SOLUTION BRIEF

HYPR

Meet PCI DSS Standards With HYPR

Deploy FIDO Certified passwordless MFA that ensures compliance with PCI DSS 4.0 and empowers your workforce with fast, secure access to accounts and systems

PCI DSS 3.21, introduced in 2018 outlines security requirements for organizations that handle payment card data to ensure the protection of sensitive information. Because of the evolution of the payment industry, in March 2022 the Council released PCI DSS 4.0, which introduces 60+ new standards. PCI DSS 4.0 went into effect in March 2024, with a phased implementation timeline over twelve months.

New Regulations to Combat Increased Threats

Password-based authentication methods, including traditional multi-factor authentication (MFA), leave organizations and data vulnerable due to weak passwords, password reuse, phishing and other credential-related attacks. PCI DSS 3.21 and 4.0 both list a number of guidelines that involve authentication methodologies, risk-based assessment and identity verification. PCI DSS 4.0 significantly advances required security mechanisms, which, while important to protect consumer data, have the potential to negatively impact organization productivity and cost burden.

Passwordless MFA based on FIDO (Fast IDentity Online) standards aligns with the PCI DSS framework and presents an innovative approach to address authentication security challenges. HYPR is a passwordless multi-factor authentication (MFA) solution that strengthens identity and authentication security and streamlines user experience. PCI DSS 4.0 explicitly recognizes the benefits of FIDO, specifying it as an authentication method.

PCI DSS Compliance With HYPR

HYPR helps organizations comply with PCI DSS MFA requirements as well as multiple other provisions included in the standard.

HYPR Key Benefits

- Comply with PCI DSS 4.0 strong authentication requirements
- Reduce authentication friction and improve user experience
- Protect against credential theft, phishing and fraud with secure authentication based on FIDO standards
- Cover all your use cases including remote employees and shared workstations
- Continuously monitor authentication activities, contextual information and user behavior to detect suspicious patterns and automatically adapt authentication controls
- Deploy mature, enterprise-proven passwordless MFA that delivers validated ROI of 324%

Strong Authentication

PCI DSS requires organizations to implement strong authentication mechanisms. In PCI DSS 4.0, Requirement 8 sets forth specifications for secure implementation of multi-factor authentication systems. To improve authentication security, Version 4.0 also significantly increases required password length from a minimum length of seven characters to 12. This requirement applies only if passwords/ passphrases are used as an authentication factor.

Longer passwords are more onerous for users, are more likely to be written down and lead to an increased volume of help desk calls. Recent analysis published by Forrester Research and HYPR shows that the average help desk call costs organizations $42.50 per call.

HYPR replaces the traditional password-based approach with more secure authentication factors that include identity-based verification and risk-based passwordless authentication that is certified by FIDO and based on passkeys. Key staples of the solution such as biometrics (fingerprint, facial recognition), possession of a trusted device, and cryptographic tokens stored on the most secure portion of the device such as the TPM or secure enclave, ensure strong, phishing-resistant multi-factor authentication that meets PCI DSS requirements.

User Experience and Compliance

The average employee already uses more than four different authentication experiences every day. The stringent PCI DSS 4.0 rules mean that these multiple experiences will get even more taxing.

HYPR greatly improves the user experience. HYPR eliminates the need to both remember complex passwords as well as abide by the PCI DSS requirement to change passwords every 90-days. Moreover, HYPR streamlines multi-factor authentication to a single user gesture, significantly reducing authentication friction and improving user satisfaction. This, in turn, can lead to better adherence to security practices and compliance.

Protection Against Credential Theft

PCI DSS mandates protection against credential theft as this is a major vector for attackers to gain access to sensitive payment card data. Typical attacks that harvest this type of information include MitM, phishing, brute force and social engineering. PCI DSS 4.0 Requirement 5 adds a specific requirement to detect and protect personnel against phishing attacks. Additionally, Requirement 8 stipulates that passwords/ passphrases for application and system accounts be protected against misuse. HYPR eliminates the risk of stolen passwords and credential phishing since there are no passwords or shared secrets to steal.

User Behavior Analytics

Behavioral analytics monitors activities and establishes a baseline on a per-user basis. Deviations from this baseline can indicate potential security threats or unauthorized access attempts. HYPR's risk-based authentication approach aligns with PCI DSS Requirement 10, which emphasizes the tracking and monitoring of user activities.

3 in 5

organizations were breached
due to authentication weaknesses
in the last 12 months

$2.95M

average cost of
authentication-related cyber breaches
in the last 12 months

Source: The State of Passwordless Security Vol. 3, Vanson Bourne and HYPR, March 2023

Fraud Prevention

PCI DSS requires organizations to implement measures to prevent fraud. HYPR's risk-based authentication engine helps detect fraud by analyzing transaction data and comparing it against known patterns of fraudulent behavior and customizable policies. By identifying unusual transactions, behavior or policy violations, HYPR empowers organizations to prevent fraudulent activities.

Continuous Monitoring and Threat Detection

PCI DSS emphasizes the importance of continuous monitoring to identify and respond to security threats. HYPR's risk-based authentication actively monitors authentication activities, user behaviors, device profiles and policy adherence, detecting anomalies and suspicious patterns. By identifying potential threats promptly, HYPR helps organizations prevent data breaches and unauthorized access, thereby aligning with PCI DSS 4.0 Requirement 10 for tracking and monitoring access.

Adaptive Authentication

PCI DSS encourages the use of adaptive authentication based on a real-time and detailed risk assessment. HYPR's risk-based authentication evaluates various factors, such as user location, device used, transaction history, and behavioral patterns, to determine the risk level of a transaction or authentication attempt. Based on the risk assessment, the authentication process can be adjusted. This aligns with PCI DSS 4.0 Requirement 8, which emphasizes the use of multi-factor authentication for higher-risk scenarios.

Threat Mitigation and Response

HYPR provides a policy and anomaly-based approach that empowers organizations with the ability to take immediate action when high-risk activities are detected. This can be done as a standalone product or used in conjunction with signals to and from the organization's existing security ecosystem. This proactive and collaborative response helps mitigate threats before they escalate. Rapid incident response aligns with PCI DSS's focus on minimizing the impact of potential breaches and responding effectively to security incidents (Requirement 12).

User Identification

Identity verification mechanisms help in definitively identifying individual users. This aligns with PCI DSS Requirement 8, which emphasizes user identification and accountability. It also helps with the PCI DSS 4.0 standard (Requirements 3 & 5) that establishes adherence to user roles and responsibilities. By accurately identifying users through strong authentication methods, organizations can maintain an audit trail of user activities and quickly trace any unauthorized or suspicious actions back to specific individuals.

Multi-Factor Authentication (MFA) for Remote Access

PCI DSS mandates multi-factor authentication for all remote network access originating from outside the network perimeter. This is typical for users that are remote, hybrid or have supporting roles outside the organization. They typically will use RDP, VPN and VDI to access resources and can be the achilles heel in the authentication process. HYPR provides a convenient and secure way to implement MFA for remote access. Users can authenticate using either a smartphone or hardware-based solution depending on what best fits the requirements for their unique use case.

Strong Cryptography and Security Protocols

PCI DSS requires the use of strong cryptography and security protocols for authentication. HYPR implements robust cryptographic techniques to secure biometric data and cryptographic tokens used in the authentication process, ensuring that data transmission and storage are well-protected.

The private key is stored on, and never leaves, the most secure portion of the device. For the organization, there is no longer a centralized database of credentials that can be hacked. A hacker would have to effectively hack into each individual's phone and crack this secure area of the phone. This makes it both a difficult and unattractive prospect for attackers.

Prevention of Unauthorized Access

Effective identity verification helps organizations comply with PCI DSS by preventing unauthorized access to cardholder data. Requirement 7 of PCI DSS focuses on restricting access to cardholder data based on the principle of least privilege. By implementing strong identity verification methods, organizations can ensure that only authorized personnel can access specific data and systems, minimizing the risk of an authentication and/or an identity based security incident.

Unique User Identification and Access Control

HYPR helps organizations meet the PCI DSS requirement of assigning unique IDs to each person with access to systems and implementing authentication mechanisms to prevent unauthorized access. Biometric authentication and device-based possession factors ensure unique user identification and access control.

Eliminating Vendor-Supplied Defaults

PCI DSS guidelines advise against using vendor-supplied defaults for system passwords and other security parameters. HYPR completely eliminates the need for traditional passwords and shared secrets, reducing the reliance on vendor supplied defaults for authentication.

Rely on the Identity Assurance Leader

HYPR offers organizations a robust and convenient way to enhance security while aligning with PCI DSS guidelines. By replacing traditional passwords with stronger authentication factors, HYPR mitigates the risks associated with compromised credentials and contributes to overall data protection and compliance efforts.

HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments, including 2 of the 4 largest US banks, leading critical infrastructure companies, organizations that take and/or process payment datam and other technology-forward businesses. HYPR's solutions have been independently validated to return a 324% ROI.

HYPR

THE IDENTITY ASSURANCE COMPANY

www.hypr.com | hypr.com/contact