McAfee Database Activity Monitoring

Protección económica de bases de datos para satisfacer sus requisitos de cumplimiento

Las empresas almacenan sus datos más valiosos y confidenciales en una base de datos, pero la protección perimetral y la seguridad básica que acompañan a la base de datos no le protegen frente a los sofisticados hackers actuales o las posibles amenazas del personal interno no fiable. La investigación[1] demuestra que más del 96 % de los registros que sufrieron un ataque estaban relacionados con una base de datos y que el 66 % de las fugas siguen sin descubrirse durante meses o incluso más tiempo. McAfee® Database Activity Monitoring detecta automáticamente las bases de datos en su red, las protege con un conjunto de defensas preconfiguradas y le ayuda a elaborar una directiva de seguridad personalizada para su entorno, facilitando la tarea de demostrar a los auditores el cumplimiento de las normativas y mejorando la protección de los activos de datos críticos.

Ventajas principales

- Máxima visibilidad y protección contra todas las fuentes de ataques.
- Supervisión de las amenazas externas, las internas de usuarios con privilegios y las sofisticadas que proceden de la base de datos.
- Reducción al mínimo de riesgos y responsabilidad gracias a la neutralización de los ataques antes de que causen daños.
- Ahorro de tiempo y dinero mediante un despliegue más rápido y una arquitectura más eficaz.
- Flexibilidad para desplegarse fácilmente en la infraestructura de TI de su elección.
- Se integra con los productos básicos de McAfee, incluida la plataforma de administración McAfee® ePolicy Orchestrator® (McAfee ePO™) y McAfee Vulnerability Manager for Databases.

Con McAfee Database Activity Monitoring, las organizaciones obtienen visibilidad sobre toda la actividad de la base de datos, incluido el acceso local con privilegios y los ataques avanzados desde dentro de la base de datos. McAfee Database Activity Monitoring les ayuda a proteger sus datos más valiosos y confidenciales contra ataques externos y amenazas de personal interno malicioso. Además de proporcionar una pista de auditoría fiable, McAfee Database Activity Monitoring también evita las intrusiones terminando las sesiones que infringen las directivas de seguridad.

Con McAfee Database Activity Monitoring, las organizaciones pueden:

- Generar rápidamente una directiva de seguridad personalizada para cumplir las normativas del sector o las normas de administración de TI internas.
- Registrar el acceso a los datos confidenciales para fines de auditoría, con detalles completos de las transacciones.
- Terminar las sesiones que infrinjan las directivas y poner en cuarentena a los usuarios sospechosos, con el fin de evitar que los datos corran peligro.
- Mantener la separación de funciones, tal y como requieren muchas normativas.

McAfee Database Activity Monitoring protege los datos frente a todas las amenazas de manera rentable: supervisa la actividad local de todos los servidores de bases de datos, aunque funcionen en entornos virtualizados o en la nube, e identifica y pone término a los comportamientos maliciosos en tiempo real.

Protección frente a todos los vectores de amenazas de bases de datos

Los ataques dirigidos a los valiosos datos almacenados en las bases de datos pueden proceder de otras partes de la red, de usuarios locales conectados al propio servidor e incluso de dentro de la propia base de datos mediante procedimientos o activaciones almacenados. McAfee Database Activity Monitoring utiliza sensores basados en memoria para capturar los tres tipos de amenazas desde una sola solución no intrusiva. Luego puede utilizar esta información para demostrar el cumplimiento ante los auditores y para mejorar el nivel global de seguridad de los datos más valiosos de una organización.

Identificación de las amenazas cuando se producen, reduciendo el riesgo y la responsabilidad

A diferencia de los análisis de registros o auditorías básicos, que solo le indican lo que ha ocurrido a posteriori, las funciones de supervisión y prevención de intrusiones en tiempo real detienen las infracciones antes de que provoquen daños. Las alertas se envían directamente al panel de supervisión con todos los detalles de la infracción de la directiva necesarios para corregirla. La configuración se puede ajustar de forma que las infracciones de alto riesgo pongan fin automáticamente a las sesiones sospechosas y pongan en cuarentena a los usuarios maliciosos, lo que da tiempo al equipo de seguridad para investigar la intrusión.

La aplicación de parches virtuales protege de exploits conocidos y de muchas amenazas de tipo zero-day

No siempre es posible instalar los parches del proveedor inmediatamente, ya que suelen requerir pruebas de aplicaciones y tiempo de inactividad para aplicar la actualización. Además, algunas aplicaciones todavía utilizan versiones de bases de datos antiguas para las que ya no se proporcionan parches. McAfee Database Activity Monitoring detecta los ataques que intentan aprovechar las vulnerabilidades conocidas, además de los vectores de amenazas comunes y se puede configurar de forma que emita una alerta o ponga fin a la sesión en tiempo real. Las actualizaciones de parches virtuales se proporcionan regularmente para las nuevas vulnerabilidades descubiertas y se pueden implementar sin inactividad de la base de datos, lo que protege los datos confidenciales hasta que el proveedor de la base de datos publica un parche y puede aplicarse.

Despliegue de forma rápida y discreta con un mínimo de recursos

McAfee Database Activity Monitoring, una solución basada exclusivamente en software, puede implantarse y empezar a proteger las bases de datos en menos de una hora, sin necesidad de hardware especial ni servidores adicionales. Acelerando aún más el despliegue, McAfee Database Activity Monitoring analiza automáticamente la red en busca de bases de datos y utiliza plantillas dirigidas por asistentes para los distintos entornos normativos con el fin de guiar al usuario en la rápida creación de directivas de seguridad personalizadas que satisfagan los requisitos de auditoría. Al distribuir la responsabilidad de aplicar la directiva de seguridad entre los sensores autónomos que se ejecutan en cada servidor de base de datos, McAfee Database Activity Monitoring se adapta de manera económica para dar soporte a las empresas más grandes.

Compatible con la moderna infraestructura de TI actual, incluida la virtualización y la nube

Otros sistemas de supervisión de bases de datos se basan en el análisis del tráfico de red para identificar las infracciones de las directivas, algo imposible o ineficiente en las arquitecturas distribuidas y muy dinámicas que se utilizan para la virtualización de centros de datos y la prestación de servicios informáticos desde Internet. En cambio, los sensores de McAfee se pueden configurar de forma que se aprovisionen automáticamente junto con cada nueva base de datos, soliciten la directiva de seguridad en función de los datos que albergan y a continuación empiecen a enviar las oportunas alertas al servidor de administración. Incluso si se interrumpe la conectividad de red, los datos siguen protegidos ya que el sensor implementa la directiva de seguridad de forma local y las alertas se ponen en cola y se envían cuando el servidor de administración vuelve a estar disponible.

Integración con la plataforma McAfee ePolicy Orchestrator

McAfee Database Activity Monitoring está totalmente integrada con el software McAfee ePolicy Orchestrator, proporcionando generación de informes y datos de resumen centralizados para todas sus bases de datos desde un panel consolidado. El software McAfee ePO se conecta con otras soluciones de seguridad de McAfee ajenas a la protección de bases de datos, para proporcionar una vista única que facilita la administración y la visibilidad integral.

Soluciones de protección de bases de datos de McAfee

McAfee ofrece algunas soluciones de seguridad de bases de datos para proporcionarle una visibilidad total de todas las bases de datos y su estado de seguridad de manera global. Para obtener más información, visite www.mcafee.com/es/products/database-security/index.aspx o póngase en contacto con su representante local de McAfee o con un reseller próximo.

Acerca de la protección de endpoints de McAfee

La protección de endpoints de McAfee ofrece seguridad para todos sus dispositivos, los datos que utilizan y las aplicaciones que ejecutan. Nuestras soluciones completas y adaptadas reducen la complejidad de lograr una defensa para endpoints de varios niveles que no afecte a la productividad. Para más información, visite www.mcafee.com/es/products/endpoint-protection/index.aspx.

[1] *Estudio de Verizon Business*, 2013.

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 85 00
www.mcafee.com/es