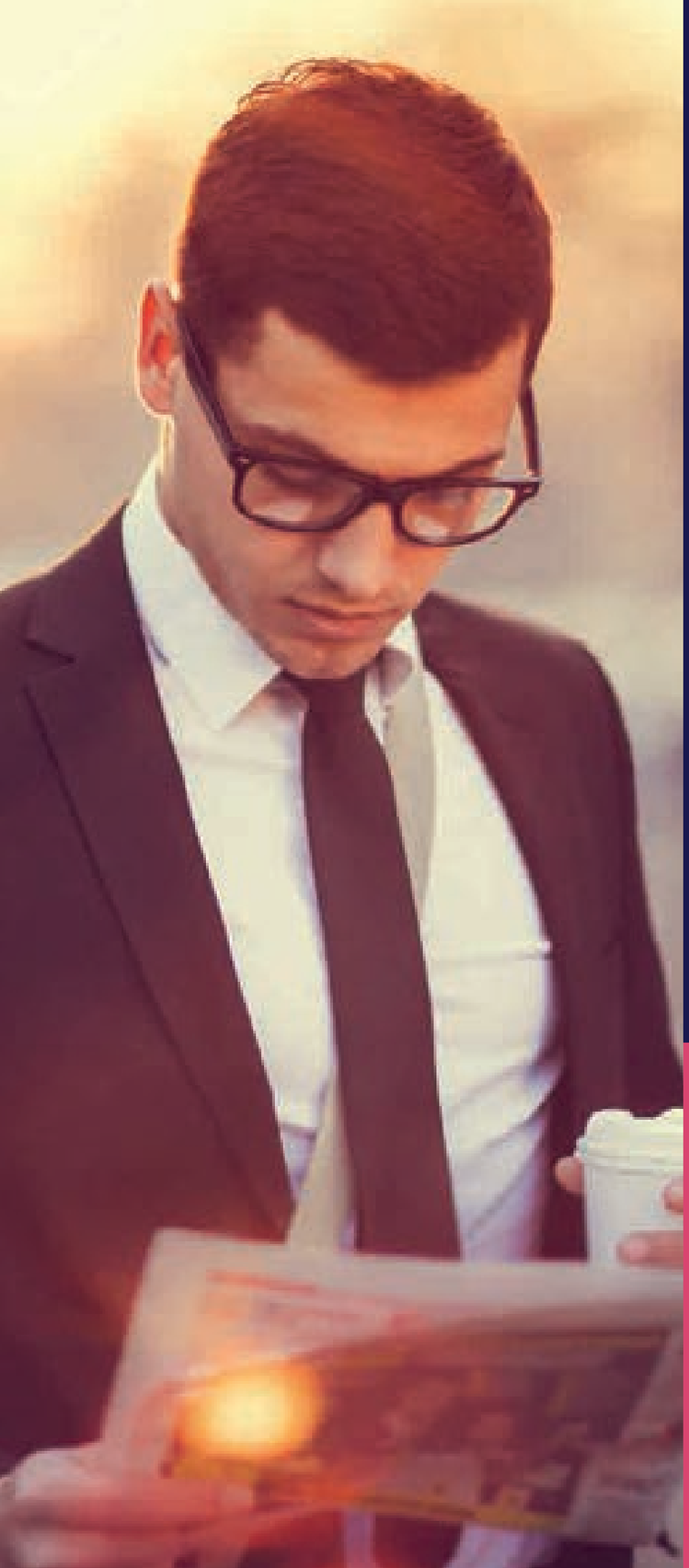
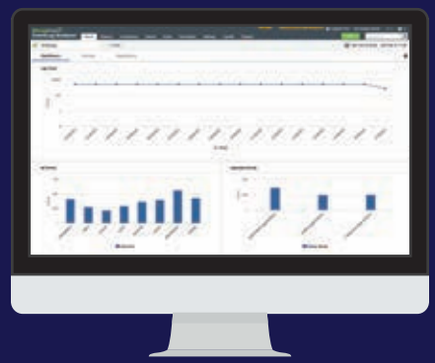




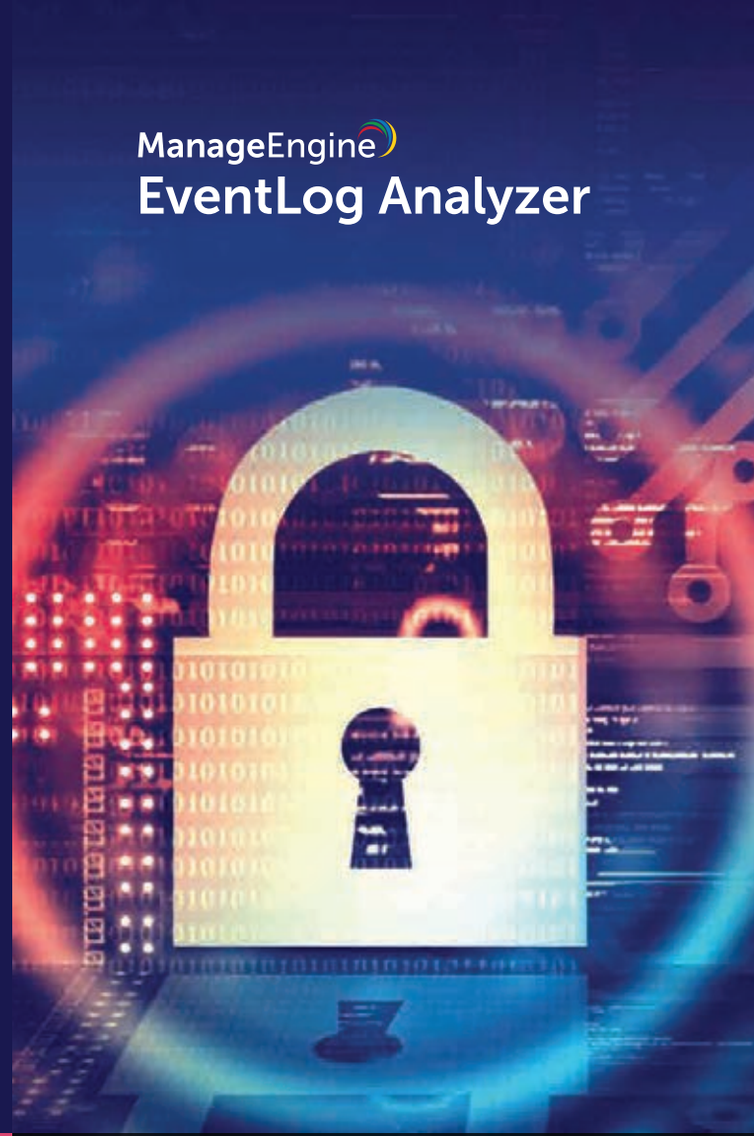
About Us

ManageEngine EventLog Analyzer is a web-based, real-time log management, and IT auditing solution for SIEM needs. The solution provides insightful security information by analyzing log data from all the devices across the network. Offers prepackaged reports and alerts for security, auditing, and compliance needs.

To learn more, visit
www.eventloganalyzer.com

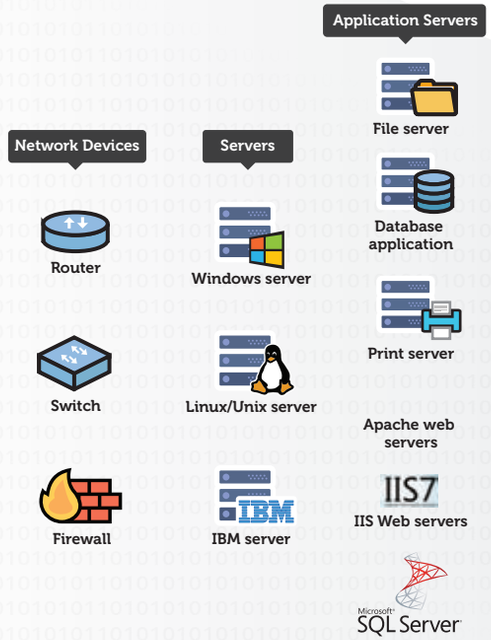
Get in touch with us at
support@eventloganalyzer.com

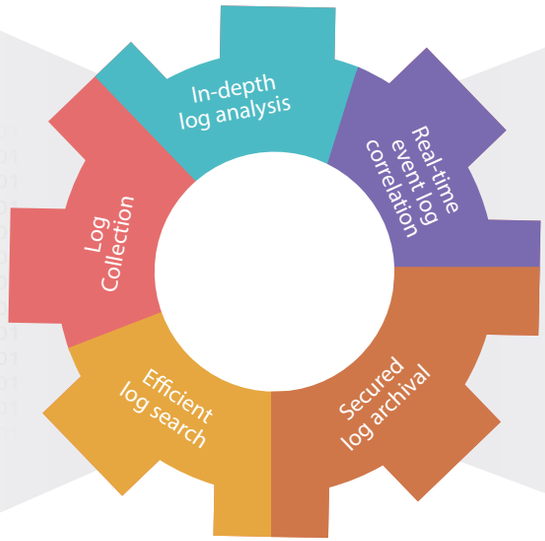
ManageEngine
EventLog Analyzer



Your perfect security and auditing partner!

www.eventloganalyzer.com





- Perimeter network devices auditing
- Web server auditing
- Database auditing
- Threat intelligence
- Integrated compliance management
- In-built file integrity monitoring

Comprehensive Log Collection

- **Supports 700+ log sources across 70+ vendors. Centrally collects logs from**
  - Perimeter network devices such as routers, switches, firewalls, and IDS/IPS.
  - Critical Linux/Unix servers, Windows servers, file servers, print servers, and more.
  - Business-critical applications such as MS SQL and Oracle database, IIS and Apache web servers, and more.
  - IBM AS400 machine
  - VMware and vCenter systems
  - Windows workstations
- **Offers both agentless and agent based log collection.**
- **Includes custom log parser for analyzing any in-house application log data.**

In-depth log analysis

Gain better visibility into network anomalies and security incidents with intuitive dashboards and 1000+ out-of-the-box reports.

Real-time event log correlation

Mitigate security threats effectively by correlating event log data in real-time. Recreate security attacks using the custom correlation rule builder.

Effcient log search

Perform high-speed log search with various search options such as boolean search, range search, group search, and more to find out root cause of attacks. Save the search results as forensic reports and create alert profiles based on the search queries to mitigate attacks of same kind in future.

Securely archive log data

For a custom period, securely archive the collected log data using the time stamping and hashing techniques.

Perimeter network devices auditing

Guard the perimeter devices by monitoring critical changes including configuration or rule changes, privilege user account misuse, failed logon activities and more.

Secure business critical applications

Protect important business apps including IIS and Apache web servers, Oracle and MS SQL databases and more by continuously auditing critical changes.

Augmented threat intelligence platform

Identifies malicious communications with blacklisted IPs, URLs, and domains by corroborating data from threat intelligence services.

Provides deep insights into the threats flagged such as the reputation score, geolocation of the malicious source, threat category, and more to facilitate quick incident investigation and response.

Integrated compliance management

Get out-of-the-box reports and alerts for PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX, and more. Modify the existing template or create your own compliance reports.

In-built file integrity monitoring

Track critical changes to confidential files and folders instantly.

Securing remote work

Tracks VPN usages and alerts upon unusual VPN activities, VPN access from malicious source, and more.

Monitors the active VPN connections and alerts you upon reaching the threshold limit of connections to avoid operational bottlenecks.