a fully independent IT infrastructure to support the ship and its guests, including a wide range of authentication requirements. As cruise ships streamline check-in with travel document pre-checks and enhance on-board experiences with NFC technology, the need to protect identities increases.

Cruise ships typically operate their own Active Directory Certificate Services (AD CS) to run secure wireless networks, encryption, authentication systems, and more. Poor cryptographic key handling can lead to accidental copying and distribution of cryptographic keys or remote extraction of private keys. The solution to protecting AD CS services must also meet the performance and size requirements of a cruise ship. [Learn more about the ultra-portable YubiHSM2.](#)

Customer-facing retail stores or hospitality locations

A customer-facing location in retail or hospitality is where employees directly engage with staff to buy or consume their product and/or service / stay. These locations may be owned and managed by the parent organization or may be franchise locations. Typically these locations have a mix of users and predominantly favor shared devices that tie into the brand's corporate environment.

Supply chain



The supply chain includes any input—physical item or part, hardware, software, code—or any digital interaction between people, applications, and processes. Within this broader context, protecting the security and integrity of the supply chain requires oversight over hundreds, if not thousands, of entry points—particularly for retail and hospitality organizations who regularly exchange data with third-party booking, reservation, or partner programs.

Global business and inventory supply chain networks can result in expansive attack surfaces. If even a single point in the supply chain is weak or unsecured, it can cause significant operational disruptions, financial loss, damage to brand, product integrity, safety issues, and the loss of intellectual property (IP). Just recently, Volkswagen disclosed a breach related to a security lapse with a third-party vendor, exposing the data of 3.3 million current and potential customers.²⁶

Organizations can begin their journey to reducing risk in the supply chain by identifying and mitigating risk by protecting third-party access with strong MFA and protecting the software supply chain with the [YubiHSM 2](#).

Retail manufacturing

One of the risks inherent in supply chain security is the possibility of compromise to the integrity, quality, or reliability of the product, software or service being delivered. For retail manufacturers, this involves a much broader security focus that ensures the integrity of IP and product parts that are involved in the manufacturing process.

The traditional approach to protect intellectual property (IP) and prevent counterfeiting in manufacturing involves the use of digital cryptographic signing keys and encryption, which are vulnerable to attack vectors, or with a hardware security module (HSM), which are large and expensive rack-mounted HSM devices. The future of securing the supply chain is further detailed in our whitepaper, [Protecting manufacturing with highest-assurance security](#).



Shared device scenarios



Shared workstations

Workstations or kiosks with many different users sharing productivity applications (e.g. front-of-house in a restaurant or hotel)



Point-of-sale (POS)

Specialized workstations or terminals used for customer-facing financial transactions



Inventory scanner

Inventory scanner (RFID) and management applications used to accept deliveries and manage inventory

There are many common shared device scenarios across retail and hospitality, often leveraging legacy hardware and/or software in hotel management, restaurant management, or POS. The nature of shared devices make them low-hanging targets for cyber criminals.

Shared workstations & POS

75% of POS compromises can be tied back to social engineering/phishing²⁷

Shared kiosks are workstations providing a set of common applications shared by many different users in front-of-house scenarios which are common in retail and hospitality organizations. These shared devices are used by many people, in high traffic areas, and are prone to insecure practices around password sharing or password saving to cut down on login time necessary to be productive or to service guests. Often these positions are prone to high turnover, temporary, or seasonal workers. Further, accounts with elevated access to customer or system data (e.g. to issue refunds or access databases) are often not protected with more secure authentication.

Research indicates that 75% of POS compromises can be tied back to social engineering / phishing, with POS malware kits now widely available that target known vulnerabilities in POS systems.²⁸ A notable example of such tactics is the 2021 breach at Neiman Marcus that exposed names and payment card details for 4.6 million customers.²⁹ The growing use of smartphones, tablets, wireless devices and near field communication (NFC) technology also introduces other mobile and wireless interception vulnerabilities.



Organizations need a way to secure shared kiosks and devices, 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, with restrictions to prevent password savings and protections for administrative accounts.

The PCI PIN Transaction Security (PTS) Point of Interaction (POI) standard under the umbrella of PCI defines the hardware and software requirements for POS terminals, and customer facing pin pads.³⁰ While POS systems are highly regulated, and soon fall under the strict MFA requirements of PCI DSS v4.0.1 mandate, there is a wider need to optimize authentication across all of these shared device scenarios to support employee efficiency and productivity. In customer-facing scenarios, ease of authentication ties directly to customer experience (CX) goals.

Inventory Scanner

Warehouses use RFID scanners to accept and manage inventory before it is sent to stores or consumers. The seasonal nature of retail means that warehouse workers may be hired and put to work on the same day, increasing the pressure for a streamlined onboarding process to payroll, time clock and scanning devices and the need for an enhanced authentication solution to track inventory risk. Further, there exists a need to differentiate and protect elevated access for supervisors.



Modernize MFA to address security, user and customer experience

Risk of account takeover rates



0%

FIDO security key (YubiKey)

10%

On-device prompt

21%

Secondary

24%

SMS Code

50%

Phone number

Given the many incentives and imperatives to tighten cybersecurity postures, it's clear that traditional models of MFA fall short. Most authentication scenarios across retail and hospitality have relied heavily on usernames and passwords, which are no longer effective to protect against modern cyber threats. However, the same can be true for more conventional MFA solutions including mobile-based authenticators such as SMS-based one-time-password or push app.

While further ahead in security, mobile authentication actually increases the friction in the authentication experience—adding more steps and delays to authenticate. And that friction can impact the end customer, whether the friction originates during a customer-staff interaction or during customer authentication workflows to loyalty or booking systems.

Conventional MFA may be familiar, but falls short on security



Vulnerable to attack

Every mobile authenticator can be phished



Expensive to maintain

\$1840/user in enterprise mobility costs



Poor user experience

Complex to operate and manage



Security gaps

Many users can't or won't use it

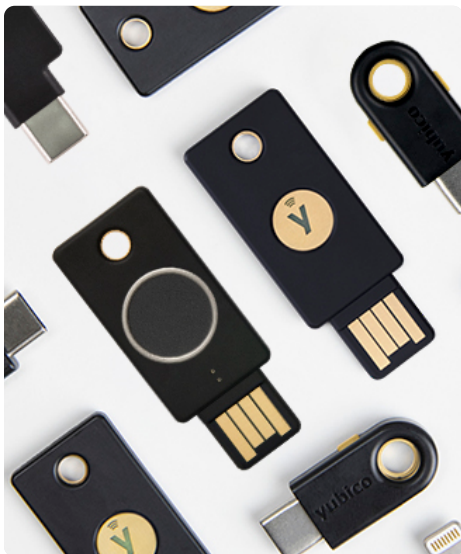


Short-term solution

Legacy MFA isn't built for the future

Research by Google, NYU, and UCSD, based on 350,000 real-world hijacking attempts, revealed that a SMS-based OTP only blocked 76% of targeted attacks and a push app only blocked 90%.³¹ That's, at minimum, a 10% penetration rate. With this approach, it's not a matter of if you will be attacked—it's a matter of when.

While considering authentication solutions for retail and hospitality 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 (e.g. cell signal and batteries) and the long-term total cost of ownership.



The YubiKey delivers strong defense against phishing, convenient portable authentication and an exceptional UX while acting as a bridge to passwordless

Cultivating phishing-resistant users

The only effective approach to remove phishing from an organization's threat landscape is to ensure that every user within the organization becomes phishing-resistant—and that resistance must move with the users no matter how they work, across devices, platforms and systems. Deploying phishing-resistant authentication across the entire user lifecycle, including the registration, authentication and recovery processes, is what creates a phishing-resistant user.

The future is passwordless

Ultimately the actions of the user are the biggest weakness in legacy authentication, and multi-step authentication is a big contributor to user dissatisfaction, which is why the global best practice is moving toward passwordless authentication—authentication that does not require the user to provide a password at login. While moving from legacy MFA to passwordless authentication may seem like a big jump, it's a jump that completely bypasses the unnecessary dissatisfaction found with more conventional MFA methods.

The FIDO modern authentication standard enables strong two-factor, multi-factor, and passwordless authentication. FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.

Modern, phishing-resistant authentication with the YubiKey

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 [thousands of applications and services](#) out-of-the-box including Google Suite, Microsoft Azure, and Microsoft Office 365 across a variety of devices with a simple tap or touch.

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 multi-protocol support allows organizations to leverage the YubiKey as a bridge to transition towards passwordless authentication.

By simply plugging a YubiKey into a laptop or tapping it against a smartphone to authenticate, YubiKeys help organizations create phishing-resistant users by using the highest-assurance passkeys in the market. The passkeys that reside in YubiKeys can be used to register the user and secure the other passkeys they use across devices and services. In other words, YubiKeys can be used to secure other forms of phishing-resistant MFA used within organizations to create phishing-resistant users, who then ultimately create phishing-resistance that can't be circumvented.

Reduce credential theft by 99.9% and helpdesk tickets by 75%, all while seeing an ROI of 203% with the YubiKey.

[Read the Forrester Consulting study →](#)

The Total Economic Impact™ Of Yubico YubiKeys commissioned by Yubico



“ We are taking great strides in protecting the safety of our guests and colleagues by requiring phishing-resistant MFA methods for all applications that can expose both PII and Card Holder data.





Using a Yubikey not only provides a more seamless experience for the colleague while keeping our data safe, but also allows those colleagues to keep their cell phones stored away while performing guest-facing roles.

Art Chernobrov | Hyatt Hotels Corporation Director of Identity, Access, and Endpoints



yubi.co/Hyatt

The versatile YubiKey requires no software installation, battery, or cellular connection, making it ideal for mobile-restricted, shared workstation and POS environments. 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, as is common in many POS terminals and can be supported on RFID devices with Identity Access Management (IAM) support.

	Username & password	Mobile-based authenticators	YubiKey
 Security	Low, easily hacked	Medium, 10-15% account takeover rates ³²	High, 0% account takeover rate ³³
 Efficiency	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 ³⁴
 Reliability	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
 Cost	No up-front cost. High IT support cost. High potential risk	\$1,840 is the true cost of enterprise mobility per owned device ³⁵	Low cost compared to mobile MFA, and 92% reduction in support tickets ³⁶

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.³⁷ As a phishing-resistant solution, the YubiKey helps simplify the information security policy requirements of PCI DSS v4.0 (12.1 and 12.2) while providing users with an easy to use, tap-and-go experience that removes roadblocks that legacy forms of authentication such as passwords, mobile-based MFA provides.

Yubico offers simple procurement and distribution of phishing-resistant security at scale



Yubico also offers YubiEnterprise Services to help organizations simplify procurement and distribution of YubiKeys at scale. These flexible and cost-effective enterprise plans, help organizations move away from legacy and broken MFA and accelerate towards phishing-resistant authentication.



YubiKey as a Service



YubiEnterprise Delivery

With [YubiKey as a Service](#), organizations with 500 users or more can greatly simplify the acquisition and roll out of phishing-resistant authentication. Organizations can move authentication spend from CAPEX to a predictable OPEX model, and ensure security is always covered as business needs evolve, and experience benefits such as the flexibility to meet user preferences with choice of any YubiKey, upgrades to the latest YubiKeys, and faster rollouts with easy access to deployment services, priority support and a dedicated Customer Success Manager.

Subscription customers are automatically entitled to access the Console, a web-based interface that helps organizations easily view orders, shipments, inventory status and a wide range of other information that helps with enterprise planning, and are also eligible to purchase additional services and product offerings, such as [YubiEnterprise Delivery](#), a global turnkey hardware key distribution service to residential and office locations across 49 countries. Additionally, new YubiEnterprise offerings and additional enterprise capabilities will be designed explicitly for Subscription customers.

[Yubico's Professional Services](#) team can provide technical and operational guidance to help streamline your YubiKey implementation and rollout with services mapped to your needs. In addition, Yubico Professional Services can provide documentation as well as services for user training to meet and surpass what is stated in the PCI DSS v4.0.1 Requirement 12 mandates.



Lifecycle management: empowering your users with YubiKeys

Key questions Yubico can help you with:

- ☐ Which YubiKey should my organization use?
- ☐ What is the best way to integrate YubiKeys into my environment?
- ☐ How can I get YubiKeys to my globally distributed workforce?
- ☐ How do I enroll a YubiKey in my MFA platform?
- ☐ How can I train and support end users?
- ☐ How does my help desk support the lifecycle of the YubiKey?

Once your users have their YubiKeys, the next step involves registering the keys with the applications and devices they will use. If a user leaves, some organizations retrieve YubiKeys prior to their departure while others prefer to allow departing users to keep their YubiKey and continue using it for their own personal accounts.

Depending upon your needs and use cases, from standard implementations to complex enterprise rollouts, Yubico Professional Services has the skills and expertise to help guide you through all technical and operational facets of a YubiKey implementation and deployment.



CASE STUDY

Supporting 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. Further, when implemented, the authentication method would need to not only scale with the growth of both the RCS customer base, but also their client's growth and needs.

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. Their YubiKey deployment enables them to secure their endpoints, whether desktop computers, laptops, or POS hardware into a unified authentication platform that aids in security and PCI compliance.



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."

RCS



Learn more from the Retail Control Systems' case study

yubi.co/RCS →

CASE STUDY

Hyatt Hotels leverages passwordless to reduce risk & elevate the guest experience

Hyatt Hotels Corporation has approximately 1,500 hotel and all-inclusive properties spanning across 70 countries. Art Chernobrov, Director of Identity, Access, and Endpoints, and his team of fifteen are responsible for managing the identities of all 200,000 colleagues as they move around the organization, as well as over 50,000 endpoint devices around the globe.

They are taking important steps to protect the safety of guests and colleagues by requiring phishing-resistant MFA methods for all applications that expose both PII and cardholder data. The YubiKey is also being used in their call center and with their loyalty programs, who either work in mobile-restricted environments or remotely on insecure networks, and for access to privileged access management (PAM) and enterprise resource planning (ERP) systems.

“There’s no amount of social engineering or MFA fatigue that will get past the fact that I can’t get into this system without a YubiKey in my hand.”

HYATT®

Yubico and Microsoft deliver strong identity, endpoint and access controls to Hyatt's global operations. With the YubiKey and Entra ID (formerly known as Azure AD), they are now able to provide passwordless authentication to all the apps a user needs to access for their role. They provide front-of-house colleagues with the YubiKey 5 NFC to support portable tap-and-go authentication and provide call center colleagues and back-of-house knowledge workers with the 5C Nano, although users are provided information to support the choice in form factor. With the aid of videos demonstrating the YubiKey in action, the rollout has been easy for them. In fact, the rollout has been so easy that the anticipated support calls simply “never materialized.”



Read the case study

yubi.co/Hyatt →



The YubiHSM 2 and YubiHSM 2 FIPS

From left to right: YubiHSM 2 and YubiHSM 2 FIPS



The YubiKey

From left to right: YubiKey Bio - FIDO Edition, YubiKey C Bio - FIDO Edition, YubiKey 5C NFC, YubiKey 5 NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

Summary

For retail and hospitality organizations meeting corporate security demands and the increased MFA requirements of PCI DSS v4.0.1, the YubiKey is an extremely robust and reliable solution across every authentication scenario, including the critical supply chain. The YubiKey offers high security and exceptional user experience, replacing time-consuming and insecure authentication methods with a consistent tap-and-go experience that not only supports the user experience, but also reduces IT support costs and costs associated with user training to meet PCI DSS v4.0.1 Requirement 12 mandates.

The YubiKey meets and surpasses the efficiency requirements of today's retail and hospitality organizations, empowering users to quickly authenticate and become more productive and eliminating friction in the authentication experience that could be witnessed by customers and guests. Further, leading retail and hospitality organizations are prioritizing the safety and privacy of consumer authentication experiences to drive competitive differentiation and show their customers that they care about their digital safety.



Contact us
yubi.co/contact



How to get started
yubi.co/7fu



Sources

- ¹ IBM, [2024 Cost of Data Breach Report](#), (Accessed March 15, 2024)
- ² Sophos, [The State of Ransomware 2022](#), (April 2022)
- ³ SonicWall, [2022 SonicWall Cyber Threat Report](#), (Accessed August 30, 2022)
- ⁴ Michal Christine Escobar, [Ninety Percent of Hospitality IT Professionals Cite Email Phishing Attacks as Top Concern](#), (November 4, 2021)
- ⁵ Verizon, [2024 Data Breach Investigations Report](#), (July 2024)
- ⁶ Trustwave, [2020 Trustwave Global Security Report](#), (Accessed August 5, 2022)
- ⁷ Verizon, [2024 Data Breach Investigations Report](#), (Accessed July 29, 2024)
- ⁸ Zscaler, [2022 ThreatLabz Report](#), (April 20, 2022)
- ⁹ Verizon, [2024 Data Breach Investigations Report](#), (Accessed July 29, 2024)
- ¹⁰ Trustwave, [2020 Trustwave Global Security Report](#), (Accessed August 5, 2022)
- ¹¹ Carly Page, [Hotel giant Marriott confirms yet another data breach](#), (July 6, 2022); [Carly Page, Marriot hit with 184 million GDPR fine over 2018 data breach](#), (October 30, 2020)
- ¹² Catherine Stupp, [Inside a Ransomware Hit at Nordic Choice Hotels](#), (January 12, 2022)
- ¹³ Lawrence Abrams, [7-Eleven stores in Denmark closed due to a cyberattack](#), (August 8, 2022)
- ¹⁴ Shiona McCallum, [Holiday Inn hotels hit by cyber-attack](#), (September 6, 2022)
- ¹⁵ Erin McCarthy, [Wawa will pay \\$8 million to states affected by massive 2019 credit card data breach](#), (July 26, 2022)
- ¹⁶ Salesforce, [Multi-Factor Authentication FAQ](#), (Accessed July 6, 2022)
- ¹⁷ Centrifry, [The Impact of Data Breaches on Reputation & Share Value](#), (May 2017)
- ¹⁸ PwC, [Experience is everything. Get it right.](#), (Accessed August 4, 2022)
- ¹⁹ Ibid
- ²⁰ Deloitte, [Next-gen hotel guests have checked in](#), (Accessed July 29, 2022)
- ²¹ PwC, [How to tell hospitality industry stakeholders a compelling ESG story](#), (Accessed July 29, 2022)
- ²² PCI SSC, [PCI DSS v4.0.1 Quick Reference Guide](#), (July 2018)
- ²³ PCI SSC, [PCI DSS v4.0](#), (March 2022)
- ²⁴ Andrew Froehlich, [How to train agents on call center fraud detection](#), (December 9, 2021)
- ²⁵ Lisa Vaas, [Carnival Cruise Cyber-Torpedoed by Cyberattack](#), (June 18, 2021); [Robert McGillivray, Carnival to Pay Fine Over Data Breach That Impacted Staff and Customers](#), (June 23, 2022)
- ²⁶ Zack Whittaker, [Volkswagen says a vendor's security lapse exposed 3.3 million drivers' details](#), (June 11, 2021)
- ²⁷ Trustwave, [2020 Trustwave Global Security Report](#), (Accessed August 5, 2022); [Symantec, Attacks on point-of-sales systems](#), (November 20, 2014)
- ²⁸ Ibid
- ²⁹ Emily Walsh, [Neiman Marcus is notifying nearly 5 million customers about a data breach that exposed names and payment card numbers](#), (October 1, 2021)
- ³⁰ PCI SSC, [PCI PTS POI v5.1](#), (March 2018)
- ³¹ Kurt Thomas, [Angelika Moscicki, New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019),
- ³² Ibid
- ³³ Ibid
- ³⁴ Ibid
- ³⁵ [Wander: Uncovering the true costs of enterprise mobility](#) (Accessed August 5, 2022)
- ³⁶ Kurth Thomas, et. al, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ³⁷ Ibid



About Yubico

Yubico (Nasdaq Stockholm: YUBICO), the inventor of the YubiKey, offers the gold standard for phishing-resistant multi-factor authentication (MFA), stopping account takeovers in their tracks and making secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries.

Yubico's solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

As part of its mission to make the internet more secure for everyone, Yubico donates YubiKeys to organizations helping at-risk individuals through the philanthropic initiative, Secure it Forward. The company is headquartered in Stockholm and Santa Clara, CA. For more information on Yubico, visit us at www.yubico.com.