yubico

Champion PCI DSS 4.0.1 with the YubiKey

The multi-protocol security key that bolsters compliance

Embracing for the next evolution of PCI DSS

The PCI Security Standards Council (SSC) publishes the PCI Data Security Standard (DSS). The PCI SCC continues to demonstrate investment and expertise as they enhanced the core 4.0 standard with a 4.0.1 update. PCI DSS holds organizations accountable around the world for implementing higher levels of cybersecurity to safeguard sensitive information and the payment ecosystem—impacting all industries.

Organizations collect a treasure trove of payment card data (PCI) as well as employee and customer identifiable information (PII) which necessitates stronger cybersecurity practices, starting with authentication. In fact, 90% of all cyber breaches are due to the theft of login credentials, passwords or other weak authentication methods.[1] While any form of multi-factor authentication (MFA) provides significant advantages over traditional username and password, some methods are more effective than others. Legacy mobile-based authentication such as SMS, OTP and push notification apps are not phishing resistant and create costly downtime risk for organizations. Not all MFA is created equal.

How PCI DSS 4.0.1 defines MFA

The language specifically references FIDO Alliance when choosing authentication factors and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 on **phishing-resistant MFA** stating that all MFA processes using shared secrets are vulnerable to phishing attacks—including: passwords, security questions, mobile-based authentication (SMS) and magnetic stripe cards. According to NIST SP 800-63-B4 only two forms of authentication currently meet the mark for phishing-resistant MFA: Smart Card/PIV and FIDO2/WebAuthn.

Specifically within v4.0.1:

- Requirement 8.X enhances MFA requirements to include at least one factor for users and administrators and at least two factors of MFA for all access into the cardholder data environment (CDE) and related systems.
- Requirement 12.X details the need to focus on user experience that encourages the ease of use of MFA while focusing on user training and education.

At least one factor for users / administrators
At least two for access to the CDE

- Something you know
- Something you have
- Something you are

And must include

- Strong cryptography
- Verified user identity
- Security policies and training

The MFA system must meet minimum requirements

- Resistant to attack
- Cannot be bypassed

What this means for your authentication strategy

The weaker your MFA posture, the greater your compliance burden: longer policies, more user training, and more controls to manage risk. The solution: apply strong phishing-resistant MFA, passwordless to all users. With AI-driven phishing attacks, QR code phishing attacks (Quishing) and other social engineering attacks, it necessitates the need for phishing-resistant authentication to address the evolving sophisticated threat landscape.

Protect your organization with the high-assurance YubiKey to bolster your PCI DSS 4.0.1 strategy

The YubiKey is a modern hardware security key that offers phishing-resistant multi-factor and passwordless authentication providing authentication that moves with users, and is highly suitable to secure payment services within all industries (financial services, retail and hospitality, healthcare, telcos, and more) as well as secure a wide range of scenarios:

- Privileged users
- Customer-facing locations
- Call center
- Shared devices including point-of-sale (POS) terminals
- Office and hybrid workers
- End customers

Why choose the YubiKey for phishing-resistant authentication?

- With the YubiKey deploy the most secure passkey strategy: device-bound that is purpose-built for security, FIPS 140-2 validated and Authenticator Assurance Level 3 (AAL3) compliant
- Bridge to modern passwordless with multi-protocol support for Smart Card/PIV, FIDO2/WebAuthn, FIDO U2F, and OTP on a single key
- Cultivate phishing-resistant users, all the way from registering new employees on new devices, to daily authentication tasks, and even through account recovery processes
- Login without a password using phishing-resistant FIDO2 authentication to provide the strongest level of protection with the YubiKey-you can't compromise what you don't have
- Reduce risk of credential theft by 99.9% and stops account takeovers while delivering 203% ROI[2]
- Provide secure user access at scale on any device with the best user experience
- Drive business continuity, satisfy cyber insurance and regulatory requirements
- Ensure that any remote cyberattack will be unsuccessful because the YubiKey enforces human presence as a requirement when submitting credentials for authentication

The YubiKey Family

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

Get started today and seamlessly deploy YubiKeys

Yubico offers flexible and cost-effective enterprise plans that help organizations with 500 users or more move away from legacy and broken MFA and accelerate towards phishing-resistant authentication at scale.

With YubiKey as a Service, organizations can benefit from a predictable OPEX model, 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.

Experience global turnkey YubiKey distribution through YubiEnterprise Delivery, to residential and office locations across 49 countries, or through local channel partners.

At Yubico we meet you where you are on your cybersecurity journey and bolster your compliance posture to meet the needs of today and into the future.

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

Dustin Morse | Bussiness Operations Manger | Retail Control Systems

Yubi.co/RCS

Contact us
yubi.co/contact

Learn more
yubi.co/yk5

[1] Statistica, Most reported cyber crime..., (August 2023)

[2] Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: www.yubico.com.