



SenSage offers unparalleled, enterprise-class scalability

Foundation Analytics

The SenSage Foundation Analytics Package is designed to enable customers to monitor the operational security and effectiveness of the enterprise at a glance. Users can utilize this package to generate summary level reports on system, application and device activity in order to produce a comprehensive infrastructure baseline view of the activity and health of the enterprise. The categories of reporting include the following:

- SenSage self-monitoring and statistics
- General perimeter activity summary
- Authentication summary to systems, applications and devices
- Email and proxy server activity

Event Summary

Report Name	Description
All Events By Dest IP	Displays all events which were targeted at a particular IP.
All Events By Dest User	Displays all events which were targeted at a particular user
All Events By Source IP	Displays all events which originated from a particular source IP
All Events By Source User	Displays all events which originated from a particular source user

Network Security Activity

Report Name	Description
Firewall Denies by Source Host	Displays connection requests denied by the firewall organized by source host
Firewall Statistics Summary	This report provides a top level summary of all firewall activity across all firewalls for the specified period. It categorizes events by criticality level and breaks down bandwidth utilization by packet direction and by the major categories of network traffic. Use the SenSage Analyzer to compare multiple periods to detect anomalies and trends. Anomalies may provide early warning of security or operational problems while trends can assist in security and operational planning.
Firewall Summary by Protocol	This report provides a breakdown of firewall events and bandwidth utilization by application protocol and port. The firewall administrator should regularly review this report to identify successful and unsuccessful usage of any protocols that are not allowed in the security policy, and should observe changes in the volume of usage of various protocols over time to notice anomalies and trends. The bandwidth utilization by various protocols can also assist in managing bandwidth costs and may indicate the need for policy changes to control costs.
Per Source Host Firewall Statistics	This report provides a top level summary of all firewall activity across all firewalls for each source host attempting connections during the specified period. It categorizes events by criticality level and breaks down bandwidth utilization by packet direction and by the major categories of network traffic. This report is the starting point for investigating issues related to a specific source host. It may also be reviewed on a regular basis to spot hosts that are the sources of unusual event patterns relative to other hosts.



User Activity Reports

Report Name	Description
Excessive Password Failures	Lists users with excessive password failures on a host.
Authentications by Destination	Summary of the number of successful and failed logins to all hosts.
Authentications by User	Authentication successes and failures by originating host.
Authentication Summary	This report summarizes authentication events across the enterprise as reported by dedicated authentication applications and by operating system utilities.
Object Level Access Summary	Summarizes the number of users and processes opening, modifying, and deleting files
Web Surfing Summary	Sessions and requests from known users, average minutes spent surfing, and average hits per user

Email Activity Summary

Report Name	Description
Email Message Detail	Retrieves all mail arrival and delivery events.
Email Statistics Summary	Summarizes number of messages, delivery attempts, bytes, failures, and average delay.
Top Recipients	Email addresses most often sent to
Top Senders	Email addresses most often sent from

Firewall Activity / All Firewalls

Report Name	Description
Firewall Activity by Port	Summary of bytes sent to or from all source or destination ports.
Activity by Protocol by Direction	Summarizes activity by vendor and comm direction



About SenSage, Inc.

SenSage, the leading provider of enterprise security analytics, offers unparalleled performance and a scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store massive amounts of event log data. Our solutions empower companies to readily respond to business-critical threats, conduct thorough and precise investigations, and maintain compliant operations. Based in San Francisco, CA, SenSage currently protects Global 2000 customers in financial services, government, healthcare, manufacturing and technology. The company markets its product directly and through partners including Cerner, EMC, Hewlett-Packard, Sendmail and Lockheed Martin.

For more information, please visit www.sensage.com.

SenSage, Inc.
55 Hawthorne Street, Suite 700
San Francisco, CA 94105
415.808.5900
info@sensage.com