

Continuous Monitoring and Auditing for SAP



Audit user activity to meet security, audit and separation of duties requirements

SenSage Continuous Monitoring and Auditing for SAP automates and enables a 360° view of SAP user activity, and uniquely does so without the need to maintain audit logs within the SAP system. SenSage installs quickly and provides the 360° view both within the SAP environment and across the entire IT infrastructure and systems. Management, internal auditors, security and compliance professionals use SenSage to detect fraudulent behavior such as failed or fraudulent transactions, failing controls, SOD violations or overrides, profile changes enabling unauthorized access to transactions, locked accounts, or unauthorized changes to master data files through exception-based alerts and reporting.

SAP customers face a number of data management challenges for Continuous Controls Monitoring and SAP User Activity Monitoring. An enterprise scale solution is essential to maintain the huge volumes of data necessary to monitor and audit SAP controls, privileged user activity, and to detect transaction fraud, anomalies, and trends. Specific requirements include the ability to:

- » Ensure ERP controls are working as intended
- » Monitor transaction fraud, duplicate payments, SOD violations, and master data
- » Provide deep visibility into user activity
- » Adhere to multiple regulations: SOX, PCI DSS, HIPAA, NISPOM, FISMA, etc.
- » Manage & analyze large volumes of SAP events over long time frames
- » Support highly customized business processes
- » Monitor transactions across ERPs, custom apps, IT systems and infrastructure, etc.

SAP and SenSage

With SenSage, organizations can safeguard critical enterprise assets and processes. Specifically:

- » Enable continuous monitoring to prevent transaction failures and fraud (e.g. identify duplicate payments)

- » Maintain a single view of transactions across multiple instances of the same ERP, and instances of different ERPs and custom financial applications
- » Correlate user activity within SAP to activity outside SAP such as access to databases, unstructured data files on the network, systems, applications, and email
- » Monitor changes to master data tables
- » Jumpstart deployments with pre-packaged analytics, and implement custom analytics to complete the control framework
- » Perform ad-hoc forensic investigations
- » Conduct real-time analysis and response for subsets of applicable transactions
- » Maintain and query years of data for historical trend analysis and to meet audit requirements



Fig. 1

SenSage provides 13 ABAP certified transport modules and 35 pre-built analytics in the product to support immediate controls monitoring. SenSage Report Wizard is also included for easily creating ad-hoc investigative reports.

Intelligent and simple extraction of SAP data sources

Auditing user activity requires an understanding of where within the thousands of SAP tables the relevant security and event data exist for appropriate audits and investigations. The Continuous Monitoring and Auditing for SAP solution focuses on the six most common data sources for security events:

- » Security Audit Log
- » Business Object Change Data
- » Financial Accounting and Controlling
- » Material Management
- » Sales and Distribution
- » User Access

Auditing and detecting fraudulent user activity

SenSage converts years of data into actionable reports in minutes.

Monitor suspicious transaction activity: SenSage provides reports that track users' modifying profiles that enable unauthorized transactions. SenSage also tracks all key transactions, including transactions that operate against master data tables such as creating vendor records or against the data dictionary.

Monitor suspicious financial activity: SenSage provides reports that track transactions where values for orders or for invoices are above a threshold level.

Monitor user access: SenSage provides reports to validate which groups users belong to, if they are authorized to perform certain actions, for what time periods, and for maintaining user profiles or updating accounts.

Trending reports: SenSage provides wizards for creating new reports that analyze trends over time. Trending

information on user activities, failed logins and other actions can be quickly analyzed for anomalies and policy violations.

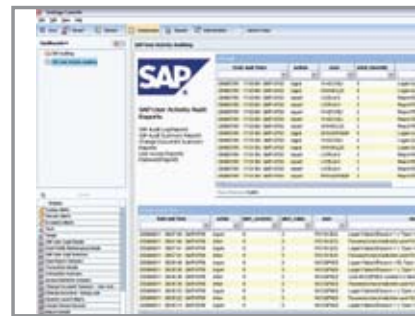
Out-of-the-box audit reporting: SenSage provides dashboard reports for tracking user activity and transactions necessary for meeting SAP audit requirements. Examples include tracking logins or viewing if reports and transactions started successfully.

Ad-hoc forensic queries: Each organization has unique reporting requirements, SenSage provides a query-building wizard that does not require any SQL knowledge.

Unlimited online audit record retention: Many security incidents take place over an extended period of time. The SenSage repository is fully on-line, compressed and supports local, NAS and SAN storage devices.

Gain a 360° view with SenSage

Unlike other solutions that are strictly tracking SAP transactions, SenSage uniquely gives users a true 360° view of user activity through a combination of powerful features. SenSage uses agent-less technology to collect event data from any source, and unlike other log management solutions, creates a unique table for every data source rather than using a single generic schema to store log records. Through the use of a powerful feature called Intellischema™, SenSage is able to correlate events from multiple sources such as databases, applications, servers, network infrastructure and access control systems to provide complete and accurate alerts and reporting. SenSage does not require coding SQL or “regex” statements and can be used by auditors, management or anyone who needs access to event data for security.



User Activity Auditing Dashboard for tracking security events

SenSage, Inc. offers patented event data warehouse solutions that provide actionable results from massive amounts of log and event data. Hundreds of customers have deployed SenSage solutions to reduce security, fraud and compliance risks at a fraction of the cost of traditional data warehouses and log management solutions. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, Hitachi Data Systems, McAfee, Tokyo Electron Device and many others. Visit www.SenSage.com for more information.