WHITE PAPER

PCI Compliance for Power Systems™ running IBM i

ABSTRACT:

The Payment Card Industry Data Security Standard (PCI DSS) applies to every organization that processes credit or debit card information. This includes merchants and third-party service providers that store, process, or transmit credit card data. The launch of PCI DSS has helped to expose serious security shortcomings, companies' failure to follow security best practice, and a general lack of awareness of the security threats facing organizations today. This white paper examines how the standard relates to Power Systems servers running IBM i (System i, iSeries, AS/400) and also highlights when PowerTech products can provide a solution to specific requirements in the PCI standard.

By Robin Tatam

Introduction to the PCI Standard

Visa originally started the Cardholder Information Security Program (CISP) in 2001. In 2004, it joined with MasterCard and other credit card issuers to publish the Payment Card Industry (PCI) Data Security Standard. American Express, Diners Club International, and Discover Bank also endorsed the standard. The PCI standard is unique in that, unlike many other regulations, it comes from private industry rather than government mandate. The PCI Security Standards Council now has the responsibility of managing the standard.

PCI is not just a standard for banks and card issuers. Compliance is required of all merchants and service providers that store, process, or transmit credit cardholder data. The standard outlines four different merchant levels, depending on the volume of transactions per year. Originally required by June 2005, initial compliance efforts were lax. At the beginning of 2007, Visa reported only 15 percent compliance among Level 2 merchants. However, a series of fines and incentives were subsequently put in place to encourage compliance.

Any company that stores credit card data should be actively working toward compliance with the PCI requirements if they have not already achieved this state. The data security standard requires implementation of a sound security policy including, for example, the use of firewalls, access control, and keeping log data for 90 days. Many of the general requirements are consistent with some of the sound security practices that companies have put into place to comply with Sarbanes-Oxley (SOX) and similar regulations, but PCI is the first that explicitly states that encryption is required. Requirements 3 and 4 of the standard specifically call out the need for encryption and have proven the most troublesome for information technology organizations.

Originally published in December 2004, the PCI standard was updated several times, with the most recent version, 2.0, released in October 2010.

The PCI standard currently consists of 12 main requirements; you can find the complete text of the standard online at *https://www.pcisecuritystandards.org.* In this white paper, PowerTech has extracted parts of the standard that are relevant specifically to Power Systems servers (System i, iSeries, AS/400) and their operating system IBM i (i5/OS, OS/400), Each standard is mapped to the applicable PowerTech security solution. PowerTech commentary (shown in blue) describes the relevant issues and explains when PowerTech can provide a solution to the standard requirements and be used as compensating controls.

Build and Maintain a Secure Network

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

A firewall is part of a computer system that is designed to control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employee Internet-based access via desktop browsers, or employee e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

1.1 Establish firewall configuration standards that include:

1.1.5 A documented list of services/ports necessary for business

1.1.6 Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN

1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented

1.1.8 Periodic review of firewall/router rule sets

IBM i servers allow network access through interfaces such as ODBC, FTP, and Remote Command. Many of the applications that store critical data on the IBM i server were architected when users accessed the system directly from a console, and a menu system provided the only way to get to data. Even in the presence of perimeter firewalls, the implementation of protocols like FTP, ODBC, and Remote Command has exposed back doors to download and change critical data stored on the system, including credit card information.

PowerTech Network Security monitors and secures all internal network traffic to IBM i servers using exit programs. With Network Security, you can establish rules that limit access to only those users that have been preauthorized. All others can be excluded by default.

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

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and are easily determined via public information.

2.1 Always change the vendor-supplied defaults before you install a system on the network (for example, change passwords and SNMP community strings, and eliminate unnecessary accounts).

All default system profiles on IBM i begin with the letter "Q," such as QSECOFR and QPGMR. Check these profiles on a regular basis to ensure that the password is not set to default, which means it's the same as the user name.

PowerTech Compliance Monitor provides the capability to run regular audit reports to monitor the security compliance status of IBM i systems. For example, one of the default reports included with Compliance Monitor is "User Profiles with Default Passwords." In addition, it also includes a predefined filter specifically for IBM system profiles.

While a password validation program can provide additional restrictions beyond the operating system's own controls, the existence and function of such a program should be monitored as it is a way to collect passwords as they are changed. Compliance Monitor reports on the compliance of password system values against a policy to quickly determine if all of the values are set as expected, and event log reports will identify the source of any deviation.

2.3 Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access.

IBM i provides a capability to secure all Telnet sessions to the system with SSL. Connections that are not secured can be rejected.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Encryption of cardholder data is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable. PCI rules also control the storage of elements of the cardholder data to limit risk.

IBM i contains strong object-level security controls that can restrict access to data to only approved users. PowerTech Network Security provides a supplemental layer to audit and limit access from requests originating from the network. DataThread should be deployed to monitor all accesses to critical data.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs.

This requirement ensures that systems are protected from current and evolving malicious software threats.

5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

StandGuard Anti-Virus, powered by McAfee, provides native virus protection for your Power Systems servers running IBM i, and should be considered a requirement for any server that uses the Integrated File System (IFS). Support for Lotus Domino, Linux, and AIX extend the investment in StandGuard Anti-Virus beyond the normal boundaries of IBM i.

PowerTech Compliance Monitor can report on the system values that define the state of the anti-virus controls for IBM i, and analyze event logs to determine the cause of any deviation.

Requirement 6: Develop and maintain security systems and applications.

Security vulnerabilities in systems and applications may allow criminals to access cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches. In addition, secure coding practices for developing applications, change control procedures, and other secure software development processes should be followed.

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.

You should have a process in place for applying system OS and PTF updates in a timely manner.

6.4 Follow change control processes and procedures for all changes to system components.

Change control processes are a key component of complying with this requirement, and numerous commercial applications exist to aid the promotion of application programs into a production environment.

PowerTech Authority Broker allows you to monitor and control who can make changes to system components through powerful user profiles and special authorities. It controls the elevation to privileged user profiles and maintains an audit log of user activities. DataThread can monitor for changes to critical data.

Implement Strong Access Control Measures

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

This requirement ensures that only authorized personnel can access critical data.

7.1 Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

7.2 Establish a mechanism for systems with multiple users that restricts access based on a user's need-to-know, and is set to "deny all" unless specifically allowed.

*PowerTech Network Security allows you to limit access to only those individuals who need access to data for business reasons. PowerTech recommends exclusion-based security where rules in Network Security are used to grant network access to data to only those users with a demonstrated need. All others are excluded by default (set *PUBLIC access to *EXCLUDE).*

PowerTech Authority Broker audits and controls the access that users have to sensitive data through the special and private authorities associated with their user profile.

DataThread monitors database access in real-time at the record and field level. Powerful workflow capabilities provide notification, authorization, and reporting capabilities for regulatory compliance.

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

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

PowerTech Compliance Monitor provides comprehensive reporting of all audit information on IBM i servers, including events such as:

- *Invalid Log-in Attempts*
- *Default Passwords*
- *Expired Passwords*
- *Changes to User Profiles*
- *Password and Sign-on System Values*
- *Powerful User Accounts (root-level access)*
- *Group Profiles with Passwords*

Users also can customize their own specific reports.

8.4 Encrypt all passwords during transmission and storage, on all system components.

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

8.5.1 Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

Compliance Monitor report: Changes to User Profiles

8.5.2 Verify user identity before performing password resets.

8.5.3 Set first-time passwords to a unique value per user and change immediately after first use.

Compliance Monitor report: Default Passwords

8.5.4 Immediately revoke accesses of terminated users.

Compliance Monitor report: Inactive Profiles

8.5.5 Remove inactive user accounts at least every 90 days.

Compliance Monitor report: Inactive Profiles

8.5.6 Enable accounts used by vendors for remote maintenance only during the time needed.

IBM i profiles can be placed on activation schedules.

Compliance Monitor report: All Profiles

8.5.7 Distribute password procedures and policies to all users who have access to cardholder information.

8.5.8 Do not use group, shared, or generic accounts/passwords.

Compliance Monitor report: Default Passwords

8.5.9 Change user passwords at least every 90 days.

IBM i System Value setting: QPWDEXPITV = 90

8.5.10 Require a minimum password length of at least seven characters.

Note: *Most other standards recommend only at least six characters.*

IBM i System Value setting: QPWDMINLEN=7

8.5.11 Use passwords containing both numeric and alphabetic characters.

IBM i System Value setting: QPWDRQDDGT = 1

8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

IBM i System Value setting: QPWDRQDDIF = 8 (LAST 4)

8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.

IBM i System Value setting: QMAXSIGN = 6

IBM i System Value setting: QMAXSGNACN = 2

8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID.

8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

IBM i System Value setting: QINACTITV=15

QINACTMSGQ should be set to a message queue monitored by PowerTech Secure Screen.

Or, alternatively, place restrictions on the Windows systems that are used to access the IBM i server.

8.5.16 Authenticate all access to any database containing cardholder information. This includes access by applications, administrators, and all other users.

***Authority Broker** supports user restrictions to sensitive data, while enabling emergency access with user auditing and reporting.*

***DataThread** can monitor data access from any method. Workflow features enable optional filtering of access made by trusted sources.*

Regularly Monitor and Test Networks

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

Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

Operating system-level security auditing allows you to turn on detailed auditing for system objects, including creation and deletion of the objects. PowerTech software simplifies the management and interpretation of these logs through regularly scheduled reporting. PowerTech audit data can be saved and backed up to central servers.

- *IBM i System Value settings: QAUDCTL, QAUDLVL, QCRTOBJAUD*
- *Use the CHGOBJAUD command to turn on auditing for specific files and objects.*

PowerTech Compliance Monitor provides comprehensive reporting capability of all audit information on IBM i servers, including events such as:

- *Invalid Log-in Attempts*
- *Creation and Deletion of Objects*
- *Authorization Failures*
- *System Value Changes*
- *User Profile Changes*
- *Changes to Audit Settings*

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

PowerTech Authority Broker enables the elevation of privileges while maintaining a detailed audit log of user activities. Logs are tied to the originating user.

10.2 Implement automated audit trails to reconstruct the following events, for all system components:

10.2.1 All individual user accesses to cardholder data.

Compliance Monitor report: Object Accessed (reads)

Network Security audit report of network requests

DataThread real-time reporting and notification of access to critical files

10.2.2 All actions taken by any individual with root or administrative privileges.

Authority Broker reports

10.2.3 Access to all audit trails

Compliance Monitor report: Object Accessed (reads) for audit journal commands

10.2.4 Invalid logical access attempts

Compliance Monitor report: User/ Password Failures

10.2.5 Use of identification and authentication mechanisms

10.2.6 Initialization of the audit logs

Authority Broker reports

10.2.7 Creation and deletion of system-level objects.

Compliance Monitor report: Objects Created (Note: Report can be filtered for system-level objects.)

10.3 Record at least the following audit trail entries for each event, for all system components:

10.3.1 User identification

10.3.2 Date and time

10.3.4 Success or failure indication

10.3.5 Origination of event

10.3.6 Identity or name of affected data, system component, or resource.

Operating system captures native events with necessary information.

Compliance Monitor reports on native events.

Network Security audits and reports on network-initiated events.

10.4 Synchronize all critical system clocks and times.

10.5 Secure audit trails so they cannot be altered, including the following:

10.5.1 Limit viewing of audit trails to those with a job-related need.

Compliance Monitor has a comprehensive authority model so that viewing audit trails is limited only to those with a job-related need.

10.5.2 Protect audit trail files from unauthorized modifications.

IBM i contains a custom tamper-proof repository, the security audit journal QAUDJRN.

10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.

Compliance Monitor uses an innovative log aggregation approach that backs up log data to a centralized consolidation server where it is stored in a secure database.

10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.

10.5.5 Use file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

The IBM i Security audit journal repository is tamper-proof and cannot be altered.

10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).

Note: Log harvesting, parsing, and alerting tools can be used to achieve compliance with Requirement 10.6.

PowerTech Compliance Monitor can harvest logs to a centralized repository. Interact can parse the complex IBM i audit journal data into a simple-to-read event, and escalate it to external monitors such as a security information manager (SIM).

10.7 Retain audit trail history for at least one year, with a minimum of three months online availability.

PowerTech Compliance Monitor stores the audit data compressed on a central server (with 90% or better compression), enabling the retention of much more audit data than normally can be stored on servers.

Requirement 11: Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and through changes.

While IBM i servers don’t have a published vulnerability list like the Windows and UNIX platforms, PowerTech Compliance Monitor enables the regular review and assessment of the servers. Compliance Monitor includes a number of reports that users can run on a regular basis to monitor the security settings on their systems. System values are compared against a policy. Compliance Monitor ships with a default policy based on best practices, which companies can customize for their environment and specific systems. Scorecard reports also provide specific metrics that assess the security settings against best practices.

PowerTech Interact exports security-related events from the IBM i server to a syslog format that can be read by many Security Information Management solutions.

DataThread monitors database access in real-time and contains powerful notification features.

OS-level security auditing allows you to turn on detailed auditing for critical files. PowerTech Compliance Monitor provides for regular auditing and reporting on any activity related to these files.

11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless networks scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.

11.4 Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up-to-date.

11.5 Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.

Critical files are not necessarily those that contain cardholder data. For file integrity monitoring purposes, critical files usually are those that do not change regularly, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the merchant or service provider.

In IBM i, auditing can be turned on for specific objects and user profiles. PowerTech Compliance Monitor provides full audit reporting over all object access, including object reads, changes, deletes, and moves. The reports can be filtered by objects and users. DataThread, from PowerTech, allows you to perform real-time database monitoring and receive notification of changes to selected fields. IBM's Intrusion Detection System defends against network-initiated attacks, and PowerTech Network Security manages and audits network access to critical files.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel.

A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

PowerTech recommends that your Information Security Policy should specifically address your IBM i systems. The Compliance Guide included with PowerTech Compliance Monitor contains a wealth of useful information that provides guidance on creating a security policy for IBM i servers. Compliance Monitor can compare security configuration against an IBM i-specific policy. PowerTech also makes available an open source Security Policy containing baseline security standards that you can use as is, or modify for your organization.

Appendix B: Compensating Controls

Compensating Controls for Requirement 3.4.

For companies unable to meet the PCI DSS requirement for making cardholder data unreadable through encryption due to technical constraints or business limitations, compensating controls may be considered. *Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance.* Companies that consider compensating controls for rendering cardholder data unreadable must understand the risk to the data posed by maintaining readable cardholder data. Generally, the controls must provide additional protection to mitigate any additional risk posed by maintaining readable cardholder data. The controls considered must be in addition to controls required in the PCI DSS, and must satisfy the "Compensating Controls" definition in the PCI DSS Glossary. Compensating controls may consist of either a device or combination of devices, applications, and controls that meet all of the following conditions:

1. Meet the intent and rigor of the original PCI DSS requirement.
2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.
3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.)
4. Be commensurate with the additional risk imposed by not adhering the PCI DSS requirement.

PowerTech Network Security can be considered for qualification as a compensating control when used in conjunction with native access controls, such as command line restrictions or object-level security. Companies can implement Network Security quickly to protect from network-based access while strategizing and developing a longer-term encryption initiative that may require extensive programming changes.

SUMMARY

PCI REQUIREMENT	Network Security	Compliance Monitor	Authority Broker	Interact	DataThread	StandGuard Anti-Virus
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 or programs						◉
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 for all personnel		◉				