

TURNKEY AND AUTOMATED PCI COMPLIANCE

ArcSight PCI Logger is an all-in-one log collection, storage and analysis solution for cost-effective automation of PCI audits and proactive protection of cardholder data.

HP Enterprise Security Product Brief

Ease of Deployment and Management

PCI compliance monitoring is seamless with the self-contained ArcSight PCI Logger solution for log collection, storage and analysis. No database administration expertise is required and a 100 percent web-based interface simplifies deployment and ongoing management by eliminating the need for any client installations.

Self-Managing Log Collection and Storage Repository

ArcSight PCI Logger can automate collection from hundreds of devices and device types that typically comprise a merchant's network, including various firewalls, IDS devices, directories, desktops, servers, mobile networks, handhelds, POS terminals, databases and mainframes or mid-range servers. A wizard-based interface simplifies collection from legacy sources and POS applications.

All aggregated logs are stored on ArcSight PCI Logger in a compressed format. Each instance can store and search 8TB of effective logs, and PCI retention policies are automatically enforced – eliminating the need for manual and error-prone log rotation.

Cost-Effective and Automated Reporting

Most merchants spend countless hours collecting logs and executing manual scripts across disparate log types to generate reports for PCI compliance. ArcSight PCI Logger automates the entire audit through pre-packaged reports that span all PCI DSS requirements. The reports can be easily scheduled and automatically sent in various graphical formats for review.

Proactive Protection of Cardholder Data

Merchants often focus on eliminating the cost and effort associated with manual audit reporting. However, reports can only indicate whether or not compliance was achieved after the fact. ArcSight PCI Logger adds proactive protection for the cardholder network through pre-packaged real-time alerts that deliver continuous visibility into PCI DSS violations. Alerts can be viewed within the live alerting console or can trigger external notification via SNMP, SMTP or syslog.

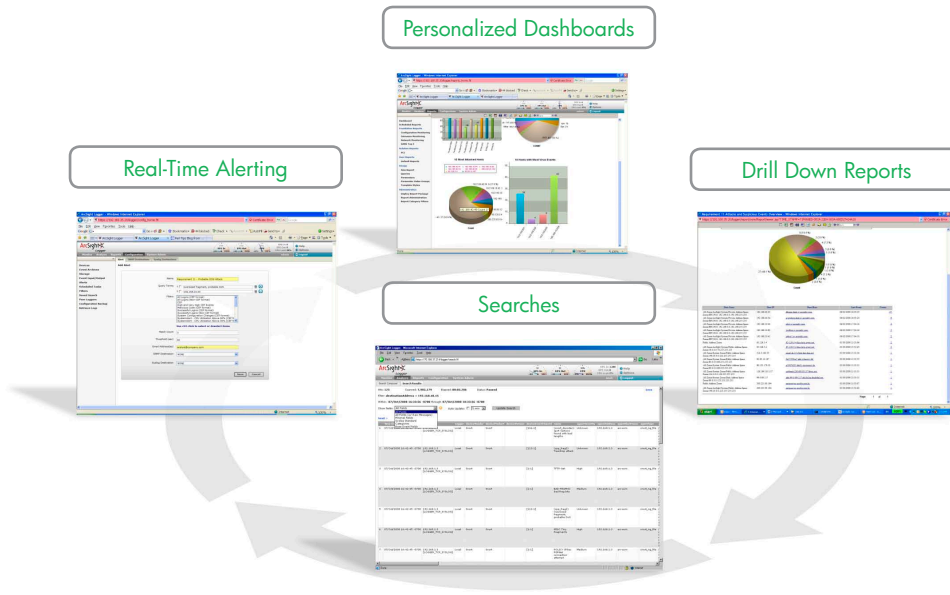
"Forensics on the Fly"

With most other log management solutions, each subsequent step of analysis requires building another report or constructing a new search filter, which is both complex and time consuming. ArcSight PCI Logger eliminates such tedious effort through "forensics on the fly," which enables easy drill down from dashboards through reports, to searches, real-time alerts and base events.

Users are presented with interactive and personalized PCI dashboards that combine relevant PCI reports into a single role-based view. From these aggregate dashboards, users can drill into and across PCI requirement-specific reports and investigate potential violations. Report results can be further analyzed using an intuitive search interface to conduct quick and easy ad hoc investigations for root cause analysis. In turn, the search patterns can be converted into real-time alerts to ensure that subsequent matches lead to instant notification. Finally, users can directly drill down from the alert to underlying events that triggered it.



Figure 1: "Forensics on the Fly." From dashboards to reports and from alerts to base events, "forensics on the fly" enables rapid and intuitive analysis.



Highlights

- Cost-effective PCI log management optimized for Level 2 through Level 4 merchants
- Comprehensive and pre-packaged reporting and alerting across PCI DSS requirements
- "Forensics on the fly" for rapid investigation and simplified analysis

Model	L3200 & L3200-PCI (Appliances)	L30GB with Installed PCI Application (Software)
Management	Web browser, CLI	
Supported Sources	Raw syslog (TCP/UDP), raw file-based logs (FTP, SCP, SFTP) Analysis optimized collection for 300+ commercial products FlexConnector framework for legacy event sources ArcSight Common Event Format (CEF), ArcSight ESM	
OS	Oracle Enterprise Linux 4, 64-bit	Supported OS: Red Hat Enterprise Linux, CentOS and Oracle Enterprise Linux
Compression	Up to 10:1	
Devices	200	
Maximum Input Rate	2,000 events/second	30 GB of logs/day
Local Connector EPS	200	N/A
CPU	1 x Intel Xeon E5504 Quad Core 2.0 GHz	N/A
RAM	12GB	N/A
On-Board Storage	2 x 1TB - RAID 1	N/A
Chassis	1U	N/A
Power	480W - Non-Redundant 100-240 VAC	N/A
Ethernet Interfaces	2 x 10/100/1000	N/A
Dimensions (DxWxH)	24.7" x 17.1" x 1.7"	N/A

Actual performance will depend on factors specific to a user's environment.

© Copyright 2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

All other product and company names may be trademarks or registered trademarks of their respective owners.

ESP-PRB022-082510-02, Created November 2011

