About EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandates’ requirements with ease.

Jim Lloyd
Information Systems Manager,
First Mountain Bank

Windows event logs and device syslogs are a real time synopsis of what is happening on a computer or network. EventLog Analyzer is an economical, functional, and easy-to-utilize tool that allows me to know what is going on in the network by pushing alerts and reports, both in real time and scheduled. It is a premium software intrusion detection system application.

To learn more, visit www.eventlogalyzer.com
Get in touch with us at support@eventlogalyzer.com
Log management and compliance

- Comprehensive log collection
  - Monitor logs from your network servers, applications, and other devices.
  - Auto-discover log sources and add them for monitoring.
  - Centralized, secure log collection using either agentless or agent-based methods.
  - Custom log parser that can process and analyze any human-readable log format.

- Secure log archival
  Retain network log data for as long as needed. Archives are secured using time stamping and hashing techniques.

- Integrated compliance management
  - Get predefined reports and alerts that make PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX, and GDPR audits easier.
  - Create custom compliance reports to meet future or in-house regulations.

Auditing and analysis

- In-depth log auditing and analysis
  More than 1,000 predefined reports and alerts that provide information on events from various log sources, such as:
  - **Network devices**: Configuration or rule changes, privileged user account misuse, failed logon activities.
  - **Applications**: Database activity, column integrity, user account changes.
  - **Servers and workstations**: Logon activity, registry changes, commands executed.
  - **Vulnerability scanners**: Top vulnerabilities, exposed ports.

- Built-in file integrity monitoring
  Track all changes to critical files and folders on both Windows and Linux platforms instantly.

Network security

- Real-time event log correlation
  Discover security incidents by correlating events across your network. Includes more than 30 predefined correlation rules and a custom correlation rule builder.

- Dynamic threat intelligence
  Detect interactions with malicious entities using the built-in threat intelligence module.

- Efficient log forensics
  Perform high-speed log search using flexible search options, discover the root cause of attacks, and perform forensic investigations.

- Streamlined incident management
  - Use the built-in ticketing system to assign incidents as tickets, track their status, and speed up the incident resolution process.
  - Forward incident information and raise tickets in your help desk tool—ServiceNow, ServiceDesk Plus, JIRA, Zendesk, and more.