

Meet VISA PCI Log Management Mandates with Enterprise Security Analytics

SenSage's Enterprise Security Analytics 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.

What log data should be captured and retained?

Payment card industry (PCI) security 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 and retain to meet Visa PCI auditing requirements. Typically, the following types of data must be logged:

- *Inbound and outbound* Internet traffic
- *Internal* network traffic
- *Firewall* events
- *Intrusion detection system events*
- Network and host *activity*
- *Operating system access*, (especially high-level administrative or root access)
- *Application access*, (especially users and objects with write and execute privileges)
 - Database applications
 - eCommerce applications
 - CRM applications

To demonstrate completeness and verifiability, all logs with digital chain-of-custody must be captured and stored.

SenSage Advantages for Visa PCI Audit Requirements

- Consistent log collection, correlation & retention
- Validation and fortification of controls
- Broad source support across the enterprise
- High performance for log capture & analysis
- Empowers IT Security staff to conduct efficient audits and precise investigations

To protect businesses, cardholders and the integrity of the payment system, Visa has established audit requirements governing the safekeeping of account information as part of the Payment Card Industry (PCI) Data Security Standard. This standard requires network monitoring and testing procedures for verification, automation, recording, synchronizing, integrity, daily review, and retention for all audit logs. Log data and their associated audit trails must be collected, stored, monitored and assessed on a routine basis – ensuring data integrity and verifiability at all times. Considering that most retail businesses generate gigabytes of event log data each day, leveraging a log management solution that optimizes the storage and analysis of event log data is paramount. Additionally, being able to readily identify internal violations and sophisticated threats, as well as conduct thorough investigations is necessary to reduce the risks to sensitive data leakage, and support the PCI audit standards.

Compliance with Visa PCI requires not only deploying several mandated security countermeasures, but also frequent review of safeguards and policies to ensure their continued effectiveness. The Visa PCI standard mandates that merchants, banks and service providers implement network monitoring and testing procedures for verification, automation, recording, synchronizing, integrity, daily review, and retention for all audit logs. Log data and the associated audit trails must be collected, retained and reviewed on a routine basis – ensuring data integrity and verifiability.

Enabling Efficient Compliance Audit with a Scalable, High Performance Solution

Faced with audit deadlines, some IT departments have developed in-house technology, while others have attempted to use a variety of IT management tools to meet PCI audit objectives. However in many cases, such 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, SenSage Enterprise Security Analytics streamlines PCI event log monitoring and audit processes.

The Value of Enterprise Security Analytics

SenSage Enterprise Security Analytics provides a cost-effective solution to manage high-volume event log information related to the infrastructure supporting sensitive consumer transactions. SenSage customers are meeting the PCI requirements as well as international privacy standards, while at the same time realizing greater productivity, lower operational costs and more comprehensive results. They are able to easily collect and retain comprehensive consumer-relevant event data generated from transaction-specific events and consumer private information, thereby achieving both compliance and improved corporate governance and control.

Designed for flexibility and performance, SenSage is able to efficiently collect and store a wide variety of logs—including remote access and authentication events from retail stores, data from e-commerce applications, CRM and database information, and firewall and network equipment activity—in a centralized data store, even if multiple gigabytes or even terabytes of data are generated daily. In fact, SenSage can support over 170 log source types, including homegrown and proprietary applications.

By leveraging an optimized data storage model, SenSage enables organizations to satisfy long-term data retention requirements – *data is accessible for multiple years*. SenSage can compress stored event data to as little as 10 percent of the original, raw, event-log data, and 2.5 percent the size of that stored using an RDBMS-based solution. Since SenSage is based on a purpose-built repository with self-optimized storage, users can store all their event data without outrageous storage and administrative costs, and ensure that long-term data retention requirements are met.

SenSage enables organizations to meet compliance requirements with both pre-defined and customized reports as part of its out-of-the-box solution. This is a significant advantage, since our customizable query and reporting capabilities augment pre-defined report packages, and accelerate compliance and facilitate investigations.

Visa has instituted the Cardholder Information Security Program (CISP) with the PCI standard as its framework. Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring that merchants, banks and service providers maintain the highest standard of information security possible.

See http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

SenSage specifically satisfies Visa PCI Requirement 10: *“Track and monitor all access to network resources and cardholder data.”*

As described in that section, *“Logging mechanisms and the ability to track user activities are critical.*

The presence of logs in all environments allows thorough tracking and analysis when something does go wrong.

Determining the cause of a compromise is extremely difficult without system activity logs.”

Requirements	Testing Procedures Addressed by SenSage
10.1 Establish a process for linking all access to system components (especially those with administrative privileges such as root) to an individual user.	10.1 Verify, via observation and inquiry of the system administrator, that audit trails are enabled and active, including for any connected wireless networks.
10.2 Implement automated audit trails to reconstruct the following events, for all system components:	10.2 Confirm through inquiry, review of audit logs, and review of audit log settings for (insert as-of dates) for the samples of (insert number and/or description of sample) system components, that the following events are logged:
10.2.1 All individual accesses to cardholder data	10.2.1 Logging of access to cardholder data
10.2.2 All actions taken by any individual with root or administrative privileges.	10.2.2 Logging of actions taken by any individual with root or administrative privileges
10.2.3 Access to all audit trails.	10.2.3 Logging of access to all audit trails
10.2.4 Invalid logical access attempts.	10.2.4 Logging of invalid logical access attempts
10.2.5 Use of identification and authentication mechanisms.	10.2.5 Logging of use of identification and authentication mechanisms
10.2.6 Initialization of the audit logs.	10.2.6 Logging of initialization of audit logs
10.2.7 Creation and deletion of system-level objects.	10.2.7 Logging of creation and deletion of system level objects
10.3 Record at least the following audit trail entries for each event, for all system components:	10.3 Confirm through inquiry and observation, for each auditable event mentioned at 10.2 above, that the audit trail captures the following information:
10.3.1 User identification	10.3.1 User identification
10.3.2 Type of event	10.3.2 Type of event
10.3.3 Date and time	10.3.3 Date and time stamp
10.3.4 Success or failure indication	10.3.4 Success or failure indication, including those for wireless connections
10.3.5 Origination of event	10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Identity or name of affected data, system component, or resources



SenSage solutions empower companies to readily respond to business-critical threats, conduct thorough and precise investigations, and maintain PCI-compliant operations.

Requirements	Testing Procedures Addressed by SenSage
<p>10.4 Synchronize all critical system clocks and times.</p>	<p>10.4 Obtain and review the process for getting and distributing the correct time within the organization. Also obtain and review related system parameter settings for the sample of <i>(insert number and/or description of sample)</i> system components.</p>
<p>10.5 Secure audit trails so they cannot be altered in any way, including the following:</p> <p>10.5.1 Limit viewing of audit trails to those with a job-related need.</p> <p>10.5.2 Protect audit trail files from unauthorized modifications.</p> <p>10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.</p> <p>10.5.4 Copy logs for wireless networks onto a log server on the internal LAN.</p> <p>10.5.5 Use file integrity monitoring/change detection software (such a Tripwire) on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).</p>	<p>10.5 Verify the following via inquiry of the system administrator and review of file permissions:</p> <p>10.5.1 Only individuals who have a job-related need can view audit trail files.</p> <p>10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.</p> <p>10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.</p> <p>10.5.4 Offload or copy logs for wireless networks onto a centralized internal log server or media that is difficult to alter.</p> <p>10.5.5 Verify the use of file integrity monitoring or change detection software for logs by observing system settings and monitored files, as well as results from monitoring activities.</p>
<p>10.6 Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like IDS and authentication (AAA) servers.</p>	<p>10.6.a Obtain security policies and procedures and determine that they include procedures to review security logs at least daily, and that follow-up to exceptions is required.</p> <p>10.6.b Through observation and interviews, determine that regular log reviews are performed for all system components.</p>
<p>10.7 Retain your audit trail history for a period that is consistent with its effective use, as well as legal regulations. <i>An audit history usually covers a period of at least one year, with a minimum of three months available online.</i></p>	<p>10.7.a Obtain security policies and procedures and determine that they include audit log retention policies and require audit log retention for at least one year.</p> <p>10.7.b For the sample of <i>(insert number and/or description of sample)</i> system components, verify that audit logs are available online or on tape for at least one year.</p>

About SenSage, Inc.

SenSage, the leading provider of enterprise security analytics, offers unparalleled performance and a scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store massive volumes of event log data. Our solutions empower companies to readily respond to business-critical threats, conduct thorough and precise investigations, and maintain compliant operations. Based in San Francisco, CA, SenSage currently protects Global 2000 customers in financial services, government, healthcare, manufacturing, and technology. The company markets its product directly and through partners including Cerner, EMC, Hewlett-Packard, and Lockheed Martin.

SenSage, Inc. ♦ 415.808.5900 ♦ www.sensage.com

© Copyright 2005 SenSage, Inc. All rights reserved. SenSage and Scalable Log Server are trademarks of SenSage, Inc. in the United States.

