McAfee Database Activity Monitoring

Proteção econômica de bancos de dados para satisfazer os seus requisitos de conformidade

As empresas armazenam seus dados mais valiosos e confidenciais em um banco de dados, mas a proteção de perímetro e a segurança básica fornecidas com o banco de dados não podem proteger você contra os sofisticados hackers de hoje em dia ou contra ameaças de elementos maliciosos internos. Uma pesquisa[1] mostra que mais de 96% dos registros violados envolviam um banco de dados, e que 66% das violações permanecem sem ser descobertas por vários meses ou mais. O McAfee® Database Activity Monitoring localiza automaticamente bancos de dados na sua rede, protege-os com um conjunto de defesas pré-configuradas e ajuda você a construir uma política de segurança personalizada para o seu ambiente — tornando ainda mais fácil demonstrar conformidade para auditores e aprimorar a proteção de ativos de dados críticos.

Principais vantagens

- Maximiza a visibilidade e a proteção contra todas as fontes de ataques
- Monitora ameaças externas, elementos internos com privilégios e ameaças sofisticadas de dentro do banco de dados
- Minimiza o risco e a suscetibilidade jurídica ao interromper os ataques antes que estes causem danos
- Poupa tempo e dinheiro com uma distribuição mais rápida e uma arquitetura mais eficiente
- Oferece a flexibilidade de uma distribuição fácil na infraestrutura de TI de sua escolha
- Integra-se com os principais produtos da McAfee, como a plataforma de gerenciamento McAfee® ePolicy Orchestrator® (McAfee ePO™) e o McAfee Vulnerability Manager for Databases.

Com o McAfee Database Activity Monitoring, as empresas passam a visualizar melhor toda a atividade no banco de dados, incluindo acesso local privilegiado e ataques sofisticados de dentro do banco de dados. O McAfee Database Activity Monitoring ajuda as empresas a proteger seus dados mais valiosos e confidenciais contra ameaças externas e elementos maliciosos internos. Além de proporcionar uma trilha de auditoria confiável, o McAfee Database Activity Monitoring também evita intrusões encerrando sessões que violem a política de segurança.

Com o McAfee Database Activity Monitoring, as empresas podem:

- Criar rapidamente uma política de segurança personalizada para satisfazer regulamentos da indústria ou padrões internos de governança de TI.
- Registrar o acesso a dados confidenciais para fins de auditoria, incluindo detalhes completos das transações.
- Encerrar sessões que violem as políticas e colocar em quarentena os usuários suspeitos, impedindo que os dados sejam comprometidos.
- Preservar a separação de funções, conforme exigido por vários regulamentos.

O McAfee Database Activity Monitoring protege economicamente os seus dados contra todas as ameaças monitorando localmente a atividade em cada servidor de banco de dados e alertando ou encerrando comportamentos maliciosos em tempo real, mesmo quando executado em ambientes virtualizados ou de computação na nuvem.

Proteção contra todos os vetores de ameaça a bancos de dados

Os ataques que visam dados valiosos armazenados em bancos de dados podem vir pela rede, de usuários locais conectados ao próprio servidor e até mesmo de dentro do próprio banco de dados, através de gatilhos ou procedimentos armazenados. O McAfee Database Activity Monitoring utiliza sensores com base em memória para capturar todos os três tipos de ameaça com uma única solução não invasiva. As informações podem, então, ser utilizadas para demonstrar conformidade para fins de auditoria e para aprimorar a segurança total dos dados mais valiosos de uma empresa.

Identifique as ameaças quando elas ocorrerem, reduzindo o risco e a suscetibilidade jurídica

Diferente de auditorias básicas ou análises de registros, que só dizem o que aconteceu após o ocorrido, as capacidades de monitoramento e prevenção de intrusões em tempo real interrompem as violações antes que elas causem danos. Alertas são enviados diretamente para o dashboard de monitoramento, com detalhes completos da violação da política para fins de correção. Violações de alto risco podem ser configuradas para encerrar automaticamente sessões suspeitas e colocar usuários maliciosos em quarentena, dando à equipe de segurança tempo para investigar a intrusão.

Correção virtual protege contra explorações conhecidas e muitas ameaças de dia zero

Nem sempre é possível instalar imediatamente correções de fornecedores, uma vez que estas costumam exigir testes dos aplicativos e paradas para aplicação das atualizações. Além disso, alguns aplicativos ainda utilizam lançamentos antigos dos bancos de dados, para os quais não são mais fornecidas correções. O McAfee Database Activity Monitoring detecta ataques que tentam explorar vulnerabilidades conhecidas, bem como vetores de ataque comuns, e pode ser configurado para emitir um alerta ou encerrar a sessão em tempo real. Atualizações de patches virtuais são fornecidas regularmente para vulnerabilidades recém-descobertas e podem ser implementadas sem paralisação do banco de dados, protegendo dados confidenciais até que um patch seja lançado pelo fornecedor do banco de dados e possa ser aplicado.

Distribua de maneira rápida e não invasiva, com o mínimo de recursos

Sendo uma solução exclusivamente de software, o McAfee Database Activity Monitoring pode ser implementado e começar a proteger bancos de dados em menos de uma hora, sem a necessidade de hardware especial ou servidores adicionais. Acelerando ainda mais a distribuição, o McAfee Database Activity Monitoring procura automaticamente bancos de dados na rede e utiliza modelos orientados por assistentes, adequados a vários ambientes regulatórios, para orientar o usuário na criação rápida de políticas de segurança que satisfaçam os requisitos de auditoria. Ao distribuir a responsabilidade pela implementação da política de segurança com sensores autônomos executados em cada servidor de banco de dados, o McAfee Database Activity Monitoring escalona efetivamente os custos para acomodar até mesmo as maiores empresas.

Suporte para a moderna infraestrutura de TI de hoje em dia, incluindo virtualização e nuvem

Outros sistemas de monitoramento de banco de dados se baseiam na análise do tráfego de rede para identificar violações de políticas, algo que é impossível ou ineficiente nas arquiteturas altamente dinâmicas e distribuídas utilizadas em virtualização de centros de dados e "cloud computing" (computação na nuvem). Diferentemente disso, os sensores da McAfee podem ser configurados para se provisionar automaticamente com cada novo banco de dados, solicitar a política de segurança com base nos dados hospedados e, então, começar a enviar quaisquer alertas para o servidor de gerenciamento. Mesmo que a conectividade da rede seja interrompida, os dados ainda estarão protegidos, pois o sensor implementa a política de segurança localmente e os alertas são enfileirados para serem enviados assim que o servidor de gerenciamento estiver novamente acessível.

Integração com a plataforma McAfee ePolicy Orchestrator

O McAfee Database Activity Monitoring é totalmente integrado com o software McAfee ePO, oferecendo relatórios centralizados e informações resumidas de todos os seus bancos de dados a partir de um dashboard consolidado. O software McAfee ePO conecta-se a outras soluções de segurança da McAfee além da proteção de banco de dados a fim de fornecer uma visualização em painel único, oferecendo facilidade de gerenciamento e visibilidade total.

Soluções de segurança de banco de dados da McAfee

A McAfee oferece várias soluções de segurança de banco de dados para ajudar você a obter visibilidade total do seu panorama geral de banco de dados e da sua postura de segurança. Para saber mais, visite www.mcafee.com/br/products/database-security/index.aspx ou entre em contato com o revendedor ou representante da McAfee mais próximo.

Sobre risco e conformidade da McAfee

Os produtos de gerenciamento de risco e conformidade da McAfee proporcionam segurança para todos os seus dispositivos, para os dados que passam por eles e para os aplicativos executados neles. Nossas soluções abrangentes e sob medida reduzem a complexidade para conseguir uma defesa de terminais multicamada que não afete a produtividade. Para saber mais, visite www.mcafee.com/br/products/endpoint-protection/index.aspx.

[1] *Estudo da Verizon Business*, 2013.

McAfee do Brasil Comércio de Software Ltda.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.mcafee.com/br

60603ds_dam_1013_fnl_ETMG