

SolarWinds Security Information Management in the Payment Card Industry: Using SolarWinds Log & Event Manager (LEM) to Meet PCI Requirements

Eric Siebert
Author and vExpert

SolarWinds Security Information Management in the Payment Card Industry: Using SolarWinds LEM to Meet PCI Requirements

The Challenge of PCI Compliance

Today, more than a billion people around the world use payment cards to support commercial transactions. The use of these payment cards represents an enormous opportunity for businesses to increase sales at the counter as well as through rapidly expanding channels such as online shopping.

However, the information associated with these payment cards - commonly referred to as "cardholder data" - is the focus of a growing number of identity theft activities.

To address the need to improve payment card security, the card industry has created a set of global requirements called the Payment Card Industry (PCI) Data Security Standard (DDS). Basically, PCI is a set of 12 data-centric control objectives and associated requirements for ensuring the security and privacy of cardholder data. All 12 requirements must be met for compliance, and the penalties for non-compliance are severe.

Compliance with Security Information and Event Management (SIEM)

A SIEM can give you deep visibility into data generated by devices across networks, platforms and environments. SolarWinds LEM acts as a central collection point for device data, automatically aggregating and then normalizing this data into a consistent format. Data normalization, in turn, supports correlation - so anomalies and security threats can be easily and quickly identified. Other advantages with SIEM technologies can include automated responses to suspicious events, as well as advanced reporting functionality.

Simply deploying a security solution cannot guarantee that you will meet every PCI requirement in full. However, SIEM provides the data, visibility, log management, end-point security and active response required to demonstrate PCI compliance.

In short, SIEM can help you meet your PCI auditing requirements through increased visibility, security and control over consolidated data. With SolarWinds LEM in particular, you can take advantage of the following capabilities.

Enhanced Security

- Full 24x7 network security coverage, from the perimeter to the desktop, even with limited IT staff and minimal budget
- Real-time log collection and encrypted agent communication that ensures chain of custody and data integrity
- Real-time event analysis and correlation
- USB detection and prevention
- Bundled Snort® Intrusion Detection System (IDS)

Comprehensive Automation

- Automated remediation that actively responds to defend your network

- Automated notification of network security events to the SolarWinds LEM Console, email, cell phone, pager or handheld device
- Automated filtering, aggregation and normalization of network device logs

Ease of Use and Ownership

- Rapid deployment of the appliance, with no network downtime
- Over 700 correlations, prebuilt with rules specific to PCI compliance
- Over 300 reports to meet the increasing demand of auditors and regulatory compliance
- Usable and affordable - designed and priced for the mid-market

How SolarWinds LEM addresses PCI Requirements

In the following pages, we will discuss each of the 12 requirements of PCI and how SolarWinds LEM can help you meet these requirements in an efficient, cost-effective manner.

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

This requirement is designed to clearly separate the outside world from sensitive areas of the network. To achieve that objective, a firewall must be deployed and also properly configured. Once it is configured, and subsequent access to that configuration must be carefully monitored.

SolarWinds LEM supports Requirement 1.1.9, which stipulates that logs must be monitored for changes that are generated by the firewall. The SolarWinds LEM change management correlation rules will capture, in real-time, any attempts to change the firewall configuration - whether successful or not. Appropriate notifications or responses can be initiated.

Requirement 1.3.7 states that any traffic from an untrusted environment must be denied unless it is explicitly allowed. To support compliance, you can configure access control lists (ACLs) and add access monitoring and control rules to your SolarWinds LEM rules arsenal. SolarWinds LEM also enables you to block an offending IP address at the firewall if it has violated your ACLs or rules.

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

SolarWinds LEM can help you prove that you are enforcing your password policies by tracking and reporting any changes made to a user password and changes made to the properties of a user account such as group membership. SolarWinds LEM comes with an extensive set of change management rules and reports designed specifically to help you detect and track system access and configuration changes - events that are often linked to privilege escalation or insider abuse.

This section also requires that all remote or "non-console" communications are encrypted. SolarWinds LEM can help enforce this policy by monitoring IDS events for communication attempts to remote servers or devices that use non-secure protocols, such as TFTP or telnet.

Requirement 3: Protect stored cardholder data

Merchants must protect cardholder data stored by their point-of-sale (POS) applications and databases. SolarWinds LEM database auditors can help you detect attempts to access the database by unauthorized users, changes made to the database configuration itself, errors and other security-related events. When data is stored in flat files, SolarWinds LEM can work with the native file auditing capabilities of the operating system to monitor access to these critical files. SolarWinds LEM also includes default rules to monitor excessive file "touches" to a critical file or directory, as well as unauthorized access attempts and attempts to delete a file. In addition, the bundled Snort IDS can be configured to "sniff" the wire and look for Primary Account Number (PAN) data patterns, alerting you if anomalies are found.

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

SolarWinds LEM can monitor devices that transmit data across secure channels such as virtual private networks (VPNs) to identify errors, unauthorized access attempts or configuration changes. Communication attempts to the VPN from an unauthorized source can also be monitored, with the offending IP blocked if required.

Wireless communications can be especially vulnerable to security breaches, due to eavesdropping or “trusted” addresses acquired illegally by rogue devices. SolarWinds can monitor the logs produced by your wireless access points and look for rogue devices or unauthorized user attempts. As with Requirement 3, the bundled Snort IDS can be configured to sniff incoming and outgoing traffic to ensure that no PAN data is being transmitted in clear text.

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

SolarWinds LEM can help you monitor all aspects of your antivirus infrastructure. By monitoring the services and processes that start and stop on your servers and workstations, SolarWinds LEM can immediately alert you—and even attempt to restart the service—if a critical service like antivirus protection stops unexpectedly. Built-in reports help you prove to your auditors that you are upholding your update procedures and remaining compliant.

In addition, SolarWinds LEM can help you sort through the mountain of data produced by an antivirus application. For example, it can notify you if a virus is detected but left in a renamed or quarantined state, which could leave your network in jeopardy. SolarWinds LEM will also disable relevant networking or even shut down the offending source machine to prevent the attack from spreading.

Requirement 6: Develop and maintain secure systems and applications

SolarWinds LEM can help with maintenance through integration with patch management products like PatchLink™ from Lumension Security™, alerting you when an un-patched system has been detected. Similarly, vulnerability assessment products such as Nessus™ can report vulnerable systems to the SolarWinds LEM, which then alerts you or allows you to run regular reports to verify that these systems are being patched, updated, or hardened. SolarWinds LEM also has built-in rules to detect events such as cross-site scripting attacks.

Compliance also requires that unauthorized changes to the configuration are not made after a system is in production. With SolarWinds, all changes to users, groups, machines, policy and configurations can be monitored to alert you if a new user has been added to the domain, a critical group has been changed, or a policy has been altered on a system that contains sensitive data.

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

Access restrictions for stored cardholder data are usually based on permissions set at the database, user or file level. SolarWinds LEM can monitor the database itself for unauthorized access attempts, errors, and changes. For access restricted at the user level, SolarWinds LEM has built-in rules to monitor occurrences and automatically alert you if changes occur. In addition, an appropriate action can be taken, such as disabling the offending user account.

At the file level, SolarWinds LEM can work with the operating system’s native file auditing to monitor access for files that contain sensitive data and system files where manipulation could result in a compromised system. SolarWinds LEM’s out-of-the-box rules can monitor access to these files on a strictly need-to-know basis and automatically disable the accounts if users access a file unnecessarily.

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

According to the requirement, organizations must ensure that group, shared, or generic accounts

and passwords are not used for abuse or to “mask” the activity of a particular user. In Microsoft® Windows®, these accounts include the administrator and guest accounts. SolarWinds LEM can detect attempts to authenticate these accounts and then disable the offending source machine.

SolarWinds LEM can also monitor unique account usage to detect insider abuse and suspicious logon attempts outside of the normal operating hours of a particular user. Associated rules can track the source or location, the time a logon occurred and the specific account that was used, as well as trigger notifications and automated responses.

Requirement 9: Restrict physical access to cardholder data

This requirement deals mainly with physically securing and managing data - always the first step to securing network assets. In many cases, users are authenticated not only on the network but also by some physical device, like a token card. SolarWinds LEM can use the data from these devices to help report on physical security anomalies as well.

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

This is by no means the only PCI requirement that a SIM can assist in monitoring, but it is the most comprehensively covered by SIM technology. SolarWinds LEM addresses each of the following categories.

10.1 Establish a process for linking all access to each individual user

SolarWinds LEM collects and consolidates logs from all of the systems in your network into one location. It also provides cross-device, cross-event correlation facilities to link identity, source, application and a variety of related details into an enterprise-wide view of network and user activity.

10.2 Implement automated audit trails to reconstruct specific system and user events

The SolarWinds LEM console, event exploration tools and associated reports combine to provide a comprehensive picture of system and user events. A best-practice implementation is to build console filters and associated rules specifically to monitor privileged or high value accounts. This makes it easy to “watch the watcher” and ensure that privileged users are accessing only authorized data and for legitimate business purposes.

10.3 Record specific audit trail entries

SolarWinds LEM collects the data from many different devices in you network and stores then in a central database, noting the time the event occurred, where it originated, the type of event, the user (where applicable) and any further details that the logging device is able to provide.

10.4 Synchronize all critical system clocks and time

Though SolarWinds LEM itself is not a time server, it can notify you when time synchronization has occurred, thus alerting you to potential discrepancies in your log data.

10.5 Secure audit trails so they cannot be altered

SolarWinds LEM’s agent helps ensure chain of custody by collecting data directly from the operating system in real-time and then immediately encrypting it and sending it to the central database for storage. This virtually eliminates the risks associated with agent-less and polling systems where data can be altered or even simply deleted before it can be collected.

10.6 Review logs daily, especially for servers/devices that perform security functions

While daily log analysis is the minimum requirement, SolarWinds LEM provides continuous, real-time, analysis. When anomalies are detected according to rules you have configured, SolarWinds LEM generates notifications, creates incidents, and can even be configured to respond automatically. By automating the analysis of literally millions of log events per day, SolarWinds allows you to focus on the events of interest that may require additional investigation or remediation.

10.7 Retain audit trail history for a minimum of one year, with 3 months of online data

SolarWinds LEM provides a variety of storage models that meet or exceed the PCI requirements for both online and historical data retention. This data can also be supplemented by regular archives of the data and scheduled/stored reports.

Requirement 11: Regularly test security systems and processes

SolarWinds LEM can help you provide a full audit trail for system vulnerability tests, along with proof that these tests occur as required.

Requirement 11 also specifies the use of an IDS. SolarWinds LEM comes bundled with a fully configured version of Snort IDS to help you meet this requirement and provide a more signature-based, packet-level analysis of attack patterns.

In addition, SolarWinds LEM integrates with host-based IDS products such as Tripwire to detect host-level changes to particularly critical files and provide an alert on these events. It also correlates them with other potentially suspicious events on the network.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

SolarWinds LEM can automatically disable an account, whether vendor or employee, if the account is correlated with suspicious activity. An example could be when the account is used to login outside of normal business hours or a defined time frame or from an unauthorized machine or location.

Requirement 12.5 dictates that security information must be analyzed and controlled, and that incidents must be responded to in a timely fashion. SolarWinds LEM has the most extensive suite of active responses available in the industry, allowing you not only to build rules to monitor your security events but also to automatically respond to them when necessary.

In much the same way, Requirement 12.9 dictates that an incident response plan must be in place and that designated staff must be available 24/7 to respond to security events. SolarWinds LEM can issue a variety of notifications to alert IT staff or company executives to a critical issue, and it can respond automatically to specified events - according to PCI requirements and corporate security policies - even when security staff is not present.

Summary

In today's marketplace, payment cards represent both tremendous opportunities for businesses and significant threats to the data stored on payment cards and in accounts. PCI requirements are designed to ensure the security and privacy of cardholder data in these complex and diverse environments.

SolarWinds LEM can help deliver and demonstrate compliance for all 12 PCI requirements, combining real-time log management, event correlation and endpoint security with a unique active-response technology. The result is a powerful, flexible and cost-effective solution that supports compliance while delivering unprecedented network visibility, security and control.

About the Author

Eric Siebert is an IT industry veteran, author and blogger with more than 25 years of experience, most recently specializing in server administration and virtualization.

Siebert has published books, including his most recent, Maximum vSphere from Pearson Publishing and has authored training videos in the Train Signal Pro series. He also maintains his own VMware information web site, vSphere-land.com, and is a regular blogger and feature article contributor on TechTarget's SearchServerVirtualization and SearchVMware web sites. Siebert has presented at VMworld in 2008 and 2010 and has been recognized as a vExpert by VMware in 2009 and 2010.

About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds online user community, <http://thwack.com>, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company's products. Learn more today at <http://solarwinds.com>.

For additional information, please contact SolarWinds at 866.530.8100 or e-mail sales@solarwinds.com. To locate an international reseller near you, visit http://www.solarwinds.com/partners/reseller_locator.aspx

Did you like this white paper? Tweet about it.  <http://www.twitter.com>