

Features & Benets

Comprehensive Event Collection – collects application, system, and security event data from enterprise-wide Windows and UNIX systems, Cisco Routers and Switches, and other Syslog devices. Automatically stores them all in a centralized event database.

Exhaustive Application Log Analysis – analyzes the application logs like SQL, web and FTP server applications to enable the user to optimize the application and network performance.

Real-time Alerting & Automatic Notification – automatic alerting allows you to set the specific criteria on hosts/group of hosts for which you need to be notified.

Historical Trending – view trends of events based on event severity, and event type. Trends on alerts triggered are also available.

Compliance Reporting – generate pre-defined reports to meet HIPAA, GLBA, PCI, and Sarbanes-Oxley compliance requirements. Customize the pre-defined reports to suit your needs.

Create Reports for new Compliances – generate new reports to meet any new regulation to be complied with.

Pre-defined Event Reports – comprehensive reports include top reports on events generated across hosts, users, processes, and host groups, apart from top events by count.

Instant Reports – generate reports in real-time and get instant access into last events generated. View last events generated, for any host from which event logs are collected.

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.

Security Analysis – identify unauthorized and failed logins, and malicious user(s). Set alerts for suspicious hosts, and monitor events exclusively.

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

Anytime, Anywhere Access & Management – generate reports and set up archiving from just a web browser.

Built-in Database – integrated MySQL database is already configured to store all log data. No external database configurations are needed.

Support for MS SQL Database – supports MS SQL database so that the user has a choice to select.

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

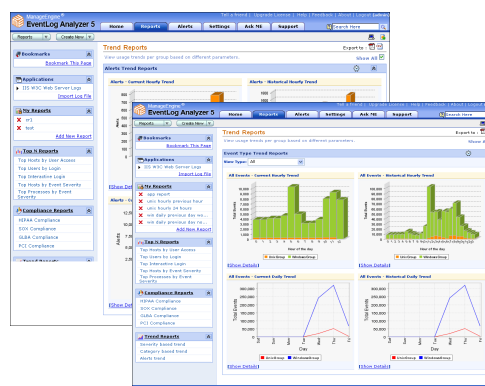
Customizable Reports – build custom reports with event filters and report format options tailored to meet your specific needs.

Report Scheduling – automatically generate reports at specified time intervals and get them delivered via e-mail.

Multiple Report Export Formats – generate and view reports in HTML, PDF, and CSV formats.

Supported Operating Systems EventLog Analyzer can collect and report on event logs from the following operating systems and devices:

- Windows NT/2000/2003/XP/Vista
- Linux - RedHat, Debian
- UNIX – Solaris, HP-UX, IBMAIX
- Cisco Switches and Routers
- Eventlogs forwarded as Syslogs from Windows
- And, Other Syslog devices



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

For more information
 Website : www.eventloganalyzer.com
 E-mail : support@eventloganalyzer.com
 Phone : +1 888 720 9500