



Protecting Stored Cardholder Data for PCI Compliance

Check Point solutions enable PCI compliance
for data stored on all retail endpoints

Contents

- Executive summary 3
- PCI imposes broad security requirements 3
- PCI Requirement 3: Protect stored cardholder data 4
- Specifying protection for data on endpoints 6
- Check Point equals PCI compliance for retailers 8

Executive summary

The Payment Card Industry Data Security Standard (PCI DSS) was developed by Visa in partnership with MasterCard International and is now supported by every other major international payment card brand as an institutional mechanism to protect cardholder data. PCI is now an industrywide standard consisting of six control objectives and 12 requirements. The scope of PCI requirements is broad, encompassing nearly every aspect of network and information security. Requirements include a mixture of security technologies and best practices. Verification of compliance and related audit procedures are tailored to the number of card transactions processed by retail businesses and all other organizations involved in card transactions.

Compliance is an important topic for the retail community because of public scrutiny triggered by recent data breaches affecting millions of consumers. Noncompliance may result in a data breach event, loss of consumer trust and related business, and requirements to pay costs related to identity theft, mass notifications, and likely civil penalties from state or federal regulations. But as industry enforcement of PCI rises, noncompliance may also cause retailers to lose the right to accept card payments—and that would eliminate their primary source of payments.

Because PCI represents virtually all security technologies and best practices, it is important to address compliance by prioritizing requirements and settling the most consequential matters first. The bottom line is protecting cardholder data. That is the mission of PCI. This white paper will cover PCI, examine its requirements for data protection, and present its requirements for storing data securely. It details technology options such as full-disk encryption and port control, describing how each relates to PCI—particularly on endpoint devices such as laptops, PDAs, smartphones, and mobile USB storage devices. The goal is to help retailers to specify security solutions for compliance based on specific sections in the PCI standard and its Security Audit Procedures.

PCI imposes broad security requirements

The Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) has six control objectives and 12 supporting requirements to protect networks, applications, and cardholder data. PCI compliance requires the use of a broad set of security technologies and best practices. None of these are unusual—indeed, requirements for PCI are similar to policies for most information security legislation, regulations, and best practices. By following the broad provisions of PCI, a retailer will be taking the best possible steps to ensure the confidentiality, integrity, and availability of vital business systems and enterprise operations. PCI requires that retailers:¹

Build and maintain a secure network—by (1) installing and maintaining a firewall configuration to protect cardholder data and (2) by not using vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data—by (3) shielding stored cardholder data and (4) encrypting transmission of cardholder data across open, public networks

¹ PCI Version 1.1 (Sept. 2006); https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

Maintain a vulnerability management program—by (5) using and regularly updating antivirus software and (6) developing and maintaining secure systems and applications

Implement strong access control measures—that (7) restrict access to cardholder data on a business need-to-know basis, (8) assign a unique ID to each person with computer access, and (9) restrict physical access to cardholder data

Regularly monitor and test networks—by (10) tracking and monitoring all access to network resources and cardholder data and (11) regularly testing security systems and processes

Maintain an information security policy—that (12) addresses information security

PCI Requirement 3: Protect stored cardholder data

Check Point product portfolio addresses spectrum of PCI

Network Security

- Firewall/VPN
- Unified threat management
- Intrusion detection and prevention
- Endpoint security

Data Security

- Full-disk encryption and access control
- Mobile device encryption
- Port management and removable media encryption

Security Management

- Centralized platform for monitoring and reporting
- Security Management Portal

PCI Requirement 3.4 is at the heart of the provisions for stored data security. It specifies protection of the Primary Account Number (PAN). If stored in conjunction with a PAN, it is also a requirement of PCI that the Cardholder Name, Service Code, and Expiration Date are also protected. The balance of this white paper focuses on complying with PCI specifications for protecting stored data as described in Requirement 3.4.

Stored data requires the use of security controls to ensure that an unauthorized person could never gain access to sensitive information. All actual data would be unreadable and unusable to that person. Requirement 3 notes, “Encryption is a critical component of cardholder data protection.” It also states, “Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities.” The rationale is that solutions other than encryption may be appropriate for a variety of risks related to stored data. The retail environment is rife with opportunity to exploit cardholder data (see “Security challenges for retail endpoints” below), so it is important to carefully consider the risks present in your environment to ensure compliance with PCI Requirement 3.4.

Security challenges for retail endpoints

Protecting retail IT environments is a complex challenge given the variety of unique solutions deployed in headquarters and regional offices, distribution centers, and stores. Retail enterprises with hundreds or thousands of stores face the added complexity of securing endpoints typically used by people with minimal IT skills—plus little-to-no in-store technical resources.

Preventing PCI data leakage through endpoints

Securing endpoint PCs and mobile devices used for customer-facing applications includes preventing leakage of PCI data. Credit card transaction data from point-of-sale applications is frequently stored on local endpoints in addition to central servers. This is especially true for franchisees and legacy systems that require local storage for communications with merchant banks. The often-chaotic environment of retail stores requires automatic, transparent, and comprehensive security controls to protect PCI data stored on endpoints. According to PCI, controls must render PAN and associated data unreadable. They must also protect mobile devices and prevent data leakage to unauthorized mobile storage devices.

Requirement 3.4—Rendering PAN unreadable

The specifications for PCI Requirement 3.4 state that it is a necessity to:

Render PAN, at a minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

- Strong one-way hash functions (hashed indexes)
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key management processes and procedures

Using encryption for PCI compliance

Encryption is the cryptological process of taking data in plain-text format and rendering it unreadable to anyone without special knowledge and permission. Technology options for encrypting stored data include file- or column-level encryption and full-disk encryption. If the latter is used, Requirement 3.4.1 states:

If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local system or Active Directory accounts). Decryption keys must not be tied to user accounts.

Testing procedures

To test for compliance with Req. 3.4.1, the PCI Security Standards Council defines the testing procedures in section 3.4.1.a through 3.4.1.c of its Security Audit Procedures² noting:

3.4.1.a If disk encryption is used, verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism (for example, not using local or Active Directory accounts)

3.4.1.b Verify that decryption keys are not stored on the local system (for example, store keys on floppy disk, CD-ROM, etc., that can be secured and retrieved only when needed)

3.4.1.c Verify that cardholder data on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media)

PCI Requirement 3.4 concludes that, “If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: ‘Compensating Controls for Encryption of Stored Data.’”

Specifying protection for data on endpoints

PCI does not specify any particular kind of encryption for compliance (the standard states that strong cryptography, such as 3-DES (128-bit) or AES (256-bit) should be used, with associated key management processes and procedures). Indeed, the mandatory annual Self-Assessment Questionnaire only asks in 3.5: “Are account numbers (in databases, logs, files, backup media, etc.) stored securely—for example, by means of encryption or truncation?”³ The answer required is a simple “yes” or “no.”

File- or folder-level vs. full-disk encryption

File- or folder-level encryption works by protecting data stored in specific files or folders on a storage device. Speed is the cited advantage: by only encrypting specific data, the machine is able to perform faster, which may be especially important for a server processing transactions on hundreds of thousands or millions of cardholders.

For endpoint devices, full-disk encryption is a better option because it automatically protects the entire contents stored on all devices. If a device is lost or stolen, full-disk encryption fulfills PCI compliance better because it protects PAN and related data anywhere it may reside on the device, in any application, and in any storage format. Unlike file- or folder-level encryption that requires users to specify target files or folders, full-disk encryption is automatic—and so is compliance with the stored data security requirements of PCI.

As for performance, under ordinary business usage conditions, an endpoint computer running Check Point Endpoint Security™ Full Disk Encryption operates at 95 to 98.5 percent⁴ of the performance level of a computer without encryption, based on tests with PassMark performance measuring software. This variance is a negligible cost for automatically ensuring absolute protection of all stored data.

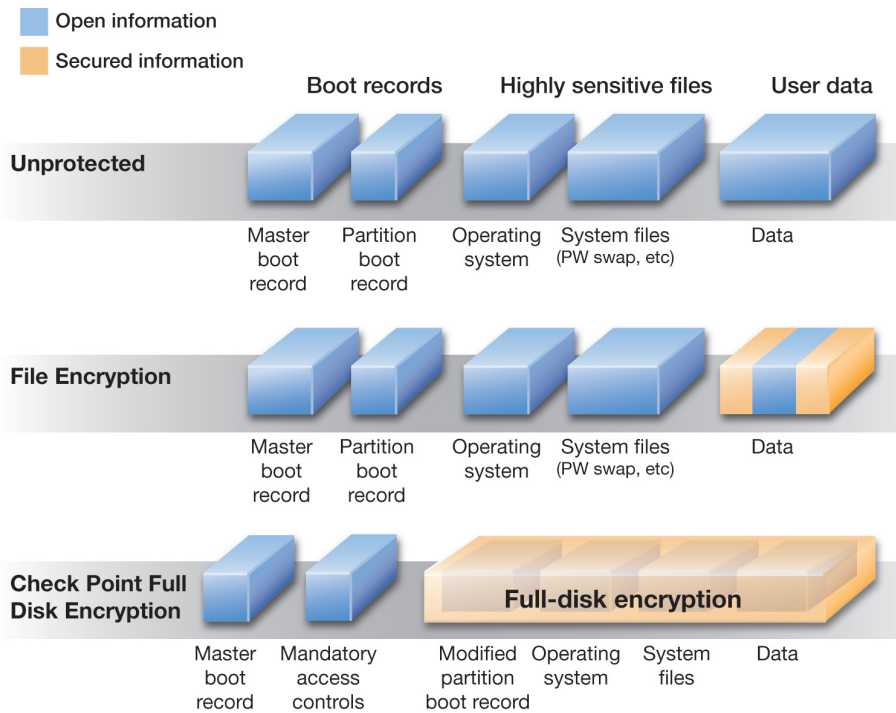
² See https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf

³ See Questionnaire at https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf

⁴ Check Point report, “Testing the Effect of Encryption on Disk Performance.”

Comparing the encryption processes of file/folder vs. full-disk

Unprotected endpoints are open and available to anyone who accesses a device containing PAN and related data. File- or folder-level encryption protects only the data residing in prespecified locations on a storage device. Location-specific encryption may be compromised if unauthorized people access copies of PAN and related data that may simultaneously reside in operating system and application files such as a virtual drive or temp file. The latter are not protected by file- or folder-level encryption, so PCI compliance is questionable.



Check Point Endpoint Security Full Disk Encryption protects all PCI data on endpoints.

Full-disk encryption with Check Point products begins with the Master Boot Record and Mandatory Access Control mechanism of the endpoint. This driver-based “pre-boot” authentication process must be fulfilled, otherwise, access to the entire disk is blocked and the machine does not boot. Because Check Point Full Disk Encryption runs in the background after system boot, contents of the entire disk are automatically encrypted all of the time—including data and temporary system files. When an endpoint computer goes into standby, hibernation, or shuts down, reauthentication is required to access the device.

Other issues for securing stored data on retail endpoints

Desktops and laptops are not the only places that can leak PAN and related data. Leaks can come from networked devices used for retail sales processing or mobile devices like PDAs or smartphones using popular operating systems such as Symbian, Pocket PC, Windows Mobile Smartphone, or Palm. A comprehensive encryption strategy for PCI compliance should include mobile and handheld devices that can store data.

“Full-disk encryption is a practical, effective way to protect PAN and related, stored data on endpoint devices in a retail environment for PCI compliance.”

Alan Phillips
7Safe Ltd.
Qualified Security Assessor
for PCI DSS

Likewise, data leak protection is essential to control transfers of PCI data to mobile storage devices that plug into auxiliary ports such as Universal Serial Bus (USB). This includes USB flash drives, iPods, digital cameras, and Bluetooth devices. Without appropriate controls, protected data can easily be transferred onto unauthorized mobile storage devices and trigger noncompliance with PCI.

Check Point equals PCI compliance for retailers

The Check Point data security portfolio includes three products for compliance with PCI Requirement 3: Protect stored cardholder data. Check Point Full Disk Encryption provides data security for PCs and laptops. Pointsec Mobile provides encryption for PDAs and smartphones. Check Point Endpoint Security Media Encryption prevents data leakage and encrypts removable media. Together, these products address the major risks of securing stored data on endpoints in the retail environment.

Meets PCI Requirement 3.4

Check Point encryption completely renders PAN and all related data unreadable anywhere it is stored on retail endpoints—including PCs, laptops, and handheld devices. The Check Point set-and-forget full-disk encryption technology with preboot authentication provides automatic and transparent operation on every endpoint, strong authentication, central policy management, and key recovery.

Meets PCI Requirement 3.4.1 audit guidelines

Check Point Full Disk Encryption uses driver-based preboot access control to completely separate logical access to the encrypted file system from the native operating system. Without verified authentication, an unauthorized person cannot access decryption keys or anything on the disk because the machine will not boot. Check Point encryption can automatically protect all removable media.

Comprehensive controls to ensure compliance

Check Point Full Disk Encryption with preboot authentication provides the most comprehensive controls for protecting PCI data stored on retail endpoints. Preboot launch protects operating systems from all known attack methods and totally secures stored PCI data no matter where it resides or in what application or format. Neither does it release keys nor allow network connectivity prior to successful authentication against a local proprietary database. Check Point Media Encryption offers control for port and storage-device management to block PCI data transfers to unauthorized devices and can encrypt data that is moved to a preauthorized device.

Learn more

Please contact Check Point for more information about PCI compliance requirements for stored cardholder data. Deployment of Check Point data security products is rapid, automatic, and unobtrusive in any size retail environment. Centralized management and operations makes using Check Point data security products a scalable, efficient, cost-effective way to protect stored data for PCI compliance. To learn more, please contact your Check Point sales representative, call Check Point at 800-429-4391, or visit www.checkpoint.com/products/datasecurity/index.html.



About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters

5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2003–2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.