

## PCI DSS Compliance with the Snare System

PCI (Payment Card Industry) is a set of security requirements issued by the Payment Card Industry Security Standard Council. In very general terms, it is the joint effort of the Payment Card brands (VISA, MasterCard, American Express, Discover) to reduce the risk of payment/credit card fraud by protecting the areas within an organization that stores, processes, or transmits cardholder data in addition to requiring confirmation of the safeguards put in place.

### Tackling PCI DSS

The SNARE System, is a comprehensive Event Log Management toolkit, designed to collect and report on activities from within your network. Its ability to collect from a wide variety of computing devices and operating systems makes this a powerful tool for Auditing and Reporting. There are 12 requirements for PCI DSS, and although SNARE is designed specifically for Requirement 10 (Track and Monitor all access to network resources and cardholder data), it can be a complimentary tool to ensure compliance with a variety of the requirements, including the necessity for passwords to be changed on a regular basis, authentication mechanisms, tracking access to sensitive information, and much more.

The SNARE System addresses requirement 10, as briefly described below, for more detailed information, contact your SNARE representative.

Section	Description	How SNARE Can Help
10.1	<p>Establish a process for linking all access to system components (especially done with administrative privileges such as root) to each individual user.</p> <p><i>(Verify through observation and interviewing the system administrator that audit trails are enabled and active for system components)</i></p>	<p>When the SNARE Agents are installed on the individual host devices, they will by default, enable the auditing process. When configured, the events will then be sent to the SNARE Server which can be confirmed via the latest events in the web interface or via the SNARE Server web console.</p> <p>For devices such as firewalls, routers, etc, the events can be forwarded via remote syslog UDP to the SNARE Server. This can be confirmed by accessing the web interface of the SNARE Server, and confirming receipt of the system log files.</p> <p>With the SNARE Health Checker, this can be configured to provide reports on Agents that have not sent information, which can then be investigated further, either through the Web Console of the SNARE Server or on the host device(s).</p>
10.2	Implement automated audit trails for all system components to reconstruct the following events:	
10.2.1	<p>All individual access to cardholder data.</p> <p><i>(Verify all individual access to cardholder data is logged)</i></p>	<p>With the Enterprise SNARE Agents, you can define specific directories or files as areas where more detailed tracking is required, such as areas where cardholder data is held or financial information. If an individual attempts to access (success and failure) that information the event log is forwarded to the SNARE Server.</p>

**Contact Us:**  
 Symtrex Inc.  
 264 Jane Street  
 Toronto, Ontario  
 Canada M6S 3Z2  
 416.769.3000 ph.  
 866.431.8972 Toll Free  
 416.769.4477 fax  
 snaresales@symtrex.com  
 www.symtrex.com  
 www.snare-server.com



*Who's Watching Your Network?*

Section	Description	How SNARE Can Help
10.2.2	All actions taken by any individual with root or administrative privileges. <i>(Verify actions taken by any individual with root or administrative privileges is logged)</i>	All agents are preconfigured to monitor login/logoffs of their systems, all *nix based SU logins are automatically forwarded to the SNARE Server. The SNARE Server will pull the information from the Windows Systems on Administrative privileges. Additionally, the SNARE Server will monitor changes to sensitive users and groups by pulling the information from the Enterprise SNARE Agents.
10.2.3	Access to all audit trails. <i>(Verify access to all audit trails are logged)</i>	SNARE will track anyone accessing/modifying/deleting audit trails on their individual host systems, as well as changes to the Audit policy, plus SNARE will monitor access to the Server itself.
10.2.4	Invalid Logical access attempts. <i>(Verify invalid logical access attempts are logged)</i>	SNARE by default tracks all logins and logoff attempts, including failed logins.
10.2.5	Use of identification and authentication mechanisms. <i>(Verify use of identification and authentication mechanisms is logged)</i>	The SNARE Server will pull the information on users and groups (local and domain), and then will report on such items as password expiry, account password age, account login age, plus any attempts made by individual users to change their access privileges.
10.2.6	Initialization of the audit logs. <i>(Verify initialization of audit logs is logged)</i>	When SNARE Agents are added to the host devices, they will initiate the audit log (as per item 10.1 above). Please refer to 10.1 above
10.2.6	Creation and deletion of System-level objects. <i>(Verify creation and deletion of system level objects are logged)</i>	A system-level object is anything on a computer system required for its operation, including but not limited to application executable and configuration files, system configuration files, static and shared libraries & DLL's, system executables, device drivers and device configuration files and all 3rd party components added to make machine provide any of its' services. The SNARE Agents will recorded any creation/deletion within the host system. The SNARE Server will monitor any changes to the registry of the host system, with the Windows Registry change watcher.
10.3	Record at least the following audit trail entries for all system components for each event.	
10.3.1	User Identification. <i>(Verify user identification is included in log entries)</i>	Using the SNARE Enterprise Agent for Windows, the following information is captured and forwarded to the SNARE Server for analysis: DATE: 2009-01-19 TIME: 10:15:47 SYSTEM: mymachine.snare-server.local TABLE: WinSecurity EVENTCOUNT: 2126 EVENTID: 593 (A process has exited) SOURCE: Security USERNAME: mymachine USERTYPE: User RETURNCODE: Success Audit DATA-STRINGS: A process has exited: Process ID: 4028 Image File Name: :\WINDOWS\system32\rundll32.exe User Name: mymachine Domain: snare-server Logon ID: (0x0,0xE0BC7) FILENAME -
10.3.2	Type of Event. <i>(Verify Type of event is included in log entries)</i>	
10.3.3	Date and Time. <i>(Verify date and time stamp is included in log entries)</i>	
10.3.4	Success or failure indication. <i>(Verify success or failure indication is included in log entries)</i>	
10.3.5	Origination of event. <i>(Verify origination of event is included in log entries)</i>	
10.3.6	Identify or name of affected data, system component or resource. <i>(Verify identity or name of affected data, system component or resources is included in log entries)</i>	

**Contact Us:**  
**Symtrex Inc.**  
 264 Jane Street  
 Toronto, Ontario  
 Canada M6S 3Z2  
 416.769.3000 ph.  
 866.431.8972 Toll Free  
 416.769.4477 fax  
[snaresales@symtrex.com](mailto:snaresales@symtrex.com)  
[www.symtrex.com](http://www.symtrex.com)  
[www.snare-server.com](http://www.snare-server.com)



*Who's Watching Your Network?*

Section	Description	How SNARE Can Help
10.4	Synchronize all critical system clocks and times. Obtain and review the process for acquiring and distributing the correct time within the organization, as well as the time-related system parameters settings for a sample of system components. Verify the following is included in the process and implemented:	
10.4a	Verify that a known, stable version of NTP (Network Time Protocol) or similar technology, kept current per PCI DSS Requirements 6.1 and 6.2 is used for time synchronization.	The SNARE Server has to be synchronized to either Stratum 1 or Stratum 2 clocks (NTP Server Clocks) that your host systems are synchronized to. The SNARE Server will check with the NTP service to ensure that the Date and Time are accurate, every 24 hours.
10.4b	Verify that internal servers are not all receiving time signals from external sources.	
10.4.c	Verify that specific external hosts are designated from which the timeservers will accept NTP time updates.	
10.5	Secure audit trails so they cannot be altered. <i>(Interview system administrators and examine permissions to verify that audit trails are secure so that they cannot be altered)</i>	The SNARE Server log files are stored in a compressed text file format, with permissions of write once, and read only. Within the SNARE Serve there is also an integrity check on the files to verify the data within the SNARE Server which can be run daily. The MD5 Checksum can be downloaded and verified to ensure integrity of the data store.
10.5.1	Limit viewing of audit trails to those with job-related need. <i>(Verify that only individual who have a job –related need can view audit trail files)</i>	When the SNARE Server is configured, groups and users are setup to permit viewing of the log data, reports are sent to only those that are required to view the information.  The use of Active Directory or LDAP for user and group authentication can also be utilized.  SNARE is not designed to allow external access for technical support or updates.
10.5.2	Protect audit trail files from unauthorized modifications. <i>(Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation and / or network segregation)</i>	The SNARE Logs are held in a write once and read only directory. As above, the user of Active Directory or LDAP as an authentication mechanism can be used for who can run reports, perform archiving, etc.  The SNARE Server should not be exposed to an external IP address limiting the access.  SNARE has a data store integrity check that can be run on a daily basis (as above).
10.5.3	Promptly backup audit trail files to a centralized log server or media that is difficult to alter. <i>(Verify that current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter)</i>	The SNARE Agents send the event logs in near real time fashion, leaving a copy of the event logs on the host system. System log files that are sent to the SNARE Server are also received in prompt manner. As stated above it is difficult to alter the media once received.  This can be verified by reviewing the real time monitor on the SNARE Server.
10.5.4	Write logs for external facing technologies onto a log server on the internal LAN. <i>(Verify that logs for external facing technologies are offloaded or copied onto a secure centralized internal log server or media)</i>	The Enterprise Agents will address this with the Epilog Agents (TCP enabled) and system log files, which will send the events to the SNARE Server. In those instances where there is not a connection, ie remote destinations, a batch and forward technology can be incorporated through the use of the Enterprise Agents.

**Contact Us:**  
**Symtrex Inc.**  
 264 Jane Street  
 Toronto, Ontario  
 Canada M6S 3Z2  
 416.769.3000 ph.  
 866.431.8972 Toll Free  
 416.769.4477 fax  
[snaresales@symtrex.com](mailto:snaresales@symtrex.com)  
[www.symtrex.com](http://www.symtrex.com)  
[www.snare-server.com](http://www.snare-server.com)



**Who's Watching Your Network?**

Section	Description	How SNARE Can Help
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generated alerts. <i>(Verify the use of file-integrity monitoring or change detection software for logs by examining system settings and monitored files and results from monitoring activities)</i>	Using the MD5 Checksums on the integrity check of the data store, one can verify that the logs have not been altered.
10.6	Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like IDS and authentic authentication, authorization and accounting protocol. <i>(Obtain and examine security policies and procedures to verify that they include procedures to review security logs at least daily and that follow-up to exceptions is required and Through observation and interviews, verify that regular log reviews are performed for all system components)</i>	The SNARE Server can be setup to send email reports on a daily basis for all security relevant systems, based on the objectives that you have deemed critical, these can be sent to one or multiple staff within an organization. On those systems more critical, hourly reports can be setup.
10.7	Retain audit trail history at least one year, with a minimum of three months immediately available for analysis. <i>(Verify and examine security policies and procedures and verify that they include audit log retention policies and require audit log retention for at least one year and verify that audit logs are available for at least one year and processes are in place to restore at least the last three months logs for immediate analysis)</i>	Due to the compression ratio of the data store, the SNARE Server can store, at minimum, 3 months worth of data on a single server. With the SNARE 200 and SNARE 600, a forensics license is included (software) whereby you can import data quickly for analysis on an as needed basis going back to the initial implementation of the SNARE Server. Data can be stored on CD/DVDs or can be archived to a SANS/NAS device for more comprehensive storage.

## Snare Server Models & Hardware Specifications

**SNARE-50** SNARE Server 50 permits the collection of up to 50 devices \* (SNARE Agents and System Log Files).

**SNARE-200** SNARE Server 200 permits the collection of up to 200 devices \* (SNARE Agents and System Log Files). This model also includes the Enterprise Agent and a SNARE Server forensics license.

**SNARE-600** SNARE Server 600 permits collection of up to 600 devices \* (SNARE Agents and System Log Files). This model includes Enterprise Agents and a SNARE Server forensics license

\* Collection from additional devices over the base limit can be purchased.

Software only pricing is also available.

### Snare Server Hardware Models (50, 200 & 600) Include:

- IPC Case 2 U Compact ATX 3 Slot
- Seasonic 2U 460ATX Power Supply
- Intel P4 MB uATX, DG965WH V/L/A
- Intel Core 2 Duo E6320 (1.86 Ghz, 4MB)
- Sony DVD Recorder
- WD 250gb SATA 7.2k rpm, Hard Drives (Quantity 3)
- 1 GB DDR2-667 Memory (Quantity 4)
- Triple PCI Relocation 2U Riser Card Mtg
- 3Ware 9500S - 4LP

### Minimum Snare Server Requirement:

- An x86 compatible CPU (eg: Pentium 4, AMD, AMD64) running at a processing capacity equivalent to, or better than a Pentium 4 - 3Ghz
- 300GB hard disk or greater. Disk may be IDE, SCSI or SATA. The disk should either be one physical disk, or should appear as a single disk to the operating system, via a hardware RAID controller. Software RAID is not supported
- 4 Gb RAM
- A 100 megabit, or (preferably) a 1000 megabit (1 Gigabit) network card
- In general, the Snare Server operates on a hardened version of the 'Ubuntu Feisty' distribution of Linux

**Contact Us:**  
**Symtrex Inc.**  
 264 Jane Street  
 Toronto, Ontario  
 Canada M6S 3Z2  
 416.769.3000 ph.  
 866.431.8972 Toll Free  
 416.769.4477 fax  
[snaresales@symtrex.com](mailto:snaresales@symtrex.com)  
[www.symtrex.com](http://www.symtrex.com)  
[www.snare-server.com](http://www.snare-server.com)



*Who's Watching Your Network?*