



SenSage offers unparalleled, enterprise-class scalability

Sarbanes-Oxley (SOX) Compliance Defined

The audit control sections of the regulations require that you:

- Capture and routinely audit security events that may impact the integrity of financial reporting. Specifically, all financial applications and relevant databases, servers, and network and security infrastructure.
- Follow detailed procedures based on COSO & COBIT audit frameworks. In most cases, this requires that systems administrators and business owners explicitly review and sign off all process documentation.

Simplify Audit Control Compliance for SOX

SenSage's SOX Analytics Package has everything needed to support the IT process controls in section 404 of Sarbanes-Oxley. With a host of log adapters for collecting pertinent event data and pre-defined reports that help quickly identify any security breaches involving your organization's financial data and systems, we automate and simplify the audit control process. This automation will save you time and money while ensuring that you avoid costly penalties and lengthy discovery procedures.

What the regulation doesn't spell out is how to meet these challenges. That's where SenSage can help. We've reviewed the regulations in depth as well as researched interpretation by the top auditing firms. Based on this research we developed a comprehensive package that will ensure your ability to comply and demonstrate your due diligence.

SenSage automates the collection and review terabytes of audit trail log data from all sources. By centralizing the logs into a single repository, SenSage facilitates the correlation needed to identify security breaches across systems - a critical asset for ensuring compliance as well as investigating any security breaches. In addition, SenSage's infrastructure provides the scalability to store and process searches of billions of records rapidly. The pre-defined reports enable internal auditors to easily perform spot checks and reviews. With its clustered architecture, SenSage also ensures full data redundancy and high availability.

Investigate Users

Report Name	Description
All Events by User	Lists all the events generated by an individual user
Auth Events by User Detail	List of user authentication events to financial systems
Authentication Details for User and Host	Displays authentication events for a particular user to any financial systems
Authentication Events by User Detail	Shows user details for authentication events to any financial systems
Authentications by Destination	Summary of the number of successful and failed logins to particular financial hosts.
Authentications by Source	Lists the number of users logging in, successfully and unsuccessfully, via a financial application.
Authentications by Source and User	Authentication successes and failures by originating host.
Excessive Password Failures	Lists users with more than a specified number of password failures
Logins to Critical Systems	This report allows security personnel to review user activity against critical financial systems



Activity on Financial Systems

Report Name	Description
Process Initiation Detail for Host and Name	Events between initiation and termination of a process
Process Initiations and Terminations by Name	Summarizes the initiations and terminations of processes
Process Initiations for Host	Summarizes the initiations and terminations of processes by source financial host
Rare Source Hosts for User Account	Alerts security personnel when a user logs in from a source host that is not usually the origination point of logins for that account. Can often be a tipoff for theft of identity.

Firewalls Protecting Financial Systems / 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 communication direction
Firewall Event Classification by Protocol	Provides details of the volume of each of the unique event types associated with each protocol and port. Firewall administrators can use to research anomalies in protocol/port usage seen in the firewall summary by protocol report.
Firewall Event Classification Summary	Shows how each unique event, as described by the vendor using either or both an event id and event description, has been classified in all other firewall summary reports, and how many such events were recorded. Assists in interpreting the summary reports and ensuring their accuracy. If events appear to be misclassified in this report, the administrator should consult the documentation to determine how to update the event classifications.
Per Firewall Activity by Protocol	Provides a breakdown of firewall events and bandwidth utilization by application protocol and port, on a per-firewall basis. The firewall administrator should regularly review 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. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.
Firewall Statistics Summary	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. Run hourly, daily, weekly and monthly, and review daily. Compare each period to summaries for previous periods using SenSage's multiple period display feature to spot 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	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.



Firewall Summary by Protocol by Direction	Distinguishes traffic by protocol and port based on whether the direction of the connection is incoming or outgoing. Some protocols may be acceptable for outgoing connections, but not acceptable for incoming connections, or vice versa. The firewall administrator should review to notice whether policy is being effectively enforced by the firewall configuration and should make configuration changes if actual traffic shows that policy violations are being allowed.
Firewall Summary by Rule	Provides the number of events that triggered each rule. Useful to look at trends and anomalies in rules usage over time to determine if the network is being accessed in new ways. Review rules usage to optimize firewall performance by streamlining rules definition. Only applies to firewall products that are rules-driven.
Blocked Hosts	The blocking or blacklisting of a host and the reason for the action.
Blocked Ports	The blocking or blacklisting of an access port and the reason for the action.

Firewalls Protecting Financial Systems / Firewall Activity by Source

Report Name	Description
Firewall Activity by Source and Port	Summarizes size and number of events by source host and port.
Firewall Denies by Source Host Detail	Displays connection requests denied by the firewall organized by source host
Firewall Denies by Source Host Detail and Rule	Displays connection requests denied by the firewall organized by source host and which rule caused that deny
Per External Address Event Classification by Protocol	Event actions classified by source host, vendor, application, destination port, and transport protocol.
Per External Source Event Classification Summary	External events organized by source host.
Per External Address Activity by Protocol	External events organized by source host and protocol.
Per External Address Firewall Statistics	Successful, failed, outbound, and inbound connections organized by source.
Per Internal Address Event Classification by Protocol	Displays summary of events classified by protocol
Per Internal Address Event Classification	Provides a breakdown of firewall event classifications for each internal address. Use to analyze anomalies found in higher level summary reports.
Per Internal Address Activity by Protocol	Displays accepted and denied connections organized by source, destination, and protocol.
Per Internal Address Firewall Statistics	Provides a summary of firewall events for each internal address. Review daily and weekly to detect internal addresses whose behavior is unusual relative to other addresses. Check trend reports based on this report to identify individual internal addresses that are behaving unusually relative to past behavior, which often indicates that they have been compromised or are being used in an unauthorized way.
Per Source Host Event Classification by Protocol	Provides the details of the volume of each of the unique event types associated with each protocol and port on a per-source host basis. Firewall administrators can use this report to track down the details of anomalies in protocol usage, event patterns, or patterns by source host seen in higher level reports.
Per Source Host Event Classification	Report shows details of the classifications of events seen for each source host. Allows the administrator to spot source hosts that trigger events that others do not, and can provide detail if anomalies are seen in higher level summaries by either source host or event classification.



Per Source Host Activity by Protocol	Provides a breakdown of firewall events and bandwidth utilization by application protocol and port, on a per-source IP basis. Can help the administrator identify which source hosts are responsible for anomalous port/protocol usage noticed on higher level summary reports.
Per Source Host Activity by Protocol	Provides the number of events that triggered each rule on a per source host basis. Useful to look at trends and anomalies in rules by host - if a host is suddenly triggering a high number of events for a new rule, it may indicate that this host is beginning to attack the network.
Per Source Host Firewall Statistics	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. The starting point for investigating issues related to a specific source host. Review on a regular basis to spot hosts that are the sources of unusual event patterns relative to other hosts.
Source Hosts Below Alert Threshold	IP addresses with top numbers of denials

Firewalls Protecting Financial Systems / Firewall Activity by Destination

Report Name	Description
Activity by Destination and Port	Firewall events summarized by destination host and port
Per Destination Server Event Classification by Protocol	Provides the details of the volume of each of the unique event types associated with each protocol and port on a per destination server basis. Firewall administrators can use this report to track down the details of anomalies in protocol usage, event patterns, or patterns by destination server seen in higher level reports.
Per Destination Server Event Classification	Shows details of the classifications of events seen for each destination server. Allows the administrator to spot destination servers that are the targets events that others are not, and can provide detail if anomalies are seen in higher level summaries.
Per Destination Host Activity by Protocol	Number of accept and deny events summarized by protocol and destination port
Per Destination Host Activity by Protocol	Provides the number of events that triggered each rule on a per destination host basis. Useful to look at trends and anomalies in rules by host - if a host is suddenly triggering a high number of events for a new rule, it may indicate that this host is beginning to attack the network.
Per Destination Server Firewall Statistics	Provides a top level summary of all firewall activity across all firewalls for each destination server for attempted connections during the specified period. Categorizes events by criticality level and breaks down bandwidth utilization by packet direction and by the major categories of network traffic. The starting point for investigating issues related to a specific destination server. Also review regularly to spot destinations that are the targets of unusual event patterns relative to other servers.



Firewalls Protecting Financial Systems / Individual Firewalls

Report Name	Description
Per Firewall Activity by Protocol by Direction	Distinguishes traffic by protocol and port based on whether the direction of the connection is incoming or outgoing. Some protocols may be acceptable for outgoing connections, but not acceptable for incoming connections, or vice versa. The firewall administrator should review to notice whether policy is being effectively enforced by the firewall configuration and make configuration changes if actual traffic shows that policy violations are being allowed. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.
Per Firewall Activity by Protocol	Provides the number of events that triggered each rule on a per-firewall basis. Useful to look at trends and anomalies in rules usage over time to determine if the network is being accessed in new ways. Review rules usage in order to optimize firewall performance by streamlining rules definition. Only applies to firewall products that are rules-driven. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.
Per Firewall Event Classification by Protocol	Provides the details of the volume of each of the unique event types associated with each protocol and port on a per-firewall basis. Firewall administrators can use this report to research anomalies in protocol/port usage seen in the firewall summary by protocol report. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.
Per Firewall Event Classification by Protocol by Direction	Firewall events summarized by origin, destination port, protocol, and direction of communication.
Per Firewall Event Classification Summary	Shows how each unique event, as described by the vendor using either or both an event id and event description, has been classified in all other firewall summary reports, and how many such events were recorded. Assists in interpreting the summary reports and ensuring their accuracy. If events appear to be misclassified in this report, the administrator should consult the documentation to determine how to update the event classifications. This variant of this report provides details on a per-firewall basis. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.
Per Firewall Statistics	Provides a top level summary of all firewall activity broken down by specific firewall address for the specified period. Categorizes events by criticality level and breaks down bandwidth utilization by packet direction and by the major categories of network traffic. It should be run hourly, daily, weekly and monthly, and reviewed daily. Compare each period to summaries for previous periods using SenSage's multiple period display feature to spot anomalies and trends. Anomalies may provide early warning of security or operational problems while trends can assist in security and operational planning. Firewall administrators responsible for only a subset of the firewalls listed on this report wish to have the SenSage administrator set up filters associated with their role based on the Reporter Hostname (IP) column.



Users to Investigate for Financial Fraud

Report Name	Description
Users Active Outside Business Hours	Shows users with activity outside of business hours for their location, with the exception of specifically exempted users. Use outside of business hours is frequently an indicator of insider account misuse problems. Should trigger examination of the specific activities outside of business hours using the appropriate investigation report.
Activity Outside Business Hours by User and Hour	Summarizes the applications used outside business hours by user and hour
User Activity Outside Business Hours Detail	Shows application activity outside of business hours
User Activity by Application Summary	Summarizes the applications used by each user
Users Authenticating From Multiple Hosts	Lists users successfully logging in from multiple source systems

IDS Activity for Financial Systems

Report Name	Description
IDS Alerts by Destination	Summary of IDS alerts by destination host
IDS Alerts by Destination and Event ID	IDS alerts by destination host and event description
IDS Alerts by Event ID	Summary of IDS alerts by application and description
IDS Alerts by Source	Intrusion Detection System alerts summarized by source host.
IDS Alerts by Source and Event ID	IDS alerts summarized by source host and event ID
IDS Alerts by Source Destination and Event ID	Summary of IDS alerts by application, source, destination, and description.
IDS Alert Summary	Summary of IDS alerts by application, event ID, and category

Email Activity Summary

Report Name	Description
Delay Histogram	Histogram of relative frequencies of message delays for mail servers.
Email Sender Recipient Profile	Summary of internal and external senders, recipients, and domains.
Email Statistics Summary	Summarizes number of messages, delivery attempts, bytes, failures, and average delay.
Errors by Relay	Number of errors summarized by relay
Message Detail	Detailed TO and FROM information about messages sent and received
Message Detail for User	Shows detail of communications data for a particular user
Message Size Histogram	Histogram of relative frequency of message sizes.
# of Recipients Histogram	Histogram of the number of recipients per mail message.
Top Correspondents	Lists the top senders and recipients of email for the system
Top From Domains	Domains most frequently sent from



Top Recipients	Email addresses most often sent to
Top Senders	Email addresses most often sent from
Top to Domains	Lists top domains to which mail messages will be delivered

Business Critical System Activity

Report Name	Description
Traffic to Critical Systems	Used by administrators to identify any unusual patterns of access to critical systems based on network traffic to these systems as recorded by firewalls. It depends on implementing load or query time lookups based on originating and reporting server IP's to criticality levels and line of business.
Logins to Critical Systems	Used by administrators to identify any unusual patterns of access to critical systems based on direct logins to the operating system. It depends on implementing load or query time lookups based on originating and reporting server IP's to criticality levels and line of business.
Events by Application	Allows security and operations personnel to review totals of events summarized by originator application and category and monitor trends and spot anomalies over time. Reveals when a particular application has a surge in activity, error, or operational/administrative events that should be investigated.
Events by Application and Host	Allows security and operational personnel to review totals of events by application and host. Filter to focus on hosts of a particular business criticality or associated with a particular line of business.
Events by Application and Host Business Group	Allows security and operational personnel to review totals of events by application and host business criticality and line of business. Useful for understanding whether critical servers are experiencing a notable change in event volumes.

Logins to Financial Systems

Report Name	Description
Access Privilege Changes	Allows security and compliance personnel to review all changes in access privileges for the specified interval.
Authentications by Source	authentications by source
Authentications by Source and User	authentications by source and user
Authentication by Destination	authentication by destination
Password Changes	password changes
Blocked Users	blocked users
Account Creation Summary	account creation summary
Account Administration Summary	account administration summary
Authentication Summary	Summarizes authentication events across the enterprise as reported by dedicated authentication applications and by operating system utilities.



Use of Privilege on Financial Systems

Report Name	Description
Admin Summary	Displays configuration change events.
Top Users of Privilege	Allows security and compliance personnel to identify the most frequent users of privilege via sudo, powerbroker, or other programs that allow ordinary users to temporarily assume super user privileges. Such use of privilege is frequently abused to make unauthorized system changes such as creating new user accounts or to view unauthorized data. For organizations implementing lookups to server criticality or line of business, also summarizes the number of uses of privilege for each user on the most critical servers.
Top Uses of Privilege	Allows security and compliance officers to review the most common activities performed using super user privileges. Reviewers should pay special attention to the use of privilege to add or change user accounts, switching to the super user's identity to perform a series of tasks, deletion of files, and other security-sensitive tasks.
Privileged Use of Session	Enables an investigator who is pursuing a suspected abuse of privilege to reconstruct all activities recorded on a specific server for a specific user following that user assuming a privileged identity. It follows the trail of all change user events until the user logs out or until the end of the query time range, whichever is sooner.
Privileged Use by User, Server and Activity	Enables security and compliance personnel to review privileged use summarized by user, server, and activity, and spot any unusual behaviors. For organizations who have enabled categorization of servers in their environment by line of business and criticality, this report displays these details and permits filtering to focus on higher criticality servers or specific business lines.

About SenSage, Inc.

SenSage, the leading provider of enterprise security analytics, offers unparalleled performance and a scalable means for organizations to centrally aggregate, efficiency 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