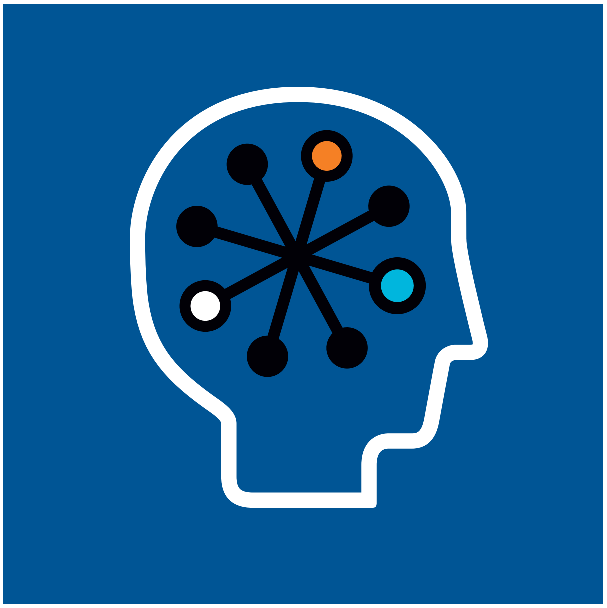

# PCI DSS Log Management Mandates with the HP Compliance Log Warehouse

Solution Brochure

**Overview**

- Collect data from any of your PCI-related log data sources
- Have online access to the entire year of log data required by PCI DSS
- Map reports to PCI DSS requirements for easy compliance
- Deploy with ease and save on time, effort, and money when complying to PCI DSS

To protect businesses, cardholders, and the integrity of the payment system, major credit card providers established audit requirements governing the safekeeping of account information as part of the Payment Card Industry (PCI) Data Security Standard (DSS). Compliance with PCI DSS requires not only deploying several mandated security countermeasures, but also frequent review of safeguards and policies to facilitate their continued effectiveness. The PCI Data Security Standard mandates that merchants, banks, and service providers monitor networks, systems, databases, and applications that use or access credit card information. Log data must be collected, retained, and reviewed on a routine basis—providing data integrity and verifiability.

Considering most businesses generate gigabytes of event log data each day, selecting a log management solution that optimizes the storage and analysis of event log data is paramount. Additionally, being able to identify internal violations and sophisticated threats readily, as well as conduct thorough investigations, is necessary to reduce the risks of sensitive data leakage, and comply with the PCI DSS audit standards.

## Enable efficient audit compliance with a scalable, high-performance solution

Faced with audit deadlines, some IT departments develop in-house technology while others attempt to use a variety of IT management tools designed for other purposes to meet PCI DSS audit objectives. In many cases, however, these efforts have proven to be costly or ineffective due to technical bottlenecks caused by the high volumes of data that are generated on a daily basis. Fortunately, the HP Compliance Log Warehouse (CLW) streamlines PCI event log monitoring and audit processes.

HP Compliance Log Warehouse enables merchants, banks, and service providers to collect, retain and assess terabytes of log data from all sources; resulting in cost-effective, compliant data retention, and timely, actionable analysis, ultimately reducing the risk of sensitive data leakage.

## HP Compliance Log Warehouse features and benefits

- **Data source collection:** Over 180 data sources are supported out-of-the-box using agentless technology. Full log capture and efficient storage are provided to eliminate the need of choosing which data sources to collect and monitor. Both batch and streaming collection is supported, from the network to the mainframe, with field-level parsing (and analysis) of custom log sources such as business applications.
- **Storage and retention:** The foundation of the CLW is a patented, purpose-built, replicated data repository for event log data. With better than 90% compression, this clustered technology scales from one to hundreds of gigabytes per day. There is no problem to keep a minimum one year of data online and queryable. Extended storage integration is also fully queryable so no archiving is required.
- **Analytics and forensics:** CLW comes with pre-defined reports mapped specifically to the PCI DSS standard. Critical events and trends are presented in graphs and table views, and dashboards. Policy exception analysis and forensic investigations can be keyed off for any data field. Reports can be ad hoc or scheduled with electronic delivery; always consistently fast.
- **Deployment:** CLW is an easy-to-deploy appliance that consists of server and storage hardware, operating system and solution software. You can configure CLW to your environment in a matter of minutes.

HP CLW for PCI Compliance enables you to

- Understand who is accessing your cardholder data environment and what privileged users are doing
- Detect anomalies and understand their scope
- Monitor dozens of applications and thousands of systems actively
- Issue alert on activities not in accordance with organizational policy
- Enhance threat mitigation efforts through real-time correlation and long-term trending to see "low and slow" attacks
- Satisfy PCI DSS Requirement 10 to track and monitor network and cardholder data access and also provide evidence of the controls put in place to address the other requirements
- Automate the log collection of all PCI-related log sources down to the cardholder business applications to reduce costs and improve efficiency
- Bank upon patented, purpose-built data repositories that eliminate the costs of database licenses and DBA support
- Acquire minimum of one year's worth of data on-line and queryable reduces the time and cost of ad-hoc queries and investigations
- Eliminate the need to deal with archived data
- Utilize pre-defined PCI analytic and investigate reports to improve the efficiency and effectiveness of your compliance efforts
- Demonstrate the existence of and adherence to PCI-related controls and increase likelihood of successful audit compliance
- Accomplish more with your existing staff

## The value of enterprise security analytics

The HP Compliance Log Warehouse provides a cost-effective solution to managing the high data volumes associated with the event logs from the IT devices and applications that support sensitive consumer transactions. With CLW, customers can meet the relevant PCI DSS requirements and other international privacy standards, while realizing greater productivity, lower operational costs, and more comprehensive results at the same time. They can easily collect and retain event data and consumer specific information generated from transaction-specific events, thereby achieving both compliance and improved corporate governance and control.

Designed for flexibility and performance, CLW is able to efficiently collect and store a wide variety of logs—including remote access and authentication events, data from e-commerce applications, CRM and database information, and firewall and network equipment activity—in a centralized data store. This data store has virtually unlimited scalability, with many customers having 100 terabytes of data under its management.

By leveraging this optimized data storage model, CLW enables organizations to exceed the PCI requirement to retain the log data for 1 year with a minimum of 3 months on-line. CLW gives you the entire year on-line and accessible for queries, trending and investigations. CLW compresses stored event data to as little as 10 percent of its original size and to 2.5 percent of its size if it were stored in an RDBMS-based solution. Since CLW is based on a purpose-built repository with self-optimized storage, organizations can store all the event data they want without outrageous storage and administrative costs, and verify that long-term data retention requirements are met.

CLW enables organizations to meet compliance requirements with not only its pre-defined reports mapped to specific sections of PCI DSS, but also with investigation reports and its ability to create new, customized reports easily. This is a significant advantage, because Requirement 10 makes it clear that it is not enough to simply put the PCI required controls in place and expect that you are done. Rather, these controls need to be monitored and any resulting anomalies need to be investigated.

## HP Financial Services

HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. For more information on these services, contact your local HP representative or visit: **www.hp.com/go/hpfinancialservices**

## For more information

For more information about the HP Compliance Log Warehouse, contact your HP sales representative or visit: **www.hp.com/go/CLW**

### What log data should be captured and retained?

Payment Card Industry (PCI) Data Security Standard (DSS) audit guidelines specify the proper procedures for handling and analyzing the log files associated with credit card processing. Merchants, banks, and service providers must determine which log information they are required to collect, retain and analyze to meet PCI DSS auditing requirements.

Typically, the following types of data must be collected and reviewed:

- Firewalls
- Routers
- Operating Systems
- IDS/IPS
- Web Servers
- Database servers
- DNS Servers
- Encryption
- Storage Devices
- Business applications
- Patch Management systems
- Change Control systems
- Identity and Access Management
- Physical access controls
- Network Vulnerability scanners
- File Integrity
- Log Management software

To learn more, visit www.hp.com/go/clw

4AA1-2725ENW, August 2008

invent

Technology for better business outcomes