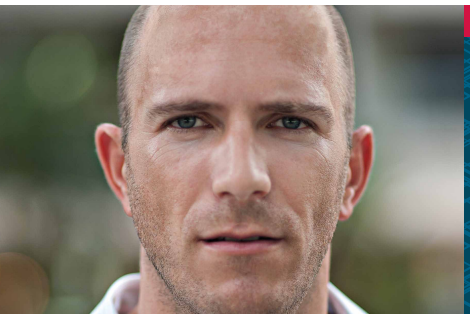

Cinco razões para implementar uma solução de segurança de bases de dados dedicada

Estabelecer uma última linha de defesa crítica

A proteção das informações valiosas e confidenciais armazenadas nas bases de dados é vital para a manutenção da integridade e da reputação de qualquer organização e para assegurar a conformidade com as regulamentações. No entanto, muitas empresas ainda dependem de soluções de segurança com limitações inerentes. Tendo em vista as complexidades das plataformas de bases de dados atuais e o nível de sofisticação dos cibercriminosos dos nossos dias, a implementação de uma solução de segurança de bases de dados completa e dedicada é essencial. Neste documento, poderá encontrar cinco razões para tal.

Vantagens do McAfee Vulnerability Manager

- Visibilidade total do nível de segurança das bases de dados
- Análise de várias bases de dados espalhadas pela empresa a partir de uma consola centralizada
- Redução do período de tempo necessário para alcançar a conformidade e minimização dos ciclos de auditoria, originando uma redução de custos significativa
- Implementação rápida com conhecimentos mínimos do sistema de bases de dados
- Geração rápida de relatórios personalizados num formato de fácil compreensão para utilizadores das mais diversas funções

Vantagens do McAfee Database Activity Monitoring

- Maximização da visibilidade e proteção contra todas as origens de ataques
- Monitorização de ameaças externas, utilizadores privilegiados internos e ameaças sofisticadas oriundas do interior da base de dados
- Minimização dos riscos e responsabilidades, detendo os ataques antes que estes causem danos
- Poupança de tempo e dinheiro graças a uma implementação mais rápida e a uma arquitetura mais eficiente
- Implementação flexível e fácil na infraestrutura de TI que selecionar

1. Não pode proteger recursos que não sabe que existem

Mesmo nos ambientes de TI mais organizados, é frequente existirem centenas ou até mesmo milhares de instâncias de bases de dados com informações altamente confidenciais, sendo difícil para os departamentos de TI fornecerem o número, a localização, a confidencialidade dos dados e o nível de segurança exatos destas bases de dados. O pior é que os criminosos sabem disto e estão constantemente à procura de ângulos mortos. Eles têm o tempo e os recursos técnicos necessários para explorarem bases de dados que pensava que estavam protegidas ou que nem sequer sabia que existiam. A sua falta de visibilidade é a oportunidade deles.

A visibilidade completa do panorama das bases de dados só é possível quando dispõe da capacidade de efetuar uma deteção completa de todas as bases de dados existentes no seu ambiente, juntamente com uma análise destinada a identificar as que contêm informações de cartões de crédito, dados de recursos humanos, valores de vendas e outros dados confidenciais. Além disso, o teste exaustivo e automatizado das vulnerabilidades é crucial para determinar a natureza exata dos seus riscos. Apenas uma solução de segurança de bases de dados dedicada pode fornecer-lhe informações detalhadas e concretas que lhe permitam atribuir prioridades e corrigir problemas de segurança, evitando simultaneamente que sua empresa tenha de incorrer nas despesas associadas à contratação de um consultor de segurança externo.

O McAfee® Vulnerability Manager for Databases deteta automaticamente todas as bases de dados existentes na sua rede, determina se os patches mais recentes foram aplicados e analisa a existência de vulnerabilidades. Na realidade, o McAfee Vulnerability Manager verifica a presença de mais de 4.200 vulnerabilidades nos principais sistemas de bases de dados e classifica as ameaças em níveis de prioridade distintos, fornecendo simultaneamente scripts de correção e recomendações. Este software necessita de conhecimentos mínimos dos sistemas de bases de dados e gera relatórios personalizados em formatos de fácil compreensão para utilizadores das mais diversas funções, tudo isto a partir de uma consola de segurança centralizada.

2. A segurança de perímetro não o protege contra ameaças internas

Investiu muito tempo, esforço e dinheiro para selecionar e implementar firewalls e outras tecnologias de segurança de rede. No entanto, como sabe, nem todos os problemas de segurança têm origem fora do perímetro. Na realidade, uma investigação anual do CERT (Computer Emergency Response Team) indica que metade dos acessos ilegais a bases de dados são causados por utilizadores internos. Consequentemente, necessita de proteger os dados críticos da sua empresa contra os inimigos mais pérfidos: utilizadores privilegiados internos, muitos dos quais têm a capacidade de contornar as funcionalidades de segurança nativas dos sistemas de gestão de bases de dados (DBMS), adulterar os registos de acesso e cobrir as suas pegadas.

A solução de segurança de bases de dados ideal tem de detetar e impedir acessos provenientes de todos os vetores possíveis: ameaças com origem no exterior e, especialmente, no interior. Além disso, tem de fornecer uma arquitetura que permite configurar e impor facilmente políticas de acesso às bases de dados que estejam de acordo com requisitos de conformidade específicos, para garantir continuamente uma segregação de deveres real.

O McAfee Database Activity Monitoring localiza automaticamente as bases de dados existentes na sua rede, protege-as com um conjunto de defesas pré-configuradas e ajuda-o a criar uma política de segurança personalizada para o seu ambiente, permitindo demonstrar a conformidade aos auditores mais facilmente e melhorar a proteção dos dados críticos. O McAfee Database Activity Monitoring permite-lhe obter a visibilidade em tempo real de todas as atividades das bases de dados, incluindo o acesso de utilizadores privilegiados locais e os ataques sofisticados oriundos do interior da base de dados. Este software protege os seus dados contra todas as ameaças através da monitorização das atividades ao nível local em cada servidor de bases de dados, independentemente da localização, e do envio de alertas ou da terminação automática das sessões que sejam consideras suspeitas ou que violem as políticas de segurança de qualquer forma. O McAfee Database Activity Monitoring pode mesmo proteger as suas bases de dados e impor as suas políticas em ambientes virtualizados ou de informática em nuvem.

3. Os hackers atacam mais depressa do que a sua equipa implementa patches

A terça-feira dos patches devia ser declarada feriado para os hackers. É aquele dia do mês em que os fornecedores de bases de dados revelam os alvos mais apetecíveis. Além disso, a terça-feira dos patches dá um certo avanço aos hackers, porque eles sabem o tempo que a sua equipa de gestão de bases de dados demora a colocar offline, aplicar os patches e testar as bases de dados. Na realidade, eles contam que o processo de aplicação de patches constitua uma interrupção tão grande que a sua equipa o atrase o mais possível, dando-lhes tempo mais que suficiente para arranjarem maneira de entrar.

Não existe nenhuma maneira de contornar o processo tradicional de aplicação de patches (e as oportunidades que este concede aos criminosos) a menos que possua uma solução de segurança de bases de dados dedicada. Esta solução tem também de lhe permitir atualizar o nível de segurança das suas bases de dados em tempo real, sem colocar uma carga de trabalho insuportável sobre os seus funcionários e sem interromper o funcionamento da sua empresa.

O McAfee Virtual Patching for Databases protege as bases de dados contra os riscos apresentados pelas vulnerabilidades não corrigidas, detetando e impedindo tentativas de ataque e intrusão em tempo real, sem necessitar de períodos de inatividade das bases de dados ou de testes das aplicações. Deste modo, poderá estar descansado sabendo que está protegido contra ameaças mesmo durante os períodos de maior vulnerabilidade: o período de tempo que decorre entre a emissão dos patches pelo fornecedor e a instalação destes.

O McAfee Database Activity Monitoring é outra solução não intrusiva e isenta de períodos de inatividade, que proporciona uma camada adicional de proteção para as terças-feiras dos patches e muito mais. Os seus sensores baseados na memória intercetam ataques em bases de dados provenientes da rede, de utilizadores locais com sessão iniciada no próprio servidor e até mesmo do interior da base de dados, através de procedimentos ou acionadores armazenados.

4. Não pode continuar a sacrificar a conformidade em nome da continuidade

Os requisitos de conformidade com as regulamentações que são aplicados em indústrias como a dos cuidados de saúde, das finanças e do retalho estão em evolução constante e a tornar-se cada vez mais exigentes. Não é portanto de estranhar que as bases de dados críticas sejam fortemente afetadas pelas práticas de conformidade, que exigem que as bases de dados sejam atualizadas com os patches mais recentemente disponibilizados pelo fornecedor de DBMS. No entanto, devido aos problemas associados à necessidade de colocar offline, aplicar patches e testar várias bases de dados de tipos diferentes, a maior parte das organizações sacrifica a conformidade para preservar a continuidade do funcionamento. Além disso, podem mesmo existir bases de dados legadas em utilização, para as quais já não são disponibilizados patches.

O McAfee Virtual Patching for Databases permite-lhe manter a continuidade do funcionamento sem sacrificar a conformidade com as regulamentações. Esta solução permite-lhe efetuar a aplicação de patches tradicional de acordo com o seu próprio plano, sabendo que as bases de dados estão protegidas e em conformidade. No que respeita às auditorias de conformidade, o McAfee Virtual Patching for Databases permite-lhe poupar tempo e controlar a compensação. Além disso, permite-lhe mesmo expandir a proteção mais recente às bases de dados legadas que já não sejam suportadas pelos fornecedores de DBMS.

Vantagens do McAfee Virtual Patching

- Proteção contra ameaças mesmo antes da instalação dos patches disponibilizados pelo fornecedor
- Eliminação da necessidade de conhecimentos específicos de DBMS para as equipas de TI e segurança
- Manutenção das bases de dados de produção online, graças à conceção não intrusiva do software
- Proteção integrada das bases de dados com distribuição automática das atualizações
- Conformidade facilitada com normas como a PCI DSS e a HIPAA, entre outras

Vantagens do McAfee ePolicy Orchestrator Software

- Visibilidade ponto-a-ponto da segurança de base de dados e da conformidade a partir de uma consola de gestão centralizada
- Consola unificada que lhe permite transpor facilmente as bases de dados para um programa de gestão de segurança unificado nas suas instalações, em localizações remotas e até mesmo na nuvem
- Arquitetura aberta e extensível que liga a gestão de soluções de segurança da McAfee e de terceiros às suas ferramentas de gestão do protocolo LDAP (Lightweight Directory Access Protocol), de operações de TI e de gestão da configuração

5. Quando os dados estão na nuvem, a visibilidade é extremamente limitada

A informática em nuvem oferece vantagens financeiras e operacionais tremendas mas, como sabe, existe um senão: os seus funcionários podem perder o controlo dos dados sensíveis e ficar com uma visibilidade praticamente nula relativamente a quem está a aceder a esses dados. No entanto, desde que disponha da solução de segurança de bases de dados adequada, pode proteger os seus dados em ambientes físicos e virtuais. A solução adequada pode impedir atividades não autorizadas nas bases de dados e apresentar todas as informações numa consola de gestão personalizada, mesmo que as bases de dados estejam virtualizadas e residam na nuvem.

Graças à exclusiva implementação de sensores baseados na memória, o McAfee Database Activity Monitoring pode ser configurado para aprovisionar automaticamente cada máquina virtual nova. Simultaneamente, poderá solicitar políticas de segurança com base nos dados alojados e, em seguida, enviar quaisquer alertas para o servidor de gestão. Além disso, os sensores podem funcionar autonomamente mesmo quando desligados do servidor, para que os dados confidenciais sejam protegidos e preservados quer a base de dados esteja online ou offline, e independentemente da sua localização em qualquer momento. Mesmo que a conectividade de rede seja interrompida, os dados continuam protegidos porque o sensor implementa a política de segurança localmente, colocando os alertas em fila para entrega quando for possível contactar novamente o servidor de gestão.

Adicionalmente, o acesso às bases de dados baseadas na nuvem pode ser monitorizado através do software McAfee® ePolicy Orchestrator® (McAfee ePO™), que proporciona uma consola de gestão de segurança da empresa para proporcionar a visibilidade ponto-a-ponto da segurança das bases de dados, da segurança da empresa e da conformidade.

Por outras palavras, com nuvem ou sem nuvem, os seus funcionários mantêm constantemente os níveis mais elevados de visibilidade. A McAfee disponibiliza a solução de segurança de bases de dados adequada para o seu ambiente de TI, independentemente da globalidade das operações ou da confidencialidade dos dados.

Vantagens da Segurança de bases de dados McAfee

- Facilidade de implementação e utilização
- Visibilidade total do nível de segurança das suas bases de dados
- Alinhamento das práticas de administração de políticas de segurança entre os funcionários responsáveis pela segurança e os funcionários responsáveis pela gestão das bases de dados
- Eficiência na manutenção da conformidade com as regulamentações
- Minimização dos riscos e responsabilidades, detendo os ataques antes que estes causem danos
- Gestão da segurança das bases de dados a partir de uma consola centralizada

Saiba como manter as suas bases de dados protegidas e disponíveis

Na McAfee, sabemos que as suas bases de dados armazenam os recursos mais críticos da sua empresa. Elas têm de estar disponíveis 24 horas por dia para que a sua empresa não pare. Tal como as suas bases de dados, nós estamos disponíveis 24 horas por dia. É por esse motivo que dizemos que a segurança nunca dorme. Pode ficar descansado enquanto a nossa equipa de peritos em segurança de bases de dados trabalha incansavelmente para manter as suas informações confidenciais protegidas e disponíveis, ajudando a sua empresa a assegurar a conformidade com políticas internas e regulamentações da indústria.

Para obter informações mais detalhadas sobre o modo como a Segurança de bases de dados McAfee pode ajudá-lo a proteger as bases de dados críticas da sua empresa, visite http://www.mcafee.com/us/products/database-security/index.aspx ou contacte o representante ou revendedor da McAfee mais próximo de si.

Siga-nos no Twitter: @McAfee_DBSecure.

Acerca da Segurança de terminais McAfee

A McAfee, uma subsidiária totalmente participada da Intel Corporation (NASDAQ:INTC), é a maior empresa mundial de tecnologia de segurança. As nossas avançadas soluções de segurança de terminais ajudam a proporcionar segurança a todos os seus dispositivos, aos dados que estes utilizam e às aplicações em execução neles. Esta soluções completas e personalizadas reduzem a complexidade para proporcionar uma defesa de terminais composta por várias camadas, sem afetar a produtividade. Trata-se de uma combinação perfeita de análise de malware inteligente tradicional, criação dinâmica de listas brancas, prevenção comportamental de intrusões de dia zero, gestão unificada e informações integradas sobre ameaças. Obtenha mais informações em http://www.mcafee.com/us/products/endpoint-protection/index.aspx.

McAfee Portugal
Avenida da Liberdade, N° 110
1269-046 Lisboa
Portugal
Tel: 00 351 21 340 45 40
Fax: 00 351 21 340 45 11
www.mcafee.com/pt

41903brf_top5-db-sec_0212_fnl_ASD