

EMC Centera/SenSage Solution for Communications Service Providers

The Big Picture

- 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

Retention and analysis of CDRs and other communications event records

Communications service providers generate hundreds of millions of event records daily. The events record every phone call placed, connected, disconnected, etc. Regulatory, security, and business drivers now require communications service providers to capture and retain years of this data for purposes such as:

- Anti-terror and anti-crime information requests from law enforcement and security agencies
- Fraud detection
- Forensics and investigations
- Operations troubleshooting and root-cause analysis
- Regulatory compliance

Global pressure from security agencies and specifically, the EU Data Retention Directive, has dictated that communications service providers find solutions to retain and analyze CDRs and other event records. Enacted in December 2005, the EU Data Retention Directive sets mandatory requirements for communications service providers for the collection, retention, and retrieval of communication records. Specifically, the following data elements need to be captured and retained for six to 24 months:

- Wireline/wireless call detail records (CDRs)
- SMS logs
- E-mail logs
- Proxy server logs
- DHCP assignment logs

The data must be retained in an accessible repository so that 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 communications service providers

Every day communications service providers generate millions of wireless and wireline phone CDRs. In many cases this is measured in hundreds of millions of events per day. With retention periods of up to 24 months, this represents billions of records and terabytes of total data to maintain and manage. In addition, communications service providers must implement a capability to perform pin-point searches over the full repository to retrieve specific records.

The EMC-SenSage approach

To manage these requirements, an entirely new approach is required. EMC Corporation and SenSage have partnered to produce an integrated solution combining the EMC® Centera® storage platform with SenSage’s powerful Event Data Warehouse technology. The EMC-SenSage solution 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

The EMC-SenSage solution is an integrated security data analytics and storage solution. This solution dramatically reduces the cost of deployment and ongoing management associated with security



monitoring, investigation, and compliance. The bundle combines SenSage™ and EMC Centera to yield a robust, high-speed, extensible security information lifecycle management solution. This feature-rich combination 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.

The SenSage Event Data Warehouse

SenSage provides communications service 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, e-mail systems, web proxies, network devices, security applications, host operating systems, and applications. Event log data is collected supporting flexible batch and streaming protocols for realtime 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 up to 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 predefined rules and reports, mapped to common security monitoring guidelines and compliance standards.

Convert years worth of data into actionable reports—within minutes

The EMC-SenSage solution eliminates the need for organizations to make operational and compliance compromises about 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 with considerably faster, more precise, and more consistent results than that of RDBMS-reliant 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.

Leveraging EMC Centera

SenSage and EMC Centera are architecturally matched to provide rapid event log loading, queries, reporting, and fixed-data management. Transparent integration allows the EMC Centera storage platform to seamlessly operate as part of SenSage's analytic repository, operating at near identical primary storage speeds. SenSage's security analytics software is EMC Centera Proven. This assures customers that a SenSage/EMC Centera solution is compliance-ready, with tested deployment, guaranteed data-retention periods, and protection against data modification. Users gain enterprise scalability at significantly reduced administrative and storage costs.

The EMC-SenSage solution delivers unmatched performance and the level of usable data retention required to manage multi-terabytes of security and compliance-relevant data. Customers can readily expand performance and capacity by simply adding related SenSage or EMC Centera nodes. High availability is further automated with daily SenSage system backup—with the option of supporting disaster recovery and business continuity scenarios that take advantage of EMC Centera replication.

- Capture and analyze all CDRs and logs
- Securely retain years of data
- Meet data-retention directives
- Lowest TCO



EMC Corporation
Hopkinton
Massachusetts
01748-9103
1-508-435-1000
In North America 1-866-464-7381
www.EMC.com

Take the next step

The unique architecture of the SenSage solution enables deep integration with EMC Centera to allow for massive storage of log information with near-online performance characteristics. To learn more about the SenSage/EMC Centera solution, contact your local EMC or SenSage sales representative, or visit our websites at www.EMC.com or www.sensage.com.