

CDR and Log Analytics and Retention

Telecommunications providers generate hundreds of millions of event records daily. Every phone call placed, connected, disconnected, etc. creates potentially critical event log data. Because of this, regulatory and business drivers now require telecommunications providers to capture and retain *years* of this data for multiple purposes:

- 1) **Operations troubleshooting and root-cause analysis**
- 2) **Fraud detection**
- 3) **Forensics and investigations**
- 4) **Anti-terror information requests**
- 5) **Regulatory compliance**

- ✓ **Capture and Analyze All CDRs and Logs**
- ✓ **Securely Retain Years of Data**
- ✓ **Meet Data Retention Directives**
- ✓ **Lowest TCO**

Enacted in December 2005, the EU Retention Directive sets mandatory requirements for telecommunication providers for the collection, retention, and retrieval of communication records. Specifically, the following data elements must be captured and retained for 6 – 24 months:

- [Wireline/wireless Call Detail Records \(CDRs\)](#)
- [SMS Logs](#)
- [Email Logs](#)
- [Proxy Server Logs](#)
- [DHCP Assignment Logs](#)

This data must also be retained in an accessible repository, so organizations can respond to information requests from competent authorities, “without undue delay.” Furthermore, organizations must be able to extract the relevant records from the repository upon request.

Implications for Telecommunications Providers

Each day telecommunications providers generate millions of wireless and wireline phone Call Detail Records. In many cases, this results in hundreds of millions of events per day. With a 6 – 24 month required retention period, this represents billions of records, and terabytes of total data, to maintain and manage. In addition, telecommunication providers must implement the capability to perform pin-point searches over the full repository to retrieve specific records.

The SenSage Approach

To effectively manage these requirements, an entirely new approach is required. The SenSage Enterprise Security Analytics solution combines enterprise-class software with regulatory and security proficiency, to provide organizations the most efficient and cost-effective means of collecting, analyzing and storing massive amounts of event data...regardless of type of data source, or number of data sources that must be monitored. This translates to more accurate and efficient security monitoring, investigations, digital forensics and field-proven regulatory compliance. SenSage’s purpose-built system offers the following benefits:

- [Captures all CDR and log records from relevant sources](#)
- [Stores years of data online with immediate access to all data](#)
- [Provides full data analysis capability – easy to extract the exact records of interest](#)
- [Offers exceptional data loading and querying performance](#)

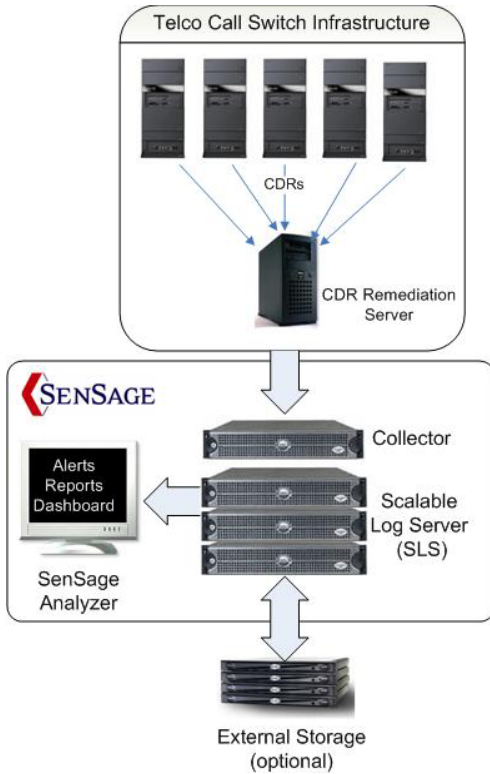
SenSage dramatically reduces the cost of deployment and ongoing management associated with security monitoring, investigation and compliance. SenSage’s patent-pending technology yields a robust, high-speed, extensible CDR retention and analysis solution.

With SenSage Enterprise Security Analytics:

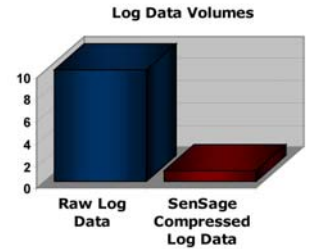
- [Leverage content addressed storage to yield enterprise-class security analytics](#)
- [Manage volumes of event data to reduce threat, violation and privacy risks](#)
- [Streamline operational reporting and automate audit processes](#)
- [Accelerate compliance efforts and address data retention guidelines](#)
- [Reduce log management storage, archive, administration and growth costs](#)
- [Readily expand capacity, performance and availability with appliance-like deployment convenience](#)

The SenSage Solution

SenSage provides telecommunication providers with the most scalable means to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively manage high-volumes of event log data. SenSage is built upon a modular architecture that takes full advantage of parallel processing, and a clustered repository – assuring consistent event collection, analysis and availability. This modular approach allows for appliance-like deployment, distributed configuration, and high performance.



SenSage captures a broad range of event log sources spanning CDRs, email systems, web proxies, network devices, security applications, host operating systems and applications. Event log data is collected supporting flexible batch and streaming protocols for real-time correlation and complete, long-term historic data analysis. The core of the SenSage system is the Scalable Log Server (SLS). It provides a scalable, high-speed analytic repository that parses, compresses and executes built-in and user-supplied queries against stored event log data. SenSage achieves a 10:1 raw log compression rate, while maintaining full access to all the data for ad-hoc and scheduled analysis. Overall alert monitoring, reporting, investigation and administration are provided by the Analyzer through an intuitive web-based interface. The solution is complemented by analytics packages of pre-defined rules and reports, mapped to common security monitoring guidelines and compliance standards.



Convert Years Worth of Data into Actionable Reports – Within Minutes

SenSage eliminates the need for organizations to make operational and compliance compromises with regard to which systems to monitor, which data to collect, and how long to utilize and retain event data online. SenSage’s purpose-built data store does not rely on relational database management system (RDBMS) technology. This results in more cost-effective data retention, as well as high performance reporting and analysis. SenSage customers analyze years and gigabytes worth of information considerably faster, and with more precision and consistent results than do their counterparts relying on RDBMS-based systems. SenSage’s optimized data store also avoids the high administrative costs associated with managing an RDBMS architecture. Finally, having access to years worth of data online also eliminates tedious sub-dataset queries and labor-intensive archive restoration processes.

SenSage ESA Selection – Choose the right solution

SenSage’s solutions are designed to meet varied organizational size, environmental and evolutionary requirements.

ESA System Included	Online Retention	Physical Storage*	Uncompressed Raw Event Storage**	Expected Daily Report Volume
ESA-300	> 25 months	2.2 TB	11.3 TB	80 – 100
ESA-500	> 14 months	2.2 TB	11.6 TB	100+
ESA-1000	> 14 months	4.4 TB	23.35 TB	120+

* Physical storage is represented by the raw physical space available within the solution

**Compressed raw event storage is equivalent to how much raw uncompressed log data can be stored within the solution

About SenSage, Inc.

SenSage, Inc. is the leading provider of enterprise security analytics. The company offers unparalleled performance and a highly scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor, and cost-effectively store massive volumes of event log data. By solving the compliance data management dilemma, our solutions enable companies to readily respond to business-critical threats, conduct thorough and precise investigations, and maintain compliant operations. The company is based in San Francisco, California, and was founded in 2000.