ManageEngine
EventLog Analyzer
Powering IT ahead

Log Analytics & Compliance Reporting for SIEM

Unlock the Real Value of your Machine Generated Logs

IT Security and Compliance

Your IT infrastructure generates huge amount of logs every day and these machine generated logs contain vital information of all network activities such as user logons/logoffs, policy changes, object deletion and more. This information helps organizations to audit their network for internal threats and meet regulatory compliance requirements.

With organizations generating terabytes of log, analyzing these logs manually is painful and time consuming. That's where **Security Information and Event Management (SIEM)** solutions like EventLog Analyzer come in.

EventLog Analyzer helps organizations to collect, analyze, report, archive and search logs without any hassle. Unlike other IT management tools which are hard to use, difficult to install and expensive, EventLog Analyzer boasts about its ease of use, agent-less installation, instant reports, and cost effective pricing.

EventLog Analyzer offers a centralized repository to collect and archive machine generated logs from heterogeneous systems, network devices, and applications in your organization. The product supports a wide variety of IT Security and Regulatory Compliance reports such as SOX, HIPAA, FISMA, GLBA, ISO 27001/2, etc. Its intelligent log search and alerting engine helps network administrators to quickly troubleshoot and identify the root cause of IT problems. Also, EventLog Analyzer using its powerful **Universal Log Parsing and Indexing (ULPI)** technology allows you to index new fields and decipher any log data regardless of the source and log format.

Now you can stop sifting through voluminous logs manually and get it all done with EventLog Analyzer.

"The best thing, I like about the application, is the well structured GUI and the automated reports. This is a great help for network engineers to monitor all the devices in a single dashboard. The canned reports are a clever piece of work"

Joseph Graziano, Senior Network Engineer, Citadel

Why Choose EventLog Analyzer?

Unlock the Real value of your logs

- Supports an extensive array of machine generated logs which includes system logs, device logs, and application logs
- Provides a wide variety of reports for internal threat monitoring and regulatory compliance audits

Productivity improvement for IT teams

- From product deployment to report generation in minutes!
- Real-time alerts to network events enable IT to respond instantaneously to security threats

Meet dynamic business needs quickly

- Rapidly transforms machine generated logs into actionable information
- Receive reports in user friendly formats and meet regulatory business requirements

Attractive TCO & Rapid ROI

- No additional hardware required, minimal IT overhead, ease-of-deployment and ease-of-use ensures a low TCO and rapid ROI
- Starts at $795/year

EventLog Analyzer

Simplifying Log Management

Log Collection

- Agentless log collection (optional agents available)
- Collects logs from heterogeneous sources (Windows systems, Unix/Linux systems, Applications, Databases, Routers, Switches and other Syslog devices)

Privileged User Monitoring

- Collects and analyzes all events on user and administrator activity
- Get precise information of user access such as which user performed the action, what was the result of the action, on which server it happened and track down the user workstation from where the action was triggered

Compliance Reports

- Generate pre-defined/canned compliance reports for Event logs & Syslogs, to meet HIPAA, GLBA, PCI DSS, SOX, and FISMA
- Provides value added new feature to create custom report for new compliance to help comply with growing new regulatory acts demanding compliance in future

Internal Threat Monitoring

- Analyzes security events and identifies unauthorized and failed logins, and rogue user(s) in real-time
- Set alerts for suspicious hosts, and monitor events exclusively to find out who is responsible for them

Log Forensics

- Drill down to the raw log events and do a root cause analysis within minutes, and drastically reduce the time-to-remediate
- Generates network forensic reports like user activity reports, system audit reports, regulatory compliance reports, etc.

Log Search

- Conduct a search using Wild-cards, Phrases, Boolean operators, etc.
- Search for anything, not just a handful of pre-indexed fields, and quickly detect network anomalies - misconfigurations, viruses, user activities, system/applications errors, etc.

File Integrity Monitoring

- Centrally track all changes when files and folders are created, accessed, viewed, deleted, modified, renamed, etc.
- Get a complete audit trail of all the changes that happen on files and folders. Audit trail answers the 'what, when, where and how' of all changes in real-time!

Universal Log Parsing & Indexing (ULPI)

- Decipher any log data regardless of the source and log format
- Allows you to index any machine-generated logs (provided it is in human readable, non-encrypted format) by defining and extracting log fields of your choice using regular expression (regex) patterns

Real-time Alerting

- Automatic alerting allows you to receive real-time alert notifications directly via Email, SMS or Program execution
- Set Alert based on specific type of compliance violation for HIPAA, GLBA, PCI, SOX, FISMA, etc., based on failed logon attempts, policy changes, account changes, and audit logs cleared

Log Archive

- Automatically archives all machine generated logs - system logs, device logs & application logs to a centralized repository
- Archived log files are encrypted to make it secure and are hashed & time-stamped to make it tamper-proof

Minimum System Requirements: Pentium Dual Core, 1GHz, 2GB RAM, 5GB disk space, Windows™ 2000,XP, Vista,7 | Windows™ 2000,2003,2008 Servers or Linux

Trusted By

WELLS FARGO, Bank of America, at&t, hp, FUJITSU, vodafone, SONY

Awards

U.S.ARMY, SC MAGAZINE, Window Security.com READERS' CHOICE WINNER