- Licencias que le permiten solo pagar por lo que necesita
- Implementación rápida y fácil
- Interfaz de usuario intuitiva

Las EventLog Analyzer ventajas

Simple

Avanzado

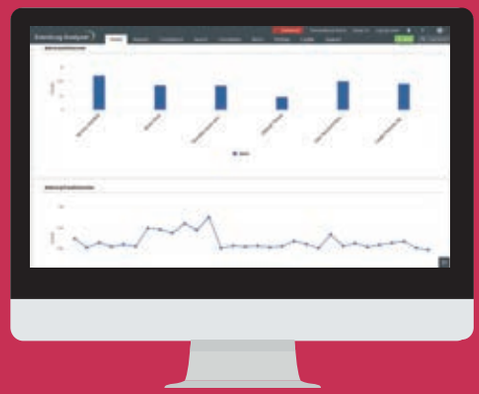
- 700+ fuentes de log soportadas
- 50+ proveedores soportados
- 1000+ plantillas de informes predefinidos y perfiles de alerta

Integral

- Correlación de eventos avanzada
- Inteligencia de amenazas dinámica
- Gestión de incidentes optimizada

Los logs de eventos de Windows y los syslogs del dispositivo son un resumen en tiempo real de lo que sucede en un equipo o red. EventLog Analyzer es una herramienta económica, funcional y fácil de usar que permite saber qué está sucediendo en la red mediante alertas e informes, tanto en tiempo real como programados. Es una aplicación de sistema de detección de intrusos de software premium.

Jim Lloyd
Gerente de Sistemas de Información
First Mountain Bank



Acerca de EventLog Analyzer

EventLog Analyzer es una solución web de cumplimiento de TI y gestión de logs en tiempo real que combate los ataques a la seguridad de la red. Gracias a las funciones integrales para la gestión de logs, EventLog Analyzer ayuda a las organizaciones a satisfacer sus diversas necesidades de auditoría. También ofrece informes y alertas de cumplimiento out-of-the-box que cumplen fácilmente los estrictos requisitos reglamentarios de TI.

Para obtener más información, visite
www.eventloganalyzer.com

Contáctenos en
latam-sales@manageengine.com

ManageEngine
EventLog Analyzer

¡Su socio perfecto de seguridad y auditoría!

www.eventloganalyzer.com

Cumplimiento y gestión de logs

Recopilación de logs integral

- Monitoree los logs de sus servidores de red, aplicaciones y otros dispositivos.
- Descubra automáticamente las fuentes de log y agrégelas para monitorearlas.
- Recopilación de logs centralizada y segura utilizando métodos sin agente o basados en agente.
- Analizador de logs personalizado para analizar cualquier formato de log legible por humanos.

Archivo de logs seguro

Conserve los datos de log de la red durante el tiempo que sea necesario. Los archivos se protegen con marcas de tiempo y valores hash.

Recopilación de logs integral

- Obtenga informes y alertas predefinidos que facilitan las auditorías de PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX y GDPR.
- Cree informes de cumplimiento personalizados para cumplir con las regulaciones futuras o internas.

Auditoria y análisis

Auditoría y análisis exhaustivos de logs

Más de 1.000 informes y alertas predefinidos que proporcionan información sobre eventos de varias fuentes de log, como:

- **Dispositivos de red:** Cambios de configuración o reglas, uso indebido de la cuenta de usuario privilegiado, actividades de inicio de sesión fallidas.
- **Aplicaciones:** Actividad de la base de datos, integridad de la columna, cambios en la cuenta del usuario.
- **Servidores y estaciones de trabajo:** Actividad de inicio de sesión, cambios en el registro, comandos ejecutados.
- **Analizadores de vulnerabilidades:** Principales vulnerabilidades, puertos expuestos.

Monitorización de la integridad de archivos pre-integrada

Rastree al instante todos los cambios en archivos y carpetas críticos en plataformas Windows y Linux.

Seguridad de la red

Correlación de logs de eventos en tiempo real

Descubra incidentes de seguridad al correlacionar los eventos en su red. Incluye más de 30 reglas de correlación predefinidas y un generador de reglas de correlación personalizadas.

Inteligencia de amenazas dinámica

Detecta interacciones con entidades maliciosas mediante el módulo de inteligencia de amenazas incorporado.

Análisis forenses de logs eficiente

Realice búsquedas de logs rápidas utilizando opciones de búsqueda flexibles, descubra la causa raíz de los ataques y realice investigaciones forenses.

Gestión de incidentes optimizada

- Utilice el sistema de tickets incorporado para asignar incidentes como tickets, realizar un seguimiento de su estado y acelerar el proceso de resolución de incidentes.
- Reenvíe la información sobre incidentes y emita tickets en su herramienta de mesa de ayuda: ServiceNow, ServiceDesk Plus, JIRA, Zendesk y más.