**Sensage AP** is a data analytics platform, providing an event data collection and event management solution to organizations faced with targeted threats to security that require forensic analysis and to organizations needing to comply with federal regulations that typically require regulatory analysis. Though the product has been specialized for security monitoring with the addition of specific data collection and reporting configurations, it can be used for general purpose.

Among the features and capabilities of **Sensage AP** are:

- Security Intelligence:
    - Ability to perform sophisticated correlations and contextual investigations against large volumes of data over time.
    - An open access interface that lets users query event data directly from the Business Intelligence tools they prefer using ODBC/JDBC interfaces.
    - Rich reporting and query capabilities including ad hoc reporting, predefined report templates for regulatory compliance, and customized reporting through console (dashboard) tools that provide flexible querying.

- Event Data Collection:
    - Agentless collection of any event with a timestamp.
    - Open architecture that interfaces with a variety of related technologies, including endpoints and network systems, storage, mobile solutions, other SIEMs, call center applications, etc.

- Event Data Warehouse:
    - **Sensage AP**'s clustered, columnar-based event data warehouse provides the ability to store all event data in its native form (rather than metadata, an aggregation, or a normalized form) ensuring integrity for future data use.
    - Real-time ability to access terabytes of event data, without the need to extract from any archive – allowing for rapid response to investigations and queries.
    - Massively Parallel Processing (MPP) enables linear scalability in handling large data volumes in a highly compressed format that reduces storage requirements.

Product can be decomposed in a few subsystems:

| | |
|---|---|
| **EDW** | The **E**vent **D**ata **W**arehouse (EDW) is a scalable database built for and dedicated to loading, storing, and analyzing event data. Event data from multiple sources is stored in a highly compressed format. Parallel processing enables clustered servers to execute as a single instance, allowing high-speed loading and querying on terabytes of data. This architecture allows users to load and query massive data volumes in a single, logical database instance without partitioning. The EDW uses a proprietary data model that achieves high levels of compression, while still making all data fully available to query. |
| **Collector** | Before the enterprise can analyze event log data, original event-log data must be collected into the system. System supports batch data collection in which events are collected from log files and other event repositories maintained by network devices and software applications. |
| **Analyzer** | SIEM user application (**S**ecurity **I**nformation and **E**vent **M**anagement), used by security analysts from where, among other functionalities, it can visualize reporting dashboards, execute reports, schedule different operations and configure alerts. |
| **Deployment Manager** | With this component every node installation, health and administrative service operation is managed. It provides a graphical interface to operate sensage infrastructure. |
| **Analytics** | Analytics (also known as IntelliSchema) is a set of tables and views, which describe the most standard event logs schemas in the industry, like Cisco switches logs, Apache logs, Microsoft security event logs, etc. These tables/views can be installed in the EDW, to provide the customer the foundation for collecting these standard logs from their systems. |

The interactions between the internal subsystems can be described high level with this diagram: