

Sensage Log Adaptor List – Updated November 2011

Firewalls / VPN

Aventail SSL VPN
Check Point Firewall-1 fwexport
Check Point Firewall-1 LEA *
Check Point VPN-1
Cisco ASA
Cisco FWSM *
Cisco PIX *
Cisco VPN Concentrator
Juniper Networks NetScreen *
Juniper Networks SSL VPN - Secure Access
Nortel Contivity VPN
Secure Computing Gauntlet (McAfee) *
Secure Computing Sidewinder G2 (McAfee) *
Symantec Enterprise Firewall

Routers / Switches

Cisco Catalyst Switch *
Cisco IOS *
HP ProCurve
Juniper Networks JUNOS

Servers / Desktops

Concurrent PowerMAX logs
HP OpenVMS system logs
HP NonStop EMS
HP NonStop SafeGuard *
HP-UX logs *
IBM AIX logs *
IBM VSE/ESA
Microsoft Windows logs *
Novell Netware system logs
Red Hat Linux logs *
SGI IRIX logs *
Sun Solaris logs *
SuSE Linux Syslog *

Web Proxy

BlueCoat CacheFlow
CA eTrust SiteMinder Secure Proxy Server
ContentKeeper logs
Microsoft ISA Web Proxy
NetApp NetCache
Squid.org Squid
Websense Web Security Suite

Intrusion Detection (IDS) / Intrusion Protection (IPS)

Cisco IPS Sensor
Cisco Secure IDS
Cisco Security Agent (Okena)
Enterasys Dragon IDS
HP Tipping Point
ISS Proventia IDS Sensor
ISS RealSecure
ISS Site Protector
Juniper Networks IDP (NetScreen)
McAfee Host Intrusion Prevention for Server
McAfee Network Security Platform (IntruShield) *
Snort (Open Source) *
SourceFire
SourceFire Management Console
TopLayer Attack Mitigator
Tripwire

Traffic Management

Nortel Alteon Load Balancer
Radware Linkproof

Traffic Analysis

Open Source TCP Dump
QoSient Argus

Remote Access

Microsoft Remote Access Server (RAS)
Nortel Annex

Network Monitoring

Fortinet Fortigate
LBNL Network Research Group arpwatch
Microsoft System Center Operations Manager (SCOM)

Other Network Sources

ISC DHCP
Microsoft DHCP

SIM / SEM / SIEM

ArcSight ESM (Enterprise Security Manager)
CA Audit
Cisco MARS
HP OpenView NNM
IBM Tivoli Netcool/NeuSecure
IBM Tivoli T/EC (Enterprise Console)
LogLogic
Novell Sentinel (e-Security)
Novell ZenWorks Remote Control
Trustwave Intellitactics NSM

Security Management Console

McAfee ePolicy Orchestrator (ePO) *
McAfee SCM (Messaging and Web Security) *
McAfee Total Protection (ToPS) for Network

Encryption and Key Management

HP Secure Key Manager *
Ingrian DataVault
Vormetric Coreguard

Sensage Self-Audit

Sensage Analyzer Activity Log *
Sensage Collector Transaction Log *
Sensage Collector Activity Log *
Sensage Scalable Log Server Transaction Log *

Email & IM

Communicator Bondhub IM
Exim Main log
IronPort Email Gateway
Postfix.org Postfix
McAfee Email and Web Security (MWS)
McAfee Secure Computing E-Mail Gateway (IronMail)
Microsoft Exchange *
Open Source MIMedefang
Open Source Postfix *
Open Source Smapd
Sendmail Flow Control
Sendmail Mailcenter logs
Sendmail Mailstream Manager
Sendmail MTA (Open Source) *
Sendmail Switch MTA

Web / App Server / Middleware

Apache HTTP Server logs *
BEA Tuxedo logs
BEA WebLogic Server
IBM IHS/WebSphere access log
IBM MQ Series
IBM WebSphere logs
IBM WebSphere Edge Server
Microsoft IIS *
Sun iPlanet Webserver

Vulnerability Management

ISS Internet Scanner
ISS System Scanner
McAfee Vulnerability Management Service (Foundstone) *
nCircle IP360 Appliance
Qualys QualysGuard

Anti-Virus / Anti-Spam

Barracuda Networks Web Filter
Clearswift MIMESweeper for SMTP
Sendmail Flow Control
Sendmail Mailcenter
Sendmail Mailstream Manager
Sendmail Message Proxy
Symantec Brightmail Anti-Spam
Symantec Enterprise Antivirus Corporate Edition
Symantec Enterprise Vault
Symantec Mail Security (SMS) Appliance
Symantec Mail Security (SMS) for Exchange
Symantec Mail Security (SMS) for SMTP 5.0
McAfee AntiVirus VirusScan
TrendMicro Control Manager
TrendMicro eManager
TrendMicro InterScan VirusWall

Access Control / Identity Management

Cisco ACS (Access Control Server) logs *
Cisco ACS / TACACS+ Radius *
CA Access Control
CA eTrust Siteminder Authentication Server
CA SiteMinder Web Access Manager
Juniper Networks Steel-belted RADIUS logs
Microsoft Active Directory
RADIUS logs (Open Source)
RSA ACE Server *
Sun ONE iPlanet Directory Server
Symark Powerbroker event log

Database

IBM DB2 z/OS
IBM DB2 UDB
Microsoft SQL Server
Oracle Alerter
Oracle Database
Oracle Fine Grained Auditing (FGA)
Sybase Adaptive Server Enterprise (ASE)

Database Activity Monitors

Guardium
Imperva

Mainframe

CA ACF2 TSO Violation
CA ACF2 General Resource Event Log
CA ACF2 Logon Access Report Log
CA ACF2 SMF Audit Logs
CA Top Secret SMF Audit Logs
IBM iSeries (AS/400) OS Logs

IBM RACF SMF Audit Logs

ERP / Financials / HR Systems

Digital Insight MIBS

Lawson Financials

Oracle PeopleSoft Application Server logs

Oracle PeopleSoft Enterprise

SAP Change Doc Log

SAP Security Audit Log

SAP Financial Accounting and Controlling (FI/CO)

SAP Material Management (MM)

SAP Sales and Distribution (SD)

SAP transaction log

SAP workflow log

Oracle Siebel

ePHI Patient Management

Cerner Millennium

McKesson Horizon

McKesson Star Audit

Call Detail Records (CDR) Mediation Systems

Comptel (mediation system)

Intec Mediation

3rd Party Audit Products

CA eTrust Audit

Concurrent PowerMAX C2 audit log

Fcheck (Open Source)

HP OpenVMS C2 audit logs

HP Tru64 C2 audit logs

IBM AIX C2 audit logs

IBM Tivoli Access Manager for O/S

Intersect Alliance Snare Linux C2 Audit

McAfee Policy Auditor

SE (Security Enhanced) Linux

SGI IRIX C2 Audit

Sun BSM (Basic Security Module) *

Other Infrastructure Applications

Citrix Metaframe

Merant Version Manager

Serena Dimension Version Manager

Novell FTP logs

Internet Banking Infrastructure

Magnet Internet Banking Business Suite

IBM Autonomic

IBM CBE (Common Based Event)

Service Assurance

EMC Smarts

Storage Management / File Servers

CA ARCserve

IBM Tivoli Storage Manager

Network Appliance Filer

Netezza Performance Server

Novell ZENworks Suite

Samba (Open Source)

Custom Data Sources

The term “custom data source” refers to any log source not currently supported by Sensage—such as those produced by business-critical applications or legacy management systems. Sensage simply requires a small amount of sample data to create a parsing statement and a list of column names into which data will be parsed. The patented Sensage data repository builds all data tables dynamically at load time, enabling full field-level reporting, analysis and investigation.

Some vendors use "universal" log parsers to accommodate unfamiliar data but can only parse it into simple tables of four or five fields (i.e., time/date and IP address).

Other vendors use generic indexing. Neither approach supports field-level reporting of custom data and instead allows only "Google-like" searches that return “Google-like” raw log entries.

Sensage is able to use its IntelliSchema Views to easily populate its out-of-the-box reports with custom sources allowing organizations to have a more complete view of their security and compliance environments.