COMPLIANCE GUIDE

How Zero Networks Helps with PCI DSS Regulation Requirements

The Payment Card Industry Data Security Standard (PCI DSS) mandates that all organizations handling credit card information implement robust security measures to protect cardholder data and maintain the integrity of their payment systems. This standard applies to any entity that stores, processes, or transmits credit card data, including merchants, financial institutions, and service providers.

Below are the specific PDI DSS requirements Zero Networks helps achieve.

Network Security and Access Control

Requirement	Description	How Zero Helps
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	This requirement mandates the implementation and maintenance of firewalls to protect cardholder data environments by restricting unauthorized traffic and regularly reviewing and updating firewall rules.	Zero Networks' microsegmentation solution acts as a distributed firewall using logical segmentation, enabling organizations to create isolated network segments for cardholder data environments, implement granular access controls, and restrict inbound and outbound traffic to the Cardholder Data Environment (CDE).
Requirement 7: Restrict access to cardholder data by business need-to-know	This requirement focuses on limiting access to cardholder data and system components to only those individuals whose job requires such access, implementing role-based access control, and regularly reviewing user access rights.	Zero Networks' identity segmentation enforces fine-grained, role-based access control across all system components. This ensures users only access the resources necessary for their job roles—especially those involving sensitive assets or cardholder data. With just-in-time MFA, Zero Networks also grants elevated access only when needed, strengthening authentication and reducing risk.
Requirement 8: Identify and authenticate access to system components	This requirement mandates unique identification for each person with computer access, ensuring accountability, and requires the implementation of strong authentication methods, including multi-factor authentication for remote access.	Zero Networks provides robust network and identity segmentation features, enabling unique user identification and secure authentication mechanisms for all communication across users, processes, apps, and assets, including multi-factor authentication for remote access to streamline auditing.
Requirement 8.4: Multi-factor authentication (MFA) for non-console access	PCI DSS 4.0.1 requires MFA for all access to the CDE, including personnel, systems, and remote connections. MFA must use at least two independent factors (e.g., password, token, or biometric) to prevent unauthorized access.	Zero Networks provides seamless network-layer MFA integration for all access to the CDE, ensuring compliance with Requirement 8.4 by enforcing authentication across all users and systems. Its identity segmentation and secure remote access solutions leverage strong authentication methods, such as app-based tokens or biometrics, to meet PCI DSS standards while minimizing friction for financial customers.

Data Protection and Encryption

Requirement	Description	How Zero Helps
Requirement 3: Protect stored cardholder data	This requirement focuses on securing stored cardholder data through methods such as encryption, truncation, or tokenization, and mandates proper key management practices for cryptographic keys.	Zero Networks' microsegmentation capabilities help organizations isolate systems storing cardholder data from non-sanctioned networks, business areas, or systems and implement strict access controls to stored cardholder data, allowing only sanctioned users to access sensitive systems with just-in-time MFA.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	This requirement mandates the use of strong cryptography and security protocols to protect cardholder data during transmission over public networks, including wireless networks.	Zero Networks' secure remote access capabilities ensure strong encryption for all transmissions of cardholder data over public networks and implement secure protocols for remote access technologies.

Monitoring and Testing

Requirement	Description	How Zero Helps
Requirement 10: Track and monitor all access to network resources and cardholder data	This requirement involves implementing logging mechanisms to track user activities, requiring daily log reviews and retention of audit trail history for at least one year.	Zero Networks' solutions provide detailed logs of all access attempts to the CDE and enable real-time monitoring of network segmentation effectiveness, integrating with SIEM tooling and providing streams of network activity and audit data to support comprehensive tracking and monitoring.
Requirement 11: Regularly test security systems and processes	This requirement mandates regular testing of security systems and processes, including conducting vulnerability scans and penetration tests to identify potential vulnerabilities.	Zero Networks' microsegmentation and identity segmentation support regular testing of network segmentation effectiveness and enable simulated attack scenarios to verify the ability to detect and prevent unauthorized access. With a unified view of network and identity activity, Zero Networks delivers end-to-end communications visibility, providing testing validation and proof. In short, Zero does not take the place of an effective test plan and procedure, but can provide validation to an assessor or engineer.

Maintaining an Information Security Policy

Requirement	Description	How Zero Helps
Requirement 12: Maintain a policy that addresses information security for all personnel	This requirement focuses on establishing, publishing, maintaining, and disseminating a comprehensive security policy that addresses all PCI DSS requirements and includes an annual process for identifying vulnerabilities.	Zero Networks' solutions support the implementation of security policies related to network segmentation and access control, enabling organizations to provide proof of the required policies to auditors without draining resources.

ZERO. Networks

Catalyze compliance and protect your network.

Try Zero today