

## SenSage Frequently Asked Questions

### What does SenSage do?

SenSage Security Intelligence solutions provide essential decision support for security, risk management, and compliance operations. SenSage offerings include security information and event management (SIEM), log management, and SAP continuous controls monitoring, which are supported by a single data management architecture, access model, and console. More than 450 corporations and government agencies worldwide are currently using SenSage solutions to safeguard their data in today's cyber-threatened environment.

### Why do I need Security Intelligence?

The digital infrastructure used today by businesses and governments faces unprecedented attacks that are costing organizations billions of dollars a year through interrupted operations, data loss, lawsuits, and damage to customer confidence. According to one study, \$1 trillion in intellectual property was stolen online in 2008.<sup>1</sup>

Regulatory agencies and business imperatives now require organizations to capture and retain years worth of event data for regulatory compliance purposes as well as for fraud detection, forensics and investigations, law enforcement and security agency requests, and operations troubleshooting.

The many point products currently being used to manage event data have proven inadequate:

- Traditional data warehouses lack a security context and struggle with the unstructured nature of event data.
- Traditional security information and event management (SIEM) systems do not scale to support the sheer volume and long-term storage requirements of an event data warehouse.
- Traditional log management systems lack the real-time monitoring functionality necessary to keep pace with critical operations such as security incident response.
- Both SIEM and log management systems lack the sophisticated analytics necessary to detect and investigate state-of-the-art cyber-threats.

It is quite clear that a new approach is required, one that leverages the power of scalable data warehousing and flexible information analytics but in the context of security management. Just as Business Intelligence solutions leveraged data warehouses to facilitate decision support for business management, now Security Intelligence solutions must leverage the power of event data warehouses to facilitate decision support for security management.

---

<sup>1</sup> — "Google and China: the new era of cybercrime," Editorial Board, January 26, 2010, Christian Science Monitor: <http://www.csmonitor.com/Commentary/the-monitors-view/2010/0126/Google-and-China-the-new-era-of-cybercrime>

## How do Security Intelligence Solutions work?

All SenSage Security Intelligence solutions have three primary components:

- **Interactive Analytics** – provides an analytics environment that can be completely customized. It performs three operations: real-time monitoring, contextual investigation, and reporting.
- **Event Data Warehouse** – serves as the underlying foundation for the Security Intelligence solution, consisting of patented technologies that include a collector, a real-time monitor, and a columnar database. The Event Data Warehouse can scale to handle the multiple-petabyte-sized event data volumes of the largest organizations.
- **Administration Console** – provides graphical user interface (GUI) delivered through an intuitive console for administrators that make it easy to manage users, privileges, and schedules and to generate security and compliance reports.

These SenSage components can be deployed in the form of software, hardware appliance, and/or virtual machine, and each may support a variety of storage technologies including on-board storage, storage area network (SAN), network attached storage (NAS), and content addressable storage (CAS). Together, these SenSage and third-party components comprise a Security Intelligence solution.

## Why is the SenSage columnar-based Event Data Warehouse uniquely suited for Security Intelligence?

Because event data has several unique characteristics that are different from other types of business data, SenSage has developed and patented a columnar data warehouse solution to address the issues. A columnar database organizes data by column rather than by the row format used by relational database management systems. While the difference may sound trivial, a columnar architecture provides distinct advantages for certain classes of data including event data:

- Data for each column is stored together, and this provides performance gains by allowing queries to reference only the data selected.
- Indexes are unnecessary in columnar databases as each column is actually an index, thus significantly reducing the storage and maintenance requirements of relational databases.
- Data organized in columns provides a massive opportunity for data compression as the data in columns is similar, unlike the compression of an entire row with different data types.

## Some use cases require several years of event data retention. Is it possible to retain these vast amounts of event data online using SenSage solutions?

SenSage solutions were purposely designed to retain historical data online. By leveraging an optimized data storage model, SenSage solutions enable organizations to satisfy long-term data retention requirements—including storing multiple years worth of event data—all online and accessible.

When storing event data, SenSage solutions can compress it to a little as 10 percent of volume of the original raw event log data, and 2.5 percent of the volume of data (compressing 40 times more effectively) that must be stored when using a relational database management system (RDBMS)-based solution for data retention.

Since SenSage solutions are 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.

## What is event data?

Event data is a set of chronologically sequenced data records that capture information about what happens in the digital infrastructure. Virtually every form of information technology produces event data, which is sometimes referred to as log data, audit trails, or the system of record.

Examples of event data include:

- Logs for compliance (PCI DSS, Sarbanes-Oxley, HIPAA, etc.)
- Banking transactions such as online, ATM, and debit card use
- Updates to shipping status in RFID records
- Historical prices of stocks and other instruments
- Call detail records (CDRs) of telephone transactions
- Internet protocol detail records (IPDRs) of web-based access and transactions
- Network, Windows, Email, and other systems management activity events
- Profile changes, database access to sensitive data, failed transactions

Event data differs in many ways from transactional data that is stored in traditional data warehouses:

- **Cumulative volume** – Event data accumulates rapidly and often must be stored for years; many organizations are managing hundreds of terabytes, and some are managing petabytes.
- **Format** – Because of the huge variety of sources, event data is unstructured and semistructured.
- **Collection** – Event data is difficult to collect because of broadly dispersed systems and networks.
- **Time-stamped** – Event data always is inserted with a time-stamp once and never changes.

Driven by changes in security threats, compliance mandates, and risk management initiatives, organizations are collecting event data from more sources and storing it longer, and they have been trying to piece together systems to enable them to analyze this data more deeply, more broadly, and more frequently.

## Does SenSage support integration with major storage vendors?

SenSage supports integration with major storage vendors including EMC, NetApp, HDS, HP, and IBM. SenSage works with any storage type including direct attached, network attached storage (NAS), and storage area networks (SAN).

SenSage customers have the option to leverage the compliance-ready, scalable, and reliable storage of the EMC Centera platform. The SenSage Security Intelligence solution is one of a few field-proven Centera-certified solutions, and SenSage is a top-tier EMC partner.

## What are the minimum hardware and OS requirements for the SenSage software?

The SenSage solution operates on inexpensive, commercial off-the-shelf platforms. Specifically, the recommended OS and hardware configurations for a SenSage deployment include Red Hat or SuSE Linux on a modest server hardware platform, which is typically a dual CPU, 3.2+ GHz, 4 GB RAM, minimal 150 GB hard disk. The SenSage solution takes advantage of new CPU technologies and is architected to work well with and leverage multicore processors.

## What are the advantages of SenSage Security Intelligence solutions over traditional SIEM, log management, and data warehouse solutions?

SenSage Security Intelligence solutions offer better log management, security information and event management, security data visualization, and security dashboards. SenSage software is thoroughly interoperable and can show what was happening in an organization's entire environment, not just on a few devices.

Based on patented, proprietary technology, SenSage solutions provide organizations with a scalable means to centrally aggregate, efficiently analyze, and dynamically monitor massive volumes of data. In addition, SenSage solutions substantially reduce the cost of deployment and ongoing management associated with IT monitoring, investigation, and compliance.

## About SenSage, Inc.

SenSage® Inc. delivers Security Intelligence solutions that provide essential decision support to cyber-security, risk management, and compliance operations. These solutions enable the necessary convergence of security information and event management (SIEM), log management, and continuous controls monitoring through a single console and data management architecture. Over 450 organizations and government agencies around the world rely upon SenSage to combine these functions in support of more holistic IT oversight, real-time alerting and investigation, incident response, and compliance reporting. Combining a patented event data warehouse platform and interactive analytics environment, SenSage Security Intelligence solutions are more scalable, flexible, and affordable than traditional point products. SenSage goes to market with industry-leading OEMs and strategic alliance partners including Cerner, Cisco, EMC, HP, McAfee, and SAP. Visit [www.SenSage.com](http://www.SenSage.com) for more information.



### Corporate Headquarters

SenSage, Inc.  
55 Hawthorne Street,  
Suite 700  
San Francisco, CA 94105 USA  
Phone: +1.415.808.5900  
Email: [info@sensage.com](mailto:info@sensage.com)

### EMEA Headquarters

SenSage, Inc.  
Venture House, Arlington Square  
Downshire Way,  
Bracknell, RG12 1WA UK  
Phone: +44 1344 741 053  
Email: [emea@sensage.com](mailto:emea@sensage.com)