NEOHAPSIS

Achieving PCI Compliance with Red Hat Enterprise Linux

June 2009

CONTENTS

EXECUTIVE SUMMARY

The Payment Card Industry Data Security Standard (PCI DSS) provides best practice security standards to protect systems and parties handling credit and debit card data.

Key Benefits of RHEL for PCI Compliance

- Ability to continuously maintain compliance and adjust to changing requirements
- Simple and cost effective management
- Scalable solutions that support integration
- Simplified deployment and configuration
- Security oriented Operating System with built-in logging, monitoring and auditing
- Red Hat Security Response Team provides continuous alerts and guidance as vulnerabilities are identified
- Configuration recommendations provided in Security Content Automation Protocol (SCAP) documentation recommendations

PCI DSS requirements not only focus on controls targeted at networks, systems and applications, but address issues of policy, process and operations. Having reliable infrastructure that is easy and cost-effective to maintain is key to supporting the operational maturity required to maintain compliance, reduce risk of exposure, and protect critical information.

While enterprises are often able to achieve compliance during an audit, they often have difficulty maintaining compliance on an ongoing basis. A technology platform that enables IT organizations to deploy and configure new systems reliably, manage systems and users efficiently, enforce policy, and meet audit and logging requirements will provide continuous return and numerous ongoing benefits. Red Hat Enterprise Linux and additional Red Hat solutions provide enterprises with the necessary platforms, mechanisms, and applications to manage environments in accordance with PCI DSS compliance requirements. Red Hat Enterprise Linux has built-in features and functions that allow a merchant or vendor to develop a robust implementation for managing all aspects of security necessary to achieve and maintain compliance on an ongoing basis.

Many of the recent attacks on payment card data involved capturing of administrator credentials to escalate privileges. Red Hat Certificate System provides a powerful security framework to manage user identities and ensure privacy of communications, effectively removing the dependency on the use of passwords for administration and lowering the risk of attackers obtaining network-wide administrator level access.

In addition to implementation of security controls, Red Hat provides the tools necessary to manage a PCI environment. Red Hat Network (RHN) keeps systems up-to-date directly and immediately from Red Hat. When implemented with Red Hat Satellite, an on-premises Red Hat Network product, it provides the systems management platform that makes Linux deployable, scalable, and manageable across the enterprise. Red Hat Satellite offers superior security by having a single centralized tool, secure connection policies for remote administration, and secure content. Enterprises use Red Hat Network to ensure security fixes and configuration files are consistently applied across the environment.

The threats to payment card data are continuously evolving, and the PCI DSS will continue to mature and require more stringent enforcement of requirements. Implementing technology platforms that support the implementation of protective measures will be necessary to reduce the risk of increasingly advanced threats. The Red Hat platform provides a foundation that supports continuous implementation of controls and enforcement of policies, and allows administrators to avoid implementing complex solutions that increase the ongoing cost of maintaining secure solutions.

The combination of Linux's inherent security strengths and Red Hat's security features, management tools, and products provides a strong foundation for implementing and maintaining PCI-compliant applications and solutions.

OVERVIEW OF PCI

1.1. What is PCI DSS?

The Payment Card Industry Data Security Standard is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. The PCI DSS was developed to help facilitate the broad adoption of consistent data security measures on a global basis. This comprehensive standard is intended to help enterprises proactively protect customer account data, and will be continually enhanced as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks.

1.2. Who is impacted by PCI?

PCI DSS applies to all enterprises that store, process or transmit cardholder data, and provides guidance for software developers and manufacturers of applications and devices used in those transactions. The PCI Security Standards Council is responsible for managing the security standards, while compliance with the PCI is enforced by the founding members of the Council -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

While the PCI DSS is specific to applications and systems that store, process, or transmit payment card data, the standard is derived from industry best practices applicable to many regulations and industry standards. Consequently, many enterprises may find benefit in implementing the controls required to achieve compliance with PCI DSS in areas outside of their payment card environment. By establishing an enterprise-wide framework and standards for implementing controls, organizations will benefit by attaining compliance in other areas of their business where they are subject to regulation or wish to meet industry standards.

1.3. Requirements for achieving PCI compliance

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized. Enterprises with a mature security and information risk management program will have the foundational elements already in place to attain PCI compliance. Enterprises that currently do not have a security program based upon best practices should build from these fundamentals to address risk and achieve compliance with the following core PCI DSS principles:

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

OVERVIEW OF RED HAT SOLUTIONS

1.4. Industry Solutions

Red Hat provides solutions that span the needs of the Education, Financial Services, Government, Healthcare and Life Sciences, Oil and Gas, and Telecommunications industries. All of these industries have areas where payment applications are used, and many organizations are subject to compliance with PCI requirements. Each of these industries has additional and increasing regulatory compliance requirements. For example, many Financial Services companies are subject to Gramm-Leach-Bliley Act (GLBA), FDIC, OCC and SEC regulations; Healthcare organizations may be subject to Health Insurance Portability and Accountability Act (HIPAA) and FDA regulations; and Oil and Gas are subject to Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) compliance requirements. Additionally, there are compliance regulations and standards that apply across industry lines, such as the Sarbanes-Oxley ACT (SOX) and state privacy laws.

The complexity of compliance requirements, both specific to industry verticals and for enterprises in general, demand technology solutions that have inherent controls necessary to attain compliance, support efficient and effective maintenance of systems and applications, integrate into operational environments, and provide cost-effective solutions for managing distributed systems with distinct and evolving compliance requirements.

1.5. Virtualization, Cloud Computing, and Software Appliances

Virtualization

Many enterprises are beginning to adopt virtualization strategies for payment applications for increased cost-efficiency, scalability, manageability, and reliability. In order to achieve PCI compliance in a virtualized environment, management of virtualized environments and enforcement of controls will be increasingly complex. Centralized, policy-driven management solutions will provide the strong base to ensure segregation of data and applications, proper application of security controls, and support the stringent operational monitoring requirements. Red Hat plans to significantly expand and enhance its server, client, and management products to enable ubiquitous adoption of virtualization across the enterprise with the forthcoming delivery of the Red Hat Enterprise Virtualization portfolio of solutions.

Cloud Computing

When deploying payment applications in a cloud computing environment, security of the underlying infrastructure and mechanisms for provisioning applications will be fundamental. The

PCI standard will continue to evolve to address new technology patterns, but as enterprises deploy new applications in next-generation technology solutions today they need to consider the compliance ramifications of shared environments. When developing applications that will leverage cloud computing infrastructure, it is paramount to ensure data is protected, applications are developed in a secure manner, monitoring solutions are integrated and incorporated in to operations, and access to systems and applications are restricted only to authorized users.

ACHIEVING COMPLIANCE WITH RED HAT ENTERPRISE LINUX

1.6. Compliance Management

Compliance is a process of identifying, implementing, maintaining, and reporting on controls in order to meet the requirements of a standard or regulation. By its very nature, Red Hat provides the tools and methods to ensure compliance with the technical requirements specified by standards and regulations, including PCI. Effective compliance management requires an enterprise to use these tools in a manner that reduces costs, ensures compliance with regulations and standards, and allows for requirements that change over time. This last point is extremely important to having an effective program.

The following reference model outlines various features, provided throughout the Red Hat product set, that support effective compliance management. These features provide the foundation to address individual components of specific compliance requirements and when combined enable enterprises to achieve compliance with standards and regulations.

Red Hat Compliance Reference Model			
Access Control	Auditing	Communications Security	Configuration Management
Data Protection	Logging	Network Security	Patching
Policy Enforcement	Secure Administration	Secure Deployment	System Security

Figure 1 - Red Hat Compliance Reference Model

1.7. Red Hat Compliance Reference Model Definitions

***Access Control*:** the ability to permit or deny the use of a particular resource by a particular entity.

Auditing: capturing and storing security critical events in system logs.

Communications Security: protecting data while in transit.

Configuration Management: maintaining configuration to support systems security

Data Protection: preventing unauthorized access or modification of data using access control or encryption.

Logging: collecting events for analysis and archival.

Network Security: preventing unauthorized access to system resources over the network.

Patching: maintenance of system software to address vulnerabilities.

Policy Enforcement: ensuring effectiveness of configuration and system security parameters.

Secure Administration: managing systems in a secure and authorized manner.

Secure Deployment: configuring and implementing servers and software.

Systems Security: proper implementation of controls to prevent malicious activity.

RED HAT ENTERPRISE LINUX TECHNOLOGIES

An important part of an enterprise security strategy is to select technologies that will support *on-going* compliance with standards and regulations. There are a number of technologies provided by Red Hat that map to these requirements, and are discussed in this section.

Effectively maintaining PCI compliance requires an operating system platform that is easy to deploy, simple to manage, flexible, and available.

Red Hat Enterprise Linux includes facilities to build, deploy, and maintain secure environments.

Red Hat Enterprise Linux PCI compliance features include:

- Security Enhanced Linux (SELinux) to secure systems and protect card data via mandatory access control
- Services are provided with targeted policies enabled by default
- Significant ease-of-use enhancements with the inclusion of the SELinux Troubleshooter, a GUI-based analyzer
- Auditing tracks activities and modifications to the entire system
- Network security including host-based firewall

Centralized management of configurations and policies enables enterprises to efficiently implement and monitor controls.

Red Hat Satellite provides a systems management platform for a growing Linux infrastructure. Built on open standards, Red Hat Satellite provides powerful systems administration capabilities such as management, provisioning, and monitoring for large deployments.

PCI compliance features provided by Red Hat Satellite include:

- One-click software updates in an easy-to-use interface
- Role-based administration
- Flexible delivery architectures- Satellite, Proxy, Hosted
- Group systems together for easier administration
- Automate formerly manual tasks
- Manage the complete lifecycle of Linux infrastructure
- Track the performance of Linux systems

A fundamental requirement for achieving PCI compliance is the use of encryption to protect data in transit and at rest.

Red Hat Certificate System provides a powerful security framework to manage user identities and ensure privacy of communications; it also simplifies enterprise-wide deployment and adoption of a Public Key Infrastructure.

Red Hat Certification System features supporting PCI compliance include:

- Supports all aspects of deploying and maintaining a Public Key Infrastructure for managing user identities
- Integrates easily with third-party security software and existing applications
- Web-based administration from a centralized console
- Key recovery and revocation
- Distributed architecture and scalable solution

Consistent management of user access is essential for protecting data and access to systems.

Red Hat Directory Server simplifies user management, eliminating data redundancy, and automating data maintenance. It also helps improve enterprise security, by storing policies and access control information. Red Hat Directory Server creates a single authentication source across entire enterprise for both intranet and extranet applications.

Red Hat Directory Server enables PCI compliance with the following features:

- Centralizes management of people and profiles
- Acts as a central repository for user profiles and preferences
- Allows replication of data across the enterprise
- Enables single sign-on access with a partner solution
- Provides scalability
- Provides the foundation for strong certificate-based authentication

The following matrix aligns the Red Hat technologies with the Red Hat Compliance Reference Model components. When leveraged together, Red Hat solutions provide a strong foundation for achieving compliance.

Red Hat Compliance Reference Model Components	*Red Hat Security Features*	*Red Hat Satellite*	*Red Hat Certificate Server*	*Red Hat Directory Server*
Access Control	X	X	X	X
Auditing	X	X		X
Communications Security	X	X	X	
Configuration Management	X	X	X	X
Data Protection	X	X	X	X
Logging	X	X		X
Network Security	X	X	X	
Patching	X	X		
Policy Enforcement	X	X		X
Secure Administration	X	X	X	X
Secure Deployment	X	X		X
System Security	X	X	X	X

Figure 2 - Mapping of Security Technologies to Compliance Reference Model Component

MAPPING RED HAT ENTERPRISE LINUX FEATURE SET TO PCI

The following matrix demonstrates how Red Hat Enterprise Linux and supporting technologies can be used to achieve and maintain PCI compliance.

PCI DSS Requirements	Red Hat PCI Compliance Features
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	*Red Hat Enterprise Linux* provides a firewall that can be implemented, configured, and maintained for both the individual host and systems it is protecting. *Red Hat Satellite* allows administrators to standardize, manage, and monitor configurations.
Requirement 2: **Do not use vendor-supplied defaults for system passwords and other security parameters**	*Red Hat Enterprise Linux* requires users to provide individual passwords for accounts upon installation. *Red Hat Certificate Server* enables strong authentication and removes the dependency on using passwords. *Red Hat Directory Server* provides centralized user credential management and policy enforcement.
Requirement 3: **Protect stored cardholder data**	*Red Hat Enterprise Linux* contains access controls and permissions that can be configured to protect data. SELinux isolates applications and services to enforce protection schemes within the system. *Linux Unified Key Setup (LUKS)* provides standalone disk encryption for data at rest. *Red Hat Satellite* allows administrators to manage permissions centrally and by groups. *Red Hat Directory Server* centrally stores policies and access control information.
Requirement 4: **Encrypt transmission of cardholder data across open, public networks**	*Red Hat Enterprise Linux* provides multiple options for encrypting data during transmission, including SSL, SSH, and VPN. *Red Hat Certificate Server* provides management of certificates used to ensure the privacy of communications.
Requirement 5: **Use and regularly update anti-virus software**	*Red Hat Satellite* provides mechanisms to centrally deploy and maintain anti-virus software applications.
Requirement 6: **Develop and maintain secure systems and applications**	*Red Hat Satellite* provides centralized and automated mechanisms for tracking, distributing, and updating packages and applications.
Requirement 7: **Restrict access to cardholder data by business need-to-know**	*Red Hat Enterprise Linux* uses access controls and permissions to restrict access to data. *Red Hat Satellite* provides centralized administration of polices and permissions. *Red Hat Certificate Server* provides mechanisms for establishing identities of users and enables strong authentication. *Red Hat Directory Server* provides centralized user credential management and policy enforcement.
Requirement 8: **Assign a unique ID to each person with computer access**	*Red Hat Enterprise Linux* allows individual credentials with unique IDs to be configured for each user with computer access. *Red Hat Satellite* provides management of unique IDs for each administrator. *Red Hat Certificate Server* provides mechanisms for establishing identities of users and enables strong authentication.

PCI DSS Requirements	Red Hat PCI Compliance Features
	Red Hat Directory Server provides centralized management of unique IDs for each person.
Requirement 9: **Restrict physical access to cardholder data**	*Red Hat Enterprise Linux* utilizes LUKS disk encryption protects the data on physical disk.
Requirement 10: **Track and monitor all access to network resources and cardholder data**	*Red Hat Enterprise Linux* system logs and audit mechanisms can be configured to track all access to resources and data. *Red Hat Satellite* provides centralized tracking of administrative access changes from the management solution. *Red Hat Certificate Server* enables the use of certificates for identify management. *Red Hat Directory Server* provides mechanisms for tracking all authentication requests.
Requirement 11: **Regularly test security systems and processes**	*Red Hat Satellite* provides centralized monitoring of systems, patch level, and user activity.
Requirement 12: **Maintain a policy that addresses information security**	*Red Hat Enterprise Linux* supports configuration options to meet PCI policy requirements. *Red Hat Satellite* provides mechanisms to centrally manage and enforce policies. *Red Hat Directory Server* stores policies and user information.

WHY RED HAT ENTERPRISE LINUX FOR PCI

1.8. Security is Built-in

Red Hat Enterprise Linux has extensive security features and applications which provide important security controls. The system can be secured at the access points, and within the host, based upon roles. The host-based firewall enables enterprises to control access to systems and applications. The available VPN and SSL allow enterprises to encrypt the transport of data and credentials. Extensive system level access controls enable the ability to contain and protect data. Disk and file based encryption allow the protection of data in circumstances when either the physical system is compromised or unintended system access is achieved. Powerful logging and auditing mechanisms allow the identification of unacceptable access and the capability of determining what happened. Strong authentication mechanisms protect the compromise of user credentials. For security critical implementations, SELinux provides additional controls for protecting systems, applications, and data.

1.9. Security Guidance

The Red Hat Security Response Team is responsible for ensuring that security issues found in Red Hat products and services are addressed. The Security Response Team works with customers who have found security issues in products or services, track alerts and security issues that may affect users of Red Hat products and services, investigates and addresses security issues in Red Hat's supported products and services, and ensures that customers can easily find, obtain, and understand security advisories and updates.

Additionally, Red Hat supports the development of the Security Content Automation Protocol (SCAP) to provide security configuration recommendations for the Red Hat Enterprise Linux operating system. The guidance provided is applicable to all variants (Desktop, Server, and Advanced Platform) of the product. The guide provides recommended settings for the basic

operating system, as well as for many commonly-used services that the system can host in a network environment.

1.10. Reduced Impact of PCI-Oriented Malware

Many of the attacks on payment data have involved the use of malware. The majority of existing malware tends to target Microsoft Windows based operating environments. While the potential for a Linux-based variant of malware to be developed does exist, deploying payment applications on a Linux platform reduces the risk of compromise from a majority of currently identified malware. Additionally, the most common forms of malware target operating system services. By configuring SELinux on Red Hat Enterprise Linux, the risk associated with compromised services is reduced, as compromising a service may not provide access to the system.

1.11. Ease of Management

Red Hat centralized management tools enable enterprises to manage the access and separation of duties of administrators, maintain standardized configurations for building and rebuilding systems, and flexibly group systems for administrative purposes. Enterprises can apply or remove updates, fixes, and applications changes and monitor the state of systems relative to group and configuration associations.

1.12. Ease of Maintaining Compliance

The easier it is to manage systems and applications, the easier it is to enforce and maintain compliance. PCI DSS Requirement 6 requires enterprises to develop and maintain secure systems and applications. In order to maintain system compliance to meet this requirement, enterprises must have the capability to institute changes and controls to systems and applications on an as needed basis or schedule the appropriate date and time.

Red Hat system and configuration mechanisms provide effective means for easily monitoring and maintaining system compliance according to defined groups and configurations. For example, in the event of an identified application vulnerability, Red Hat's tools provide the means for understanding which systems are affected. Upon release of a configuration change or application update the management tools can be used to push the necessary updates to all impacted systems and verify success or failure. Changes can be scheduled appropriately to minimize business impact and can be done on an adhoc or immediate basis as necessary.

1.13. Auditing

Red Hat auditing tracks activities and modifications to the entire system, including file system operations, process system calls, user actions such as password changes, account additions/deletions/modification, use of authentication services, and configuration changes (such as time changes). Provides powerful searching and reporting tools and a unique real-time interface that permits applications to analyze and react to events as they occur.

Auditing allows Red Hat Enterprise Linux to meet US Government certifications such as CAPP/LSPP and NISPOM and enables enterprises to meet regulatory requirements such as PCI, Sarbanes-Oxley, and HIPAA.

1.14. Security Enhanced Linux

For security critical applications, such as payment data processing, Red Hat support of the Security-Enhanced Linux kernel provides the implementation and enforcement of mandatory access control policies that confine user programs and system server to the minimum amount of privilege required. SELinux enforces mandatory access control policies that confine user

programs and system servers to the minimum amount of privilege they require. For example, administrators may minimize the attack surface by requiring authorization to core operating system services such as DNS. When confined in this way, the ability of these user programs and system daemons to cause harm when compromised (via buffer overflows or misconfigurations, for example) is reduced or eliminated. The additional controls provided by SELinux may significantly reduce the impact of a compromise or effectiveness of malware.

SUMMARY

With the challenges of compliance in general, and PCI specifically, it is essential to have a strategic technology program that builds out and supports the components of long-term compliance management. Red Hat Enterprise Linux and Red Hat solutions provide a strong foundation to build a compliance program that is able to address changing regulations and evolving security threats. When selecting technologies to support applications with compliance requirements, the following traits will provide enterprises the ability to continuously attain compliance.

Technology solutions supporting a PCI compliance program should:

- Ensure maintainability in an efficient and cost effective manner
- Adapt to changing requirements and evolving threats
- Simply administration and centralize management
- Support policy enforcement and monitoring of implemented controls
- Easily deploy and manage payment applications in a secure manner

Headquarters

215 First Street
Suite 005
Cambridge, MA 02142
Tel: +1 773 269 6300
Fax: +1 617 577 7922
www.neohapsis.com

Regional Offices

San Jose, CA
Chicago, IL
Alexandria, VA
Edmonton, Canada
London, UK
Chennai, India

REDHATWP0460409