Using the HP Compliance Log Warehouse to Help Meet PCI DSS

August 28, 2008
Hewlett-Packard Company
Speakers Today
August 28, 2008

Steve Scott
Senior Product Marketing Manager
Hewlett Packard

Dan Barahona
Vice President, Business Development
SenSage
Topics for today

- HP Secure Advantage and compliance
- Log data management challenge
- Payment Card Industry Data Security Standard
- HP Compliance Log Warehouse: Overview
- Questions and answers
HP Secure Advantage and compliance
“Security and compliance continues to be a top concern for CIOs as the enterprise has evolved – whether spurred by growth, threats or ongoing regulatory pressure.”

Chris Christiansen
Security analyst, IDC
an industry analyst firm
# Adaptive Infrastructure

## Key enablers

<table>
<thead>
<tr>
<th>Current state</th>
<th>High-cost IT islands</th>
<th>Future state</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Systems &amp; Services</td>
<td>Power &amp; Cooling</td>
<td>Management</td>
</tr>
<tr>
<td>• Scalability based on standards</td>
<td>• Energy-efficient computing</td>
<td>• Unified infrastructure management</td>
</tr>
<tr>
<td>• IT services and support</td>
<td></td>
<td>• Integrated IT and business services management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Scalability based on standards**
- **IT services and support**
- **Energy-efficient computing**
- **Unified infrastructure management**
- **Integrated IT and business services management**
- **HP Secure Advantage**
- **Pro-active, built-in infrastructure and data protection**
- **Compliance validation**
- **Pooling and sharing of IT resources**
- **Dynamic control of IT service delivery**
**HP Secure Advantage**

**From desktop to datacenter, from laptops to printers**

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect resources</strong>&lt;br&gt;By improving availability and protecting your networks, systems, software and DBMS, using trusted platforms</td>
<td><strong>Protect data</strong>&lt;br&gt;In all its forms:&lt;br&gt;Data at rest&lt;br&gt;Data in transit&lt;br&gt;Data in use</td>
<td><strong>Provide validation</strong>&lt;br&gt;Establish a secure audit trail across the organization as proof of compliance for internal and external auditors, with real-time alerts</td>
</tr>
<tr>
<td>Minimize disruptions due to security breaches with a trusted and hardened infrastructure</td>
<td>Use encryption and identity management, in combination with other pro-active security management techniques</td>
<td>Encryption and key management, working with integrated compliance solutions across organization</td>
</tr>
</tbody>
</table>

**Technology**

**People and process**
Compliance... it is everywhere

These are just a few examples as there are over 20,000 compliance requirements worldwide

If your company isn’t directly affected by compliance, think about your suppliers and partners; they may be and may pass down the request directly to you
Log data management challenge
Compliance mandates ask serious questions
The answers are in your logs

• Compliance is growing
  – Industry-specific and cross-industry
  – Government and international
  – Real penalties for non-compliance

• Common goals
  – Manage corporate risk
  – Protect sensitive information
  – Detect potential security threats

• Common requirements
  – Collect and review log data
  – Keep data online for long periods
  – Conduct forensic investigations
Market evolution of log analysis

Intrusion Detection Systems

Event Correlation

Compliance Reporting

Compliance Warehouse

Event Data Warehouse

Network and threat focused
- Visible attacks
- Real time alerting
- Network centric
- Limited data availability
- Security “cockpit”

Process and governance focused
- Sophisticated threats
- Long term analysis
- Application centric
- Massive data analysis
- Log data warehousing
The log data management challenge

• Massive data volumes
  – Daily volumes often exceed 100 GB
• Massive storage requirements
  – 1 year minimum retention for compliance and forensics
• Data comes from myriad sources
  – No standards on log formats
• Multiple analysis requirements:
  – Real-time to identify threats as they happen
  – Over time to detect low-slow threats
  – Forensics and investigations over months of data
Payment Card Industry (PCI) Data Security Standard (DSS)
# Payment Card Industry’s Data Security Standard (PCI DSS)

- **VISA, MasterCard, AMEX, Discover, JCB**
  - Current version 1.1 formed PCI Security Standards Council (SSC)
- **To ensure security of cardholder data**
  - Never store sensitive cardholder authentication data
  - Encrypt cardholder elements or address via compensating controls
- **Compensating controls (App. B)**
  - Specification not met, but related risk has been sufficiently mitigated
- **Requirement 10: collection, retention and analysis of logs**
  - Focus on access to cardholder data

## Build and Maintain a Secure Network

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td>2</td>
<td>Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
</tbody>
</table>

## Protect Cardholder Data

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Protect stored cardholder data</td>
</tr>
<tr>
<td>4</td>
<td>Encrypt transmission of cardholder data across open, public networks</td>
</tr>
</tbody>
</table>

## Maintain a Vulnerability Management Program

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Use and regularly update anti-virus software</td>
</tr>
<tr>
<td>6</td>
<td>Develop and maintain secure systems and applications</td>
</tr>
</tbody>
</table>

## Implement Strong Access Control Measures

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td>8</td>
<td>Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td>9</td>
<td>Restrict physical access to cardholder data</td>
</tr>
</tbody>
</table>

## Regularly Monitor and Test Networks

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td>11</td>
<td>Regularly test security systems and processes</td>
</tr>
</tbody>
</table>

## Maintain an Information Security Policy

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>
 PCI DSS logging requirements

PCI Section 10 – Track/Monitor Access to Network and Cardholder Data

10.1 Trace all IT activity to specific users

10.2 Implement audit trails for the following events:
  10.2.1 All individual user accesses to cardholder data
  10.2.2 All actions taken by any individual with root or admin privileges
  10.2.3 Access to all audit trails
  10.2.4 Invalid logical access attempts
  10.2.5 Use of identification and authentication mechanisms
  10.2.6 Initialization of audit logs
  10.2.7 Creation and deletion of system-level objects

10.3 Record the following audit trail entries for all system components for each event:
  10.3.1 User identification
  10.3.2 Type of event
  10.3.3 Date and time
  10.3.4 Success or failure indication
  10.3.5 Origination of event
  10.3.6 Identity or name of affected data, system component, or resource

10.4 Synchronize all critical system clocks and times

10.5 Secure audit trails so they cannot be altered
  10.5.1 Limit viewing of audit trails to those with a job-related need
  10.5.2 Protect audit trail files from unauthorized modifications
  10.5.3 Promptly back-up audit trail files to a centralized log server
  10.5.4 Copy logs for wireless networks onto a log server on the internal LAN
  10.5.5 Ensure that existing log data cannot be changed without generating alerts

10.6 Review logs for all system components at least daily.
## PCI DSS compliance and log data

<table>
<thead>
<tr>
<th>Section</th>
<th>Log Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Use Firewalls to protect cardholder data</td>
<td><strong>FW logs:</strong> provides proof, identifies areas of non-compliance</td>
</tr>
<tr>
<td>2. Don’t use default passwords or settings</td>
<td><strong>System/device logs:</strong> identifies changes of password/settings</td>
</tr>
<tr>
<td>3. Protect stored cardholder data</td>
<td><strong>Database/Storage/System logs:</strong> shows access to cardholder data</td>
</tr>
<tr>
<td>4. Encrypt transmission of cardholder data</td>
<td><strong>Network logs:</strong> identifies non-encrypted traffic. Log management is ‘compensating control’.</td>
</tr>
<tr>
<td>5. Use anti-virus software</td>
<td><strong>AV logs:</strong> provides proof, identifies areas of non-compliance</td>
</tr>
<tr>
<td>6. Develop secure systems and applications</td>
<td><strong>System/App logs:</strong> allows forensics, trouble shooting, and routine monitoring</td>
</tr>
<tr>
<td>7. Restrict access to cardholder data</td>
<td><strong>Authentication/Database/App logs:</strong> shows who’s accessing cardholder data</td>
</tr>
<tr>
<td>8. Assign unique IDs to users</td>
<td><strong>System/Application logs:</strong> shows ID usage, can identify shared IDs</td>
</tr>
<tr>
<td>9. Restrict physical access to cardholder data</td>
<td><strong>Building/card swipe logs:</strong> shows physical access</td>
</tr>
<tr>
<td>10. Monitor access to cardholder data</td>
<td><strong>Authentication/Database/App logs:</strong> shows who’s accessing cardholder data</td>
</tr>
<tr>
<td>11. Regularly test systems and processes</td>
<td><strong>System/Application/Network logs:</strong> proof, identifies areas of non-compliance</td>
</tr>
<tr>
<td>12. Maintain security policy</td>
<td><strong>Log management</strong> key to overall security policy</td>
</tr>
</tbody>
</table>
PCI: Protecting sensitive data

- Credit card data
- Personally identifiable data
- Transaction data
- Billing information

Data resides in:
- Servers
- Databases
- NonStop systems
- Applications
PCI: Protecting sensitive data

- Step 1: Build a fence
  - Firewalls
  - IDS/IPS
PCI: Protecting sensitive data

- Step 2: Lock the doors
  - Authentication
  - Identity & Access Management
PCI: Protecting sensitive data

- Key insiders bypass all these protections and safeguards

- Employees
- Administrators
- Customer service
- Consultants
- Social engineers
- Vendors
PCI: Protecting sensitive data

- **Step 3: Secure communications**
  - Email
  - Internet – Proxy servers
  - IM
  - Data Loss Prevention (DLP)
  - Policy auditing
PCI: Protecting sensitive data

- Step 4: Secure the infrastructure
  - Web servers
  - Applications servers
  - Server platform
  - Databases
  - Storage
PCI DSS is not about ‘checking the box’

- Checkbox compliance means always playing catch up
  - Buying a new product or solution every time the compliance regulations change
- Log management is a good way to run your business
- If you tackle PCI DSS compliance as a better way to run your business:
  - You not only meet the PCI DSS requirements (checkbox)
  - You also identify, mitigate, respond to threats better, faster, and more proactively
Choice Hotels

• Objective is PCI compliance
  – Need a solution in place ASAP for VISA audit
  – Enable comprehensive forensics and investigations
  – Provide immediate access to years of data

• Technical challenges:
  – Needed solution to grow (log volumes expected to increase)
  – Handle difficult sources
    • Informix database: monitoring the cardholder database access/activity
    • Symark Powerbroker: granular authentication and user activity reporting
    • Windows, Unix, Cisco PIX
  – Retain 1+ years of data online

• 3-node HP CLW solution for PCI compliance
  – Predefined PCI compliance reporting package
  – Fast deployment – in time for upcoming Visa audit
How CLW works
How CLW works

Only 100% solution
- Source support
- Parsing
- Query accuracy

Purpose built
- Clustered, compressed, columnar data
- No DBA, no indices
- Flexible reporting engine

Lowest TCO
CLW log event collection

Over 150 existing log adapters for commercial products

- Supports any log source
  - New custom log adapters easily created
- Agent-less log collection
- Complete log record content
- Able to load historic records
- Support for remote sites
  - Collect and compress data

100% coverage
100% accuracy
100% performance
Powerful and complete pre-packaged Collection and reporting for PCI DSS

Complete PCI Analytics Package

- Consolidates all audit events in one enterprise repository
- Collects from cardholder systems as well as network sources
- Reports can be run ad-hoc or pre-scheduled
- Role-based access supports multiple sites and administrators
- Aggregates events, reporting, and statistics

PCI 1.1 Compliance Analytics

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Restrict Inbound Internet Traffic to IP Addresses Within the DMZ
- Requirement 3.1: Restrict Outbound Firewall Traffic
- Requirement 3.7: Deny Inbound & Outbound Traffic Not Specifically Allowed
- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
  - 8.1: All Users Have Unique User Names
  - 8.5.1: Control Addition, Deletion and Modification of User IDs
  - 8.5.2: Verify User Identity Before Password Resets
  - 8.5.4: Immediately Revoke Access for Terminated Users
  - 8.5.5: Remove Inactive User Accounts
  - 8.5.6: Vendor Accounts During Time Period Needed
  - 8.5.13: Lock Out User IDs After Number of Failed Login Attempts
- Requirement 10: Track and monitor all access to network resources and cardholder data
  - 10.2.1: All Individual User Accesses to Cardholder Data
  - 10.2.2: All Actions Taken by Root or Administrative Privileges
  - 10.2.3: Access to All Audit Trails
  - 10.2.5: Use of Identification and Authentication Mechanisms
  - 10.2.6: Initialization of Audit Logs
  - 10.2.7: Creation and Deletion of System-Level Objects
  - 10.3: Monitor System Component Information
  - 10.5.1: Limit Viewing of Audit Trails
  - 10.5.3: Promptly Back-up Audit Trail Files
  - 10.6: Review Logs for All System Components
Requirement 10.2.1
All individual user accesses to cardholder data

- Monitor access to sensitive files, directories, and file systems
- Use filters to find suspicious activity
- Quickly find out what else happened on that server or by that user
PCI Requirement 8.5.6
What are my insiders doing?

- Automated CLW report shows logins after business hours from various sources
- Identify improper access and immediately investigate
- Unique filtering capability allows quick analysis through thousands of events
HP CLW is a fully integrated appliance for PCI DSS compliance log management

- Simplified provisioning
  - Integrated 2U Integrity server-based appliance
  - Simple, quick installation and configuration
  - Fast Return on Investment
- Solution performance
  - Exceptional scalability
- One source for customer support
HP CLW helps you meet PCI DSS

Compliance & log data management

- Compliance is growing everywhere
- ‘Best Security Practices’
- Log data management challenge

PCI Data Security Standard

- Protect customer credit card information
- Requirement #10 calls out log analysis
- Other answers are in your log data

HP Compliance Log Warehouse

- 100% accurate, fast, & consistent
- Flexible, expandable, and scaleable
- Low TCO and a rapid time to value
Questions and answers
For more information on the HP Compliance Log Warehouse

Contact your HP NonStop sales representative or go to:

- HP Compliance Log Warehouse
  - www.hp.com/go/clw
- HP Secure Advantage
  - www.hp.com/go/security
- Steve Scott
  - Steve.Scott@hp.com
- Dan Barahona
  - Dan.Barahona@sensage.com
Technology for better business outcomes