

Payment Card Industry (PCI) Compliance Solution for the Retail Industry



Helping you protect cardholder data, anticipate auditor requests, and avoid fines

Business challenge

Over the past few years, CEOs have awoken to find their companies in the position of disclosing the loss or theft of consumer credit card information. In response, the payment card brands established the Payment Card Industry (PCI) Data Security Standard (DSS), a set of best-practice requirements for protecting credit card data throughout the information lifecycle.

Under PCI DSS, level 1 retailers—those that process more than six-million credit card transactions a year—are subject to an annual onsite audit and quarterly network scans performed by an approved vendor.

Level 2 and 3 companies that process 20,000 to six-million credit card transactions a year must fill out an annual self-assessment questionnaire and have an approved vendor conduct quarterly network scans.

There are stringent due dates and fines for non-compliance.

Retailers are looking for better ways to gain insight into how PCI impacts their businesses. They want to understand how PCI necessitates interaction with payment processors and with others in their complex, global, and increasingly mobile supply networks—today and in the future.

EMC's PCI compliance solution

EMC and selected partners are working together to help retailers comply with PCI. EMC makes it easy for retailers to identify commonly used elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and if each data element must be protected. Table 1 on the next page illustrates how the 12 requirements of PCI can be organized into six logically related groups, or control objectives, and the corresponding EMC® hardware, software, and services available to help retailers meet these objectives.

Whether you are a general merchandiser, grocer, food provider, specialty retailer, or service provider, EMC can help you meet one or more of the 12 PCI requirements.

The Big Picture

- Protect your customers' credit card information beyond just the point of sale—for one year, 18 months, or forever if that is your company's policy thanks to EMC's world-class intelligent information infrastructure
- Discover, secure, maintain, control access, monitor, and report on compliance from all your storefronts, e-commerce sites, and headquarters with EMC's portfolio of best-of-breed security, resource management, and information rights software and services
- Anticipate and prepare for specialized audit biases of the Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs) thanks to EMC's network of specialized, regional partners
- Avoid penalties and lost business that can result from a public data breach
- Leverage your investment of time, money, and human resources to further gain customer trust and build long-term loyalty

Every retailer’s IT configuration, business processes, and inhouse skills are unique, so when and how you choose to apply EMC’s PCI solution in your environment will vary.

Control Objective	PCI Requirement & Description	EMC Products, Services, and Best Practices
Build and maintain a secure network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters 	<ul style="list-style-type: none"> • EMC PCI Readiness Assessment Service • RSA Data Discovery Services with Data Loss Prevention RiskAdvisor • Documentum Information Rights Management (IRM) Services • EMC IT Compliance Analyzer • EMC Server Configuration Manager • EMC VoyenceControl • EMC Partner: Cisco
Protect cardholder data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks 	<ul style="list-style-type: none"> • RSA Key Manager • RSA File Security Manager • RSA DLP Suite
Maintain a vulnerability management program	<ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications 	<ul style="list-style-type: none"> • EMC Application Security Design and Assessment Service • EMC Product Security Policy • EMC ILM Suite (Symmetrix, CLARiiON, EMC Centera, Celerra, PowerPath, EMC Server Configuration Manager, EMC Disk Library, Replication and Business Continuity Software)
Implement strong access control measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data 	<ul style="list-style-type: none"> • RSA Access Manager • Documentum Information Rights Management (IRM) • EMC Server Configuration Manager • RSA SecurID • EMC Physical Security Solution for Retail (IP Video Surveillance) • EMC Data Erasure Services
Regularly monitor and test networks and ease compliance	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes 	<ul style="list-style-type: none"> • RSA enVision • EMC Partners: Accuvant, Ezenta, Integralis, Mnemonic & Remington • EMC Server Configuration Manager
Maintain an information security policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security 	<ul style="list-style-type: none"> • EMC PCI Information Security Policy Service

Reporting:

- RSA enVision
- EMC VoyenceControl
- EMC IT Compliance Analyzer—Application Edition
- EMC ControlCenter
- EMC Server Configuration Manager

According to the Privacy Rights Clearinghouse, more than 224 million personal records have been compromised since January 2005. That’s more than twice the population of Germany and 40 times the number of people in Singapore. Source: www.privacyrights.org

“We selected RSA enVision because it includes packaged compliance reports that allow us to easily implement compliance with industry standards.”

Data Security Analyst, Giant Eagle Supermarket

Table 1: EMC PCI Compliance Solution Components Aligned by Requirement

Breadth of professional services

If you’re new to PCI, find out more about EMC’s PCI Pre-Assessment and Gap Analysis Service. Or jump right into Card Data Discovery. Once you have set your process, consider EMC’s ongoing Policy Management Services.

EMC Global Services can help you successfully build the appropriate strategy and then implement an information infrastructure for addressing your business and IT challenges and attaining your near- and long-term business objectives. Let EMC experts take care of it, so you don’t have to.

Information security, resource, and rights management software

RSA®, The Security Division of EMC, leads the way in PCI and can offer unique expertise unmatched by anyone. As the leading provider of information-centric security solutions, RSA helps retailers address the most challenging aspects of PCI: data discovery and classification, encryption, key management and data leakage protection, as well as user authentication and access control, and finally, security information management.

“The ability to demonstrate PCI compliance has become a real differentiator...By bringing us into compliance, EMC Documentum has greatly improved our competitive advantage.”

Chief Information Officer, Card Management Corporation

With EMC’s family of resource management software products, including **IT Compliance Analyzer—Application Edition**, **VoyenceControl PCI Advisor**, and **Server Configuration Manager**, retailers can simplify and automate compliance initiatives. IT infrastructure discovery, compliance analysis, change/remediation, and reporting can all be automated with out-of-the box toolkits for retail. The automated approach combines continuous discovery of dependencies, connections, configurations, and changes to the entire application, network, and server infrastructures, and supports physical and virtual environments.

With **EMC Documentum® Information Rights Management** technology you can enhance your document security by applying rights for who can view, edit, print, or forward information, ensuring that sensitive information remains secure as it is shared both internally and externally. When your business needs change, you can dynamically change or revoke access policies and confirm compliance with corporate policies through a detailed audit trail of all activity.

World-class information infrastructure

Many of the world’s largest retailers rely on EMC information infrastructure to keep their business up and running—no matter what. This helps them comply with PCI.

EMC Celerra® brings powerful, high-availability IP storage to your organization in convenient integrated models and flexible gateways. All are easy to deploy and manage. Plus, simplify management with powerful software. Use Celerra Manager to easily configure, administer, and monitor your EMC Celerra IP storage environment from a single web-based interface—ensuring high availability.

EMC CLARiON® allows retailers of all sizes to achieve the high availability and scalability they need to manage and consolidate more data. Use **EMC Navisphere® Management Suite** for simple, secure, web-based management from any location. Discover, monitor, configure, and report on multiple CLARiON arrays from your browser. Use these insights to gain more value from your investment and aid your PCI compliance practices.

Retailers use **EMC Connectrix®** to move their organization’s vital information where it needs to go—quickly, easily, and reliably. Advanced directors and switches make it happen. Obtain best-in-class availability and easy management. And further optimize your environment with **EMC PowerPath®** host-based multipathing.

Use **EMC® Centera®** content-addressed storage (CAS) systems to store and manage your “fixed content”—unchanging digital assets—and keep them available online and accessible. Be ready for growth with petabyte scalability.

EMC Symmetrix® allows you to make high-end networked storage part of your information infrastructure with systems that take performance, availability, and security to new heights. Manage and protect your information today—and expand in the future. **Symmetrix Management Console** helps you simplify day-to-day management of your EMC Symmetrix storage with a powerful, easy-to-use, browser-based management tool.

A Retail Case Study

A \$9B retailer with more than 3,000 stores in over 30 countries was facing \$10M in annual fines if it didn’t demonstrate movement toward PCI compliance. A third-party audit showed the retailer needed a way to effectively manage cardholder data access logs, encrypt the stored credit card data, and authenticate users who were accessing the mainframe.

EMC RSA PCI experts were called in to consult with the retailer. Within days, EMC RSA enVision, Key Manager, and SecurID were implemented and compliance reporting started. To save implementation time and achieve economies of scale, additional information storage capacity to handle the storage log requirement of PCI was implemented at the same time. The result was faster time to compliance and a significantly reduced fine.

IP video surveillance—helping you comply in every store

The **EMC Physical Security Solution for Retailers**, provided by EMC and partners, consists of best-of-breed data, storage, video surveillance, and networking hardware technologies and software applications as well as best-practice services. Retailers use it to deliver automated, policy-based surveillance over each store’s IP network as part of their enterprise-wide PCI compliance program.

Reporting—across all 12 PCI requirements

Retailers can benefit from the specialized reporting capabilities available in RSA’s enVision®, EMC’s IT Compliance Analyzer, VoyenceControl, and Server Configuration Manager, as well as those within Documentum’s IRM software. Each product and report has its place in helping you meet the PCI requirement.

Validated PCI reference architecture

RSA works closely with Cisco on PCI infrastructure architecture designs. Designed expressly for small, medium-size, and large retail stores, enterprise data centers, and the Internet edge to support e-commerce operations, these designs are fully documented in the “**PCI Solution for Retail 2.0 Design and Implementation Guide**.” Ask your EMC account manager for a copy.

The Cisco PCI Solution for Retail Validated Network Designs has been tested and deployed in Cisco's labs as well as validated for both the wired and wireless environments, by Verizon Business (formerly CyberTrust). See Figure 1 for an example design.

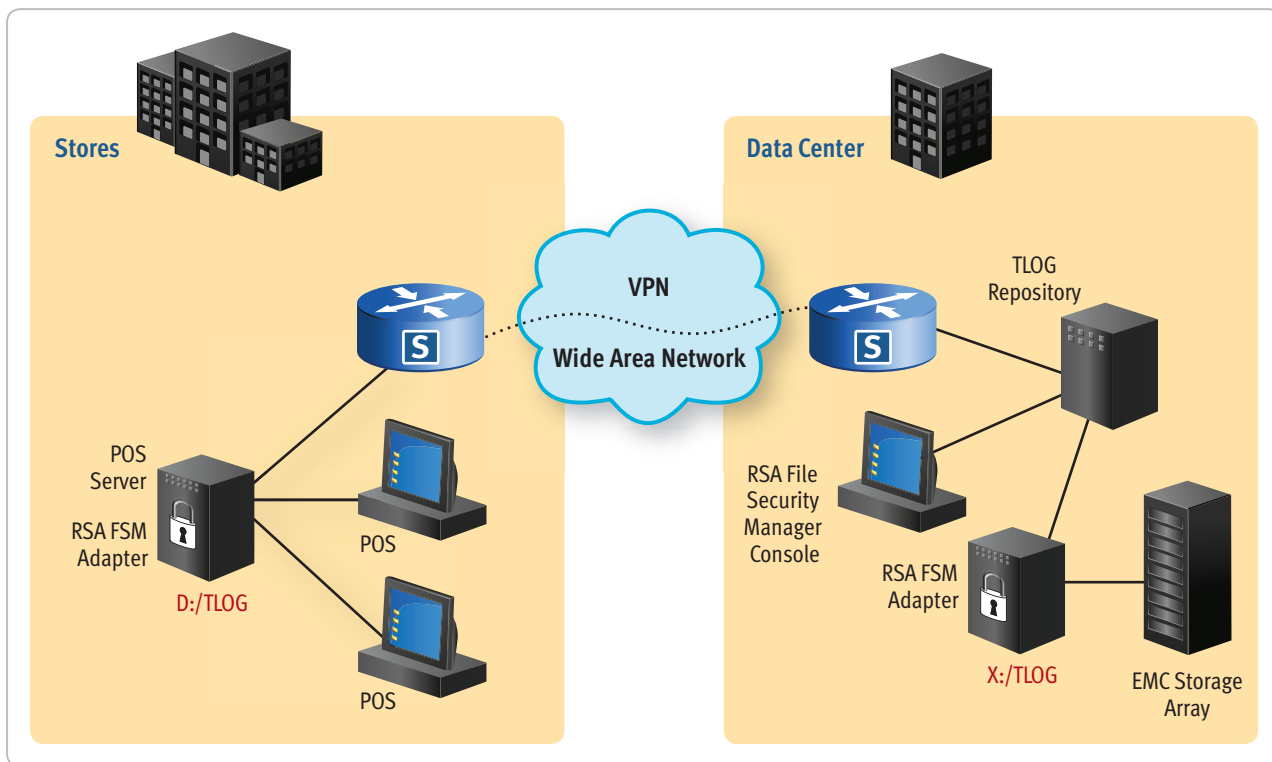


Figure 1: Conceptual View of PCI Solution Deployed at Stores and Headquarters Data Center

EMC and RSA are members of the PCI Security Standards Council. To obtain a copy of the most recent PCI standard, go to www.pcisecuritystandards.org.

To help merchants address immediate challenges associated with achieving PCI Compliance, including data discovery, protection, strong authentication, and information and event management, RSA is offering a pair of convenient PCI packages. To learn more about these affordable offerings, contact RSA today.

Security is built in—not just around—EMC products and services

EMC is committed to embedding security functionality within its products wherever possible to support PCI.

EMC closely monitors external security resources including CERT, National Vulnerabilities Database, and Bugtraq for vulnerability notifications regarding embedded third-party products.

A final note: it's an evolving standard

The PCI standard will continue to evolve to keep up with new threats and technologies. For example, analysts expect to see increased attention on wireless security in the PCI standard. Retail CIOs don't always have the ability to know where the network stops or where it is going. Consumers are using their cell phones to make credit card transactions. All of this presents a significant challenge for point-of-sale entities.

Rest assured that as the standard evolves, EMC will continue to work with the PCI Council and partners to help you maintain compliance.

EMC²
where information lives®

EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

To learn more about how your organization can benefit from an EMC solution, visit us online at www.EMC.com/retail.