Zaperon

WHITEPAPER

PCI-DSS Cybersecurity Compliance Made Easy With Zaperon



Introduction

The financial sector is a prime target for cyber criminals due to its handling of substantial volumes of sensitive data and transactions. The 2024 Thales Data Threat Report reveals that nearly two-thirds (64%) of financial services organizations have observed an uptick in attacks. As cyberattacks surge, financial data of users is increasingly at risk. As per Cybernews, the Dark Web has over 26 billion records from 3800+ data breaches globally that includes financial information of the individual users. The security of IT systems that hold users' payment data is therefore the need of the hour.

Payment Card Industry Data Security Standard (PCI-DSS), launched on September 7, 2006, is a global regulatory standard that establishes fundamental technical, physical, and operational security controls essential for safeguarding payment card account data. According to Verizon's Payment Security Report, only 27.9% of the organizations have achieved full compliance with the PCI DSS.

26 Billion

Records from over 3,800+ data breaches globally are exposed on the dark web

Source: Cybernews Report



PCI-DSS Rolls Out Version 4.0 for Payment Card Industry

PCI-DSS has undergone several revisions to keep pace with the evolving threat landscape and technological advancements. The current version is **PCI-DSS v4.0, which was released in March 2022** and includes 64 requirements in 12 categories for organizations.

GOALS	PCI DSS REQUIREMENT
Build & Maintain a Secure Network & Systems	**1.** Install and maintain network security controls **2.** Apply secure configurations to all system components
Protect Account Data	**3.** Protect stored account data **4.** Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems and networks from malicious software **6.** Develop and maintain secure systems and software
Implement Strong Access Control Measures	**7.** Restrict access to system components and cardholder data by business need to know **8.** Identify users and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor & Test Networks	**10.** Log and monitor all access to system components and cardholder data **11.** Test security of systems and networks regularly
Maintain an Information Security Policy	**12.** Support information security with organization policies and programs

Who Needs to Comply?

- Payment Processors
- Banks and Financial Institutions
- Service Providers
- E-commerce Sites
- Retailers & Merchants
- Hospitality & Healthcare Businesses
- Transportation Companies
- Utility Companies



Consequences of Non-Compliance

FINES
Hefty fines from $5,000 to $100,000 per month until compliance is achieved.

LEGAL RISKS
Potential lawsuits and legal expenses.

REPUTATION LOSS
Damage to trust and brand reputation.

BUSINESS IMPACT
Loss of ability to process card payments.

SECURITY RISKS
Increased vulnerability to data breaches.

AUDITS
More stringent and frequent compliance checks.

Adobe settled for **$1 Million** across 15 states when it experienced a data breach impacting 38 million customers.

Adobe™

EQUIFAX

Equifax data breach resulted in a **$425 Million** settlement, affecting over 143 million Americans and leaving a significant impact.

PCI-DSS Compliance with Zaperon's Identity Protection Platform 2.0

Requirement 1

Install and maintain network security controls

1.3. Network access to and from the cardholder data environment is restricted.

COMPLY WITH ZAPERON

Zaperon is based on zero trust architecture that enforces microsegmentation by creating software-defined parameter for the enterprise applications. Users can only access applications that are authorized by company policy, enforcing least privilege access and mitigating insider threat. Each user device is assigned a unique PKI certificate, facilitating passwordless single sign-on and Zero Trust Access control. Continuous monitoring of device posture (antivirus,operating system, IP, location) ensures only secure devices are connecting to enterprise resources.

Requirement 2

Apply secure configurations to all system components

2.1. Processes and mechanisms for applying secure configurations to all system components are defined and understood.

2.2. System components are configured and managed securely.

2.3. Wireless environments are configured and managed securely.

COMPLY WITH ZAPERON

Zaperon provides secure access to applications, servers and network devices from inside the corporate network and remote locations. This prevents phishing attacks on resources that otherwise only rely on weak/default passwords. Additionally, device binding eliminates unauthorized access to resources from BYOD or unmanaged devices.

Requirement 5

Protect all systems and networks from malicious software

5.1. Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

5.2. Malicious software (malware) is prevented, or detected and addressed.

5.3. Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4. Anti-phishing mechanisms protect users against phishing attacks.

COMPLY WITH ZAPERON

Zaperon continuously monitors security posture of the user devices and ensures that the antivirus or an endpoint security tool mandated by the organization is active on the device. In case the allowed antivirus is not found, user access to the enterprise resources is immediately blocked, protecting users from malware attacks. Zaperon also checks the operating system version installed on the device and blocks access if the latest patches have not been installed.

The platform prevents phishing attacks on organizations by implementing PKI-based passwordless authentication and multi-factor authentication that validates 15+ factors including device certificate, user behavior, device posture and context.

Requirement 6

Develop and maintain secure systems and software

6.4. Public-facing web applications are protected against attacks.

COMPLY WITH ZAPERON

Zaperon offers passwordless single sign-on and certificate-based authentication to all major public-facing web applications that support out-of-the-box integrations. For 3rd-party or in-house applications, the platform uses an intelligent authentication gateway that restricts access to web applications from corporate-sanctioned devices (including BYOD) only and also adds phishing-resistant MFA for additional layer of security, ensuring only authorized users can access applications.

Requirement 7

Restrict access to system components and cardholder data by business need to know

7.1. Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood

7.2. Access to system components and data is appropriately defined and assigned.

7.3. Access to system components and data is managed via an access control system(s).

COMPLY WITH ZAPERON

Zaperon enforces role-based access control (RBAC) and least privilege principles, ensuring users access enterprise resources and data strictly according to their assigned roles and from registered devices.. Continuous monitoring ensures adherence to zero trust access policies, with activities of privileged users in the Zaperon management console logged for comprehensive audit trails.

Zaperon also prevents data leak from endpoints by blocking file transfer through USB ports, bluetooth and airdrop. Data in cloud applications is also secured by preventing downloads from Google Drive, Gmail, OneDrive, Sharepoint and Outlook.

Requirement 8

Identify users and authenticate access to system components

8.1. Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2. User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3. Strong authentication for users and administrators is established and managed.

8.4. Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5. Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6. Use of application and system accounts and associated authentication factors is strictly managed.

COMPLY WITH ZAPERON

Zaperon is based on zero trust framework to provide least privilege access, continuous device trust, and proactive identity threat detection. Users are assigned specific applications, as per business needs, that they can access strictly from authorized and secure devices.

Zaperon uniquely identifies each user device with a PKI-based certificate and continuously monitors device posture (IP, location, antivirus, operation system, access time) to ensure secure access from any user, device and location. The platform also offers additional security with phishing-resistant multi-factor authentication (MFA) that validates 15+ factors including device certificate, user behavior, device posture and context.

Requirement 10

Log and monitor all access to system components and cardholder data

10.1. Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2. Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3. Audit logs are protected from destruction and unauthorized modifications.

10.4. Audit logs are reviewed to identify anomalies or suspicious activity.

10.5. Audit log history is retained and available for analysis.

COMPLY WITH ZAPERON

Zaperon logs all applications accessed by users along with the context-based parameters - location, device used, access time. Assessment of security posture (IP, antivirus, operating system) of all the user devices is done continuously and logged. Any anomaly in the user behavior and device posture is immediately flagged and alerts are sent to admins.

Additionally, system logs track activities performed by admin users in the Zaperon console for comprehensive monitoring. Zaperon also offers dashboards for real-time visibility and comprehensive monitoring.



Zaperon Identity Protection 2.0

PKI-BASED PASSWORDLESS AUTHENTICATION

Leverages PKI for secure, passwordless access, minimizing the risk of data breaches from credential compromise.

PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Employs phishing-resistant MFA, boosting security with over 15 factors.

CONTINUOUS ZERO TRUST ACCESS CONTROL

Continuously applies zero trust policies based on user behavior and device status, ensuring compliance and security.

PROACTIVE IDENTITY THREAT DETECTION AND RESPONSE

Identifies anomalies and addresses identity threats proactively, reducing potential security risks.

COMPREHENSIVE IDENTITY PROTECTION

Provides thorough identity protection with proactive threat detection and response, ensuring strong security for users, devices, applications, and cloud infrastructure.

Zaperon sets a new standard in identity protection with its advanced platform, protecting organizations from identity-based attacks. By integrating PKI-based passwordless access and phishing-resistant multi-factor authentication, it enforces ongoing zero-trust policies according to user behavior and device posture. Proactive identity threat detection and response ensure robust security across users, devices, applications, and cloud infrastructure.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com
© 2024 Zaperon, Inc.
All Rights Reserved.