



Phishing-resistant MFA and passwordless for retail and hospitality using the YubiKey

Legacy authentication puts your organization at risk of a security breach

Multi-factor authentication (MFA) can be a strong first-line of defense to protect against modern cyber threats, however not all forms of MFA are created equal. Legacy authentication such as usernames and passwords can be easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to modern phishing attacks, malware, SIM swaps, and man-in-the-middle (MiTM) attacks. In addition to security, it's also important to consider usability, portability, and scalability of authentication solutions. Poor user experiences, low portability, and lack of scalability can result in MFA gaps, low user adoption, and an increased risk of a breach.

Cybersecurity postures across the industry need to modernize drastically to protect against increasing cyberattacks, which can have large monetary repercussions. According to the [2021 IBM Security Cost of a Data Breach Report](#), the average cost of a data breach in retail is \$3.27 million, and \$3.03 million in hospitality, and security breaches can also result in regulatory non-compliance and dissatisfied customers. The 2020 SolarWinds and 2021 Kaseya attacks, and the more recently discovered [Apache Log4j API vulnerability](#), alerted the industry to the danger posed by security vulnerability-related cyberattacks. These attacks highlight the critical need for Zero Trust and phishing-resistant MFA solutions to defeat modern cybercriminals.



Safeguard people, technology, and data with the YubiKey

To protect against modern cyberthreats, Yubico offers the [YubiKey](#)—a hardware security key for phishing-resistant two-factor (2FA), MFA, and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research.¹ The YubiKey helps retail and hospitality organizations secure their employees, customers, data, and supply chains against cyberthreats, while driving regulatory compliance.

The YubiKey is simple to deploy and use—a single YubiKey can be used across both legacy and modern applications, services, and devices, with multi-protocol support for SmartCard, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key. YubiKeys don't require a battery or internet connection, and are highly durable, crush-resistant, and water-resistant. YubiKeys meet you where you are today on your MFA and passwordless journey, future-proofing security and empowering you to focus on providing an exceptional experience and quality of service to your customers.

“ 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



Here are five ways you can leverage the YubiKey:

1 Secure access to critical systems and data

A simple, yet effective way is needed to secure access to critical systems, applications, and employee and customer Personal Identifiable Information (PII), for your employees—in-person, hybrid, or remote. Mobile-based MFA isn't secure, and can be costly as organizations may be liable for mobile-related and service costs.

YubiKeys offer phishing-resistant MFA, ensuring only authorized people have access to PII data and critical systems, such as O365. YubiKeys integrate seamlessly with existing IAM solutions such as Microsoft, Okta, Duo, and Ping, and provide secure authentication for **hundreds of applications and services**, eliminating any rip or replace of existing solutions. YubiKeys are an ideal solution to strengthen security for privileged users and accounts as a first step in your phishing-resistant authentication journey.

2 Modernize security for POS terminals, shared workstations/devices to streamline interactions

A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and even shared workstations/kiosks, and point-of-sale (POS) terminals, enabling employees to utilize the same key as they navigate between devices delivering a convenient user experience—even for remote access. YubiKeys are easily re-programmed, making them suitable for seasonal and temporary workers. They also ensure self-service password resets, significantly reducing IT support costs and increasing employee productivity. YubiKeys with NFC capability, in combination with wearables, are also highly suited for tap-and-go convenience.

3 Protect your entire supply chain and eliminate vulnerability gaps

If your supply chain or business partners don't follow the same Zero Trust and phishing-resistant MFA approach as you do, this can result in major vulnerabilities and costly consequences putting your critical IP and/or goods at risk. With the YubiKey, your supply chain vendors, call centers, contractors, and business partners can also deploy phishing-resistant MFA, which minimizes your cyber risk, liability, and prevents damage to your brand reputation.

4 Provide a secure, passwordless experience for customer accounts and loyalty programs

Drive competitive differentiation by showing your customers you care about the safety and privacy of their sensitive information by offering phishing-resistant, passwordless 2FA or MFA for their digital accounts using the YubiKey. You and

your customers get peace of mind knowing that they are always protected against account takeovers, as well as have quick access to their customer accounts.

5 Drive compliance to industry regulations and authentication standards

Over **2.14 billion people** consumed goods and services digitally in 2021, which makes securing customer PII and strengthening cybersecurity across retail and hospitality more critical than ever. Industry Regulations such as The Payment Card Industry Data Security Standard (PCI DSS) v3.2 require the use of MFA to process payments, with more regulations expected in 2022. YubiKeys enable strong verification of users before providing access to sensitive data, keeping organizations compliant with existing and emerging regulations such as PCI DSS, Payment Services Directive (PSD) 2, GDPR, and more. YubiKeys are also **FIDO2/WebAuth compliant** streamlining workflows and increasing productivity.

Seamlessly procure and distribute YubiKeys at scale

Yubico makes it very convenient to get phishing-resistant MFA directly into the hands of your employees and supply chain vendors.

- **YubiEnterprise Subscription**, provides a service-based and affordable model for purchasing YubiKeys with predictable spending, upgrades to the latest offerings, customer support, and more. This is especially beneficial for industries with frequent employee turnover and seasonal employee coverage.
- **YubiEnterprise Delivery**, provides turnkey service with shipping, tracking, and returns handled by logistics experts, helping you get YubiKeys out to call centers, stores, remote locations, or anywhere you need them to be.

Contact the Yubico sales team today to be a cyber security leader in retail and hospitality with the YubiKey.



The YubiKey Family

The YubiKey is available in multiple form factors for desktop, laptops, mobile devices and tablets.

About Yubico As the inventor of the YubiKey, Yubico makes secure login easy. As a leader in setting global standards for secure access to computers, mobile devices, and more, Yubico is also a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards. For more information, please visit: www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

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

¹ Yubico, Google defends against account takeovers and reduces IT costs, <https://www.yubico.com/resources/reference-customers/google/>