# McAfee Database Event Monitor for SIEM

## Consiga visibilidad de las transacciones de las bases de datos sin afectar al rendimiento.

Para garantizar el cumplimiento de las normativas es imprescindible una auditoría fiable de las transacciones de las bases de datos. Sin embargo, las soluciones de auditoría de bases de datos nativas tradicionales pueden afectar enormemente al rendimiento de las bases de datos y a la productividad de sus administradores. El diseño no intrusivo de McAfee® Database Event Monitor for SIEM es una ayuda para las auditorías de cumplimiento y los requisitos de reportes en aumento, así como una mejora para las operaciones de seguridad.

McAfee Database Event Monitor for SIEM proporciona un registro de seguridad detallado y no intrusivo de las bases de datos y las aplicaciones, con la supervisión de todo acceso a los datos confidenciales de la empresa y de los clientes. Con un esfuerzo de despliegue mínimo, puede disponer de visibilidad de las transacciones y los eventos relacionados con bases de datos, así como de las consultas y las respuestas específicas de bases de datos, con información de quién accede a sus datos y por qué.

McAfee Database Event Monitor for SIEM es la única solución de su género que consolida las actividades de las bases de datos en un repositorio de auditoría central y proporciona normalización, correlaciones, análisis y reportes sobre esa actividad.

Las reglas y reportes predefinidos, así como las funciones de registro, con protección de la privacidad, facilitan el cumplimiento de las normativas y, al mismo tiempo, consolidan su estado de seguridad general.

### Acceso a las bases de datos en contexto

McAfee Database Event Monitor for SIEM no se limita al mero registro; además, normaliza los datos y correlaciona las transacciones de bases de datos con otra información para ayudarle a llevar a cabo un análisis en tiempo real.

Gracias a la ampliación de la visibilidad para incluir la información de los usuarios, el contenido de aplicaciones, la actividad del sistema operativo, las vulnerabilidades e, incluso, la ubicación de red, McAfee Database Event Monitor for SIEM le permite:

- Realizar un seguimiento de los usuarios en todas las aplicaciones
- Examinar la actividad de la sesión completa, desde el inicio hasta el cierre
- Detectar los datos confidenciales e identificar las infracciones de directivas
- Detectar la pérdida de datos a través de los canales autorizados
- Correlacionar la actividad de las bases de datos con los eventos de seguridad
- Generar una pista de auditoría de toda la actividad de las bases de datos
- Generar reportes detallados para las normativas PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX y SOX, entre muchas otras

### Ventajas principales

- Supervisión pasiva basada en la red que no afecta en absoluto al rendimiento de las bases de datos
- Identificación de todas las instancias de base de datos, incluidas las no autorizadas o no fiables
- Autorización de la supervisión y el registro de acceso a las bases de datos con información sometida a normativas
- Conservación de los datos de todas las transacciones de bases de datos desde el inicio hasta el cierre de sesión para facilitar las auditorías
- Simplificación del análisis gracias a la reconstrucción de las sesiones mediante "un solo clic"
- Integración total con McAfee Enterprise Security Manager para permitir el uso de las transacciones de bases de datos en la correlación de eventos y otras actividades SIEM avanzadas
- Opciones de distribución flexible e híbrida, que incluyen dispositivos físicos y virtuales

intel Security

## Visibilidad completa de cada transacción

McAfee Database Event Monitor for SIEM supervisa todas las transacciones de bases de datos y proporciona una pista de auditoría completa de todas las actividades de bases de datos, incluidos los resultados, las consultas, la actividad de autenticación y las elevaciones de privilegios. Gracias a que conserva los detalles completos de las sesiones de todas las transacciones, McAfee Database Event Monitor for SIEM le permite ver lo que pasó antes y después de cada transacción, desde el inicio hasta el cierre.

## Proceso de cumplimiento de normativas automatizado

Las reglas de detección basadas en directivas preconfiguradas y los reportes de cumplimiento de normativas aseguran que pueda generar la información de acceso a los datos que requieren las normativas PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, GPG13, JSOX o SOX, entre otras. Además, McAfee Database Event Monitor for SIEM se integra totalmente con McAfee Enterprise Security Manager y con McAfee Enterprise Log Manager para proporcionar funciones de análisis y correlación de eventos sin precedentes, además de almacenamiento y enmascaramiento de los datos confidenciales, según las normativas, en los registros de actividad.

Una lista de excepciones muestra los servidores de bases de datos que no se están supervisando, así como los puertos ilegales abiertos para acceder a la información desde las bases de datos.

## Seguimiento de usuarios y cuentas

Mediante las funciones avanzadas de la línea de soluciones de administración de la seguridad de McAfee, los usuarios y administradores pueden realizar de forma sencilla un seguimiento de varias aplicaciones y cuentas, lo que ofrece una visión integral para determinar la responsabilidad de toda la actividad de los usuarios, independientemente de cómo accedan a la base de datos.

## Creación de perfiles de actividad de los usuarios

McAfee Database Event Monitor descompone cada consulta SQL en tokens, es decir, objetos (tablas, vistas y procedimientos almacenados) a los que se accede en los servidores de bases de datos de destino, al tiempo que genera un perfil del comportamiento de cada usuario, identificando tanto la actividad nueva como la que se desvía de la norma.

## Inyección SQL

Se supervisa el éxito o fracaso de todos los paquetes de respuesta a consultas SQL. Los errores de gravedad baja, como errores de sintaxis, sintomáticos de un ataque de inyección SQL, se controlan y correlacionan si ocurren de forma consecutiva, lo que garantiza la detección proactiva de este tipo de ataques.

## Detección de riesgos y amenazas

McAfee Database Event Monitor for SIEM analiza toda la actividad supervisada en relación a un conjunto personalizado de reglas de directivas, y detecta y alerta sobre la actividad sospechosa. Además, la detección basada en anomalías indica actividad de usuarios, consultas y respuestas no habituales, así como otros comportamientos inusuales.

## Mayor eficiencia, sin sobrecarga

Los dispositivos McAfee Database Event Monitor for SIEM, dotados de un motor de captura de datos de alto rendimiento, supervisan su base de datos a través de la red, sin sobrecargar la propia base de datos y garantizando la conservación de los datos de auditoría que necesita.

McAfee Enterprise Security Manager facilita la administración y conecta la supervisión de las bases de datos con el resto de su ecosistema de seguridad y cumplimiento de normativas. Para agregar visibilidad a la actividad de los terminales locales, utilice un agente de host opcional, que tiene un menor impacto en el rendimiento que los agentes de host de la competencia o la auditoría nativa.

**Funciones de supervisión de bases de datos**

- Supervisar y registrar toda la actividad de las bases de datos
- Apoyar sus iniciativas de cumplimiento de normativas
- Impedir las escuchas ilegales
- Aumentar la determinación de responsabilidad
- Alertar sobre objetos, acciones e infracciones de directivas
- Obtener datos que permitan evaluar el nivel de servicio de las bases de datos/la administración del rendimiento
- Supervisar todas las vías de acceso a los datos, como:
  - Aplicaciones
  - Usuarios
  - Malware
  - Utilidades
  - Puertas traseras (backdoors)
  - Consultas
  - Secuencias de comandos LAMP
  - Open Database Connectivity (ODBC)

## Casos de uso

**Cumplimiento de normativas**

Para ayudarle a garantizar el cumplimiento de normativas, McAfee Database Event Monitor for SIEM es capaz de identificar los datos confidenciales que se están utilizando. Puede supervisar estas bases de datos y crear una pista de auditoría sobre el acceso a los datos protegidos, la actividad de las cuentas de usuario y los cambios. Las responsabilidades de seguridad pueden separarse de la administración de bases de datos con el fin de mejorar el control, y los datos confidenciales se pueden enmascarar en el registro. Los reportes pueden destacar quiénes son los principales consumidores de los registros protegidos. En cualquier momento pueden generarse reportes preconfigurados para las distintas normativas.

**Detección y clasificación de bases de datos**

Gracias a la monitorización de la red para controlar los comandos de bases de datos, McAfee Database Event Monitor for SIEM es capaz de detectar todas las instancias de bases de datos, incluidas las desconocidas o no fiables. Además, McAfee Database Event Monitor for SIEM supervisa todas las transacciones, incluidos los resultados de las consultas, y las compara con las reglas de directivas y diccionarios para detectar qué bases de datos almacenan datos de tarjetas de crédito, números de identificación u otra información confidencial.

**Supervisión de la seguridad**

McAfee Database Event Monitor for SIEM supervisa directamente sus bases de datos y puede detectar y alertar en tiempo real si se producen inicios de sesión por fuerza bruta, ataques de inyección SQL, patrones de acceso anormal y otros indicios de que su servidor de bases de datos podría estar sufriendo un ataque. Puede supervisar la actividad de las aplicaciones de servidor y detectar la presencia de actividades sospechosas, como la recuperación fraudulenta de datos y las cuentas de usuario falsas.

Si el ataque se originó en la red, puede realizar un seguimiento de la actividad de los usuarios y correlacionar esta información con los datos de flujo de red para localizar al infractor. En caso de ataques externos, el ataque puede correlacionarse con otra actividad saliente de la red y las aplicaciones con el fin de detectar fugas de datos, canales de comunicación encubiertos y otros vectores de pérdidas.

Intel y el logotipo de Intel son marcas comerciales registradas de Intel Corporation en EE. UU. y en otros países. McAfee y el logotipo de McAfee son marcas comerciales o marcas comerciales registradas de McAfee, Inc. o de sus empresas filiales en EE. UU. y en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros. Los planes, especificaciones y descripciones de productos mencionados en este documento se proporcionan únicamente a título informativo y están sujetos a cambios sin previo aviso; se ofrecen sin garantía de ningún tipo, ya sea explícita o implícita. Copyright © 2014 McAfee, Inc. 61321ds_db-event-monitor_0914

**McAfee. Part of Intel Security.**
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.intelsecurity.com