PCI DSS Requirements

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

PCI DSS provides a baseline of technical and operational requirements designed to protect account data (cardholder data and / or sensitive authentication data). The standard applies to all entities involved in payment card processing — including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data and / or sensitive authentication data.

PCI DSS consists of 12 sections of requirements and more than 200 controls that are focused on the security of the data of credit cards. Appropriate policies and procedures, technical measures, administrative efforts, and physical security should supplement each other in the organization in order to ensure continuous compliance with PCI DSS Requirements.

Failure to comply with PCI DSS may result in fines, loss of reputation, and inability to accept major credit cards.

Find out which specific PCI DSS requirements you can address with Netwrix Change Tracker

PCI DSS security standard is designed to protect cardholder data by requiring organizations to have an appropriate combination of policies, procedures, technical measures, administrative efforts and physical security. Netwrix Change Tracker helps you achieve and maintain compliance with PCI DSS requirements by delivering enterprise-wide visibility into your on-premises and cloud-based applications and systems, as well as deep insight into your sensitive data. In addition to helping you establish the security controls required to protect cardholder data, this PCI DSS compliance software enables you to provide evidence that those security controls are aligned with the following requirements:

PCI DSS v3.2	Requirement Detail	Netwrix Solution
Requirement 1: 1.1, 1.2, 1.3	Install and maintain a firewall configuration to protect cardholder data	Use Netwrix Change Tracker to apply configuration baselines. Apply FIM to firewall rules and security configuration settings, collect logs to detect security incidents related to any breach
Requirement 2: 2.1, 2.2, 2.3	Do not use vendor-supplied defaults for system passwords and other security parameters	Prebuilt device hardening templates derived from CIS Benchmarks are used to audit for any vulnerabilities present: database systems, servers and network devices are then continuously monitored for any drift from the desired, hardened state
Requirement 3: 3.5, 3.6	Protect stored cardholder data	File Integrity Monitoring technology ensures access to cryptographic keys is restricted, and any attempted unauthorized access is logged and alerted, including changes of accounts, privileges and permissions
Requirement 4: 4.1	Encrypt transmission of cardholder data across open, public networks	Built-in vulnerability reports verify the use of encrypted console access methods, thereafter any configuration change affecting the devices' hardened state will be detected
Requirement 5: 5.2	Protect all systems against malware and regularly update antivirus software or programs	Netwrix Change Tracker will check that AV services are activated and running. Netwrix Log Tracker will alert on all significant AV events
Requirement 6: 6.1, 6.4	Develop and maintain secure systems and applications	Netwrix Change Tracker maintains host and application security settings, even for bespoke applications, and records all software and patch updates. Netwrix Log Tracker provides a complete audit trail of application and host access attempts
Requirement 7: 7.1, 7.2	Restrict access to cardholder data by business need to know	At all times, Netwrix Log Tracker will provide a 'checks and balances' audit trail of all account and privilege changes

PCI DSS v3.2	Requirement Detail	Netwrix Solution
Requirement 8: 8.1, 8.2, 8.5	Identify and authenticate access to system components	Initial hardening audit will verify correct password and authentication policies are in use, with all subsequent account and privilege changes audited
Requirement 10: 10.1, 10.2, 10.3, 10.5, 10.6, 10.7	Track and monitor all access to net- work resources and cardholder data	Audit trails are constructed automatically using predefined Netwrix Log Tracker templates for PCI DSS V3.2, including default alerts for security threats
Requirement 11: 11.1, 11.4, 11.5	Regularly test security systems and processes	File Integrity Monitoring across all systems is an essential defense against malware and insider threats to card and customer data built-in templates for PCI DSS V3.2 provided
Requirement 12: 12.2, 12.3, 12.5, 12.9	Maintain a policy that ad- dresses in- formation security for all personnel	Security Management procedures can be automated and audited using built-in intel- ligent alerting and reporting

About Netwrix

Netwrix makes data security easy thereby simplifying how professionals can control sensitive, regulated and business-critical data, regardless of where it resides. More than 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Next Steps

Learn More - Check out more information about Change Tracker: netwrix.com/integrity

Live demo — Take a product tour with a Netwrix expert: netwrix.com/integrity

Request quote — Receive pricing information: netwrix.com/integrity

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social