McAfee Enterprise Log Manager

Réduction des coûts de conformité grâce à l'automatisation de la collecte, du stockage et de la gestion des journaux

La collecte et le stockage adéquats des journaux permettent de réduire le coût de la conformité tout en offrant une piste d'audit des activités à la fois claire et irréfutable. McAfee® Enterprise Log Manager collecte, compresse et stocke efficacement tous les fichiers journaux. De plus, l'intégration avec McAfee Enterprise Security Manager fournit des fonctionnalités avancées de recherche, d'analyse, de mise en corrélation, d'alerte et de génération de rapports. La solution améliore également les investigations numériques en rendant accessibles en un clic les enregistrements de journal de la source d'origine, à partir de tous les événements et alertes.

Principaux avantages

- Collecte et conservation universelles des journaux pour respecter les exigences de conformité
- Stockage et conservation flexibles pour s'adapter à chaque source de journalisation
- Prise en charge de la chaîne de traçabilité et des investigations numériques
- Analyse et recherche dans les journaux
- Stockage des journaux en local ou sur un réseau de stockage SAN managé
- Intégration complète avec McAfee Enterprise Security Manager
- Options de déploiement hybrides et flexibles comprenant des appliances physiques et virtuelles

Aucun fichier journal n'échappe à McAfee Enterprise Log Manager : ils sont tous collectés, signés, enregistrés. La solution automatise la gestion et l'analyse de tous les types de journaux, y compris les journaux d'événements Microsoft Windows et les journaux système, de bases de données et d'applications. Ceux-ci sont signés et validés afin de garantir leur authenticité et leur intégrité, une mesure imposée par les impératifs de conformité réglementaire. De plus, des rapports et des ensembles de règles de conformité prêts à l'emploi permettent de démontrer facilement la mise en œuvre des stratégies et le respect des réglementations au sein de l'entreprise.

Cet environnement étroitement intégré de collecte, de gestion et d'analyse des journaux renforce la sécurité de l'entreprise tout en facilitant considérablement le respect des obligations réglementaires, notamment les normes PCI DSS et NERC-CIP ainsi que les lois HIPAA, FISMA, GLBA et SOX.

Gestion intelligente des journaux

McAfee Enterprise Log Manager collecte les journaux de façon intelligente, en conservant les fichiers nécessaires pour démontrer votre conformité, puis en soumettant à une analyse syntaxique ceux qui présentent un intérêt pour la sécurité. Vous pouvez conserver les journaux dans leur format d'origine aussi longtemps que nécessaire afin de respecter les impératifs de conformité réglementaire de votre entreprise. En outre, dans la mesure où la solution n'apporte aucune modification aux fichiers journaux d'origine, elle respecte les principes de chaîne de traçabilité et de non-répudiation.

Les besoins en matière de rétention des informations varient selon la source de journalisation et les impératifs de conformité auxquels l'entreprise est tenue. McAfee Enterprise Log Manager utilise des pools de stockage facilement personnalisables pour garantir un stockage approprié des journaux pendant la durée nécessaire. Choisissez l'option de stockage la mieux adaptée à vos besoins : stockage sur les disques durs des appliances et cartes Fibre Channel en option pour les réseaux SAN haute vitesse.

Les fichiers journaux n'apportent pas en tant que tels des réponses à toutes vos questions. Ils contiennent bien évidemment d'importants éléments de preuve et constituent un lien précieux pour établir la chaîne de traçabilité. Toutefois, ils soulèvent également des questions importantes en termes de sécurité. Ainsi, un journal d'accès peut indiquer un nom d'utilisateur, mais sans pour autant fournir d'informations sur le rôle ou les privilèges de cet utilisateur. De même, il se peut que le journal précise le système soumis à l'accès, sans détailler les types de données qu'utilise ce système ni dévoiler les accès autorisés.

Intégration avec McAfee Enterprise Security Manager

McAfee Enterprise Log Manager est un composant intégré à McAfee Enterprise Security Manager, proposé en option. Alors que McAfee Enterprise Log Manager prend en charge le stockage des journaux, McAfee Enterprise Security Manager assure l'analyse syntaxique approfondie, la normalisation et l'exploration des informations de journal, les rendant immédiatement disponibles pour des activités liées à la sécurité informatique telles que la réponse aux incidents ou l'investigation en temps réel.

Lorsqu'un événement de sécurité est généré, les fichiers d'événements analysés sont directement liés au fichier journal d'origine et à l'enregistrement de journal correspondant. Par conséquent, ceux-ci sont accessibles en un clic tout au long des processus de gestion des événements et d'investigation numérique. Il n'est pas nécessaire de passer par une quelconque étape supplémentaire, de lancer une autre application ou de perdre du temps à explorer les journaux manuellement.

Abondance de contexte pour l'analyse

McAfee Enterprise Security Manager et McAfee Enterprise Log Manager fournissent du contexte sur tous les journaux, augmentant ainsi la valeur de chaque enregistrement analysé. Voici quelques-unes des informations disponibles :

- Adresse IP source ou de destination
- Contexte relatif à l'identité
- Nom d'hôte ou service utilisé
- Informations de vulnérabilité fournies par une solution d'évaluation ad hoc
- Informations sur la topologie du réseau
- Informations sur les stratégies et la confidentialité

Pools de stockage flexibles

Grâce aux pools de stockage, McAfee Enterprise Log Manager offre plus de flexibilité dans la conservation des journaux à long terme. Les pools de stockage sont des groupes virtuels de stockage utilisable pouvant être distribués vers divers groupes de périphériques de stockage physiques (stockage local, NFS, SAN, CIF, etc.) en fonction des besoins de gestion des journaux de l'entreprise.

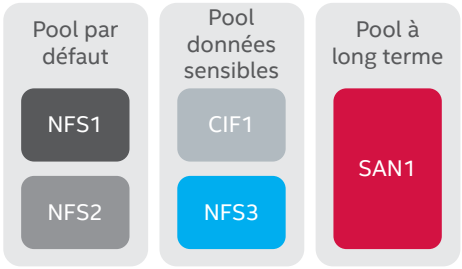

Figure 1. Conservation des journaux personnalisée à l'aide de pools de stockage flexibles

Dans la mesure où un pool de stockage peut comprendre plusieurs périphériques, et où les données peuvent être affectées à un pool spécifique en fonction du périphérique source, il est possible de stocker les journaux dans des emplacements distincts selon qu'ils ont trait à la sécurité, à la conformité, à la confidentialité ou à d'autres aspects. Par exemple, le stockage de journaux essentiels pour la conformité peut être confié à un pool constitué de plusieurs périphériques de stockage réseau redondants, tandis que les journaux de moindre importance seront stockés sur des systèmes moins redondants. Dans la même logique, le fait de stocker localement des journaux utilisés principalement pour l'investigation numérique permet d'accélérer le processus.

Déploiement rapide

McAfee Enterprise Log Manager et McAfee Enterprise Security Manager peuvent être déployés conjointement à l'aide d'une appliance unique ou distribués de manière à prendre en charge même les plus grands réseaux d'entreprise. Vous pouvez opter pour des options de déploiement hybrides flexibles comprenant à la fois des appliances physiques et virtuelles

Intégration avec l'infrastructure de votre entreprise

Contrairement à la plupart des solutions de gestion de journaux, McAfee Enterprise Log Manager ne fonctionne pas de manière isolée mais opère de concert avec d'autres systèmes de sécurité informatique. En effet, l'intégration avec McAfee Enterprise Security Manager permet à la solution de se connecter au reste de votre infrastructure de sécurité, ce qui présente de nombreux avantages : simplification des opérations de sécurité, amélioration de l'efficacité globale et réduction des coûts. Vous pouvez ainsi intégrer la gestion intelligente des journaux avec d'autres fonctionnalités puissantes, telles que l'inspection du réseau, la surveillance des événements de bases de données, des fonctions d'analyse, etc.

Pour plus d'informations, consultez la page **www.mcafee.com/fr/products/siem/index.aspx**.

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com