



# Advanced Security Information and Event Management

Sensage® solutions are designed to meet the needs of the most proactive security professionals who are continuously improving their security posture. Sensage goes beyond typical Security Information and Event Management (SIEM) to provide the industry's most flexible and scalable solution, being used by the largest government agencies, Telcos, and enterprises in detecting threats, shoring up defenses, and maintaining compliance with industry regulations.

## Flexibility

Optimizing security and staying ahead of changing compliance regulations demands flexibility. Sensage captures data from any source with a timestamp, and retains that data in its native log format. No specialized collector agents, no normalization that reduces the fidelity of the data, and no restrictions to access that data in its raw form. This enables analysts to correlate and perform complex queries, across their entire event data landscape. Sensage also delivers flexible analytic functionality to transform data into insight. By adding ODBC/JDBC support to its unified security database, Sensage makes it possible to build finely tuned security analytics and dashboards that leverage the deep contextual knowledge that security professionals have about their unique environment and threats. Sensage also provides role-based access to the entire security data set to support such diverse needs as compliance reporting, forensic investigation, and continuous trend-line dashboards for operations.

## Scalability

Sensage easily handles petabytes of event data in a single, unified event data warehouse that provides access to real-time as well as historic data from years past. This makes it the ideal choice for large or growing organizations, and those with complex security and compliance event management needs.

Sensage uses a patented, columnar database that stores security event data in a highly compressed, clustered, environment without the use of indices. Complete log records are stored in their native format with their original time stamp to create a secure, tamper-proof repository for rapid and 100% accurate data querying and analysis. Sensage scales easily to meet growing needs, as additional nodes can be added without disruption. This includes the ability to sit side-by-side with traditional SIEM solutions that are unable to address a broader set of requirements, including large volumes of data being captured, analyzed and retained indefinitely.

## Sophisticated Data Analysis

According to the recent Verizon Business 2011 Data Breach Investigations Report (DBIR), 69% of the breaches had log evidence available for forensics, yet less than 1% of the breaches were discovered by internal log analysis and/or review. In fact, 86% of breached companies were notified of a breach by a third party—not through internal processes. These chilling statistics are demanding that analysts have the ability to accurately and quickly query any data sets and drill down on real-time or exception reports to assess any historical patterns. In order to facilitate more rapid analysis, Sensage has incorporated ODBC/JDBC interfaces that make it possible for security analysts to leverage the same Business Intelligence tools and methods to increase their understanding of security operations and enhance their ability to improve them.

### Sensage Advanced Security Information and Management

- Flexibility
- Scalability
- Sophisticated Data Analysis
- Reduced Security Operating Costs

## Reduced Security Operating Costs

Sensage's columnar database delivers 40:1 data compression advantages over competitive relational data stores, which translates into significant storage savings. Because its columnar architecture does not require any index administration, Sensage is also less expensive to administer than other SIEM offerings. Finally, through open access to analyze the data using standard SQL querying and BI tools, organizations do not have to learn proprietary languages or pay for additional analytic licenses.

## Sensage Architecture

The Sensage architecture has three primary components: Event Data Collection, an Event Data Warehouse, and Security Intelligence.

The Sensage solution can be deployed in the form of software, appliance, and/or

virtual machine, and each may support a variety of storage technologies, including Direct Attached Storage (DAS), Storage Area Network (SAN), Network Attached Storage (NAS), and Content Addressable Storage (CAS).

### Event Data Collection

The Sensage Event Data Warehouse (EDW) comprises a collector (called a Log Adapter), real-time monitor, and columnar database. The collector performs the externally facing data acquisition functions often referred to as Extract, Transform, Load (ETL).

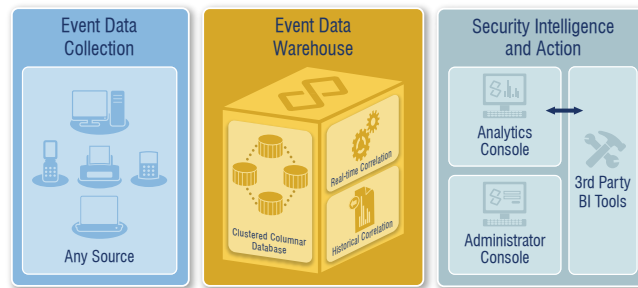
Extraction is performed by Sensage Log Adapters, which operate in agentless mode so that agents are not required on or near the event data source. The Log Adapters obtain and parse data from over 250 event data sources through a variety of protocols including, but not limited to, Syslog, Syslog NG, SNMP, FTP, SFTP, SCP, SMB, RPC, SQL\*Net/ RDBMS, HTTP(S) GET and PUSH.

It is very easy for customers to add their own Log Adapters as needed, and also determine whether to operate Log Adapters in streaming or scheduled batch mode.

### Event Data Warehouse

As each new event data set is collected by Sensage Log Adapters, one copy is delivered to the real-time monitor for dynamic parsing, normalization, filtering, analysis, and alerting. A second copy is delivered to the columnar database for tamper-resistant storage in its native/raw format. This unique data forking approach bridges real-time and historic analysis

while maintaining the complete event log for forensic evidence. Further, this approach supports instant replay visualization; events may be replayed graphically to review their sequence and interdependency.



Sensage Architecture

The Sensage Columnar Database incorporates patented technology optimized for the warehousing of event data. Unlike traditional relational database management systems (RDBMS) that use a row format, Sensage organizes data by column in a single, centralized data repository, using a time-based hierarchical series of folders and flat files. This results in dramatic performance gains and eliminates the need for indexes, reducing storage requirements and maintenance costs. With data compression rates ranging from 10:1 to 40:1 compared to RDBMS, storage savings generated by Sensage can be sizable.

The real-time monitor is a highly scalable and sophisticated correlation engine that supports threshold- and scenario-based rules built from logical operations on event data and displayed in dashboards in the Analytics Console. It also correlates events from multiple sources over a sliding time window to enable real-time threat detection that goes beyond attack pattern recognition for true analysis of threat

### Any Source

- Industry Specific Applications (*Financial, Healthcare, Telco...*)
- Infrastructure Applications (*Email, Web Proxy...*)
- Databases
- Systems (*Server, PC, Mainframe...*)
- Network and Security Devices (*Firewall, IDS/ISP, Antivirus...*)

### Sensage Log Adapters exist for a variety of products and platforms, including:

- Firewalls
- VPN concentrators
- Proxies
- IDS systems
- DLP
- Databases
- Web/Application servers
- Operating systems (Windows, UNIX, Linux, mainframe, etc)
- Networking equipment
- E-Mail systems
- Anti-virus
- Traditional SIEM systems

**Sensage event data warehouse's sophisticated database delivers:**

- Distributed and parallel data loading
- Distributed and parallel query processing
- Compressed data retention
- Linear scalability using Massively Parallel Processing
- Highly optimized for storing and retrieving event data
- Accelerated sparse query retrieval

**Intelligence and Action**

- Compliance Reporting
- Real-time Monitoring
- Exception Reports
- Forensic Investigations
- Ad-hoc Queries
- Security Dashboards
- Operational Workflow Solutions
- IT/Risk Dashboards

**Compliance Coverage**

- SOX
- FFIEC
- GLBA
- PCI
- HIPAA/HITECH
- NERC/FERC
- FISMA
- NISPOM

behavior. Because real-time correlation is fully integrated with historical event analysis, operators can easily look for historical occurrences of similar events to fine-tune future correlation.

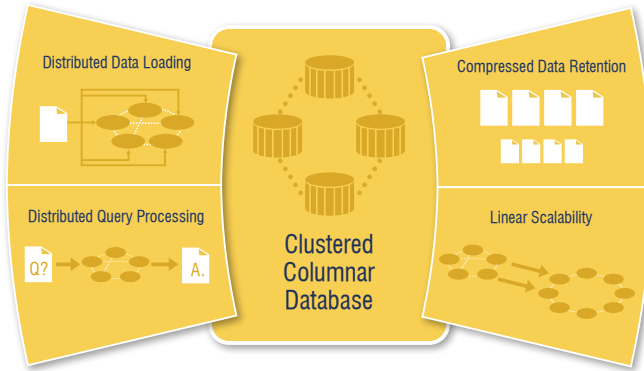
The event data warehouse features

a Massively Parallel Processing architecture that scales up or down depending on the number of nodes present in the system. This architecture enables the insertion of hundreds of thousands of records per second. Each node in the cluster may take advantage of advanced hardware features such as multi-core processors and faster disk drives. To maintain constant availability, backup copies of each node's data are stored on another node for data redundancy and automatic failover.

**Security Intelligence and Action**

This component performs three core functions: real-time monitoring, contextual investigation, and reporting. Comprehensive built-in analytics and an extensive dashboard that is easily customized enables powerful real-time monitoring. Exact-match querying across any data column enables the user to create data aggregation, trending, business, and technical reports with bar, line, and tabular charts. This eliminates the frustrations of more typical "Google-style" searches and increases the speed and precision of investigations. Sensage's wide array of available reports can be accessed and enhanced even by non-technical users using a drag-and-drop interface that makes drill down and ad-hoc investigations as fast as they are powerful.

In addition to common security reporting scenarios such as application and database activities, compliance reports to meet specific regulatory requirements (e.g., PCI, HIPAA, Sarbanes



Sensage columnar database

Oxley, FISMA, DCID/3, and NISPOM) are readily available. The Interactive Analytics component is completely customizable and can extend Security Intelligence using in-built report and system wizards, underlying SQL code and IntelliSchema,

or via the Open Security Intelligence API and ODBC/JDBC interface. Sensage Professional Services are available to assist with custom source integration, targeted analytics development, and executive dashboard implementation.

Sensage GUI-based administrative screens enable easy management of users, privileges, schedules, and reports. Sensage delivers robust and secure authentication, administration, and access control with multiple security levels to support highly granular access rights, including those necessary to support multi-tenant services leveraging a combined cluster. Users can install Sensage administration clients in any location with a secure and encrypted connection between client and server.

**About Sensage, Inc.**

Sensage, Inc. delivers unified Security Information and Event Management (SIEM) and log management systems that are open to all event data types, scale to petabytes, minimize storage costs and perform sophisticated data analysis. Hundreds of customers worldwide leverage patented Security Intelligence solutions from Sensage to identify, understand and counteract cyber-threats, fraud and compliance violations. Sensage partners include Cerner, Cisco, EMC, McAfee, Pentaho and SAP.



Sensage, Inc.  
1400 Bridge Pkwy.  
Suite 202  
Redwood City  
CA 94065  
www.sensage.com