



Enterprise Customer Survey by SenSage Shows Growing Dependence on Log Data for Compliance and Threat Response

Three Quarters of Respondents Check Log Data Daily; Standards Compliance and Security Threat Protection and Investigation Top List of Concerns

SAN FRANCISCO – March 4, 2008 – According to a recent customer survey by enterprise software developer SenSage, the obscure form of computer information known as log data is now playing a vital role in protecting companies from security threats and improving their audit and compliance postures.*

Seventy-five percent of the senior IT management and network administration staff who responded to the SenSage survey stated that they checked their log data on a daily basis. Ninety percent of the participants, who represent diverse industries including healthcare, insurance, telecommunications and financial services, noted that they have used log data analysis in the past year to investigate a security breach.

“With all the excitement around the Web 2.0 craze, log data is definitely the unsung hero of the IT world,” said Ed Chopskie, vice president of marketing for SenSage. “IT staffs largely ignore it unless something goes wrong. In the past, trying to use log data to prove a process was sound or to reconstruct what happened when an IT process failed or was breached was very cumbersome and time consuming. Today, tools like SenSage’s software have streamlined the process and have given harried IT staffs an efficient way to quickly respond to increasing regulatory and audit demands and new security threats.”

Reams of log data are created whenever time-stamped transactions occur in an enterprise’s IT infrastructure. Popular sources of log data include routers, firewalls and other security detection and prevention appliances and applications, access management systems, and databases. Experts trying to analyze how a security breach occurred or why a particular IT process crashed would typically turn to log data as a last resort due to the complexity and time required to sift through all the records in hopes of finding the specific source of an issue.

Today, with advanced tools from SenSage for example, this analysis can occur so quickly and accurately – even for a search involving terabytes of data – that tracking of log data has become mainstream for meeting audit readiness and regulatory compliance, as well as for detecting suspicious activity, insider threats and other security breaches.

Results of note from the SenSage survey respondents include:

- Eighty-eight percent collect log data for compliance reasons, while 42 percent do so as part of best practices/industry standards initiatives such as ITIL.
- Seventy-eight percent rely on log data as part of their processes for detecting security incidents, while 70 percent use it for forensic investigation after a breach has occurred.
- Seventy-four percent are now storing the information for more than 12 months, reflecting the impact of newer compliance regulations.

- Consistent with other recent surveys, more participants are concerned about internal security breaches (56 percent) than external attacks (21 percent).
- While log data is typically associated with security analysis, 44 percent of respondents turn to this source when doing root-cause analyses of a system or application outage.

When queried about the types of security tools they planned to implement in 2008, survey participants' top priorities were access management, followed by data leakage, network behavior analysis, database activity monitoring and database encryption.

The Role of SenSage Software

SenSage's software collects data, including system log files, database event records, operating system event logs and telecommunications call detail records. It transforms this data – often the largest dataset in the enterprise – into actionable intelligence at much lower costs than traditional data warehousing and security products. The company's software solutions are standards-based and can be substantially optimized for hardware and storage products, resulting in a best-of-breed security information and event management (SIEM) appliance offering. SenSage's approach blends a high degree of performance with an array of administrative, management, analytics and reporting capabilities to meet the most stringent of compliance and regulatory requirements.

About SenSage

SenSage, Inc., www.sensage.com, offers the only patented event data warehousing solution for log management and compliance auditing applications. Over 300 customers have deployed SenSage solutions to reduce the risks associated with insider threats, system downtime and failed audits by providing faster, more granular analysis of privileged user behavior and analyzing anomalies across network, system and application activity. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, HDS, IBM, Intec Billing Systems, Lockheed Martin, Network Appliance, Sendmail, Symantec and Tokyo Electron Device.

*The survey respondents of 60 enterprise IT decision makers, including chief information officers, chief security officers, and senior compliance officers, was conducted via a questionnaire distributed between December 2007 and January 2008.

Media Contacts

Samantha Singh
The Hoffman Agency for SenSage, Inc.
Phone: 408-975-3087

Ed Chopskie, VP of Marketing
SenSage, Inc.
Tel: +1.415.808.5900