

Magic Quadrant Validates Sensage Value

An Opinion Piece by Joe Gottlieb, President and CEO of Sensage

The real-time SIEM market is crowded with capable and in some cases outstanding products. But as more sophisticated, targeted threats evolve and the sheer volume of data grows, it's clear that real-time event monitoring, while essential, is not sufficient to meet the security and compliance needs of the world's leading organizations.

Gartner's 2011 Magic Quadrant for Security Information and Event Management (SIEM) underscores Sensage's ability to meet the data analysis, compliance and reporting requirements of those large enterprises and government agencies that are taking information intelligence to the next level. These large and complex organizations are increasingly finding a need to enhance their traditional SIEM or real-time event monitoring deployment with sophisticated event analytics that scale to their immense and growing data environments.

Gartner's Perspective of Sensage

As Gartner states, "Sensage is optimized for organizations that require high-volume event collection, monitoring, analytics and reporting for large amounts of log data over long periods for audit, compliance and internal investigations." Sensage leverages its ability to analyze log data stored in native format, parsing it at query time to produce analysis of historical data. This enables organizations, for example, **to investigate long-term attacks that elude real-time monitoring**, and baseline and evaluate the effectiveness of security policies and controls over time. At its foundation are data warehousing capabilities that enable Sensage to manage and analyze huge quantities of event information.

These essential capabilities enable large organizations to analyze vast amounts of security data in order to understand their highly dynamic security environments, and empower them to set security priorities based on actionable intelligence and timely, knowledge-driven risk assessment. This goes far beyond general purpose SIEM capabilities that Gartner emphasizes for mainstream users. By Gartner's own definition, these general purpose capabilities are the focus of the Leaders, but none of the Leaders offer the data scalability and analysis capabilities offered by Sensage.

Expanding the Use of SIEM

In recognition of this, large and proactive enterprises and government agencies should consider supplementing their core SIEM capabilities with advanced event data warehousing and analytics capabilities provided by Sensage.

For example, HP/ArcSight – the leader in the Magic Quadrant and the acknowledged leader in the SIEM market – provides large enterprises with advanced real-time monitoring. It has earned this position by demonstrating outstanding performance in this and other basic SIEM capabilities identified by Gartner as central to the market over a number of years. But because ArcSight lacks the capability to store and analyze large volumes of historic event data, many organizations have deployed Sensage to serve these functions as a complement to ArcSight's real-time console capabilities.

Sensage may also be leveraged to complement other Magic Quadrant Leaders with their respective strengths. RSA gets high marks for comprehensive data collection and ease of use for enterprises with very limited staff for managing SIEM, but, Gartner notes, "Customers that have accumulated a large amount of event data frequently complain about performance issues related to ad hoc queries and reporting." Q1Labs does a nice job "collecting and processing NetFlow data to provide network and application behavior analysis," but doesn't yet provide forensic functions or comprehensive SAP monitoring.

While these other vendors have historically focused more on real-time monitoring, Sensage offers strong capabilities in this area and is distinguished for its ability to drill down from a real-time alert into supporting data. This enables security analysts to quickly assess related events that might indicate root causes and always provide for a more informed incident response.

So why didn't Gartner put Sensage in the Leader quadrant?

First and foremost, Gartner has noted that Sensage is focused on the high end of the market – primarily those large enterprises and government agencies whose security organizations seek to leverage security data analysis to drive more proactive security posture. This high end focus translates to a narrow product strategy (e.g., no “plug and play appliances”) and distribution strategy (e.g., no high-volume channels) relative to those in the Leader quadrant.

Second, Gartner has not yet added advanced data scalability and analysis to its use case criteria that drive the critical capabilities scores. As such, Sensage does not benefit much from this distinctive capability. Within its target market, Sensage's ability to execute is quite good, and the Magic Quadrant report reflects this. Gartner factors interviews with customers and clients who have completed competitive evaluations into its assessments, largely eliminating the “hype” factor and reflecting, rather, real-world experience with SIEM products. In this light, it is important to note that Gartner reports Sensage's successful deployments among large enterprises and government agencies that “require precision analytics and compliance reporting for a large data store,” in addition to organizations that require application and user monitoring.

About Sensage

Sensage®, Inc. helps organizations collect, store, analyze and interpret complex information to identify new threats, improve cyber-security defenses, and achieve industry and regulatory compliance.

Combining powerful data warehousing, scalable clustered multiprocessing and sophisticated analytics, Sensage serves our customers' most advanced Security Information and Event Management (SIEM), log management, Call Detail Record (CDR) retention and retrieval and Continuous Controls Monitoring (CCM) use cases. Sensage systems are open to all event data types, scale to petabytes, minimize storage costs and perform sophisticated data analysis.

Hundreds of customers worldwide leverage patented Security Intelligence solutions from Sensage to identify, understand and counteract cyber-threats, fraud and compliance violations. Sensage partners include Cerner, Cisco, EMC, McAfee and SAP. For more information, visit www.sensage.com, follow us on Twitter (@Sensage) and watch for us on www.youtube.com/Sensagetv.