



# McAfee Vulnerability Manager for Databases

**Una completa evaluación del riesgo para sus datos más confidenciales**

## Ventajas principales

- Visibilidad inigualable del estado de seguridad de las bases de datos.
- Análisis de varias bases de datos en toda la empresa desde una consola centralizada.
- Agiliza el cumplimiento de normativas y minimiza los ciclos de auditoría, lo que se traduce en un importante ahorro.
- Requiere un conocimiento mínimo de sistemas de bases de datos.
- Genera informes personalizados en un formato fácil de entender para distintas funciones de usuario.

Usted almacena sus datos más importantes y confidenciales en una base de datos, pero la mayoría de los productos de evaluación de vulnerabilidades no saben lo suficiente acerca de los sistemas de bases de datos para poder probarlos en profundidad, y esto pone en peligro sus datos. Prácticamente todas las semanas se produce un nuevo anuncio de una fuga de datos importante. McAfee® Vulnerability Manager for Databases —parte de la oferta de productos de Intel® Security— identifica automáticamente las bases de datos que hay en su red; determina si se han aplicado los últimos parches; y evalúa las vulnerabilidades más frecuentes, como contraseñas poco seguras, cuentas predeterminadas, etc., facilitando más que nunca la tarea de demostrar el cumplimiento de las normativas y proteger mejor los datos críticos.

Gracias a más de 4700 comprobaciones de vulnerabilidades en sistemas de bases de datos de primera línea, como Oracle, Microsoft SQL Server, IBM DB2 y MySQL, McAfee Vulnerability Manager for Databases evalúa el riesgo desde prácticamente todos los vectores de amenazas. Pero, a diferencia de otros productos en los que los resultados de los análisis a menudo le pueden abrumar con un sinnúmero de amenazas menores que ocultan los problemas críticos que hay que abordar, McAfee Vulnerability Manager for Databases va mucho más allá. Basándose en la información recibida de los expertos en seguridad de bases de datos, clasifica claramente las amenazas en distintos niveles de prioridad y proporciona secuencias de comandos de corrección y recomendaciones.

Al mejorar la visibilidad sobre las vulnerabilidades de las bases de datos (y ofrecer recomendaciones expertas para subsanarlas), McAfee Vulnerability Manager for Databases reduce la probabilidad de que se produzca una fuga de datos perjudicial y permite ahorrar costes, ya que allana el terreno de cara a las auditorías de cumplimiento de las normativas.

## La ruta más rápida al cumplimiento de las bases de datos

Con un conjunto de funciones diseñado para acelerar los análisis iniciales más los informes para uso inmediato que permiten hacer frente a la mayoría de los requisitos de cumplimiento de normativas, McAfee Vulnerability Manager for Databases proporciona resultados preparados para auditorías con unos recursos mínimos.

Para realizar rápidamente su primera evaluación, McAfee Vulnerability Manager for Databases:

- Automatiza el descubrimiento de las bases de datos de la red.
- Localiza e identifica tablas que contienen información confidencial.
- Realiza un análisis de puertos rápido que proporciona la versión de base de datos y el estado de los parches.
- Presenta los hallazgos en informes preconfigurados para distintas normativas.

### Comprobación de contraseñas de gran velocidad y eficiencia

La divulgación de contraseñas es responsable de un porcentaje significativo de las fugas de datos, y los hackers se han automatizado mucho más en sus ataques, basados en la simple adivinación de contraseñas. Los principios fundamentales de la seguridad incluyen evitar las contraseñas débiles y el uso compartido de contraseñas entre usuarios y cuentas, pero ¿cómo saber si esto se cumple?

McAfee Vulnerability Manager for Databases ofrece los métodos más rápidos de detección de contraseñas débiles, identificando las cuentas con contraseñas sencillas, contraseñas predeterminadas y contraseñas compartidas. Incluso puede analizar las contraseñas con hash, almacenadas, por ejemplo, en SHA-1, MD5 o DES.

Mediante el uso de conexiones directas a las bases de datos, la comprobación de contraseñas se realiza sin apenas recargar el servidor de la base de datos y no bloquea a los usuarios ante un número excesivo de intentos de inicio de sesión.

### Basado en conocimientos demostrados de seguridad de bases de datos

Los sistemas de administración de bases de datos son complejos e introducen su propio conjunto de riesgos de seguridad, algunos de los cuales son similares a los de otro software del sistema (como las actualizaciones de parches, la solidez de las contraseñas y otros), mientras que otros son exclusivos de las bases de datos (como las amenazas de inyección SQL o los ataques de desbordamiento del búfer). McAfee Vulnerability Manager for Databases procede de un equipo responsable de contribuciones en siete de las diez últimas actualizaciones de parches críticas que ha publicado Oracle. Aprovecha los conocimientos de los principales profesionales de la seguridad de bases de datos para:

- Identificar la susceptibilidad a riesgos específicos para bases de datos, como inyección SQL, desbordamiento del búfer y código PL/SQL malicioso o inseguro.

- Priorizar los resultados y resaltar los problemas "reales" que requieren atención inmediata.
- Proporcionar información útil sobre cómo gestionar los riesgos, con secuencias de comandos de corrección, siempre que sea posible.
- Permitir a los usuarios de seguridad y cumplimiento de normativas con un conocimiento limitado sobre bases de datos entender rápidamente los riesgos para los datos confidenciales y cómo solucionarlos.

### Integración con la plataforma McAfee ePolicy Orchestrator para una visibilidad máxima

McAfee Vulnerability Manager for Databases está totalmente integrado con el panel de McAfee® ePolicy Orchestrator® (McAfee ePO™), proporcionando generación de informes e información de resumen centralizada para todas sus bases de datos desde un panel consolidado. Proporciona información detallada y configuración de análisis además de vínculos directos para invocar la consola de administración de análisis de vulnerabilidades con control diferenciado de cada operación.

### Pasos siguientes

Para obtener más información, visite [www.mcafee.com/es/products/database-security/index.aspx](http://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 obtener más información, visite [www.mcafee.com/es/products/endpoint-protection/index.aspx](http://www.mcafee.com/es/products/endpoint-protection/index.aspx).



McAfee. Part of Intel Security.

Avenida de Bruselas n.º 22  
Edificio Sauce  
28108 Alcobendas  
Madrid, España  
Teléfono: +34 91 347 8500  
[www.intelsecurity.com](http://www.intelsecurity.com)

Intel y el logotipo de Intel son marcas comerciales registradas de Intel Corporation en EE. UU. y en otros países. McAfee, el logotipo de McAfee, ePolicy Orchestrator y McAfee ePO 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 © 2013 McAfee, Inc. 60598ds\_vm-db\_1013B