Centralized Log Management

Log management is an important need in almost all enterprises. The need for a complete event log management solution is often underestimated; leading to long hours spent searching through tons of log messages to troubleshoot. Efficient event log analysis mitigates internal user threat, helps tighten security policies, reduces system downtime and increases network performance in the enterprise. More recently enterprises need to comply with various regulations such as HIPAA, GLBA, PCI and SOX. Apart from this, system administrators look at event logs as a critical source to troubleshoot performance problems on hosts across the network. Logs need to be archived for the purpose of network and regulatory auditing.

ManageEngine® EventLog Analyzer is a web-based, real-time log management solution that collects, analyzes, and reports on event logs from distributed Windows and UNIX hosts, IBM AS/400, Cisco Routers and Switches, any Syslog device and MS IIS Web & FTP Server, MS SQL & Oracle database, Windows & Linux DHCP and VMWare applications. EventLog Analyzer uses a bundled MySQL database for analysis and reporting and securely archives all logs collected, at periodic intervals. With advanced data filtering and log management, EventLog Analyzer helps administrators manage and report on event logs across the enterprise, in a simple and effective manner.

Key Features

- Real time, centralized log management
- Comprehensive set of canned reports, custom report creation and historical trending
- Compliance reports for GLBA, HIPAA, PCI and SOX acts
- Reports to Monitor and Audit Privileged User activities (PUMA Reports).
- Automatic, scheduled report generation and distribution
- Real time alert generation and notification
- Encrypted, hashed, time stamped log archive
- MSP/MSSP friendly rebranding

How can EventLog Analyzer help you?

- Determine unauthorized access attempts and other policy violations
- Monitor privileged user activity and understand internal security risks in your network
- Identify trends in user activity, server activity, peak usage times, etc.
- Abide by the regulatory compliance acts and avoid penal actions
- Get the IT department, internal and regulatory compliance audit read
- Monitor critical servers exclusively and set alerts
- Zero in on applications causing performance and security problems
- Ensure readiness to forensic analysis at anytime
Features & Benefits

**Comprehensive Event Collection** – collects application, system and security event data from enterprise wide Windows and Unix/Linux systems, applications, databases, Routers, Switches and other Syslog devices. Normalizes, filters and stores them all in a centralized event database for analysis.

**Internal Security Analysis** – identifies unauthorized and failed logins, and rogue user(s). Set alerts for suspicious hosts, and monitor events exclusively.

**Pre-built & Instant Reports in Multiple Formats** – comprehensive reports include top reports on events generated across hosts, users, processes, and host groups, apart from top events by count. Generate and view reports in HTML, PDF, and CSV formats.

**Compliance Reporting** – generate pre-defined and custom reports for Event logs & Syslogs, to meet HIPAA, GLBA, PCI and SOX compliance act requirements.

**PUMA Reports** – generate reports exclusively to monitor users in particular Privileged User to mitigate internal threats.

**Schedule and Distribute Reports** – automatically generate reports at specified time intervals and get them delivered via Email.

**Trend Reports** – view trends of events based on event severity and event type. Trends on alerts triggered are also available.

**Real-time Alerting & Notification** – automatic alerting allows you to set the specific criteria on hosts for which you need to be notified through Email, SMS or Program execution.

**Powerful Multi-level Filters and Drill-down** – define event filter to specify criteria such as event type, severity, etc. in reports. Drill down from event reports to see specific event details about a host or a group.

**Host Grouping** – group hosts together based on your business needs, generate event reports, and analyze trend patterns exclusively.

**Anytime, Anywhere Access and Management** – monitor hosts, generate reports and set up archive from just a web browser.

**Secured Archive** – archive log storage is encrypted to secure the contents and hashed, time-stamped to make it tamper-proof.

**Bundled Database** – MySQL database is pre-configured and bundled to store all log data. Additionally, MS SQL database supported.

**Host OS Support** – Can be installed and run on Windows and Linux systems making it suitable for deployment in a wide range of enterprises.

Trend reports show you event patterns across hosts for various event types and event severity parameters.

**Supported Hosts and Applications**

EventLog Analyzer can collect and report on event logs from the following operating systems, devices and applications:

- Linux - RedHat, Debian,
- UNIX - Solaris, HP-UX
- IBM AS/400, Switches and Routers - Cisco
- VMWare - Syslog versions
- SNARE for Windows & any Syslog supported device
- Microsoft IIS W3C Web, FTP Servers
- Windows, Linux DHCP Servers
- Microsoft SQL Server
- Oracle - Audit Logs

**For more information**
Website: [www.eventloganalyzer.com](http://www.eventloganalyzer.com)
Email: eventlog-support@manageengine.com
Phone: +1 888 720 9500

**Hardware Requirements**: Pentium 5, 1GHz, 1GB RAM, 1GB disk space for the product, monitor that supports 1024x768 resolution