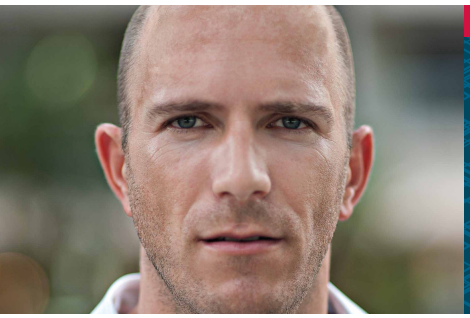

Las cinco razones principales para desplegar una solución de seguridad de bases de datos dedicada

Una última línea de defensa crítica

La protección de la valiosa información confidencial que guardan las bases de datos es vital para mantener la integridad y la reputación de las empresas en cualquier lugar, por no hablar de garantizar el cumplimiento de las normativas. Sin embargo, muchas organizaciones siguen confiando su seguridad a soluciones que tienen limitaciones inherentes. Dadas las complejidades de las plataformas de bases de datos actuales y el nivel de sofisticación de los ciberdelincuentes hoy día, desplegar una solución de seguridad de bases de datos global y dedicada es crucial. Esto se debe a las cinco razones siguientes:

Ventajas de McAfee Vulnerability Manager

- Visibilidad total del estado de seguridad de sus bases de datos
- Análisis de varias bases de datos en toda la empresa desde una consola centralizada
- Agilización del cumplimiento de normativas y reducción de los ciclos de auditoría, lo que se traduce en un importante ahorro
- Rápido despliegue con un mínimo de conocimientos de sistemas de bases de datos
- Rápida generación de informes personalizados en un formato fácil de entender para usuarios de distintas funciones

Ventajas de McAfee Database Activity Monitoring

- Máxima visibilidad y protección contra todas las fuentes de ataques
- Supervisión de las amenazas externas, las amenazas internas de usuarios con privilegios y las amenazas sofisticadas que proceden de la base de datos
- Reducción al mínimo de riesgos y responsabilidad gracias a la detención 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

1. No puede proteger un activo si no sabe que existe

Incluso en los entornos de TI más restringidos, no es raro encontrar cientos o incluso miles de instancias de bases de datos con información muy confidencial, y para los departamentos de TI no sería nada fácil averiguar el número, ubicación, nivel de confidencialidad de los datos y estado de seguridad de dichas bases de datos. Lo peor es que los ciberdelincuentes lo saben e intentan continuamente localizar los ángulos muertos. Disponen del tiempo y los recursos técnicos para atacar las bases de datos que creía seguras o que ni siquiera sabía que existían. La falta de visibilidad de sus sistemas es una oportunidad para ellos.

La visibilidad total de sus bases de datos sólo es posible cuando tiene la capacidad para realizar un descubrimiento completo de todas las bases de datos de su entorno, junto con un análisis para identificar cuáles de ellas contienen datos de tarjetas de pago, datos de recursos humanos, cifras de ventas y otra información confidencial. Además, las pruebas automáticas para determinar la vulnerabilidad de las bases de datos en profundidad son fundamentales para conocer la naturaleza exacta de los riesgos. Solo una solución de seguridad de bases de datos dedicada puede proporcionarle información detallada, sobre la que pueda actuar, y que le permita priorizar y remediar los vacíos de seguridad, ahorrándole, al mismo tiempo, a su organización el considerable gasto que supone contratar a un consultor de seguridad externo.

McAfee® Vulnerability Manager for Databases descubre automáticamente todas las bases de datos de su red, determina si se han aplicado los últimos parches y analiza los sistemas para descubrir vulnerabilidades. De hecho, McAfee Vulnerability Manager efectúa más de 4.200 verificaciones de vulnerabilidades en sistemas de bases de datos líderes y clasifica las amenazas en distintos niveles de prioridad. Además, proporciona secuencias de comandos de corrección y recomendaciones. Requiere un mínimo de conocimientos de los sistemas de bases de datos, genera informes personalizados en formatos fáciles de leer para usuarios de distintas funciones y todo, desde una consola de seguridad centralizada.

2. La seguridad en el perímetro no protege contra las amenazas que proceden del interior

Ha invertido una gran cantidad de tiempo, esfuerzo y capital en seleccionar y desplegar firewalls y otras tecnologías de seguridad de la red. Sin embargo, como sabe, no todos los ataques contra las bases de datos se originan en el exterior del perímetro. Una investigación anual realizada por el grupo Computer Emergency Response Team (CERT) indica que hasta la mitad de dichos incidentes han sido provocados por usuarios internos. Por lo tanto, debe proteger la información esencial de su empresa contra un enemigo aun más insidioso: los miembros de su empresa que cuentan con privilegios, muchos de los cuales disponen de medios para saltarse las funciones de seguridad integradas en los sistemas de gestión de bases de datos (DMBS), manipular los registros de acceso y ocultar su rastro.

La solución de seguridad de bases de datos adecuada detectará y prevendrá las amenazas sea cual sea el vector de entrada: detendrá los ataques que proceden del exterior y, particularmente, los que vienen del interior. Además, ofrecerá un marco para configurar e implementar con facilidad directivas de acceso a las bases de datos según los requisitos de cumplimiento de normativas específicos, con el fin de garantizar en todo momento la separación de deberes real.

McAfee Database Activity Monitoring detecta automáticamente las bases de datos en su red, las protege con un paquete de defensas preconfiguradas y le ayuda a elaborar una directiva de seguridad personalizada para su entorno, para que le sea más fácil demostrar a los auditores el cumplimiento de las normativas y mejorar la protección de los datos de activos críticos. Con McAfee Database Activity Monitoring, obtiene visibilidad sobre toda la actividad de las bases de datos, incluido el acceso local de usuarios con privilegios y los sofisticados ataques lanzados desde el interior de la base de datos. Para proteger sus datos contra todas las amenazas supervisa la actividad de manera local en cada servidor de base de datos, independientemente de su ubicación, y envía alertas o termina automáticamente sesiones que son sospechosas de infringir o infringen la directiva de seguridad de alguna forma. McAfee Database Activity Monitoring incluso protege sus bases de datos e implementa sus directivas en los entornos de computación en la nube o virtualizados.

Ventajas de McAfee Virtual Patching

- Protección frente a amenazas incluso antes de instalar los parches de actualización distribuidos por el proveedor
- Los equipos de TI y seguridad ya no necesitan conocimientos específicos del DBMS
- Gracias a un diseño de software no intrusivo, las bases de datos de producción permanecen online
- Protección simplificada de las bases de datos mediante la distribución automática y continua de actualizaciones
- Cumplimiento de normas como PCI DSS, HIPAA y otras

Ventajas del software McAfee ePolicy Orchestrator

- Visibilidad integral de la seguridad de las bases de datos y el cumplimiento de normativas desde una consola de administración centralizada
- Una sola consola centralizada permite incorporar las bases de datos a un programa de administración de la seguridad unificada, en las oficinas de su empresa, en ubicaciones remotas e incluso en la nube
- Una arquitectura abierta y ampliable que conecta la administración de las soluciones de seguridad de McAfee y las de terceros con el protocolo LDAP, las operaciones de TI y las herramientas de administración de configuraciones

3. Los delincuentes tardan menos en lanzar ataques que usted en aplicar parches

Los "martes de parches" se deberían declarar día de fiesta para los hackers. Es el día del mes en el que los proveedores de bases de datos revelan sus objetivos más jugosos. Y lo que es más, los martes de parches animan a los delincuentes, ya que saben lo difícil que es para su equipo de administración de bases de datos dejar inactivas las bases de datos, aplicar los parches y realizar las comprobaciones oportunas. De hecho, son conscientes de que el proceso de aplicación de parches supone una interrupción operativa tal que usted preferirá retrasarlo todo lo posible, lo que les concede un amplio margen para hallar el medio de entrar.

Realmente no hay alternativa al proceso de aplicación de parches tradicional —con el vacío de seguridad que crea para los delincuentes— que no pase por tener una solución de seguridad de bases de datos dedicada. Y esa solución debe permitirle actualizar el estado de protección de sus bases de datos en tiempo real, sin molestias para el personal y sin interrupciones de las operaciones de su empresa.

McAfee Virtual Patching for Databases protege las bases de datos frente a los riesgos que entrañan las vulnerabilidades sin parche, mediante la detección y la prevención de los intentos de ataque e intrusiones en tiempo real, sin que sea necesario que quede inactiva la base de datos o que se realicen pruebas a las aplicaciones. Tendrá la tranquilidad de estar protegido frente a las amenazas incluso durante períodos de riesgo máximo de vulnerabilidad, durante el intervalo de tiempo que transcurre desde que el proveedor distribuye las actualizaciones de parches hasta que se instalan.

McAfee Database Activity Monitoring es otra solución no intrusiva, que no requiere tiempo de inactividad, que proporciona un nivel adicional de protección en los martes de parches y después. Sus sensores basados en memoria interceptan los ataques a bases de datos procedentes de toda la red, de los usuarios locales que han iniciado una sesión en el propio servidor e incluso del interior de la base de datos a través de procedimientos almacenados o activadores.

4. No puede seguir sacrificando el cumplimiento de normativas para mantener la continuidad

Los requisitos de cumplimiento de normativas que se aplican en distintos sectores, como en sanidad, finanzas y comercio minorista, cambian constantemente y son cada vez más estrictos. Como es lógico, las bases de datos esenciales para la empresa se ven muy afectadas por las prácticas de cumplimiento, según las cuales dichas bases de datos deben estar actualizadas con los últimos parches que proporciona el proveedor de DBMS. Sin embargo, inactivar las bases de datos, aplicar los parches y luego probar las distintas bases de datos de tipos diferentes no deja de ser una tarea laboriosa, por lo que la mayoría de las organizaciones sacrifican el cumplimiento de normativas en pro de la continuidad de la actividad empresarial. Además, es posible que existan bases de datos antiguas que aun se usen y para las que ni siquiera se ofrecen actualizaciones de parches.

Con McAfee Virtual Patching for Databases, puede mantener la continuidad de la actividad empresarial sin sacrificar el cumplimiento de las normativas. Podrá aplicar como siempre los parches necesarios según su planificación, sabiendo que sus bases de datos están protegidas y que cumplen las normativas. McAfee Virtual Patching for Databases ahorra muchísimo tiempo y, ante los auditores de cumplimiento de normativas, es un control de compensación válido. Además, puede incluso ampliar la protección más actualizada a las bases de datos antiguas que sus proveedores de DBMS ya no admiten.

5. Cuando los datos residen en la nube, la visibilidad es extremadamente limitada

La nube ofrece fantásticas ventajas en cuanto a costos de TI y operatividad, sin embargo, como sabe, existe un inconveniente: sus empleados pueden perder el control de los datos confidenciales y la visibilidad de las personas que puedan acceder a ellos puede ser casi nula. Con una solución de seguridad de bases de datos adecuada puede mantener sus datos protegidos tanto en entornos físicos como virtuales. La solución adecuada puede impedir que se lleven a cabo actividades no autorizadas en la base de datos y comunicar dichas actividades a su propia consola de administración, incluso cuando su base de datos resida en la nube o en un entorno virtual.

Con su exclusiva implementación de sensor basado en memoria, McAfee Database Activity Monitoring puede configurarse para actuar automáticamente con cada nueva máquina virtual. Al mismo tiempo, puede solicitar las directivas de seguridad basadas en los datos que alberga y, a continuación, empezar a enviar las alertas, en su caso, al servidor de administración. Lo que es más, sus sensores funcionan de forma autónoma incluso cuando se desconectan del servidor, por lo que los datos confidenciales están protegidos siempre, ya esté la base de datos online u offline, y sea cual sea el lugar en el que resida en cada momento. Incluso si se interrumpe la conectividad de la 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.

Además, puede supervisar el acceso a sus bases de datos basadas en la nube a través del software McAfee® ePolicy Orchestrator® (McAfee ePO™), que ofrece una consola de administración de seguridad empresarial para disfrutar de visibilidad integral de la seguridad de las bases de datos, la protección de la empresa y el cumplimiento de normativas.

En otras palabras, con nube o sin nube, usted y sus empleados contarán con el máximo nivel de visibilidad. Sin duda, McAfee ofrece la solución de seguridad de bases de datos adecuada para su entorno de TI, sea cual sea el alcance de sus operaciones o la confidencialidad de sus datos.

Ventajas de las soluciones de seguridad de bases de datos de McAfee

- Despliegue y uso sencillos
- Visibilidad total del estado de la seguridad de sus bases de datos
- Uso coherente de directivas de seguridad entre el personal de seguridad y los responsables de la gestión de las bases de datos
- Mantenimiento eficaz del cumplimiento de normativas
- Reducción al mínimo de riesgos y responsabilidad gracias a la detención de los ataques antes de que causen daños
- Administración de la seguridad de bases de datos desde una consola centralizada

Más información sobre cómo mantener sus bases de datos a salvo y disponibles

En McAfee, sabemos que en sus bases de datos se almacenan sus activos empresariales más críticos. Para que pueda desarrollar su actividad, deben estar disponibles continuamente. Y, al igual que sus bases de datos, nosotros tampoco nos tomamos ni un día libre. Por eso decimos que la seguridad no duerme nunca. Puede estar tranquilo. Nuestro equipo de expertos en seguridad de bases de datos sigue dedicado en cuerpo y alma a mantener su información confidencial a salvo y disponible, garantizando al mismo tiempo en su empresa el cumplimiento de las normativas internas y del sector.

Para obtener más información sobre cómo pueden proteger las bases de datos críticas para su empresa las soluciones de seguridad de bases de datos de McAfee, visite www.mcafee.com/mx/products/database-security/index.aspx, o póngase en contacto con su representante local de McAfee o su reseller.

Síganos en Twitter: @McAfee_DBSecure.

Acerca de la protección de endpoints de McAfee

McAfee, empresa subsidiaria de propiedad total de Intel Corporation (NASDAQ:INTC), es líder en tecnología de seguridad. Nuestras soluciones de seguridad de endpoints de próxima generación ofrecen seguridad para todos sus dispositivos, los datos que utilizan y las aplicaciones que ejecutan. Estas soluciones completas y adaptadas reducen la complejidad de lograr una defensa para endpoints de varios niveles, sin afectar a la productividad. Se trata de la combinación perfecta de análisis de malware inteligente tradicional, listas blancas dinámicas, prevención de intrusiones zero-day con análisis de comportamientos, administración unificada e información global sobre amenazas. Para obtener más información, visite www.mcafee.com/mx/products/endpoint-protection/index.aspx.

McAfee, Inc.
6205 Blue Lagoon Drive
Suite 600
Miami, Florida 33126
U.S.A.
www.mcafee.com

41903brf_top5-db-sec_0212_fnl_ASD