Be Audit-Ready for PCI DSS 3.0 Compliance by Monitoring Log Data and Critical Files in Real Time

By Joel John Fernandes, Senior Product Marketing Analyst, ManageEngine

PCI DSS 3.0 compliance has gained worldwide acceptance by card service providers — card issuers, banks and merchants — that plan to protect their customers' cardholder data from being misused. PCI DSS 3.0 has 12 security requirements concerning the protection of cardholder data. All businesses that accept, store, process or transmit customers' card data either online or offline have to adhere to those requirements.

PCI DSS requirements 10 and 11.5 are considered to be the most challenging to fulfill for securing and protecting customers' payment card data from threats. Below are the descriptions for requirements 10 and 11.5 as found on the PCI Security Standards Council web site.

> ***Requirement 10**: Track and monitor all access to network resources and cardholder data. Logging mechanisms and the ability to track user activities are critical in preventing, detecting or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.*

> ***Requirement 11.5**: Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.*

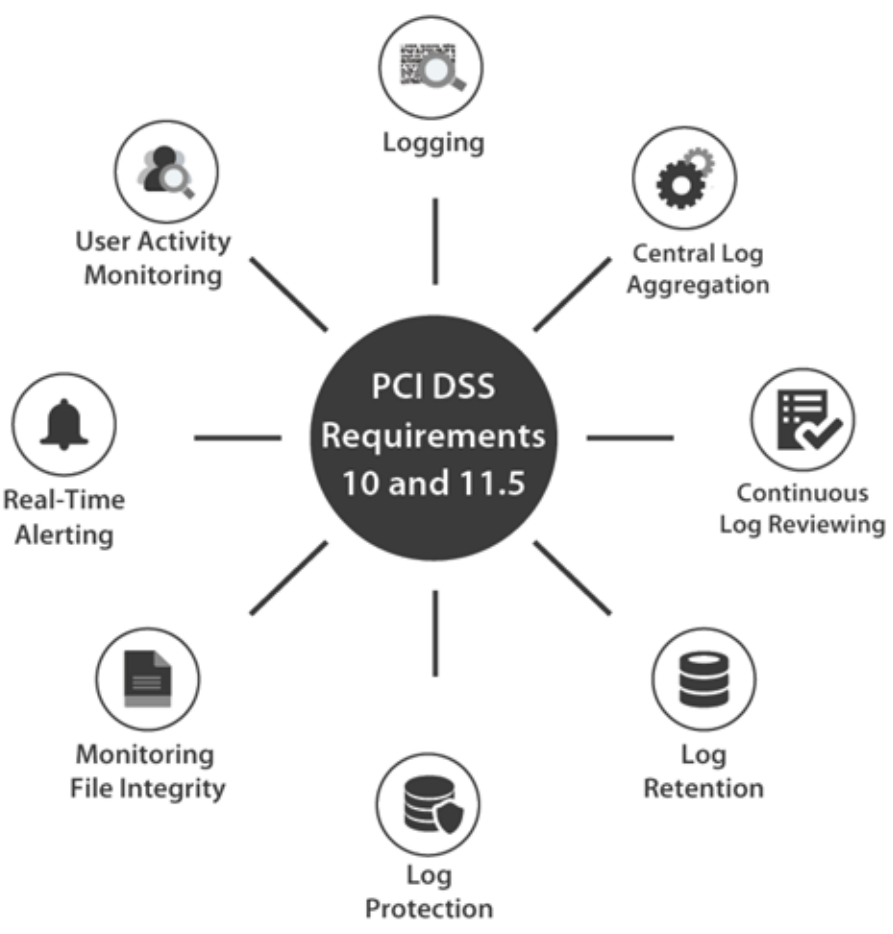
PCI DSS requirement 10 pushes enterprises to gain security intelligence to know the "who, what, where and when" of users accessing the network resources and cardholder data, whereas PCI DSS requirement 11.5 focuses on the protection of critical files from unauthorized access. In simple terms, PCI DSS requirements 10 and 11.5 are put in place so that enterprises can easily analyze the complete user audit trail to identify:

- Who is logging into their systems
- When they logged into the systems
- What activities they carried out on the systems
- Whether they accessed system files and other network resources

To meet PCI DSS requirements 10 and 11.5, the log data generated by the network systems has to be collected at a central place and monitored in real time to track all anomalous activities happening on the network. IT environments consist of heterogeneous network devices, systems and applications that generate a huge amount of log entries every day. Manually monitoring log entries and critical files is impossible given the sheer volume of data that is generated on a daily basis. Automation is the only solution to fulfill PCI DSS requirements 10 and 11.5.

Log Data and File Monitoring Automation Framework

Let us now discuss the log data and file monitoring automation framework that businesses can implement to comply with PCI DSS requirements 10 and 11.5, thereby securing cardholder data and mitigating payment card fraud.



1. **Logging**
   Identifying the network devices and systems that will be used to store, process and transmit card data information is the first step to attaining PCI DSS compliance. Logging should be enabled for all network systems and devices that fall in the scope of PCI DSS, thereby

allowing the IT security professionals to track and monitor all access to network resources and cardholder data. Relevant log information that is needed to comply with the PCI DSS requirements has to be enabled on all systems that fall in the scope of PCI DSS.

2. **Central Log Aggregation**
   PCI DSS compliance requires enterprises to collect log data from network systems at a centralized place for effective reporting, security and analysis. IT security managers should have a universal log collection tool that can aggregate logs from heterogeneous sources — including Windows systems, Unix/Linux systems, applications, databases, routers and switches — at a central location.

3. **Continuous Log Reviewing**
   Monitoring log data is not a one-time task that will keep you compliant with PCI DSS. IT security professionals should review their log data continuously to detect anomalous security events. Log analysis tools should be deployed so that the actionable security data is presented in graphs and charts on a dashboard. IT security managers should be able to quickly drill down into the data on the dashboard and perform a root cause analysis to identify why a security activity happened.

4. **Log Retention**
   Log data collected from all network systems must be stored for one year, per PCI DSS compliance requirements. Enterprises should archive, in a central repository, all log data generated by network systems, devices and applications within their PCI DSS scope. Archived log data should be easily accessible for forensics investigation, thereby helping security professionals to drill down into the log data and perform root cause analysis to identify the event activity that caused the network problem.

5. **Log Protection**
   PCI DSS compliance mandates protection of log data to avoid tampering and deletion. Enterprises should encrypt the log data files to ensure that the log data is secured for future forensic analysis as well as compliance or internal audits. Hashing and time stamping can also be used to secure the log data and make it tamperproof. Log data can also be protected by using file integrity monitoring (FIM) solutions, as discussed in the next point.

6. **Monitoring File Integrity**
   PCI DSS compliance dictates that enterprises use change-detection mechanisms such as file integrity monitoring tools to protect all sensitive data related to customers' payment cards. Security professionals need to centrally track all changes to their files and folders, such as when files and folders are created, accessed, viewed, deleted, modified, renamed and much more. File integrity monitoring tools allow IT security managers to make quick

decisions when critical files are accessed and thereby mitigate the risk of payment card data breaches.

7. **Real-Time Alerting**
   Real-time security alerting is critical for enterprises. IT security professionals should receive alerts as and when network anomalies and suspicious activities occur on the network. Real-time security alerts help IT security professionals respond to critical incidents that can affect their network infrastructure. A delay in responding to critical incidents can lead to a major security catastrophe. Deploying a real-time alerting solution that automatically monitors security events by mining the log data plays a vital role in PCI DSS compliance.

8. **User Activity Monitoring**
   Customers' payment card data can be misused by employees who access the data using brute force attacks or by employees with privileged access. Monitoring user activities in real time across the IT infrastructure can be a painful task without proper user activity monitoring tools. PCI DSS compliance mandates enterprises to audit precise information in real time on critical user activity events such as user logons, user logoffs, failed logons, successful audit logs cleared, audit policy changes, objects accessed and user account changes.

Automating to Ensure Compliance

Compliance with PCI DSS is a must for all businesses that accept card payments because keeping customers' payment card data secure is crucial for the progress of those businesses. PCI DSS compliance can bring enormous benefits to businesses such as a more secure network, higher brand value, improved reputation and lower risk of data breaches. Non-compliance, on the other hand, can have severe consequences.

Monitoring log data and critical files in real time using the automation framework will help businesses to comply with the PCI DSS requirements 10 and 11.5 with ease.

About the Author

Joel John Fernandes is a senior product marketing analyst for ManageEngine, the real-time IT management company. He has thorough knowledge in the log management and security information and event management (SIEM) domain and has consulted on network security and log management for both large and small enterprises. For more information on ManageEngine, a division of Zoho Corporation, please visit www.manageengine.com; follow the company blog at http://blogs.manageengine.com; on Facebook at http://www.facebook.com/ManageEngine and on Twitter at @ManageEngine.