

- Licence qui vous permet de ne payer que ce dont vous avez besoin
- Déploiement simple et rapide
- Interface utilisateur intuitive

Facile

**L'avantage
EventLog Analyzer**

En pointe

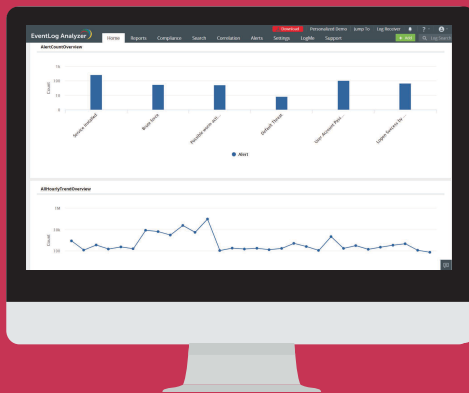
- +700 sources de journaux prises en charge
- +50 fournisseurs pris en charge
- +1000 modèles de rapports et profils d'alerte prédéfinis

Complet

- Corrélation d'événement avancée
- Intelligence dynamique sur les menaces
- Gestion simplifiée des incidents

Les journaux d'événements Windows et les journaux système des périphériques sont un synopsis en temps réel de ce qui se passe sur un ordinateur ou un réseau. EventLog Analyzer est un outil économique, fonctionnel et facile à utiliser qui me permet de savoir ce qui se passe dans le réseau en envoyant des alertes et des rapports, à la fois en temps réel et programmés. C'est une application de système de détection d'intrusion logicielle premium.

Jim Lloyd,
Directeur des Systèmes d'Information,
First Mountain Bank



À propos d'EventLog Analyzer

EventLog Analyzer est une solution Web de gestion des journaux en temps réel et de conformité informatique qui protège des attaques de sécurité réseau. Avec des fonctionnalités complètes de gestion des journaux, EventLog Analyzer aide les organisations à répondre à leurs divers besoins d'audit. Il offre également des rapports de conformité et des alertes prêts à l'emploi qui répondent facilement aux exigences strictes des réglementations informatiques.



Pour en savoir plus, visitez
www.eventloganalyzer.com



Contactez-nous à
support@eventloganalyzer.com

ManageEngine
EventLog Analyzer



**Votre partenaire de sécurité
et d'audit parfait!**

www.eventloganalyzer.com



Gestion des journaux et conformité

Collection complète de journaux

- Surveillez les journaux de vos serveurs réseau, applications et autres périphériques.
- Collecte complète de journaux
- Détectez automatiquement les sources de journaux et ajoutez-les pour la surveillance.
- Collecte de journaux centralisée et sécurisée à l'aide de méthodes sans agent ou basées sur des agents.
- Analyseur de journal personnalisé qui peut traiter et analyser tout format de journal lisible par l'homme.

Archivage sécurisé des journaux

Conservez les données du journal du réseau aussi longtemps que nécessaire. Les archives sont sécurisées à l'aide de techniques d'horodatage et de hachage.

Gestion de la conformité intégrée

- Obtenez des rapports et des alertes prédéfinis qui facilitent les audits PCI DSS, FISMA, ISO 27001, GLBA, HIPAA, SOX et GDPR.
- Créez des rapports de conformité personnalisés pour répondre aux réglementations futures ou internes.



Audit et analyse

Audit et analyse détaillés des journaux

+1.000 rapports et alertes prédéfinis qui fournissent des informations sur les événements provenant de diverses sources de journaux, telles que:

- Périphériques réseau: Modifications de la configuration ou des règles, utilisation abusive d'un compte d'utilisateur privilégié, activités de connexion échouées
- Applications: Activité de la base de données, intégrité des colonnes, changements de compte utilisateur.
- Serveurs et postes de travail: Activité de connexion, modifications du registre, commandes exécutées.
- Scanners de vulnérabilités: principales vulnérabilités, ports exposés.

Surveillance de l'intégrité des fichiers

Suivez instantanément toutes les modifications apportées aux fichiers et dossiers critiques sur les plates-formes Windows et Linux.



Sécurité de réseau

Corrélation du journal des événements en temps réel

Détectez les incidents de sécurité en corrélant les événements sur votre réseau. Comprend plus de 30 règles de corrélation prédéfinies et un générateur de règles de corrélation personnalisé.

Intelligence dynamique sur les menaces

Détectez les interactions avec des entités malveillantes à l'aide du module intégré de renseignement sur les menaces.

Analyse forensique efficace des journaux

Effectuez une recherche rapide dans les journaux à l'aide d'options de recherche flexibles, découvrez la cause première des attaques et effectuez des enquêtes forensiques.

Gestion simplifiée des incidents

- Utilisez le système de ticket intégré pour attribuer des incidents en tant que tickets, suivre leur statut et accélérer le processus de résolution des incidents.

Transférez les informations sur les incidents et

- augmentez les tickets dans votre outil d'assistance: ServiceNow, ServiceDesk Plus, JIRA, Zendesk, etc.