



The Security Division of EMC

RSA Solution Brief

## Protecting Credit Card Data

Meeting the Payment Card Industry  
Data Security Standard 1.2

# Global Accountability for Cardholder Data Security

Over the past few years, hundreds of CEOs have awoken to find their companies in the unenviable position of disclosing the loss or theft of private consumer information, such as credit card and social security numbers. The problem is global and cuts across industries: retailers, hotels, local and federal governments, healthcare organizations, universities and financial institutions were all forced to report consumer data compromises in recent years.

As the problem of data theft became more apparent, a sharper eye turned toward protecting a particularly valuable set of data: consumer credit card information. In response, American Express, Discover Financial Services, JCB, MasterCard and Visa collaborated to create an industry-wide, global framework that details how companies that handle credit card data – specifically, banks, merchants and payment processors – should protect that information. The result was the Payment Card Industry (PCI) Data Security Standard (DSS), a set of best practice requirements for protecting credit card data throughout the information lifecycle.

The PCI standard centers around six high-level control objectives—essentially, targets for security that bolster the protection of credit card information. Broad security requirements support each control objective, and these twelve requirements are further dissected through well over 200 sub-requirements that specify the technologies, policies and procedures necessary for protecting cardholder data. Released in October 2008, PCI DSS version 1.2 is the second update to the PCI DSS framework. Developed by the PCI Security Standards Council, PCI DSS 1.2 provides greater clarity on technical requirements and improves merchant flexibility with respect to control design and implementation.

Banks, merchants and payment processors approach PCI DSS compliance as an ongoing effort. Compliance must be validated annually, and companies must be prepared to address new aspects of the standard as it evolves under the auspices of the PCI Security Standards Council. In short, organizations must remain vigilant in order to not just achieve—but also maintain—PCI DSS compliance.

---

## Implications of the PCI Standard— Now and in the Future

---

C-level security and compliance officers at companies handling consumer credit card data now face unprecedented levels of accountability for securing that information. The challenges outlined by the PCI Standard are significant: companies must understand where all cardholder data resides throughout an often-distributed enterprise and ensure that this data, and access to the information, is secure. Organizations must also prove that they've taken the precautions outlined in the standard and that the company actively monitors for unauthorized access to both card data and associated cardholder data systems.

Because of these challenges, significant time and financial investments are being made to address PCI DSS compliance. This leads to the question: “At the end of the day, are my efforts only going to help comply with PCI, or are there opportunities beyond PCI compliance that I have not yet recognized?”



## RSA PCI Solution: Addressing the PCI Data Security Standard

The PCI standard identifies several core IT security technologies, as well as various processes and procedures, needed to protect cardholder data. To address these requirements, RSA, The Security Division of EMC, delivers the RSA PCI Solution, which encompasses a range of IT security technologies and services.

RSA’s information-centric approach enables customers to move beyond perimeter protection and ensure that data is secure no matter where it resides. In addition, RSA’s solutions for PCI compliance will enable you to answer these critical questions:

- 1) Where is all of the company’s credit card data?
- 2) How do I ensure all the credit card data is secure?
- 3) How do I put the proper controls in place to ensure a quick response to potential security risks and prove that PCI DSS investments can help the business beyond the audit?

### Understanding PCI DSS

#### CONTROL OBJECTIVES

6 high-level targets for securing cardholder data

EXAMPLE  
Restrict access to cardholder data by business need

#### REQUIREMENTS

12 broad categories of action needed to secure cardholder data

EXAMPLE  
Assign a unique ID to each person with computer access

#### SUB-REQUIREMENTS

200+ specific actions needed to secure cardholder data

EXAMPLE  
Implement two-factor authentication for remote access to the network by employees, administrators, and third parties

To answer these questions, RSA delivers a unique combination of product and service capabilities that enable customers to discover credit card data; secure the data, as well as protect access to the data and related technology systems; and rapidly respond to potential breaches and calls for evidence by auditors and banks.

In addition, RSA can help customers leverage these investments to protect all of the organization’s vital customer, partner and business information. Further, RSA works to ensure that PCI DSS investments can be extended to help better protect and enable your business over the long run.

#### Opportunities Beyond PCI DSS Compliance

As your organization begins to evaluate next steps in either achieving or re-certifying compliance, consider that:

- PCI DSS is about much more than information-security technology: compliance requires a thoughtful combination of people, process and technology adjustments, which can help address the PCI standard but also improve security and business processes across-the board.
- By taking a planned, strategic approach to PCI DSS compliance now, you will position your organization to avoid the significant costs associated with managing a data breach. Organizations that are prepared are better able to respond to changes in the Standard as it evolves overtime.
- Regardless of your merchant requirements (Level 1, 2, 3 or 4), view PCI DSS as a framework that minimizes data risk for mission-critical data, so that the focus can be on the business.

## Understanding PCI DSS

CONTROL OBJECTIVES	REQUIREMENTS
Build and maintain a secure network	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect cardholder data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a vulnerability management program	<ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement strong access control measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly monitor and test networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an information security policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>

## PCI Readiness Assessment

As organizations begin to approach PCI DSS compliance they must first understand any gaps that exist in order to identify remediation needs. Through a PCI Readiness Assessment, RSA Professional Services helps customers understand their current PCI posture and develop a remediation roadmap prior to undergoing a formal PCI audit. This service does not replace or serve as a PCI audit, but rather helps merchants identify and address weaknesses prior to undergoing a PCI audit.

As a key deliverable, RSA Professional Services provides a recommended reference architecture for proper handling of cardholder data. RSA consultants deliver this proposed architecture by:

1. Evaluating your current levels of compliance with the PCI DSS standard by reviewing current architectures for infrastructure elements (networks, applications, servers and storage) and by using advanced classification and discovery technologies that handle and process cardholder data.

### Customer Benefits:

#### RSA Solutions for PCI DSS Compliance

By leveraging the strengths of the RSA and EMC technology portfolio, paired with world-class professional services and consulting expertise, you will have the opportunity to:

- Know where all of your organization’s credit card data resides, in order to take steps to ensure that information is secure.
- Protect card data wherever it resides across the organization, prove the identities of individuals accessing it and ensure that only those with a true business need have rights to access the card data.
- Monitor and track access to cardholder data, so when a policy or security violation occurs, you will know and be able to respond.
- Understand how the investments you’ve made in addressing PCI DSS compliance can be leveraged beyond the audit, to help to improve data security and protect the business across the enterprise.

# Securing data is impossible without finding it first

2. Reviewing current policies and processes for handling cardholder data and comparing them with the PCI DSS standard, as well as best practices from RSA's consulting experience.
3. Producing a report to document gaps between current state of infrastructure, policies and procedures and the state desired to achieve PCI DSS compliance.
4. Developing a remediation roadmap that provides a step-by-step timeline of recommended infrastructure and process changes to ensure PCI DSS compliance while recognizing budgetary, staffing and information management limitations.

---

## Cardholder Asset Discovery and Classification

---

RSA Professional Services enables customers to understand where cardholder data exists across the organization so that it can be consistently managed across its lifecycle. To achieve this, RSA Professional Services can use a range of endpoint, application, network, and datacenter discovery tools to analyze the location and transaction flow of cardholder data.

These services ensure that cardholder data is used properly, the handling of cardholder data is documented and that only appropriate and necessary information is stored. Card data transaction flows across the enterprise are analyzed, ensuring that credit card information in dependent applications and associated lines of business, is inventoried and catalogued.

### RSA DLP Suite: Discovering Credit Card Data to Support Compliance

Beyond determining where credit card data resides within applications, files and folders, databases and in storage, organizations must uncover card data elsewhere across the enterprise. Because, over time, users may create multiple reports that are stored as PDF, Microsoft® Excel or simple text files in file shares.

The result of such behavior: hundreds, even thousands of files containing sensitive customer information, such as credit card numbers, are scattered across multiple file shares. The problem is only amplified because of the mobility factor—users often email/copy/move them to unauthorized locations. It is critical for businesses to identify these files, and secure them based on policy, in order to meet PCI DSS requirements.

RSA DLP Suite addresses this challenge by scouring file systems, networks and endpoints to discover cardholder data. Once files with sensitive information are identified and classified, they can be copied, moved, archived, deleted or secured based on policy.

In addition, RSA DLP Suite scours file systems, networks and endpoints to locate and delete full magnetic stripe data – information whose storage is strictly prohibited by PCI.

---

## Requirement 3: Protect Stored Cardholder Data—the RSA Solution

---

RSA delivers a broad range of data security solutions that enable customers to address PCI Requirement 3 by protecting stored cardholder data wherever it resides throughout the organization and purging sensitive authentication data. RSA's Data Security Solutions enable customers to protect cardholder data across all encryption endpoints, regardless of whether data resides in an application, network, files and folders, or disk/tape storage. Enterprise-wide key management, provided by RSA Key Manager, ensures that data protection solutions scale, adapt and ultimately support business changes. This means data will be both available and properly protected throughout the information lifecycle. Specific sub-requirements that may be addressed with RSA technology include:

- **Requirement 3.2: Do not store sensitive authentication data after authorization (even if encrypted).**

RSA DLP Suite scours file systems, networks and endpoints to identify instances of sensitive authentication data. Once discovered, DLP Suite can then delete the data.

- **Requirement 3.4: Render Primary Account Number (PAN), at minimum, unreadable anywhere it is stored**

RSA Key Manager provides application development libraries that support a wide range of development languages and it enables developers to easily integrate encryption into point-of-sale, payment, CRM, ERP, and other business applications that create or process sensitive information. RSA Key Manager can also be used to encrypt data as it flows to both disk and tape.

## Helping organizations to ensure that cardholder data is protected at all locations

- **Requirement 3.5: Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse**

RSA Key Manager is a centralized encryption key management technology that enables companies to centrally enforce policies across the organization. In addition, the technology enables customers to restrict key access and securely store encryption keys.

In addition, RSA Key Manager further supports compliance with Requirement 3.5 by enabling customers to restrict access to encryption keys by ensuring that users are properly authenticated and authorized, controls that PCI DSS auditors look to substantiate. Further, RSA Key Manager stores encryption keys in a hardened database (the key store) where keys themselves are encrypted using a key encryption key (KEK). Customers have the ability to store this KEK in a hardware security module (HSM), a specialized and secure hardware device that bolsters protection of all enterprise encryption keys.

- **Requirement 3.6: Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data**

RSA Key Manager provides robust support for managing encryption keys throughout the key lifecycle, from generating strong keys, to enabling secure key storage and distribution, to making the actual encryption keys virtually inaccessible.

---

## Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks—the RSA Solution

---

RSA's Data Security Solutions enable customers to protect cardholder data as it traverses the network, – including within emails – and to effectively manage the lifecycle of the associated encryption keys. Specific capabilities include:

- Requirement 4.1: Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission

RSA Key Manager integrates with a variety of applications and can be utilized to encrypt data at Point of Sale terminals. As a result, credit card data is secured as it travels over open, public networks.

- Requirement 4.2: Never send unencrypted Primary Account Numbers by end user messaging technologies (for example, e-mail, instant messaging, chat).

RSA DLP Network can automatically route messages containing cardholder data to an encryption facility to secure messages and attachments before they are sent. If desired, DLP Network can simply block or quarantine these messages.

---

## Requirement 6: Develop and Maintain Secure Systems and Applications—the RSA Solution

---

RSA Professional Services reviews application security design and implementation to ensure implementations conform to industry best practices. Specifically:

- Requirement 6.5: Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project Guide

RSA's Application Security Design Assessment Service is a packaged offering providing a quick and accurate diagnosis of the current state of application security. RSA Professional Services consultants analyze the design and operational model of the target applications and the environment surrounding them, thoroughly review current application design and associated technical documentation, examine application architecture and information flow, and produce a report highlighting areas of strength and weakness within current systems and operations relative to RSA best practices.

---

## Requirement 7: Restrict Access to Cardholder Data by Business Need-to-Know—the RSA Solution

---

RSA's Authorization Solutions enable customers to address PCI requirement 7 by ensuring that only authorized users may access cardholder data within web and file based systems. Specific capabilities include:

- Requirement 7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access

RSA Access Manager software helps customers to ensure that only authorized individuals can access cardholder data within web-based applications, and these privileges can be assigned based on an individual or group's specific job responsibilities. RSA Access Manager entitlements can be defined by select attributes, such as job role (e.g., accounting department), which helps ensure that access is automatically terminated if, for example, a member of the entitled organization moves to a new department. In addition, RSA Access Manager enables customers to centralize access to cardholder data, which helps enhance security by ensuring consistent controls are implemented across web-based access points.

- Requirement 7.2: Establish an access control system mechanism system with multiple users that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed

RSA Access Manager software provides the ability to restrict access to data based on predefined business rules and/or a user’s role in the organization. The software delivers “deny all” capabilities out-of-the-box.

---

### Requirement 8: Assign a Unique ID to Each Person with Computer Access—the RSA Solution

---

RSA’s Authentication solutions help customers ensure that users accessing cardholder data systems, regardless of their location, are who they claim to be. Specific capabilities include:

- Requirement 8.2: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: Password or passphrase, or Two factor authentication (for example token devices, smart cards, biometrics, or public keys)

RSA SecurID provides the ability to meet this requirement with a variety of hardware- and software-based two-factor authentication tokens/ authenticators. In addition, RSA Digital Certificate Solutions provide customers with the flexibility to select the authentication mechanism that best suits their needs.

- Requirement 8.3: Incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties.

RSA SecurID enables organizations to implement two-factor authentication through a variety of hardware- and software-based two-factor authentication token options. In addition, RSA Secured partners deliver remote access solutions with out-of-the-box RSA SecurID integration, which makes it simple for organizations to strongly authenticate users accessing resources via VPN connections.

#### Trusted Access to PCI Infrastructure

The RSA Secured Partner Program delivers out-of-the-box integration of RSA SecurID with hundreds of systems that can be part of the PCI infrastructure (e.g., VPNs, firewalls, application servers), enabling customers to ensure that users accessing those systems, either remotely or within the corporate firewall, are trusted. And, while the RSA Secured Partner Program helps to address PCI DSS compliance, stronger authentication for IT systems helps improve security well beyond the PCI DSS audit.

- Requirement 8.4: Render all passwords unreadable during transmission and storage on all system components

RSA SecurID (especially the RSA SID200 PINpad Authenticator and Software Authenticator) enables the end-user’s PIN to be encrypted before transmission across the wire. All communications between RSA SecurID agents and the server are encrypted, and all end-user PIN information is fully encrypted during storage on the server side. Additionally, RSA File Security Manager provides the ability to encrypt flat files used to store passwords.

- Requirement 8.5: Ensure proper user authentication and password management for non-consumer users and administrators on all system components

RSA SecurID technology helps customers exceed the requirement by providing the means to strongly authenticate users prior to access.

---

## Requirement 9: Restrict Physical Access to Cardholder Data—the RSA Solution

---

RSA and EMC provide solutions to monitor, analyze and manage the physical security of systems and facilities where cardholder data is housed and processed. Specific capabilities that address key sub-requirements include:

- Requirement 9.1.1: Use video cameras or other access control mechanisms to monitor physical access to sensitive areas

The EMC Physical Security Solution enables customers to manage, analyze, archive and scale their physical security and video surveillance information throughout its lifecycle. EMC Surveillance Manager software provides powerful analytics and automated, policy-based management. In addition, enterprise-class EMC storage systems ensure a scalable solution to growing physical security storage requirements. EMC Centera® content addressable storage platforms and Documentum content management software provide an evidence vault for the analysis and tamper-proof, long-term archival storage of video surveillance information and other physical security information. EMC Global Services designs and integrates the EMC Physical Security Solution into customer environments.

- Requirement 9.7: Maintain strict control over the internal and external distribution of any kind of media that contains cardholder data

RSA's Classification for Information Security professional service offering supports customer efforts to effectively classify media that holds credit card data. Customer can receive handling and labeling instructions for media containing cardholder data.

- Requirement 9.10: Destroy media containing cardholder data when it is no longer needed for business or legal reasons

EMC Certified Data Erasure Services use proprietary techniques and industry tools to overwrite storage media to specified levels of erasure—3x, 5x, 7x or a custom number—to replace data with a sequence of

variable-bit patterns that renders the data unrecoverable. EMC experts can perform this service at customer locations or off site on entire storage arrays or specific media after proactive replacement.

Services are available for storage arrays from EMC, as well as from Hitachi, IBM, Sun, Network Appliance and HP. At the completion of the process, EMC provides a comprehensive report and certificate of completion for the specific drives erased and the level of erasure achieved.

---

## Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data—the RSA Solution

---

RSA's solution for compliance and security information management enables customers to establish a centralized point for tracking and monitoring access to cardholder data throughout a PCI environment. RSA enVision supports end-to-end reporting with Requirement 10:

- Requirement 10.1: Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

RSA enVision enables customers to track administrative user activity and provides oversight to help verify a user is acting in accordance with established policy. Additionally, the system may send an alert to a user's supervisor if behaviors violate policy.

- Requirement 10.2: Implement automated audit trails for all system components to reconstruct key events

RSA enVision appliance helps companies to implement automated audit trails that detail user access to cardholder data, actions taken by users with root/administrative privileges, access to audit trails, invalid logical access attempts, use of identification/authentication mechanisms, audit log initialization and creation/deletion of system-level objects.

– **Requirement 10.3: Record audit trail entries**

RSA enVision will record the events as reported by associated devices. In addition, RSA enVision saves event metadata, which may be analyzed and revised to determine type of event.

– **Requirement 10.5: Secure audit trails so they cannot be altered**

RSA enVision delivers mirrored, unfiltered data to its Internet Protocol Database, which provides the ability to retain data in its original format. Further, “write once, read many” capabilities help ensure that the mirrored copy remains intact, even if the original data is compromised. RSA enVision-captured event logs are stored on a hardened operating system in a compressed form and protected via lightweight encryption.

– **Requirement 10.6: Review logs for all system components at least daily**

RSA enVision's comprehensive correlation, analysis and alerting capabilities make it easier the consolidation and daily review of logs from cardholder systems, including logs from all critical intrusion detection, authentication, authorization, and accounting protocol servers.

– **Requirement 10.7: Retain an audit trail history for at least one year, with a minimum of three months available for immediate analysis**

RSA enVision NAS3500 offers pre-configured, pre-tested and pre-racked EMC Celerra® under the covers, enabling customers to support between 3.5 TB and 7 TB of storage, which is particularly relevant to the retention on log data online. In addition, because RSA enVision is engineered to have out-of-the-box integration with networked storage platforms such as EMC Symmetrix®, CLARiiON®, EMC Centera® and EMC Celerra™, customers have the ability to easily store their critical information to meet compliance requirements.

EMC Celerra Network Attached Storage systems provide industry-leading price/performance with no-compromise availability. No-compromise availability means applications continue running at the same performance and service levels even in the event of a failure. Celerra accomplishes this via an active/

passive N+1 clustering architecture and by eliminating any single point of failure from the network to the disk drive. In addition, EMC Celerra Network Attached Storage systems implement a capability called “File Level Retention” that provides disk-based WORM protection for files. This Celerra capability protects files and directories from deletion, alteration, renaming or overwriting during a designated “retention period.” Celerra File Level Retention can provide organizations with the ability to protect the integrity of online audit logs for a specific retention period (e.g., 3 months).

EMC Centera provides a simple, scalable, secure storage solution for cost-effective retention, protection and disposition of a wide range of fixed content. Exceptional performance, seamless integration and proven reliability make EMC Centera the online enterprise archiving standard for virtually any application and data type.

Beyond its core ability to help customers address PCI DSS Requirement 10, RSA enVision technology provides a robust platform for collecting, correlating and auditing access to a wide range of PCI systems—from firewalls to wireless networks to authentication mechanisms and more. The technology significantly eases the process of demonstrating compliance with PCI's 12 requirements.

---

## **Requirement 12: Maintain a Policy that Addresses Information Security—the RSA Solution**

---

RSA Professional Services help customers create policies and processes for developing and improving their information security programs. Specifically, RSA Professional Services consultants review existing security policies, and develop new or amended policies to ensure that cardholder data is appropriately handled. RSA Professional Services also reviews processes for using, sharing, storing and labeling media containing cardholder data to ensure they are consistent with the recommended practices of the PCI DSS standard. Such policies should include specification of appropriate and necessary uses of cardholder data and proper procedures for handling it.



## RSA PCI Solution Components: Products and Solutions

- > **RSA® Access Manager** software provides the ability to control access to Web-based resources and enforce centralized user policies across the organization.
- > **RSA Data Loss Prevention (DLP) Suite** discovers credit card data on endpoints, networks and file shares. DLP suite helps organizations protect files and emails containing cardholder data and can be used to purge sensitive authentication data.
- > **RSA enVision®** appliances provide an enterprise-wide platform for collecting, correlating and analyzing security and compliance information across the organization, supporting efforts to track and monitor access to network resources and cardholder data.
- > **RSA® Key Manager** software is an enterprise-wide key management offering which helps organizations to manage encryption keys generated by disparate enterprise applications and to allow corporate software developers to easily integrate security into their applications based on established security policies.
- > **RSA SecurID®** two-factor authentication technology provides a proven means of ensuring the identity of users accessing critical resources, including cardholder data.
- > **EMC Storage Systems including EMC Symmetrix®, CLARiiON®, Centera® and Celerra™** networked storage platforms integrate with RSA enVision and provide customers with the ability to store their critical information to meet PCI DSS compliance requirements.
- > **EMC Physical Security Solution** helps enable customers to manage, analyze, archive and scale their physical security and video surveillance information throughout its lifecycle.

## Services

- > **Application Security Design Assessment Service** provides a quick and accurate diagnosis of the current state of application security.
- > **Credit Card Data Discovery & Classification Services** help enable customers to fully understand where cardholder data exists across the organization so that it can be consistently managed across its lifecycle.
- > **EMC Certified Data Erasure Services** use proprietary techniques and industry tools to overwrite storage media to specified levels of erasure.
- > **Information Security Policy Service** helps customers develop policies and processes for developing and improving their information security programs.
- > **PCI DSS Readiness Assessment Service** by RSA Professional Services helps customers understand their current PCI posture and develop a remediation roadmap prior to undergoing a formal PCI audit.

## RSA is your trusted partner

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle - no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

©2008 RSA Security Inc. All Rights Reserved.  
RSA, RSA Security, enVision, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC, Symmetrix, CLARiiON, Celerra and Centera are registered trademarks of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

PCI SB 0109