

White Paper

RETAIL SOLUTIONS

www.novell.com

PCI-DSS Solutions from Novell®

Building a Strategic, Comprehensive Solution for PCI-DSS Compliance

Novell.

Table of Contents:	2 Executive Summary
	2 PCI-DSS Background and History
	3 PCI-DSS Overview
	6 PCI-DSS—Detailed Requirements and Solutions
	16 Deployment Strategy— Essential Steps
	16 Glossary of Terms



Executive Summary

During a breach at one major retailer, hackers stole nearly 46 million cardholder records, some of which dated back to 2003. As a result, dozens of banks reported incidents of fraud from the compromised cards. Because the retailer had stored old account information instead of deleting it, the company violated a PCI requirement, which mandates that a company remove data it no longer needs.

Millions of cases of identity theft, including a number of high-profile cases where large amounts of payment card data was stolen or compromised, have fueled an urgent industry-wide movement to tighten payment card data security. In response, the leading payment card companies have worked together to develop a new Payment Card Industry Data Security Standard (PCI-DSS). This standard requires any retailer that handles, transmits or stores payment card data to meet a stringent set of data security requirements—and imposes stiff fines and penalties on businesses that don't. PCI-DSS is not a law or set of government regulations. Instead, it's a private standard that retailers and payment card service providers must meet in order to stay in compliance with their payment card company contracts. Payment card companies enforce the requirements through a number of contractual penalties or sanctions. These include:

- *Fines of \$500,000 per data security incident*
- *Fines of \$50,000 per day for non-compliance with published standards*
- *Liability for all fraud losses incurred from compromised account numbers*
- *Liability for the cost of re-issuing cards associated with the compromise*
- *Suspension of merchant accounts*

As a retailer, you obviously need to meet PCI-DSS requirements as quickly as possible—the risks and potential costs are unacceptably high if you don't. But because the PCI-DSS standard contains more than 160 specific requirements, and because retailers will be required to demonstrate ongoing compliance for the foreseeable future, you need to plan carefully, think strategically and select the best possible technology partner as

you work to comply with PCI-DSS. To make this process easier, Novell offers a tightly integrated solution set that covers all six PCI-DSS control objectives, addresses all 12 requirement sections and meets most of the automatable requirements. This solution set provides both the breadth and depth of products and services necessary to implement PCI-DSS compliance programs quickly and effectively.

This paper outlines the requirements of the PCI-DSS standard, discusses some smart approaches for meeting those requirements and describes how Novell can help you achieve compliance more quickly and efficiently.

PCI-DSS Background and History

In 2001, Visa introduced its Cardholder Information Security Program (CISP), the first program that required merchants and service providers to meet specific data security standards. More recently, Visa, MasterCard, American Express, Discover, Diner's Club, and JCB joined forces to create PCI-DSS, an updated and more all-encompassing standard. These companies required any merchant or service provider that handled, transmitted, processed or stored payment card data to become compliant with the first PCI standard by June 30, 2005.

In September of 2006, the PCI Security Standards Council updated the PCI standard to version 1.1. This updated PCI-DSS standard established an expanded set of 160 specific requirements merchants are required to follow. These requirements affect many different aspects of IT operations, including:

- *Network security and configuration*
- *Data encryption for storage and transmission*
- *Encryption key management and security*
- *Vulnerability management, alerts and testing*
- *Access control by role and policy*
- *Incident response planning*
- *Patch management*
- *Software development methodologies*
- *Anti-virus protections*
- *Physical security*
- *Business and personnel processes*
- *Auditing and logging requirements and restrictions*

The most recent PCI-DSS requirements create obvious new challenges for IT departments. Few organizations have the infrastructure and resources in place to achieve compliance with these ambitious and far-reaching requirements quickly. One report estimates that up to 20 percent of retailers are not in compliance with PCI-DSS today and may face financial penalties of up to \$25,000 each month.¹ In 2006, Visa levied \$4.6 million in fines against merchants, up 35 percent from 2005. And with a new set of deadlines approaching and enforcement increasing, there are certainly plenty of pressing PCI-DSS related issues to keep IT people up at night.

Of course, potential fines are only the tip of the iceberg. Insecure cardholder data can create huge risks and liabilities for retailers. Class action litigation and government regulations can potentially bankrupt a company that exposes cardholder data to hackers or identity thieves.

Given these risks, there is a real temptation to go for the “quick fix” approach to PCI-DSS

compliance. It’s certainly possible to deploy a “quick and dirty” solution to rush compliance, but these half-baked solutions often create unnecessary busy work and can waste valuable resources for years to come.

It makes more sense to adopt a carefully planned strategic approach to data security that addresses compliance issues, automates PCI-DSS requirements and enhances other IT and end user operations. The goals of this strategic approach are fairly straightforward:

- *Meet or exceed PCI-DSS requirements*
- *Implement a solution before non-compliance fines are imposed*
- *Implement strategic solutions that streamline IT operations and meet a wide range of IT and end-user needs*

PCI-DSS Overview

The most recent PCI-DSS is a complex standard, with more than 160 specific requirements. As with any complex IT challenge, an effective, efficient PCI-DSS compliance solution requires careful strategic planning and a commitment to creating solutions that minimize the impact on IT organizations.

Because PCI-DSS is so complex, it’s helpful to group the requirements into six simpler “control objectives.” Each control objective includes one or more logically related “summary requirements,” and each summary requirement includes a set of more detailed requirements. The following table lists the main PCI-DSS control objectives, outlines their associated summary requirements and presents a number of relevant Novell and partner solutions for each:



Shareholder Sues Retailer for Data Breach Records

“A major shareholder of a national retailer is taking legal action against the company, claiming it refused to disclose details of the security breach that affected thousands of credit and debit cardholders.

“The Arkansas Carpenters Pension Fund, which owns 4,500 shares of stock in this retailer, said the company denied its request for documents that detail what security measures they had taken to safeguard its computer system and what the company did after hackers gained access to the system and stole customers’ personal information.

“The lawsuit, filed Monday in Delaware’s Court of Chancery, comes after an investigation revealed that the company had violated portions of the PCI Data Security Standard (PCI DSS) that govern sensitive data storage.”

BankNet360

March 21, 2007

¹ “Rumors and Reluctance: PCI Standard Changes,” IT Compliance Institute, August 5, 2006

Black or White?

PCI-DSS leans heavily to the “deny all” philosophy of access management. To be compliant, IT should implement a “need to access” policy, and create “white lists” of allowed people, roles, components and applications. Novell security products are based on this white list approach.

PCI-DSS Main Control Objectives

Control Objective	Summary Requirement	Novell Solutions
Build and maintain a secure network	1) Install and maintain a firewall configuration to protect cardholder data	Novell Sentinel Novell Identity Manager SUSE Linux Enterprise Edition Partner Firewalls [†]
	2) Do not use vendor-supplied defaults for system passwords and other security parameters	Novell Sentinel Novell Access Manager Novell ZENworks SUSE Linux Enterprise Edition
Protect cardholder data	3) Protect stored cardholder data	Novell Identity Manager Novell Access Manager Novell AppArmor SUSE Linux Enterprise Edition Novell Linux POS
	4) Encrypt transmission of cardholder data across open, public networks	Novell Access Manager SUSE Linux Enterprise Edition Novell Linux POS
Maintain a vulnerability management program	5) Use and regularly update anti-virus software	Novell Sentinel Novell ZENworks Partner Anti-virus Solutions [†]
	6) Develop and maintain secure systems and applications	Novell Sentinel Novell Identity Manager Novell ZENworks Novell AppArmor
Implement strong access control measures	7) Restrict access to cardholder data by business need-to-know	Novell Sentinel Novell Identity Manager
	8) Assign a unique ID to each person with computer access	Novell Sentinel Novell Identity Manager Novell Access Manager Novell eDirectory Novell Identity Assurance
	9) Restrict physical access to cardholder data	Novell Identity Manager Activelidentity [†]
Regularly monitor and test networks	10) Track and monitor all access to network resources and cardholder data	Novell Sentinel SUSE Linux Enterprise Edition Novell Linux POS Partner Intrusion Detection [†]
	11) Regularly test security systems and processes	Novell Sentinel SUSE Linux Enterprise Edition Novell Linux POS
Maintain an information security policy	12) Maintain a policy that addresses information security	Novell Sentinel Novell Identity Manager Partner and Open Source Vulnerability Scanners [†]

[†]Recommended products from trusted Novell partners that integrate with Novell solutions.

It’s clear that most PCI-DSS requirements revolve around the concept of “limited, controlled access.” This means that any effective compliance solution must feature strong identity management capabilities that are tightly integrated with access control and monitoring tools. In fact, it’s safe to say that PCI-DSS compliance would be virtually impossible without a robust set of automated identity management and access control tools.

Novell PCI-DSS Solutions Use Identity Management

Fortunately, the Novell® solution set for PCI-DSS fully embraces this identity management-based approach (see Figure 1). Novell Identity Manager, working with an LDAP directory server such as Novell eDirectory™, forms the central identity management hub for the solution and addresses most of the identity management and access control requirements of PCI-DSS. Other Novell solutions tap into and work closely with this central identity management core to fulfill other types of PCI-DSS mandates.

Novell PCI-DSS Identity Management and Security Solutions

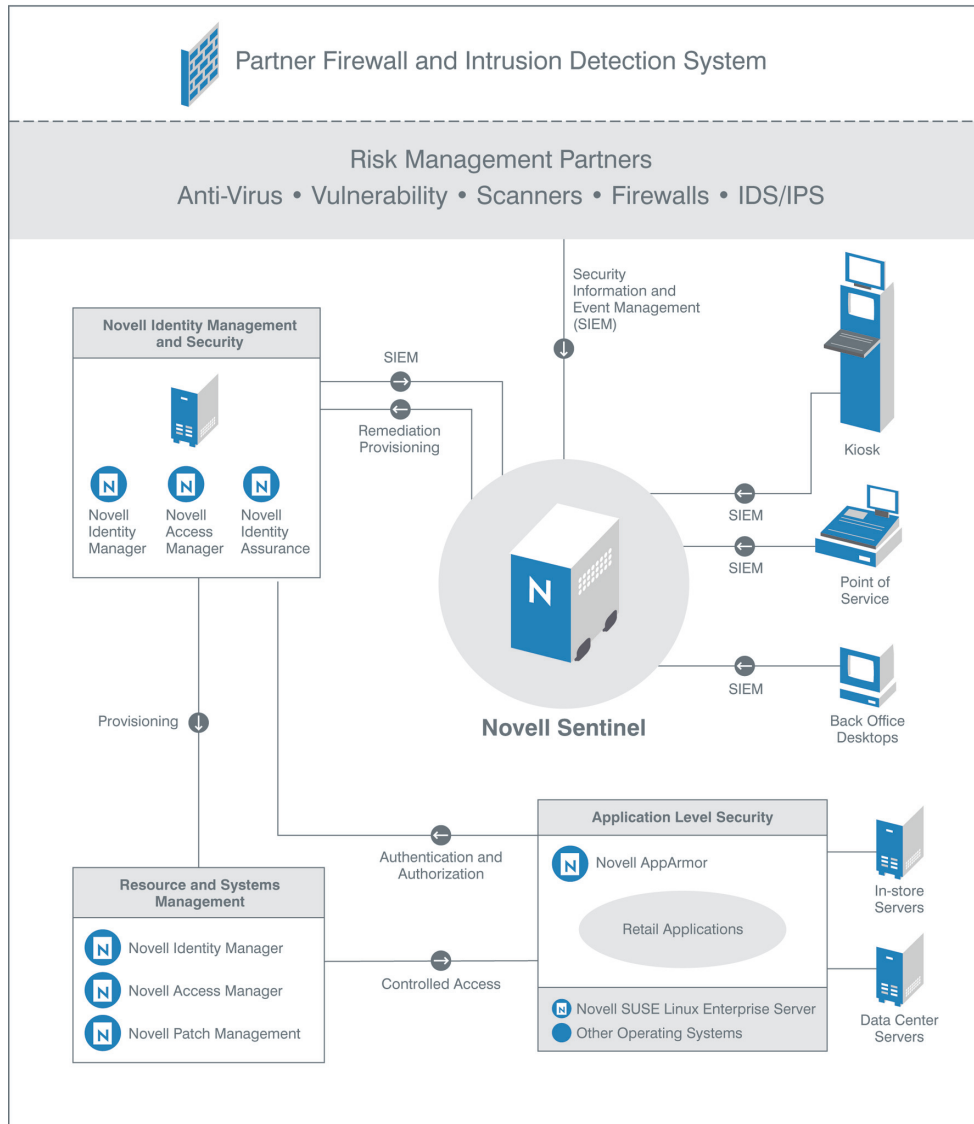


Figure 1. The Novell PCI-DSS solution set revolves around a robust set of identity management capabilities.

For example, Novell Sentinel™ fills a crucial role in monitoring and auditing your systems and networks, which is another key requirement of PCI-DSS. This includes receiving and aggregating access, intrusion and

exception data from points throughout your IT infrastructure. It also includes creating appropriate alerts and reports that meet PCI-DSS process/response requirements and auditing/reporting mandates.

An unknown hacker claimed to have stolen 300,000 credit card numbers from CD Universe and posted 25,000 of them to a Web site after the retailer refused to pay a \$100,000 ransom.

Although the Novell PCI-DSS solution set is very broad in its scope, it only requires a few points of control. With the Novell PCI-DSS solution, you manage identities and access through Novell Identity Manager, perform systems updates through Novell ZENworks®

and handle security alerts and reporting through Novell Sentinel. These limited points of control allow you to speed up initial PCI-DSS compliance—and significantly reduce the time and IT resources required to stay compliant into the future.

PCI-DSS—Detailed Requirements and Solutions

With that brief introduction to PCI-DSS and the Novell approach for addressing compliance, the next section of this paper will examine each PCI-DSS control objective with its associated summary requirements in more detail—and describe how Novell solutions can help you achieve compliance in each area.

Control Objective #1: Build and Maintain a Secure Network

Control Objective	Requirement	Novell Solutions
Build and maintain a secure network	1) Install and maintain a firewall configuration to protect cardholder data	Novell Sentinel Novell Identity Manager SUSE Linux Enterprise Edition Partner Firewalls [†]
	2) Do not use vendor-supplied defaults for system passwords and other security parameters	Novell Sentinel Novell Access Manager Novell ZENworks SUSE Linux Enterprise Edition

[†]Recommended products from trusted Novell partners that integrate with Novell solutions.

PCI-DSS requires retailers to protect cardholder data from external attacks. This involves establishing a secure infrastructure of firewalls, firewall management processes and monitoring systems. Although most organizations have firewalls in place, many firewall implementations are improperly configured, and many firewalls also go unaudited for years, which typically means they are full of security vulnerabilities.

PCI-DSS seeks to eliminate these weaknesses and oversights—and move retailers closer to a state of “best practices” firewall management. The amount of effort necessary to meet these requirements is inversely proportional to the levels of process and control automation you put in place. Deploying solutions that manage identities, control access rights and integrate with popular firewalls will greatly reduce the time and effort needed to rework and validate the state of your firewalls.

PCI-DSS Requirement 1: Install and maintain a firewall configuration to protect cardholder data

This requirement covers many different aspects of firewall configuration and maintenance. Repelling external and internal attacks through rigorous firewall configuration, testing and change management processes generally requires a burst of initial effort, followed by careful attention to ongoing maintenance processes. More specifically, PCI-DSS Requirement 1 mandates that you:

1. Establish firewall configuration standards.
2. Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.
3. Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

- 4. Prohibit direct public access between external networks and any system component that stores cardholder data (databases, logs, trace files, etc.).
- 5. Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. This includes using port address translation (PAT) or network address translation (NAT).

- *Deploying more servers so each server performs only one primary function.*
- *Identifying and disabling all unused/unnecessary ports and services.*
- *Encrypting all non-console administrative access using SSH, SSL-VPNs and other means.*

PCI-DSS Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI-DSS Requirement 2 addresses the need to proactively manage system component security defaults. Some of the more difficult requirements include:

Novell PCI-DSS Solutions

Novell PCI-DSS solutions can address most of the technical aspects of sections 1 and 2. They can also provide a level of integration with each other and with partner firewalls that makes it possible to reduce IT staff workloads and minimize human coordination and communication failures. The following table shows how specific Novell solutions address various PCI-DSS secure networking requirements:

Solution	PCI-DSS Requirements	Details and Other Benefits
SUSE Linux Enterprise Edition	<ul style="list-style-type: none"> ■ 1.1—Establish firewall configuration standards ■ 1.3.2—Don't allow internal addresses to pass ■ 1.5—Implement IP masquerading—use PAT and NAT ■ 2.3—Encrypt all non-console administrative access. Use technologies such as SSH, VPN or SSL/TLS 	<ul style="list-style-type: none"> ■ Enhances server security with incorporated firewalls ■ Provides a standard OS foundation for servers ■ Can be deployed as an inexpensive, stand-alone firewall ■ Provides native support for NAT, PAT, SSH, VPN and SSL/TLS
Novell Identity Manager	<ul style="list-style-type: none"> ■ 1.1.4—Describe groups, roles and responsibilities for logical management of network components 	<ul style="list-style-type: none"> ■ Provides a central system for identifying people who are authorized to manage firewalls and verify their roles
Novell Sentinel	<ul style="list-style-type: none"> ■ 1.1.5—Document services and ports necessary for business ■ 1.2—Implement firewall configuration that denies traffic from "untrusted" networks/ hosts ■ 1.3.7—Deny all other inbound and outbound traffic not specifically allowed ■ 1.4.2—Restrict outbound traffic from payment card applications to IP addresses within the DMZ ■ 2.2.2—Disable unnecessary and insecure services and protocols ■ 2.2.3—Configure system security parameters to prevent misuse ■ 2.2.2—Disable all unnecessary and insecure services and protocols 	<ul style="list-style-type: none"> ■ Monitors port configuration and activity to enforce policies and identify unauthorized access attempts ■ Enforces protection by alerting access from any location not on the "trusted list" ■ Monitors outbound as well as inbound traffic to catch potential internal attacks
Novell Access Manager	<ul style="list-style-type: none"> ■ 2.3—Encrypt all non-console administrative access 	<ul style="list-style-type: none"> ■ Provides clientless SSL-VPN initiation when granting systems access
Novell ZENworks	<ul style="list-style-type: none"> ■ 2.2.1—Limit each server to one primary function 	<ul style="list-style-type: none"> ■ ZENworks simplifies management of large numbers of servers
Third-party partner firewall systems	<ul style="list-style-type: none"> ■ 1.1—Establish firewall configuration standards 	<ul style="list-style-type: none"> ■ Novell Sentinel reads log data from popular fire walls and integrates firewall activity streams into policy-exception alerts and reports ■ Partner Products include: <ul style="list-style-type: none"> - Cisco Pix* - Checkpoint* - Firewall-1 Checkpoint* - Provider-1 Lucent* - Brick CyberGuard* - Secure Computing Gauntlet* - Secure Computing Sidewinder* - Sonic Wall* ■ Microsoft ISA Firewall* ■ Zone Alarm*

How Safe Is Your Data?

- 230,000 Ameriprise Financial customer records were found on a stolen laptop.
- 243,000 Hotel.com customer records were found on a stolen laptop.
- ChoicePoint had records for 160,000 consumers stolen from their databases.

Control Objective #2: Protect Cardholder Data

Control Objective	Requirement	Novell Solutions
Protect cardholder data	3) Protect stored cardholder data	Novell Identity Manager Novell Access Manager Novell AppArmor SUSE Linux Enterprise Edition Novell Linux POS
	4) Encrypt transmission of cardholder data across open, public networks	Novell Access Manager SUSE Linux Enterprise Edition Novell Linux POS

In the event that an external hacker or internal employee obtains inappropriate access to systems, cardholder information needs to remain protected through encryption, automatic deletion and application-level access restrictions. Once again, identity management systems play a key role in managing and automating these types of processes. Without identity management, supporting capabilities like automatic deletions and access restrictions becomes prohibitively difficult and expensive.

PCI-DSS also requires retailers to protect cardholder data that resides on their systems—including data that travels to and from those systems. News reports often highlight stories about unencrypted cardholder data being stolen by network hackers, malicious employees or even careless workers. To prevent these types of thefts, it's important to make sure that cardholder data is never stored for long periods of time (if at all)—and that it remains protected while it's being stored or transmitted.

Whenever encryption is required, the secure management of encryption keys is essential. This includes enforcing strict data access rights, which ultimately depends on strong identity management. You must be able to identify who is accessing data before you can control who can and cannot have access.

Encrypting discs, file systems and data transmissions will cover most PCI-DSS mandates, but encryption is not something you can leave to chance. It's important to make encryption a native part of your core infrastructure. This means your fundamental

infrastructure must be “encryption aware” and use cryptography as a default for some operations, such as network access to cardholder data systems.

PCI-DSS Requirement 3: Protect stored cardholder data

This requirement mandates that the storage of cardholder data must be kept to a minimum—and that cardholder data must be rigorously encrypted whenever it is stored. Detailed requirements include:

- *Enforcement of a strict data retention and disposal policy*
- *Data masking, truncation and one-way encryption*
- *Data access restrictions to cardholder data*
- *Secure encryption key management to keep keys from being discovered*

PCI-DSS Requirement 4: Encrypt transmission of cardholder data across open, public networks

Although PCI-DSS specifies that cardholder data must be encrypted when it travels across public networks, Novell recommends encrypting cardholder data during all network transmissions—even those that take place behind the firewall. PCI-DSS requirement 4 includes detailed requirements for socket-level cryptography, and it prohibits the use of e-mail for any cardholder data transfers.

Novell PCI-DSS Solutions

Novell solutions offer a wide range of sophisticated encryption and data protection capabilities that apply directly to PCI-DSS requirements. This starts with native encryption capabilities built into the core SUSE®.

Linux operating system and extends through other Novell data protection offerings like Novell Linux POS, Novell Access Manager™ and AppArmor™. The following table shows how these products address specific PCI-DSS requirements:

Solution	PCI-DSS Requirements	Details and Other Benefits
SUSE Linux Enterprise Edition Novell Linux POS	<ul style="list-style-type: none"> 3.4—Render PAN, at minimum, unreadable anywhere it is stored 3.4.1—If disk encryption is used, logical access must be managed independently of native operating system access control mechanisms. Decryption keys must not be tied to user accounts. 3.5—Protect encryption keys used for encryption of cardholder data against both disclosure and misuse. 4.1—Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks 	<ul style="list-style-type: none"> Includes native SSL/TSL/IPSEC in SUSE servers and POS terminals for end-to-end data transmission encryption Includes native standards-based has and cryptography functions called by major POS applications and callable by in-house code Provides a standard OS foundation for servers Provides optional disc-level encryption with key access restrictions Core OS enforces Access Control Lists and allows for role-based key management
Novell Identity Manager	<ul style="list-style-type: none"> 3.5—Protect encryption keys used for encryption of cardholder data against both disclosure and misuse. 	<ul style="list-style-type: none"> Central system for creating people/device/software identities and regulating access to key data
Novell Access Manager	<ul style="list-style-type: none"> 3.4.1—If disk encryption is used, logical access must be managed independently of native operating system access control mechanisms. Decryption keys must not be tied to user accounts. 4.1—Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks. 	<ul style="list-style-type: none"> Provides clientless SSL-VPN initiation when granting systems access Encrypts all over-the-wire HTTP content between IT components and the browser regardless of whether the Web application is configured as HTTP or HTTPS Includes an integrated SSL-VPN for non-HTTP traffic Provides access control to prevent OS-based encryption controls and keys
Novell AppArmor	<ul style="list-style-type: none"> 3.1—Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. 	<ul style="list-style-type: none"> Maintains control of production application to prevent unauthorized applications from being installed. Enforces data retention policies for cardholder data.

Control Objective #3: Maintain a Vulnerability Management Program

Control Objective	Requirement	Novell Solutions
Maintain a vulnerability management program	5) Use and regularly update anti-virus software	Novell Sentinel Novell ZENworks Partner Anti-virus Solutions ¹
	6) Develop and maintain secure systems and applications	Novell Sentinel Novell Identity Manager Novell ZENworks Novell AppArmor

¹Recommended products from trusted Novell partners that integrate with Novell solutions.

The security of your operating systems and applications can have a major impact on the overall security of cardholder data. In today's threat landscape, organized crime syndicates often hire virus authors to create tools for sniffing out cardholder information. And of course, poorly written in-house applications can expose cardholder data to a wide range of threats. PCI-DSS requires retailers to take proactive measures to detect and eliminate these types of software vulnerabilities.

This requirement creates two significant challenges for IT departments. One revolves

around the never-ending struggle to keep systems patched and anti-virus and malware definitions current and up-to-date (these two functions should be handled by the same tool or utility). The second challenge involves implementing strong controls that can provide developers, testers and production administrators with controlled, isolated access to systems—and allow newly developed code to pass through development, test and production accounts and machines in a monitored and auditable way.

PCI-DSS Requirement 5: Use and regularly update anti-virus software

PCI-DSS requirement 5 mandates the use of anti-virus utilities to detect, isolate and correct viral software penetration attacks. Good, up-to-date anti-virus software is clearly essential. But it's also important to integrate virus detection log data into compliance reports and automated alerting systems. Detailed requirements for PCI-DSS section 5 include:

- *Deploying anti-virus software on all systems prone to infection*
- *Ensuring these systems are running correctly and logging their findings*
- *Keeping anti-virus mechanisms updated*

PCI-DSS Requirement 6: Develop and maintain secure systems and applications

PCI-DSS recognizes that the misuse of data by employees is as problematic as an external attack, and the standard mandates secure software development, deployment and testing processes. The requirements for section 6 include:

- *Keeping systems patched*
- *Identifying new security threats*
- *Using best practices and secure coding guidelines for in-house development*
- *Documenting and enforcing strict change management procedures*

Novell PCI-DSS Solutions

Novell offers the following solutions that address PCI-DSS requirements 5 and 6:

Solution	PCI-DSS Requirements	Details and Other Benefits
Novell Identity Manager	<ul style="list-style-type: none"> ■ 6.3.3—Separate duties between development, test and production environments ■ 6.3.5—Remove test data and accounts before production systems become active ■ 6.3.6—Remove custom application accounts, user names and passwords before applications are released or become active 	<ul style="list-style-type: none"> ■ Provides role-based access rights that allow only authorized people to deploy software on specific machines ■ Automates the de-provisioning of test accounts
Novell Sentinel	<ul style="list-style-type: none"> ■ 5.2—Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs ■ 6.3.5—Remove test data and accounts before production systems become active ■ 6.3.6—Remove custom application accounts, user names and passwords before applications are released or become active ■ 6.5.2—Eliminate broken access control ■ 6.5.9— Denial of service 	<ul style="list-style-type: none"> ■ Integrates logs and real-time data into alerts and reports ■ Discovers unauthorized system access to prevent inappropriate software distribution ■ Creates workflows to manage deprovisioning of test accounts and production roll-outs ■ Detects and reports abnormal access control patterns of user IDs that may have been compromised ■ Monitors for network and system assaults that deny legitimate access
Novell ZENworks	<ul style="list-style-type: none"> ■ 5.1—Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) ■ 6.1—Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release. ■ 6.2—Establish a process to identify newly discovered security vulnerabilities ■ 6.3.1—Test all security patches and system and software configuration changes before deployment 	<ul style="list-style-type: none"> ■ Simplifies software distribution, configuration and control across large numbers of desktops, servers and handheld devices ■ Applies security patches to multiple systems based on pre-defined policies ■ Provides extensive pre-testing features that reduce the amount of development and testing required prior to patch deployment ■ Automatically receives and distributes patches (with prior IT approval) and deploys the latest security patches immediately ■ E-mails alerts directly to administrator(s) for proactive security management ■ Offers the largest repository of tested patches to support all major operating systems and applications ■ Automatically downloads and distributes patches to keep systems up-to-date ■ Supports heterogeneous systems, including Windows (32 and 64-bit), NetWare, Solaris, AIX, Linux and HP-UX
Novell AppArmor	<ul style="list-style-type: none"> ■ 6.6—Ensure that all Web-facing applications are protected against known attacks 	<ul style="list-style-type: none"> ■ Creates profiles for proper application behavior and identifies applications that may have become compromised, including embedded Web scripting (PERL, PHP etc.)
Partner anti-virus products	<ul style="list-style-type: none"> ■ 5.1—Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers) 	<ul style="list-style-type: none"> ■ Use ZENworks to distribute anti-virus tools to servers and desktops ■ Use Sentinel to process logs from anti-virus applications for incident reporting ■ Partner products include: <ul style="list-style-type: none"> – Symantec* – Anti-virus Corporate Edition Network Associates* – ePolicy Orchestrator* – TrendMicro* – InterScan VirusWall – CA eTrust*

Control Objective #4: Maintain a Vulnerability Management Program

Control Objective	Requirement	Novell Solutions
Implement strong access control measures	7) Restrict access to cardholder data by business need-to-know	Novell Sentinel Novell Identity Manager
	8) Assign a unique ID to each person with computer access	Novell Sentinel Novell Identity Manager Novell Access Manager Novell eDirectory Novell Identity Assurance
	9) Restrict physical access to cardholder data	Novell Identity Manager ActivIdentity ¹

¹Recommended products from trusted Novell partners that integrate with Novell solutions.

² Novell believes that all system components should also carry a unique ID to effectively manage their access.

The largest PCI-DSS control objective deals with system access. Just as the firewalls in Requirement 1 deal with logical systems access, this control objective defines how retailers should regulate daily systems interactions by:

- Restricting all access to a need-to-know basis
- Assuring that everyone in an organization has a unique, controllable and auditable identity
- Regulating physical access to system components as tightly as network access

Identity management lies at the heart of this PCI-DSS control objective. PCI-DSS requires retailers to assign unique identities to every person or thing that accesses any system that maintains or transmits cardholder data. PCI-DSS covers all aspects of identity management and access control—from logical access to an application to physical access to specific rooms in a building.

A major challenge for many IT organizations involves integrating the central identity management database with other security management tools. In an ideal situation, the who (people and machines), the what (data repositories), and the how (rules and roles for access) should all operate within a unified, integrated solution that can be centrally controlled. This solution should define access based on roles and on a person’s need to access specific data repositories.

PCI-DSS Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 7 is a prelude to requirement 8. The goal is to make sure that access to cardholder information is restricted to the people who need to see it. Many provisions of PCI-DSS require a default “deny all” status with carefully managed exceptions. Novell solutions fully support this model.

PCI-DSS Requirement 8: Assign a unique ID to each person with computer access

Granting need to know access to systems and data is impossible without strong identity management capabilities. Retailers with large numbers of network points, users, systems, databases and applications must implement a central identity management solution to meet these types of PCI-DSS mandates. PCI-DSS outlines some specific identity management requirements that include:

- Unique user names for all users²
- Password, token devices or biometric controls for local access
- Two-factor authentication for remote access by employees, administrators and third parties
- Encrypted passwords during network transmission
- Controlled and centralized management of user IDs with associated procedures and/or automated controls

PCI-DSS Requirement 9: Restrict physical access to cardholder data

Controlling physical access is at least as important as controlling network access. PCI-DSS requirements include the a number of specific mandates for accessing physical system components. These include:

- *Using tokens or cards to access secure areas*
- *Logging and auditing access to secure areas*

Novell PCI-DSS Solutions

Novell Identity Manager and Novell Sentinel form the foundation of the Novell approach for addressing PCI-DSS requirements 8 and 9. Novell Identity Manager tackles the complexity of identifying every person in the organization, including external partners that need data access rights. Novell Sentinel monitors, audits and reports access activities and exceptions. Together, these solutions become the cornerstone of effective, efficient PCI-DSS compliance.

Solution	PCI-DSS Requirements	Details and Other Benefits
Novell Identity Manager	<ul style="list-style-type: none"> ■ 7.1—Limit access to computing resources and cardholder information to the people who need it ■ 7.2—Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know ■ 7.2—Set default access state to “deny all” ■ 8.1—Identify all users with a unique user name before allowing them to access system components or cardholder data ■ 8.4—Encrypt all passwords during transmission and storage ■ 8.5—Ensure proper user authentication and password management for non-consumer users and administrators on all system components ■ 8.5.4—Immediately revoke access for any terminated users ■ 8.5.5—Remove inactive user accounts at least every 90 days ■ 8.5.6—Enable accounts used by vendors for remote maintenance only during the time period needed ■ 8.5.7—Communicate password procedures and policies to all users who have access to cardholder data ■ 8.5.16—Authenticate access to any database containing cardholder data ■ 9.1.3—Restrict physical access to wireless access points, gateways and handheld devices ■ 9.3.1— Authorize users before they enter areas where cardholder data is processed or maintained ■ 9.3.2—Provide a physical token (such as a badge or access device) that expires and that identifies visitors as non-employees 	<ul style="list-style-type: none"> ■ Identifies every unique individual and grant either role-base or individual access rights ■ Grants limited access to authorized people based on their role-defined “needs” ■ Provides a default “deny all” state ■ Provides end-to-end encryption of passwords ■ Meets section 8.5 requirements for: <ul style="list-style-type: none"> – Controlled addition, deletion and modification of user IDs, credentials and other identifying objects – Verifying user identities before password resets – Setting first-time passwords to a unique value for each user and changing them immediately after the first use – Immediately revoking access for terminated users – Removing inactive accounts ■ Provides out-of-the-box integration with major applications (Baan, J.D.Edwards, Lawson, Oracle, Peoplesoft, SAP Siebel); databases (DB2, Informix, Microsoft SQL Server, MySQL, Oracle, Sybase, JDBC); and e-mail systems (Exchange, Novell GroupWise, Notes) and more ■ Communicates password policies to end users using the Novell Identity Manager password management interface ■ Synchronizes with over 260 systems for controlling building access ■ Disables user access profiles when users are terminated via an HR application integration point
Novell Sentinel	<ul style="list-style-type: none"> ■ 7.1—Limit access to computing resources and cardholder information to the people who need it ■ 7.2—Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know ■ Set default access state to “deny all” ■ 8.1—Identify all users with a unique user name before allowing them to access system components or cardholder data 	<ul style="list-style-type: none"> ■ Discovers and reports unauthorized system access or login attempts in real-time ■ Reports all access attempts through Novell Identity Manager ■ Provides out-of-the-box monitoring for a variety of authentication and authorization events
Novell Access Manager	<ul style="list-style-type: none"> ■ 8.3—Implement two-factor authentication for remote access to the network by employees, administrators and third parties 	<ul style="list-style-type: none"> ■ Provides multi-factor authentication for Web-based applications
Novell eDirectory	<ul style="list-style-type: none"> ■ 8.5.9—Change user passwords at least every 90 days ■ 8.5.10—Require a minimum password length of at least seven characters ■ 8.5.11—Use passwords containing both numeric and alphabetic characters ■ 8.5.12—Do not allow a user to submit a new password that is the same as any of the last four passwords used ■ 8.5.13—Limit repeated access attempts by locking out the user ID after not more than six attempts ■ 8.5.14—Set the lockout duration to 30 minutes or until an administrator enables the user ID 	<ul style="list-style-type: none"> ■ Applies policies within eDirectory during authentication and password maintenance

continued on next page

Solution	PCI-DSS Requirements	Details and Other Benefits
Novell Identity Assurance Solution	<ul style="list-style-type: none"> 8.3—Implement two-factor authentication for remote access to the network by employees, administrators and third parties 	<ul style="list-style-type: none"> Provides integration for Novell Identity Manager Provides physical and logical access controls Supports multi-factor authentication
ActiveIdentity	<ul style="list-style-type: none"> 9.3.2—Provide a physical token (for example, a badge or access device) that expires and that identifies visitors as non-employees 	<ul style="list-style-type: none"> Offers one-time use factor password generation Supports physical tokens (ID cards, USB tokens, etc.) Provides full token lifecycle management within Novell Identity Manager

Control Objective #5: Regularly Monitor and Test Networks

Control Objective	Requirement	Novell Solutions
Regularly monitor and test networks	10) Track and monitor all access to network resources and cardholder data	Novell Sentinel SUSE Linux Enterprise Edition Novell Linux POS Partner Intrusion Detection [†]
	11) Regularly test security systems and processes	Novell Sentinel SUSE Linux Enterprise Edition Novell Linux POS

[†]Recommended products from trusted Novell partners that integrate with Novell solutions.

To comply with PCI-DSS, you must be able to demonstrate that your systems are secure. This includes the ability to test and audit systems that interact with cardholder data, so you can effectively prove that you have implemented secure data practices correctly, that they are functioning as designed, and that they meet PCI-DSS requirements.

Because this kind of security testing often gets overlooked, PCI-DSS requires that you monitor and log access to systems that interact cardholder data—and perform tests to ensure that your security measures are functioning properly. To fulfill this requirement without placing undue stress on your IT staff, it's important to implement a solution that provides tight integration between your access monitoring, alerting and reporting functions.

PCI-DSS Requirement 10: Track and monitor all access to network resources and cardholder data

PCI-DSS requires that you manage and monitor access down to the lowest levels. This includes system administrator (root) logins to servers, database access and even

the log files that record access information. These requirements are holistic and require a broad monitoring infrastructure.

PCI-DSS Requirement 11: Regularly test security systems and processes

Requirement 11 mandates the periodic testing of your deployed security systems, including Intrusion Detection Systems (IDS) and access monitoring systems. This testing can help ensure that these systems are functioning properly, and that there are no lapses in your access restriction and monitoring capabilities.

Novell PCI-DSS Solutions

Novell Sentinel provides all of the tools and capabilities you'll need to monitor your firewall, IDS, systems, applications, anti-virus utilities and networks as mandated by PCI-DSS. By processing input from these and other systems, Sentinel can create alerts, generate audit reports and aggregate information to create meaningful security exception profiles. Data from vulnerability scanners can also be submitted to Sentinel to test for security configuration errors.

Solution	PCI-DSS Requirements	Details and Other Benefits
SUSE Linux Enterprise Edition Novell Linux POS	<ul style="list-style-type: none"> ■ 10.2.2—Monitor all actions taken by any individual with root or administrative privileges ■ 10.2.3—Audit access to all systems ■ 10.5.5—Use file integrity monitoring and change detection software on logs ■ 11.4—Use network Intrusion Detection Systems, host-based Intrusion Detection Systems and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises ■ 11.5—Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files 	<ul style="list-style-type: none"> ■ Logs and consolidates native administration actions ■ Uses Access Control Lists (ACLs) to control who can edit files ■ Uses file system objection monitoring to alert administrators about inappropriate changes to log files and other elements ■ Uses AppArmor to prevent application tampering and log tampering
Novell Sentinel	<ul style="list-style-type: none"> ■ 10.2.1—Audit individual user access to cardholder data ■ 10.2.2—Audit all actions taken by any individual with root or administrative privileges ■ 10.2.4—Audit invalid logical access attempts ■ 10.2.5—Audit use of identification and authentication mechanisms ■ 10.2.7—Audit creation/deletion of system-level objects ■ 10.3—For access events, log user identification, the type of event, date and time, success or failure indication, origination of event and identity or name of affected data, system component or resource ■ 10.5—Secure audit trails so they cannot be altered. ■ 10.5—Limit viewing, prevent modification and create backup logs. ■ 10.5.5—Use file integrity monitoring and change detection software on logs ■ 10.6—Review logs for all system components at least daily ■ 11.4—Use network intrusion detection systems, host-based intrusion detection systems and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises ■ 11.5—Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files 	<ul style="list-style-type: none"> ■ Provides additional detail for privileged systems access ■ Includes default functions for alerting and reporting failed login attempts ■ Provides logging and reporting for all authentication events ■ Tracks system-level object changes, including creations and deletions on multiple operating systems, changes within Oracle databases (drops, adds, truncations, etc.) and Tripware* ■ Provides complete event logging that exceeds PCI-DSS requirements ■ Log integrity is delivered MD5 and additionally secured via native database security functions ■ Uses OS-level access logging to create audits, alerts and reports. Also allows aggregation with other types of access information. ■ Reporting functions automatically generate concise review information
Third-party host IDS systems	<ul style="list-style-type: none"> ■ 10.5.5—Use file integrity monitoring and change detection software on logs 	<ul style="list-style-type: none"> ■ Adds additional object-level security exception detection and native host logging by integrating Sentinel with major third-party IDS systems ■ Partner products include: <ul style="list-style-type: none"> – McAfee Entersys* – ISS RealSecure Server* – Symantec ITA* – Tripwire* – Enterasys Dragon* – CA eTrust* – Cisco Secure Agent* – SNARE*

Control Objective #6: Maintain an Information Security Policy

Control Objective	Requirement	Novell Solutions
Maintain an information security policy	12) Maintain a policy that addresses information security	Novell Sentinel Novell Identity Manager Partner and Open Source Vulnerability Scanners [†]

[†]Recommended products from trusted Novell partners that integrate with Novell solutions.

The final PCI-DSS control objective contains more than 40 specific requirements created to make sure retailers meet PCI-DSS goals on an ongoing basis. Many of the requirements in this control objective are procedural, which makes them good candidates for automation.

Clearly, tying these ongoing procedures to your automated identify, access control,

monitoring and reporting infrastructure can eliminate a great deal of manual effort and reduce the probability of overlooking important details. By implementing systems that codify procedures, define roles for executing those procedures and monitor and report on these interactions, you can achieve initial PCI-DSS compliance more quickly and simplify ongoing policy maintenance.

PCI-DSS Requirement 12: Maintain a policy that addresses information security

PCI-DSS requirement 12 is very detailed. It includes:

- *Developing annual processes that identify threats and vulnerabilities*

- *Performing a formal annual risk assessment*
- *Producing daily operational security procedures*
- *Developing proper use policies for critical employee-facing technologies*
- *Monitoring and analyzing security alerts*
- *Monitoring and controlling all access to data*
- *Implementing an incident response plan*

Novell PCI-DSS Solutions

The same family of Novell tools can provide a complete, automated solution for maintaining PCI-DSS compliance. Novell Identity Manager makes sure employees and partners can only access and install the systems and applications they're authorized to use. The workflow functions in Novell Identity Manager provide a simple way to checklist the deployment of tools and information to authorized people in selected roles. And Novell Sentinel fulfills PCI-DSS mandates for incident alerts and audit reporting on vulnerability scans.

Solution	PCI-DSS Requirements	Details and Other Benefits
Novell Identity Manager	<ul style="list-style-type: none"> ■ 12.3.1—Develop usage policies for critical employee-facing technologies. These include: <ul style="list-style-type: none"> – Explicit management approval – Authentication for use of the technology ■ 12.5.4—Administer user accounts, including additions, deletions and modifications 	<ul style="list-style-type: none"> ■ Provides central user administration with integration points to Novell solutions that monitor account changes and enforce ID and usage workflows ■ Provides workflow management that enables the codification and enforcement of technology provisioning
Novell Sentinel	<ul style="list-style-type: none"> ■ 12.2—Develop daily operational security procedures that are consistent with requirements ■ 12.5.3—Establish, document and distribute security incident response and escalation procedures ■ 12.9—Implement an incident response plan. Be prepared to respond immediately to a system breach. ■ 12.9.1—Create an incident response plan to be implemented in the event of a system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities and communication and contact strategies. ■ 12.9.5—Include alerts from intrusion detection, intrusion prevention and file integrity monitoring systems ■ 12.10—Make sure all processors and service providers maintain and implement policies and procedures to manage connected entities 	<ul style="list-style-type: none"> ■ Provides workflow management that makes it possible to codify and automate security event responses ■ Provides security event detection, alerting and workflow management capabilities for effective responses to stateful workflow or security incidents ■ Provides integration with IDS systems ■ Provides historical metrics for all accesses, including internal and external connected entities ■ Accepts input from a variety of vulnerability scanning products
Third-party partner and Open Source vulnerability scanning tools	<ul style="list-style-type: none"> ■ 11.2—Run internal and external network vulnerability scans at least quarterly and after any significant change in the network 	<ul style="list-style-type: none"> ■ Integrates access log information and produces reports to facilitate both proactive and reactive vulnerability analysis ■ Partner products include: <ul style="list-style-type: none"> – McAfee Foundstone Enterprise* – eEye Retina* – Gnu Nessus – Qualys QualysGuard* – nCircle IP360* – ISS Internet Scanner* – Harris Stat* – Gnu NMAP
Securewave Sanctuary*	<ul style="list-style-type: none"> ■ 12.3.1—Develop usage policies for critical employee-facing technologies, including: <ul style="list-style-type: none"> – Explicit management approval – Authentication for use of the technology 	<ul style="list-style-type: none"> ■ "White lists" application install, run and access controls

Four Novell PCI-DSS Products Have Won Info Security Products Guide Excellence Awards:

- Novell Identity Manager 3.5 for Excellence in Identity Management
- Novell Access Manager 3 for Excellence in Access Management
- Sentinel 6 from Novell for Excellence in Security Management
- Novell ZENworks 7 Patch Management for Excellence in Patch Management

Deployment Strategy—Essential Steps

Complying with PCI-DSS requires mapping an implementation strategy. As an IT executive, you need to accomplish PCI-DSS compliance without overloading your staff resources.

The following macro-level plan will help you organize your approach to PCI-DSS compliance. Novell is ready to assist with consultation services that will streamline implementation and minimize capital outlays. Contact Novell at 1 801 861 1349 or visit: www.novell.com/retail

Step 1—Internal education

1. IT executive review of PCI-DSS requirements
2. IT technical staff education on PCI-DSS requirements
3. Top executive review of PCI-DSS and penalties for non-compliance to assure priority buy-in
4. Business stakeholder education concerning access restrictions mandated by PCI-DSS

Step 2—Technical preparation

1. IT staff technical review of PCI-DSS requirements
2. Fit/Gap analysis of existing systems and procedures against PCI-DSS requirements
3. Identify missing foundation technologies for near-term implementation
4. “Onion peel” analysis for phased implementation

Step 3—Phased implementation

1. Establish missing foundation elements (firewalls, anti-virus, etc.)
2. Document and implement identity management policy

3. Enforce identity management policy on IT staff and debug
4. Enforce identity management policy on end users
5. Automate end-point security maintenance (patching, anti-virus updates, application authorization)
6. Automate security alerts, reporting and auditing
7. Initiate mandated data and network encryption
8. Begin periodic security/vulnerability testing and auditing
9. Review and change software development and deployment practices

Glossary of Terms

Control Objective: Logically related groups of one or more “summary requirements

DSS: Data Security Standard

IDS: Intrusion Detection System—System(s) to determine if a computer network or server has experienced an unauthorized intrusion.

NAT: Network Address Translation—a standard for routing and masquerading IP addresses.

PAT: Port Address Translation—a standard for masquerading the actual port number used behind a firewall.

PCI: Payment Card Industry

Summary Requirements: Sets of related detailed requirements.

System Component: Any data systems device including networking hardware, servers, database management system, etc.

www.novell.com



Contact your local Novell
Solutions Provider, or call
Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA