- Licenciamento que lhe permite pagar apenas o necessário
- Implantação rápida e fácil
- Interface de usuário intuitiva

Simples

A vantagem do EventLog Analyzer

Inovador

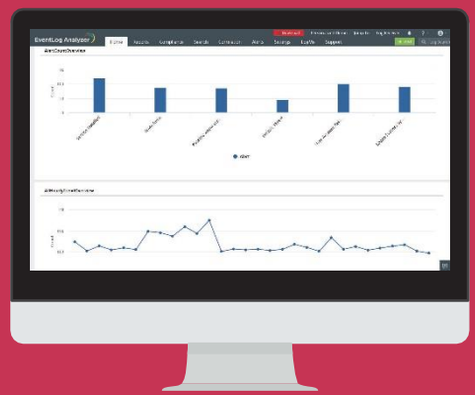
- Compatível com +700 fontes de log
- Compatível com + 50 fornecedores
- +1.000 modelos de relatório predefinidos e perfis de alerta

Abrangente

- Correlação de eventos avançada
- Inteligência dinâmica contra ameaças
- Gerenciamento simplificado de incidente.

Os logs de eventos do Windows e Syslogs dos dispositivos constituem uma sinopse em tempo real do que está acontecendo em um computador ou rede.
O EventLog Analyzer é uma ferramenta econômica, funcional e fácil de usar, que me permite saber o que está acontecendo na rede ao enviar alertas e relatórios, tanto em tempo real quanto agendados. É uma aplicação premium com um sistema de detecção de intrusão de software.

Jim Lloyd
Gerente de Sistemas de Informação, First Mountain Bank



Sobre o EventLog Analyzer

O EventLog Analyzer é uma solução de gerenciamento de logs e conformidade de TI baseada na web, em tempo real, que combate ataques de segurança de rede.

Com capacidades abrangentes de gerenciamento de logs, o EventLog Analyzer ajuda as organizações a atenderem às diversas necessidades de auditoria. Ele também oferece alertas e relatórios de conformidade prontos para uso, que facilmente atendem aos rigorosos requisitos regulatórios de TI.

Para saber mais, visite:
www.manageengine.com/br/eventlog/

Entre em contato conosco
support@eventloganalyzer.com

ManageEngine

EventLog Analyzer

Seu parceiro perfeito de segurança e auditoria!

www.manageengine.com/br/eventlog/

Gerenciamento de logs e conformidade

Coleta abrangente de logs

- Monitore logs de seus servidores, aplicações e outros dispositivos de rede.
- Descubra automaticamente as fontes do log e adicione-as para monitoramento.
- Coleta de log centralizada e segura usando métodos sem agente ou baseados em agente.
- Interpretador de logs personalizado que pode processar e analisar qualquer formato de log legível por pessoas.

Arquivamento automático de logs

Retenha os dados do log de rede durante o tempo necessário. Os arquivos são protegidos usando técnicas de estampagem de tempo e hashing.

Gerenciamento da conformidade integrado

- Obtenha relatórios e alertas predefinidos que facilitam as auditorias de conformidade com os regulamentos de PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX e RGPD.
- Crie relatórios de conformidade personalizados para cumprir regulamentos futuros ou internos.

Auditoria e análise

Auditoria e análise de logs aprofundadas

Mais de 1.000 relatórios e alertas predefinidos que fornecem informações sobre eventos de várias fontes de log, como:

- **Dispositivos de rede:** Alterações de configuração ou regra, uso incorreto da conta de usuário privilegiado, atividades de logon com falha.
- **Aplicações:** Atividade do banco de dados, integridade da coluna, alterações da conta de usuário.
- **Servidores e estações de trabalho:** Atividade de logon, alterações no registro, comandos executados.
- **Scanners de vulnerabilidade:** Principais vulnerabilidades, portas expostas.

Monitoramento integrado da integridade de arquivos

Acompanhe instantaneamente todas as alterações em arquivos e pastas crítics nas plataformas Windows e Linux.

Segurança de rede

Correlação de logs de eventos em tempo real

Descubra os incidentes de segurança correlacionando eventos em toda a rede. Inclui mais de 30 regras de correlação predefinidas e um construtor de regras de correlação personalizado.

Inteligência dinâmica contra ameaças

Detecte interações com entidades mal-intencionadas utilizando o módulo integrado de inteligência contra ameaças.

Perícia de logs eficiente

Execute uma pesquisa de log de alta velocidade usando opções de pesquisa flexíveis, descubra a causa-raiz dos ataques e execute investigações forenses.

Gerenciamento de incidentes dinamizado

- Use o sistema integrado para atribuir incidentes como tickets, controlar o seu estado e acelerar o processo de resolução de incidentes.
- Encaminhe informações sobre incidentes e crie tickets na sua ferramenta de suporte técnico – ServiceNow, ServiceDesk Plus, JIRA, Zendesk e muito mais.