- 按需购买许可
- 部署简单快速
- 直观的用户界面

开箱即用

EventLog Analyzer 优势

技术领先

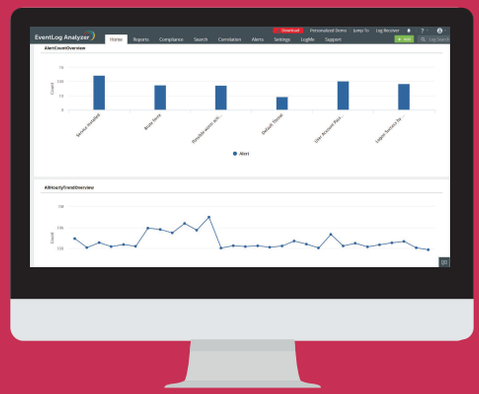
- 支持700多个日志源
- 支持50多家厂商
- 1000多个预置报表及告警配置文件

综合关联分析

- 智能事件关联分析
- 动态智能威胁感
- 知简化事件管理流程

Windows事件日志和设备系统日志是计算机或网络上发生的事情的实时概要。EventLog Analyzer是一个经济实用且易于使用的工具，通过实时和定时推送警报和报告，我可以了解网络中发生了什么。它是一个带有入侵检测系统功能的高级日志分析软件。

Jim Lloyd
某银行信息系统经理



关于EventLog Analyzer

EventLog Analyzer是一款基于web的实时日志管理和抵御网络安全攻击的合规解决方案。它既能够帮助企业满足他们的设备审计需要，又可以提供丰富的开箱即用的合规报表和告警，进而满足日趋严格的法律法规要求。

了解更多内容，您可以访问
https://www.manageengine.cn/products/eventlog/

支持邮箱
support@manageengine.cn

ManageEngine
EventLog Analyzer

您的最佳安全审计伙伴!

https://www.manageengine.cn/products/eventlog/

网络设备

路由器

交换机

防火墙功能

服务器

Windows 服务器

Linux / Unix 服务器

IBM 服务器

应用服务器

文件服务器

数据库应用

打印服务器

Apache 服务器

IIS Web 服务器

SQL Server

ORACLE

用户

工作站

自定义日志

- 外部网络设备审核
- Web 服务器审核
- 数据库审核
- 情报威胁
- 集成合规管理
- 内置文件完整性监控

日志管理及合规

日志收集广泛

- 监控您的网络服务器，应用和其它设备
- 自动发现添加日志源并进行监控
- 采用代理及非代理模式集中安全的收集日志
- 自定义日志解析器可以处理并分析任何人类可读格式的日志

安全日志存档

根据需要保留网络日志数据，通过时间戳以及散列技术确保日志安全。

合规管理

- 内置的报表和告警帮助您满足PCI DSS, FISMA, ISO 27001, GLBA, HIPAA,SOX, a以及 GDPR合规要求。
- 创建自定义合规报表特定的法规要求

审计和分析

深入的日志审计和分析

超过1000个内置报表和告警为您提供各种有价值信息：

- 网络设备：配置或规则变更，特权用户账号滥用，登录失败活动。
- 应用：数据库活动，数据完整性，用户账号变动。
- 服务器和工作站：登录活动,注册表变更，执行的命令。
- 漏洞扫描器：漏洞排行，暴露的端口。

内置文件完整性监控

跟踪所有重要文件或文件夹的变更，既支持windows平台，也支持Linux平台。

网络安全

实时事件日志关联

通过关联网络中的事件发现安全隐患。还为您提供了30种预置相关性规则以及自定义规则构建器。

动态威胁情报

使用内置的威胁情报模块检测与恶意实体的交互活动。

高效日志取证

使用灵活的搜索功能，执行高速日志搜索，发现攻击的根源，并进行调查取证。

简化的事件管理

- 使用内置工单系统将事件作为工单进行指派，跟踪其状态，以及加快事件解决过程。
- 将故障信息转发到您的—ServiceNow, ServiceDesk Plus, JIRA, Zendesk等帮助台工具中并作为工单提交。