

McAfee Database Activity Monitoring

Une solution économique pour protéger vos bases de données et répondre à vos besoins en matière de conformité



Les entreprises conservent leurs données les plus précieuses et les plus sensibles dans des bases de données. Or, la protection du périmètre et la sécurité de base offerte par ces bases de données ne suffisent pas à vous protéger contre les attaques sophistiquées d'aujourd'hui ou les menaces potentielles émanant d'utilisateurs internes malveillants. Les statistiques¹ indiquent que plus de 96 % des fichiers compromis impliquent une base de données, et que 66 % des violations passent inaperçues pendant plusieurs mois au moins. McAfee® Database Activity Monitoring détecte automatiquement les bases de données présentes sur votre réseau, les protège au moyen d'un ensemble de mécanismes préconfigurés et vous aide à mettre en place une stratégie de sécurité personnalisée pour votre environnement. De quoi pouvoir apporter plus facilement la preuve de votre conformité aux auditeurs et améliorer la protection de vos données critiques.

Principaux avantages

- Optimisation de la visibilité et de la protection contre toutes les sources d'attaques
- Surveillance des menaces externes, des utilisateurs internes disposant de privilèges et des menaces sophistiquées émanant de la base de données elle-même
- Limitation des risques et de la responsabilité grâce au blocage des attaques avant qu'elles ne provoquent des dégâts
- Gain de temps et d'argent grâce à un déploiement rapide et à une architecture plus efficace
- Déploiement aisé sur l'infrastructure informatique de votre choix
- Intégration avec les principaux produits de McAfee, dont la plate-forme de gestion McAfee® ePolicy Orchestrator® (McAfee ePO™) et McAfee Vulnerability Manager for Databases

Grâce à McAfee Database Activity Monitoring, les entreprises bénéficient d'une meilleure visibilité sur l'activité de leurs bases de données, et notamment sur les accès locaux privilégiés et les attaques sophistiquées émanant de la base de données. McAfee Database Activity Monitoring les aide à protéger leurs données les plus précieuses et sensibles contre les menaces externes et les utilisateurs internes malveillants. En plus de fournir une piste d'audit fiable, McAfee Database Activity Monitoring prévient les intrusions en fermant les sessions contrevenant à la stratégie de sécurité.

McAfee Database Activity Monitoring offre diverses possibilités aux entreprises :

- Mise en place rapide d'une stratégie de sécurité personnalisée répondant aux réglementations sectorielles ou aux normes internes de gouvernance informatique
- Journalisation de l'accès aux données sensibles, notamment à tous les détails des transactions, à des fins d'audit
- Fermeture des sessions contrevenant aux stratégies en vigueur et mise en quarantaine des utilisateurs suspects, de manière à éviter toute compromission des données
- Maintien de la répartition des responsabilités exigée par de nombreuses réglementations

McAfee Database Activity Monitoring protège, à un coût abordable, vos données contre toutes les menaces en assurant le suivi des activités localement, sur chaque serveur de base de données, et en signalant ou en bloquant tout comportement malveillant en temps réel, même lorsque le serveur tourne dans un environnement virtualisé ou dématérialisé.

Protection contre tous les vecteurs de menaces ciblant les bases de données

Les attaques ciblant les données précieuses stockées dans vos bases peuvent provenir du réseau ou d'utilisateurs locaux connectés au serveur, voire de l'intérieur même des bases de données, via des procédures stockées ou des déclencheurs. McAfee Database Activity Monitoring utilise des sondes fondées sur la mémoire pour intercepter ces trois types de menaces au moyen d'une solution unique non intrusive. Les informations ainsi collectées peuvent servir à démontrer la conformité à des fins d'audit et à améliorer la sécurité globale des données les plus précieuses de l'entreprise.

Identification des menaces à mesure qu'elles se présentent, limitation des risques et de la responsabilité

Contrairement à l'audit de base et à l'analyse des journaux, qui ne vous informent des faits qu'a posteriori, les fonctionnalités de suivi et de prévention des intrusions en temps réel bloquent les infractions avant que celles-ci ne provoquent des dégâts. Par ailleurs, des alertes sont directement envoyées au tableau de bord de surveillance, avec des détails complets concernant l'infraction à la stratégie, afin de vous permettre d'y remédier. Vous pouvez également configurer des violations à haut risque de sorte que le système ferme automatiquement les sessions suspectes et mette les utilisateurs malveillants en quarantaine, de manière à donner le temps à l'équipe de sécurité d'enquêter sur l'intrusion.

Des patchs virtuels pour se protéger des exploits connus et de nombreuses menaces de type « jour zéro »

Il n'est pas toujours possible d'appliquer les patchs des fournisseurs immédiatement, car leur installation exige souvent des tests des applications et une interruption des activités. Sans compter que certaines applications utilisent des versions plus anciennes des bases de données qui ne font plus l'objet de patchs. McAfee Database Activity Monitoring détecte les attaques qui tentent d'exploiter des vulnérabilités connues ainsi que les vecteurs de menaces courants, et peut être configuré pour émettre des alertes ou mettre fin à la session en temps réel. Des patchs virtuels sont régulièrement distribués afin de couvrir les nouvelles vulnérabilités découvertes. Ceux-ci peuvent être mis en œuvre sans temps d'arrêt de la base de données, protégeant ainsi les données sensibles jusqu'à ce qu'un patch soit publié par l'éditeur et puisse être appliqué.

Déploiement rapide et non intrusif, avec un minimum de ressources

Solution 100 % logicielle, McAfee Database Activity Monitoring peut être installée et devenir opérationnelle en moins d'une heure, sans exiger de matériel spécial ou de serveurs supplémentaires. Ce n'est pas tout : pour un déploiement encore plus rapide, elle analyse automatiquement le réseau à la recherche des bases de données et utilise des modèles basés sur des Assistants correspondant à divers environnements réglementaires. De quoi vous aider à mettre rapidement en place des stratégies de sécurité personnalisées pour répondre à vos besoins en termes d'audit. En confiant le soin d'appliquer la stratégie de sécurité à des sondes autonomes tournant sur chacun des serveurs de base de données, McAfee Database Activity Monitoring peut évoluer de manière économique, jusqu'à prendre en charge les plus grands réseaux d'entreprise.

Paré pour l'infrastructure informatique moderne, y compris la virtualisation et le cloud

Les autres systèmes de surveillance des bases de données s'appuient sur l'analyse du trafic réseau pour identifier les infractions aux stratégies — une méthode inefficace, voire impossible à appliquer, dans les architectures distribuées et hautement dynamiques utilisées pour la virtualisation des centres de données et le cloud computing.

En revanche, les sondes de McAfee peuvent être configurées pour être automatiquement mises en service chaque fois qu'une nouvelle base de données vient s'ajouter au réseau, demander la stratégie de sécurité applicable en fonction des données qu'elle contient, puis commencer à envoyer des alertes au serveur de gestion. Dans la mesure où la sonde applique la stratégie de sécurité localement, vos données restent protégées en toutes circonstances, même en cas d'interruption de la connexion réseau. Dans ce cas, les alertes générées sont envoyées au serveur de gestion dès que celui-ci redevient disponible.

Intégration avec la plate-forme McAfee ePolicy Orchestrator

McAfee Database Activity Monitoring est intégré au logiciel McAfee ePolicy Orchestrator afin de fournir des rapports centralisés et des informations récapitulatives à l'ensemble de vos bases de données à partir d'un tableau de bord consolidé. Le logiciel McAfee ePO ne se limite pas à la protection des bases de données et s'intègre à d'autres solutions de sécurisation de McAfee afin de faciliter la gestion et d'offrir une visibilité totale depuis un outil centralisé.

Solutions de sécurisation des bases de données de McAfee

McAfee propose plusieurs solutions de sécurisation des bases de données, qui vous permettent de bénéficier d'une visibilité totale sur votre environnement de bases de données et votre niveau de sécurité. Pour en savoir plus, visitez notre site à l'adresse www.mcafee.com/fr/products/database-security/index.aspx ou contactez votre revendeur ou représentant local McAfee.

A propos de la protection des postes clients McAfee

Les solutions de protection des postes clients McAfee assurent la sécurisation de tous vos équipements, des données qu'ils hébergent ainsi que des applications qu'ils exécutent. Complètes et taillées sur mesure, elles simplifient la mise en place d'un système de défense des postes clients multiniveau sans impact sur la productivité. Pour en savoir plus, consultez notre site à l'adresse : www.mcafee.com/fr/products/endpoint-protection/index.aspx.

