

Managing Enterprise Risk Requires a Robust Log Management Strategy

SenSage's Enterprise Security Analytics empowers financial institutions to collect, retain and access terabytes of log data from all sources, resulting in cost-effective, compliant data retention as well as actionable and timely analysis

What business value does SenSage provide?

SenSage addresses security information management challenges, like regulatory compliance and complex IT forensic investigations, and overcomes SEM deficiencies with its advanced, enterprise-class software. Leveraging our patent-pending enterprise, security analytics and Scalable Log Server (SLS) technologies, our customers readily respond to critical business threats, conduct thorough and precise investigations, and maintain compliant operations – with greater operator productivity, lower costs and accelerated time-to-value.

Which event data is relevant for BASEL II compliance?

Any system that houses critical financial reporting data should have its logging enabled, both at the OS level and the application level. Moreover, this event log information needs to be collected, monitored, analyzed and retained. For most organizations, this includes log data from network devices, security devices, mainframes, home-grown and proprietary applications, server operating systems, databases, etc. Solutions unable to store the complete record, and that filter or otherwise arbitrarily eliminate any of the event log information seriously expose organizations to operational risk.

Which log source types can SenSage accommodate?

SenSage has the ability to collect logs from any source on any platform. Our solution has existing support for over 170 log sources. In addition, SenSage has a flexible software framework that enables easy creation of new log adapters to provide extensibility as an organization's infrastructure evolves.

The Basel II Accord standardizes the measurement and quantification of risks within a financial services organization. In addition to the management of market and credit risk, the Basel II rules address operational risk which encompasses IT systems and their supporting infrastructure.

Perhaps the most fundamental step in reducing operational IT risk lies in the ability to understand—and attest to—the reliability and security of mission-critical system operations. This requires internal controls that are based on the enterprise-wide collection, retention and review of application and system event log data. This comprehensive body of data provides the most complete, accurate and legally admissible picture of the history of access to and modifications of mission-critical information.

Basel II Imperative: Data Retention

The Basel II guidelines call for the retention of log data over a period of three to seven years. SenSage provides the only solution with the scalability, compression technology and redundancy needed to support online access to the massive data volumes generated over these extended timeframes. SenSage also enables the online access to this data needed for routine reporting and ad hoc queries required by auditors and security incident investigators.

Unlike conventional systems based on inefficient RDBMS architectures, SenSage is able to store huge amounts of event log data – and provide online access to years of data for audit and investigation purposes. Maintaining years of event information online positions SenSage customers for success dealing with issues related to effective corporate governance and regulatory compliance.

Automated, Reliable, Comprehensive Regulatory Compliance

By providing the ability to collect, retain and review event logs from financial systems, SenSage streamlines and automates the processes of evaluating, documenting and enforcing internal controls. By offering support for virtually any event log type, and delivering over 100 out-of-the-box compliance reports, SenSage provides the foundation for a comprehensive corporate information security, audit, and investigation strategy.

In summary, with regard to BASEL II compliance, SenSage enables enterprises to:

- Ensure that event log collection, correlation and retention is consistent and usable for validating/fortifying controls and investigations
- Bridge the gap between real-time compliance monitoring and long-term, broad source investigation and audit
- Empower IT Security staff to conduct audit and investigation processes with greater efficiency and effectiveness
- Mitigate data management issues that impact compliance including:
 - Cost to capture and store the required amount of event log data for compliance initiatives
 - Performance required to capture and analyze event log data
 - Scalability to meet increased volume and evolving requirements

About SenSage, Inc.

SenSage, Inc. is the leading provider of enterprise security analytics. The company 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. SenSage 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.

SenSage, Inc. ♦ 415.808.5900 ♦ www.sensage.com

© Copyright 2005 SenSage, Inc. All rights reserved. SenSage and Scalable Log Server are trademarks of SenSage, Inc. in the United States.