



- Solutions
- Products
- Industries
- Customers
- Partners
- Support
- Company
- Contact Us



**Solutions**

**Security & Log Management**

**Compliance Auditing**

**PCI DSS**

HIPAA

Sarbanes-Oxley

NISPOM

FISMA

DCID

NERC

ISO 27002

**IT Operations & Risk Management**

**Business Data Intelligence**

SenSage for PCI DSS Compliance delivers the industry's only event data warehousing solution specifically designed to address PCI DSS management challenges. By integrating collection, storage and analysis functions, as well as designing the solution specifically for event data, SenSage for PCI Compliance provides a simple and accurate method for monitoring, analyzing and complying with PCI DSS requirements.



SenSage provides real-time analysis and long-term trending to identify security threats before they become problems. The solution has focused day-to-day monitoring of your PCI DSS-related processing environment and simple, powerful forensic capabilities that quickly meet PCI QSA audit requirements and facilitate ad hoc forensic capabilities.

**How SenSage for PCI DSS Compliance helps organizations address compliance requirements**

6.4 Follow change control procedures

- SenSage detects changes to any database object

7.1 Limit access to resources and cardholder information only to those individuals whose job requires such access

- SenSage tracks all access to cardholder data
- Exception reports can be created for access from users not on approved list

8.5.1 Control addition, deletion and modification of user IDs, credentials, and other identifier objects

- SenSage tracks all access to cardholder data
- Exception reports can be created for access from users not on approved list

10.1 Establish a process for linking all access to system components (especially access done administrative privileges) to each individual user

- SenSage captures database user id and system user id data
- SenSage captures failed login activities and can alert on anomalies

10.2 Implement automated audit trails for all system components to reconstruct the following events:

- 10.2.1 All individual access to cardholder data
- 10.2.4 Invalid logical access

**SenSage for PCI DSS Compliance Offers Powerful Features**

- Data Source Collection** - Agent-less, automated and with hundreds of supported sources and the ability to create custom adapters, SenSage for PCI DSS Compliance collects from business applications, databases, unstructured data on any platform
- Storage and Retention** - Patented, secure, purpose-built for event data storage, SenSage for PCI DSS Compliance allows for the online storage of years' worth of log data
- Analytics and Forensics** - Pre-defined reports mapped specifically to the PCI DSS standard, real-time correlation, dashboards, policy exception analysis, forensic investigations keyed off any data field, consistently rapid results

Learn more about PCI DSS requirements at <https://www.pcisecuritystandards.org/>

**Resources**

**Gartner**

- Gartner 2009 SIEM Magic Quadrant
- Critical Capabilities for SIEM Technology

**Brochures**

- PCI DSS
- Achieving PCI Compliance w/ Log Management
- Using Security Information Management Systems for PCI Compliance

**Webcasts**

- SANS - PCI
- SANS - Using SIM in your PCI compliance program

**» Contact Us**