McAfee Enterprise Log Manager

Reduzca los costos del cumplimiento de normativas mediante la recopilación, almacenamiento y administración de los registros

Una adecuada recopilación y almacenamiento de los registros le permitirán reducir los costes derivados del cumplimiento de normativas gracias a una pista de auditoría de la actividad clara e irrefutable. McAfee® Enterprise Log Manager recopila, comprime y almacena de forma eficaz todos los archivos de registro. Además, la integración con McAfee Enterprise Security Manager proporciona funciones avanzadas de búsqueda, análisis, correlación, alerta y generación de informes. Todos los eventos y alertas ofrecen un acceso sencillo mediante un solo clic al registro original, por lo que sus análisis forenses también salen beneficiados.

No se escapa ningún archivo de registro, McAfee Enterprise Log Manager los recopila, firma y almacena todos. McAfee automatiza la administración y el análisis de todos los tipos de registros, incluidos los registros de base de datos, de aplicaciones y de sistema, y los registros de eventos de Microsoft Windows. Los registros se firman y validan, lo que garantiza su autenticidad e integridad, un requisito fundamental para el cumplimiento de normativas. Los conjuntos de reglas e informes de cumplimiento de normativas que se incluyen, listos para utilizar, facilitan a su empresa la tarea de demostrar que cumple las normativas y que se están implementando las directivas.

El uso de este entorno de recopilación, administración y análisis de registros perfectamente integrado reforzará su perfil de seguridad y mejorará de manera importante su capacidad para cumplir estándares como PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA y SOX.

Administración de registros inteligente

McAfee Enterprise Log Manager recopila los registros de manera inteligente, almacenando los que son adecuados para el cumplimiento de normativas y analizado y explorando los que son importantes para la seguridad. Puede mantener los registros en su formato original durante el tiempo que necesite para satisfacer sus necesidades específicas de cumplimiento de normativas. Y puesto que no altera los archivos de registro originales, McAfee admite la cadena de custodia y las tareas de no repudio.

Ventajas principales

- Recopilación y conservación de registros universal para satisfacer los requisitos de cumplimiento de normativas
- Almacenamiento y conservación flexibles, según cada fuente de registros
- Soporte de la cadena de custodia y los análisis forenses
- Búsqueda y análisis de registros
- Almacenamiento de registros de forma local o a través de una red de área de almacenamiento gestionada
- Integración total con McAfee® Enterprise Security Manager
- Opciones de distribución flexible e híbrida, que incluyen dispositivos físicos y virtuales

Las necesidades de conservación de información varían en función de la fuente de los registros y de los distintos requisitos normativos que debe satisfacer. McAfee Enterprise Log Manager utiliza grupos de almacenamiento fácilmente personalizables para garantizar que los registros se almacenan correctamente y durante el período de tiempo adecuado. Elija la mejor opción de almacenamiento según sus necesidades: espacio en el disco duro en los dispositivos y tarjetas de canal de fibra opcionales para redes de área de almacenamiento de alta velocidad (SAN).

Los archivos de registro por sí solos no nos indican lo que necesitamos. Contienen pruebas importantes y son una pieza clave para establecer la cadena de custodia, pero también plantean importantes interrogantes. Por ejemplo, podríamos ver un nombre de usuario en un registro de acceso, pero no información sobre la función o los privilegios de ese usuario. También podríamos saber a qué sistema se ha accedido, pero es posible que no sepamos nada sobre los tipos de información que utiliza ese sistema o quién debería acceder a él.

Integración con McAfee Enterprise Security Manager

McAfee Enterprise Log Manager es un componente opcional e integrado de McAfee Enterprise Security Manager. Mientras que McAfee Enterprise Log Manager almacena los registros, McAfee Enterprise Security Manager analiza en profundidad, normaliza y explora la información de registro, de manera que esté disponible de forma inmediata para tareas de investigación de seguridad y respuesta a incidentes en tiempo real.

Cuando se genera un evento de seguridad, los archivos de eventos analizados se vinculan directamente al archivo de registro origen y a la línea de registro específica. De esta forma, se puede acceder a ellos mediante un solo clic durante los procesos de administración de eventos y de análisis forense. No hay ningún otro paso, no es necesario iniciar ninguna otra aplicación, ni hay que perder tiempo en buscar en los registros de forma manual.

Contexto amplio con fines de análisis

McAfee Enterprise Security Manager y McAfee Enterprise Log Manager proporcionan de manera conjunta información contextual sobre todos y cada uno de los registros, lo que aumenta el valor de cada registro analizado. La información incluye:

- La dirección IP de origen o destino
- Contexto de identidad
- El nombre del host o servicio que se utiliza
- Información de evaluación de vulnerabilidades
- Información topológica de red
- Información de directivas y de privacidad

Grupos de almacenamiento flexibles

Los grupos de almacenamiento de McAfee Enterprise Log Manager añaden flexibilidad a la forma de guardar los registros durante largo tiempo. Se trata de grupos virtuales de datos de almacenamiento utilizables que pueden distribuirse entre varios grupos de dispositivos físicos (almacenamiento local, NFS, SAN, CIF y otros) para satisfacer distintas necesidades de administración de registros.

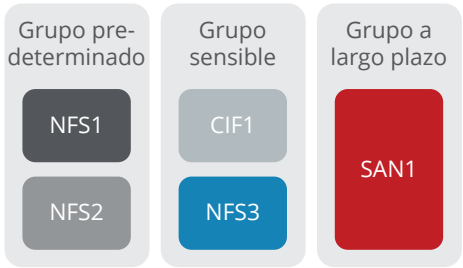

Figura 1. Los grupos de almacenamiento flexibles admiten la conservación de registros personalizada.

Un grupo de almacenamiento puede estar formado por varios dispositivos y pueden asignarse datos a un grupo concreto en función del dispositivo de origen, de manera que los registros se pueden almacenar en ubicaciones distintas según su importancia para la seguridad, el cumplimiento de normativas u otros criterios. Por ejemplo, los registros que son fundamentales para el cumplimiento de normativas pueden almacenarse en un grupo formado por varios dispositivos de almacenamiento de red redundantes. Los registros menos críticos podrían almacenarse en sistemas menos redundantes y aquellos que son más útiles para tareas forenses podrían almacenarse de forma local para llevar a cabo análisis más rápidos.

Despliegue rápido

McAfee Enterprise Log Manager y McAfee Enterprise Security Manager pueden desplegarse de forma conjunta mediante un único dispositivo que combine las dos soluciones o distribuirse para dar cobertura incluso a las redes empresariales más grandes. Opciones de distribución flexible e híbrida, que incluyen dispositivos físicos y virtuales.

Integración con su infraestructura

Mientras que la mayoría de las soluciones de administración operan de forma aislada, McAfee Enterprise Log Manager trabaja de manera conjunta con otros sistemas de seguridad de la información. A través de McAfee Enterprise Security Manager, se conecta al resto de su infraestructura de seguridad para simplificar las operaciones de seguridad, mejorar la eficacia global y reducir costos. Puede integrar de forma inteligente la administración de registros con sistemas potentes de análisis, inspección de redes, supervisión de eventos de base de datos y muchos más.

Más información

Para obtener más información, visite **www.mcafee.com/mx/products/siem/index.aspx**.

McAfee
Together is power.

Av. Paseo de la Reforma No.342 Piso 25
Colonia Juárez, México DF
C.P. 06600
+52-55-50890250
www.mcafee.com/mx