

Renforcer la sécurité des bases de données

Quand pare-feux réseau et solutions individuelles de protection des bases de données ne suffisent plus

Sommaire

Introduction	3
Les défis	4
Nos solutions	5
A propos des produits McAfee de gestion des risques et de la conformité	9
A propos de McAfee	9

Les bases de données hébergent les informations qui ont le plus de valeur pour l'entreprise. Malgré cela, elles sont bien souvent mal protégées. Il devrait aller de soi que les bases de données peuvent et doivent être sécurisées au moins aussi rigoureusement, si pas mieux, que tous les autres systèmes de l'entreprise. Les solutions McAfee® de sécurisation des bases de données sont des produits multiniveaux efficaces, parfaitement en mesure de protéger l'ensemble des bases de données et de leur contenu. Elles permettent ainsi de contrer les menaces et d'éliminer les vulnérabilités, tout en assurant la démonstration de la conformité et en optimisant l'efficacité opérationnelle. Le constat est simple : aucun autre produit ne peut les égaler à l'heure actuelle.

Introduction

« Je pirate, je pille, je gagne de l'argent à la pelle. »

— Andrew Auernheimer, accusé par un tribunal fédéral américain du vol et de la distribution des adresses e-mail de 120 000 utilisateurs de l'iPad d'Apple¹

Imaginons. Votre PDG lit dans un grand quotidien un article qui l'interpelle au plus haut point : une grande entreprise, ténor dans le secteur de la fabrication, est en sérieuse difficulté. Ses bases de données ont subi une intrusion et l'entreprise doit désormais informer des centaines de milliers de clients que leurs numéros de cartes de crédit sont probablement entre les mains de cybercriminels. Inquiet, votre PDG vous convoque dans son bureau pour vous demander : « est-ce que cela pourrait nous arriver ? Nos bases de données sont-elles suffisamment protégées ? ».

Que pouvez-vous lui répondre, en toute honnêteté ? Des études ont montré que plus de 92 % des violations de sécurité signalées impliquaient une base de données et que plus de 87 % étaient causées par des exploits exigeant des compétences techniques avancées². En d'autres mots, les responsables ne sont pas quelques ados désœuvrés vaguement doués en informatique. Il s'agit bien ici d'experts chevronnés qui, moyennant de très généreuses compensations, mettent leurs talents au service d'organisations criminelles. Ou d'employés mécontents de leur sort qui volent à leur entreprise des données propriétaires au nez et à la barbe de tous.

Quelle que soit leur identité, il ne fait aucun doute que ces criminels ont des palmarès impressionnants. Quelques exemples suffiront à vous convaincre :

- 29 juin 2010 — Quelque 470 000 clients de la société d'assurance santé Anthem Blue Cross sont informés que leurs numéros de sécurité sociale et de cartes de crédit étaient susceptibles d'avoir été révélés à la suite du piratage du site web de l'entreprise³.
- 20 août 2009 — Trois complices russes sont jugés par un tribunal fédéral du New Jersey pour le piratage présumé de la société de traitement de cartes Heartland Payment Systems, basée dans ce même Etat, ainsi que les entreprises Hannaford Brothers, 7-Eleven et deux détaillants nationaux dont les noms n'ont pas été dévoilés. Selon les documents du procès, ces pirates ont dérobé plus de 130 millions de numéros de cartes de crédit et de débit rien qu'auprès de Heartland et Hannaford⁴.
- 24 février 2011 — La banque londonienne HSBC confirme qu'un ancien informaticien de leurs bureaux de Genève a fait main basse sur les données des comptes de plus de 24 000 clients. Leur ex-employé a été pris en flagrant délit alors qu'il essayait de vendre ces données à des banques libanaises⁵.
- Septembre 2010 — Un ancien chimiste et directeur technique de Valspar Corporation plaide coupable du vol de secrets commerciaux d'une valeur approximative de 20 millions de dollars subtilisés à cette entreprise de fabrication de peinture. L'auteur du crime a avoué au tribunal qu'il avait dérobé de nombreuses formules et autres informations propriétaires dès lors qu'il allait passer à la concurrence⁶.

1. <http://www.justice.gov/criminal/cybercrime/auernheimerArrest.pdf>

2. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

3. <http://homelandsecuritynewswire.com/worst-database-security-breaches-us-uk>

4. <http://homelandsecuritynewswire.com/worst-database-security-breaches-us-uk>

5. <http://www.esecurityplanet.com/news/article.php/3870071/HSBC-Confirms-Massive-Database-Security-Breach.htm>

6. <http://cicentre.net/wordpress/index.php/2010/09/02/former-paint-manufacturing-chemist-pleads-guilty-to-stealing-trade-secrets-valued-up-to-20-million/>

Les défis

Les vieilles habitudes ont la vie dure

Un grand nombre d'entreprises se contentent de sécuriser l'entreprise au niveau du réseau et considèrent que cela est suffisant. Cette stratégie pourrait sembler raisonnable si toutes les menaces provenaient de l'extérieur. Or selon une étude annuelle réalisée par le CERT, jusqu'à la moitié des intrusions dans les bases de données sont perpétrées de l'intérieur. C'est d'ailleurs la raison pour laquelle de nombreuses entreprises déploient un second niveau de sécurisation composé de solutions individuelles qui protègent les bases de données. Elles en retirent un (faux) sentiment de sécurité superficiel, sans que cela constitue pour autant une approche efficace de la sécurité informatique. Les solutions isolées présentent des limitations inhérentes. Tout d'abord, la plupart d'entre elles ne prennent en charge qu'un seul fournisseur ou sont limitées du point de vue de la fonctionnalité. En d'autres mots, elles sont généralement réservées aux bases de données Oracle, Microsoft ou IBM, et elles ne couvrent que des sections limitées et non contiguës du grand puzzle de la sécurité des bases de données. Même après avoir totalement mis en œuvre ces produits individuels, les entreprises éprouvent des difficultés à agréger et à corréler les données issues de ceux-ci. Dans les nombreux cas où les bases de données de plusieurs fournisseurs sont éparpillées au sein de l'infrastructure, les entreprises ne savent même pas quelle base de données spécifique elles utilisent et la couverture de protection est lacunaire.

Les gestionnaires de bases de données veulent le statu quo

Dans la mesure où les bases de données sont constamment utilisées et d'une importance critique, leurs administrateurs créent généralement des configurations optimales de référence, qui maximisent la disponibilité et les performances. Ils sont peu enclins à modifier ces configurations, à appliquer des correctifs aux bases de données ou à ajouter à leurs serveurs des logiciels de sécurité dont ils craignent qu'ils affecteront les performances.

La direction rechigne à passer des investissements, même obsolètes, en pertes et profits

Cette attitude est légitime. Quand une entreprise a investi des sommes considérables dans des produits isolés, les dirigeants ont tendance à croiser les doigts en s'attendant à ce qu'une solution spécialisée supplémentaire fasse l'affaire. Le problème est que ces solutions ponctuelles ne permettent pas d'obtenir une vue d'ensemble, un point de vue général qui permettrait d'identifier les failles de sécurité béantes qu'elles laissent justement. Or, soyons clairs, quelle entreprise peut se permettre de se faire pirater ? Investir dans une solution de sécurisation complète, qui protège vos données, l'accès à vos bases de données, le réseau, les serveurs et les postes clients vous coûtera au bout du compte nettement moins qu'une violation de sécurité importante.

Chaque annonce de la publication d'un patch rend votre entreprise plus vulnérable

La période de vulnérabilité la plus forte se situe entre le moment où les éditeurs de systèmes de gestion de base de données (SGDB) publient un patch de sécurité et le moment où celui-ci est appliqué. Les pirates savent qu'il y a là une fabuleuse opportunité à saisir car cette faille est susceptible d'être exploitée pendant ce laps de temps. Prenons l'exemple suivant. Un article récemment publié sur ZDNet, intitulé *Oracle Patch Tuesday heads-up: 81 database security holes*⁷ (Avertissement à propos de la prochaine publication des patches de sécurité Oracle : 81 failles de sécurité dans les bases de données), a informé tant les responsables de la sécurité que les pirates informatiques de l'annonce future par Microsoft et Oracle de l'existence de vulnérabilités non encore corrigées. Toujours selon l'article, certaines d'entre elles étaient si graves qu'elles permettaient une exploitation à distance sans authentification (via un réseau sans qu'il soit nécessaire de fournir un nom d'utilisateur et un mot de passe). Les auteurs décrivaient ensuite certaines vulnérabilités des bases de données Oracle dans le détail.

Les pirates n'ont pas manqué l'aubaine et se sont empressés d'exploiter toutes les vulnérabilités possibles. Qui plus est, à cause des outils d'automatisation utilisés par les pirates et en raison du partage généralisé d'informations via les réseaux sociaux, la fréquence et la sophistication des attaques contre les bases de données se sont accrues de façon exponentielle entre la publication de cet article et le moment où les équipes informatiques, après la diffusion publique des patches, se sont attelées à la tâche de correction des bases de données.

Points essentiels

Les bases de données nécessitent davantage de protection qu'elles n'en bénéficient actuellement :

- Les entreprises stockent souvent leurs données les plus critiques et sensibles dans des bases de données.
- 92 % des violations en matière de sécurité des informations au sein des entreprises impliquent des bases de données.
- La moitié des intrusions que subissent les bases de données sont le fait d'une personne interne à l'entreprise.

Les solutions McAfee® de sécurisation des bases de données permettent de :

- sécuriser les informations stratégiques enregistrées dans les bases de données ;
- rationaliser la mise en conformité avec les réglementations publiques et sectorielles ;
- préserver les performances des bases de données.

Pour en finir avec les problèmes de mise en conformité

Les normes et réglementations telles que PCI DSS, HIPAA, SOX, GLBA et SAS 70 nécessitent la mise en place de contrôles spécifiques en matière d'accès aux données financières et aux données client sensibles. Et où résident ces données ? Dans vos bases de données stratégiques. Elles ne font par ailleurs que croître en volume, à un rythme effréné.

Les solutions McAfee de sécurisation des bases de données offrent une vision d'ensemble qui permet de réduire les ressources requises lors des audits, tout en protégeant les données de façon transparente contre d'éventuelles intrusions lourdes de conséquences.

Intégration avec McAfee ePO

Les composants des solutions McAfee de sécurisation des bases de données sont intégrés avec la console McAfee ePolicy Orchestrator® (McAfee ePO™). Cette intégration permet la gestion centralisée de la sécurité et des rapports de conformité pour des milliers de bases de données. Les économies sont extraordinaires et le retour sur investissement très rapide.

A ce jour, plus de 35 000 clients gèrent plus de 60 millions de postes de travail et serveurs à l'aide de McAfee ePO.

L'approche ponctuelle n'est pas viable

De nombreuses entreprises mettent en œuvre d'énormes moyens pour se conformer aux normes et réglementations dont relève leur secteur d'activités : PCI DSS, SOX, HIPAA/HITECH, etc. La plupart d'entre elles sont diligentes dans l'application de patchs aux bases de données. Toutefois, toutes ces précautions ne sont pas suffisantes pour verrouiller complètement un environnement et sécuriser efficacement les actifs. Les produits isolés pour bases de données propres à un fournisseur donné ne sont pas davantage à la hauteur. Si nombre d'entre eux sont performants, en fonctionnement isolé ils ne parviennent pas à rivaliser avec la débauche de moyens informatiques et d'ingéniosité humaine consacrée au piratage des bases de données. Même avec l'application régulière de patchs et l'association de plusieurs produits individuels, les bases de données resteront vulnérables. Et au bout du compte, même si une seule base de données est compromise, c'est peut-être l'entreprise tout entière qui joue sa survie.

Menaces persistantes avancées et cyberguerre

De nos jours, l'identité et les données en ligne sont plus importantes que jamais. Du coup, pirates et cybercriminels ont adopté des méthodes à la fois furtives et parfaitement ciblées, que l'on a baptisées du nom de « menaces persistantes avancées » (APT, *advanced persistent threat*). Ces attaques exploitent, lentement mais méthodiquement, les vulnérabilités présentes dans les réseaux, les systèmes d'exploitation et finalement, les couches de base de données avant de parvenir à dérober vos données. Elles ne sont pas aussi voyantes que des attaques par déni de service ou la dégradation de pages web. Malheureusement, un produit isolé est incapable de les contrer.

Si votre entreprise possède des éléments de propriété intellectuelle de valeur ou héberge des informations confidentielles susceptibles d'intéresser d'autres pays, la cyberguerre constitue alors un autre danger potentiel. Dans la mesure où les attaques de ce genre sont commanditées par des entités publiques, leurs auteurs disposent d'importantes ressources. Pour se protéger, les entreprises doivent mettre en place des stratégies globales, dans le but de combattre plusieurs vecteurs de menaces et de sécuriser tous les points névralgiques, du réseau aux systèmes d'exploitation et aux bases de données. Toutefois, la mesure essentielle consiste à mettre en œuvre une solution qui leur offre une vue générale sur leur état de sécurisation dans son ensemble, et pas uniquement celui des bases de données.

Nos solutions

Sécurisation de l'environnement de bases de données : une approche globale des risques et de la conformité

Les fonctionnalités de sécurisation des bases de données natives sont trop fragmentées et sollicitent l'attention soutenue d'un effectif trop important pour protéger efficacement des environnements hétérogènes de grande envergure. De plus, elles possèdent inévitablement un impact considérable sur les performances des systèmes. Les mesures de protection du périmètre sont incapables à elles seules de contrer les attaques sophistiquées ciblant des vulnérabilités propres aux bases de données, tout comme elles ne peuvent bloquer les accès non autorisés par des utilisateurs internes bénéficiant de privilèges. Dès lors, on peut se demander en quoi consiste une solution de sécurisation des bases de données complète mais pratique. Quelles en sont les fonctions et les caractéristiques essentielles ?

Les experts de McAfee ont déterminé qu'une sécurité et une mise en conformité efficaces des bases de données passe par une approche multiniveau qui présente toutes les caractéristiques suivantes :

- Visibilité globale sur les actifs et les vulnérabilités des bases de données d'entreprise, indépendamment du fournisseur et du type de plate-forme technologique
- Surveillance des activités et mise en œuvre des stratégies qui n'imposent pas une charge supplémentaire aux bases de données elles-mêmes
- Contrôles et données d'audit fiables qui assurent une séparation des rôles, pour que même les utilisateurs avec privilèges ne puissent pas passer outre les mesures de sécurité
- Protection de l'environnement de bases de données étendu qui couvre les services de fonctionnement, l'accès, le transport et le stockage
- Gestion et surveillance continues et automatisées de l'environnement étendu dans son intégralité

A tous les niveaux, ces solutions doivent être étroitement intégrées et constamment tenues à jour par des informations sur les menaces en temps réel, collectées à l'échelle mondiale. Examinons à présent, niveau par niveau, les exigences qui sous-tendent la sécurisation et la conformité d'un environnement de bases de données d'entreprise, ainsi que les technologies McAfee qui permettent de traduire ces exigences en réalité.

Niveau 1 : découverte et évaluation des vulnérabilités pour les bases de données, systèmes d'exploitation et réseaux

Pour sécuriser un environnement de bases de données, vous devez connaître tous vos actifs de bases de données ainsi que leurs états de configuration en cours. De plus, vous devez être en mesure de détecter automatiquement toutes les bases de données du réseau, quel que soit le fournisseur ou la plateforme, de dresser un inventaire complet des informations de configuration, de déterminer si les derniers patches ont été appliqués et de rechercher les faiblesses communes. Ces fonctions sont fondamentales pour parvenir à démontrer la conformité réglementaire et pour assurer la sécurité des données. Dans la gamme McAfee, elles sont proposées par la solution McAfee Vulnerability Manager for Databases. Une fois qu'une base de données est identifiée, le système d'exploitation sur lequel elle est exécutée doit lui aussi être identifié et réconcilié avec celle-ci. Ces actions sont réalisées par les logiciels McAfee Vulnerability Manager et McAfee ePolicy Orchestrator® (McAfee ePO™). Enfin, il faut établir un inventaire de tous les périphériques réseau, de leurs configurations et de leurs vulnérabilités.

McAfee Vulnerability Manager for Databases identifie automatiquement les bases de données de votre réseau et effectue plus de 3 800 vérifications des vulnérabilités sur les principaux systèmes de bases de données, notamment Oracle, Microsoft SQL Server, IBM DB2 et MySQL. Il évalue les risques posés par pratiquement tous les vecteurs de menaces et détermine si les derniers patches sont appliqués. Il contrôle les vulnérabilités courantes, telles que les mots de passe faibles ou les comptes par défaut, et recherche la présence de numéros de carte de crédit ou de sécurité sociale enregistrés en texte clair. Enfin, il trie et classe en liste hiérarchique les résultats d'analyse et propose des scripts de correction ainsi que des recommandations.

McAfee Vulnerability Manager for Databases est mis au point et géré par l'équipe ayant contribué à sept des dix derniers patches critiques publiés par Oracle. Il bénéficie des grandes compétences d'éminents experts en bases de données pour assurer diverses fonctions, à savoir :

- Identifier la probabilité de risques propres aux bases de données, dont l'injection de code SQL, les exploits par Buffer Overflow et les codes PL/SQL non sécurisés ou malveillants
- Hiérarchiser les résultats obtenus et mettre en avant les « vrais » problèmes nécessitant une attention immédiate
- Fournir des informations exploitables quant à la manière de gérer les risques, par exemple en proposant des scripts de correction chaque fois que c'est possible
- Permettre à des utilisateurs de solutions de sécurisation et de conformité possédant peu de connaissances en matière de bases de données d'appréhender rapidement les risques liés aux données sensibles et les mesures à prendre pour les limiter

McAfee Vulnerability Manager for Databases procure une visibilité complète sur les vulnérabilités des bases de données, posant ainsi les bases d'une sécurisation efficace et d'une conformité au coût mesuré.

McAfee Vulnerability Manager for Databases permet de détecter et de réconcilier rapidement les actifs présents sur le réseau. Non seulement il identifie les services en cours d'exécution, les systèmes d'exploitation et les périphériques réseau, mais il offre une plateforme permettant de mettre en œuvre et d'administrer la gestion du cycle de vie des vulnérabilités. Une base de données qui est sécurisée alors que le système d'exploitation sur lequel elle s'exécute ne l'est pas est vulnérable. Pour réduire le risque, il est essentiel de l'évaluer et de le gérer au niveau du système d'exploitation et de la couche réseau. McAfee Vulnerability Manager for Databases peut évaluer de façon approfondie plusieurs systèmes d'exploitation, périphériques réseau et workflows à la recherche de vulnérabilités et corriger ces dernières.

McAfee Change Control assure des fonctions capitales d'évaluation de la configuration réseau. Il peut analyser la configuration réseau et enregistrer les informations pertinentes. De plus, il permet de revenir à une configuration précédente si l'actuelle n'est pas optimale.

Niveau 2 : protection de tous les aspects de l'environnement de bases de données

Une fois toutes les bases de données de l'entreprise consignées dans un inventaire et configurées pour en optimiser la sécurisation, il est temps de protéger tous les autres éléments de l'environnement de bases de données étendu : le réseau, les serveurs et les données au repos. A l'instar des bases de données elles-mêmes, chaque composant de l'environnement de bases de données étendu doit être évalué, protégé et placé sous surveillance.

La sécurisation du réseau commence par un pare-feu d'entreprise qui permet de découvrir, de contrôler, de visualiser et de protéger les bases de données nouvelles et existantes, en octroyant un accès aux seuls utilisateurs et applications pertinents. Le pare-feu d'entreprise est combiné à un système complet de prévention des intrusions, ce qui assure une protection en temps réel contre les menaces de tous types.

McAfee Firewall Enterprise propose des fonctions fiables de découverte, de contrôle, de visualisation et de protection des applications, nouvelles et existantes, basées sur des analyses visuelles et l'identité des utilisateurs, qui permettent de créer des règles extrêmement efficaces. Avec la version 8 de cette solution, McAfee révolutionne véritablement la technologie des pare-feux : dans un seul produit facile à gérer et économique, il associe la visibilité et le contrôle complets sur les applications, les informations sur les menaces basées sur la réputation et la protection contre les attaques multivectorielles.

McAfee Network Security Platform est un système de prévention des intrusions de pointe, dont l'efficacité est validée par des tests indépendants. Il s'agit de la solution de sécurisation du réseau et des systèmes la plus complète et la plus fiable du marché. Cette appliance tout en un offre une protection en temps réel contre les attaques en tous genres : connues, « jour zéro », chiffrées, par déni de service, par déni de service distribué ou par requêtes de synchronisation (*SYN flood*). Capable de détecter les attaques dans tous les déploiements, même les plus exigeants, Network Security Platform a obtenu la certification « 10 Gigabit IPS » décernée par NSS Labs en matière de systèmes de prévention des intrusions.

L'étape suivante consiste à sécuriser les serveurs. Alors que les bases de données sont très dynamiques, les serveurs sur lesquels elles s'exécutent font l'objet de configurations précises et rigoureuses, verrouillées dans un souci de stabilité. Cela se prête parfaitement à l'établissement de listes d'autorisation des applications, garantissant que seules les applications approuvées peuvent interagir avec les bases de données. De plus, la protection de la mémoire et la prévention des intrusions contrent les attaques de type « jour zéro » et les injections de code SQL en recourant à l'analyse du comportement et des signatures au sein du trafic au niveau de la mémoire, des serveurs et des bases de données.

McAfee Application Control est une solution d'entreprise efficace qui protège les serveurs et les postes clients contre les applications non autorisées au moyen d'un modèle d'approbation dynamique, plutôt qu'à l'aide de listes extrêmement compliquées à gérer. Elle améliore la définition de listes de blocage, la reconnaissance de la réputation en temps réel et les approches basées sur l'analyse comportementale, aidant ainsi le personnel informatique à autoriser les logiciels légitimes, à bloquer les programmes nuisibles connus et à gérer comme il se doit les applications nouvelles et inconnues. Elle étend la couverture à Java, aux contrôles ActiveX, aux scripts, aux fichiers de commande et au code spécialisé, afin de vous offrir un contrôle accru sur les composants d'application et de bloquer les menaces évoluées sans exiger de mises à jour des signatures.

La solution McAfee Data Loss Prevention offre les niveaux de protection les plus élevés pour les données sensibles, tout en réduisant considérablement les coûts et la complexité de la sécurisation des informations stratégiques. Elle fait appel à des méthodes d'analyse uniques afin de vous permettre de conserver une longueur d'avance sur les menaces, d'illustrer les transferts de données et d'appréhender l'utilisation des données dans votre entreprise. Vous pouvez ainsi créer rapidement des stratégies efficaces de protection des données, sans risque de perturbation des activités de l'entreprise.

L'application de patchs virtuels assure une protection contre les vulnérabilités connues et les attaques par injection de code SQL sur les bases de données non corrigées. Toutes les commandes de base de données sont surveillées dans la mémoire, en vertu de règles prédéfinies. Si une règle est déclenchée, les attaques peuvent être bloquées en fermant la session ou en rejetant l'utilisateur ou l'adresse IP. En plus de fournir une piste d'audit fiable, la solution distribue régulièrement des patchs virtuels 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 le fournisseur de la base de données et que vous soyez prêt à l'appliquer. L'application de patchs virtuels constitue une fonction essentielle de McAfee Database Activity Monitoring (voir page suivante).

Pour renforcer encore la sécurité, il est recommandé de mettre en place des mesures de chiffrement ou l'utilisation de *tokens*, c'est-à-dire de chaînes de substitution aléatoires, en lieu et place de données sensibles, un processus appelé *tokenization*. Les paramètres de mise en œuvre de ces technologies dépendent de la prise de risque que l'entreprise considère comme acceptable. Vous pouvez opter pour un chiffrement au niveau des colonnes individuelles ou, si l'entreprise a besoin de mesures de sécurité strictes, choisir un chiffrement ou la *tokenization* pour l'ensemble de la base de données, ce qui peut nécessiter des modifications au niveau applicatif. McAfee recommande de choisir des produits prenant en charge les fonctions suivantes :

- Chiffrement au niveau des colonnes ne nécessitant pas de modification de l'application
- Gestion centralisée des clés
- Bases de données hétérogènes
- *Tokenization*
- Séparation des rôles

McAfee recommande Protegrity⁸, un partenaire McAfee Security Innovation Alliance spécialisé dans les logiciels de chiffrement des disques et des bases de données, les pare-feux applicatifs, les audits et rapports sur les événements de sécurité, ainsi que la *tokenization* et la sécurité des environnements dématérialisés.

Niveau 3 : surveillance et gestion de l'environnement de bases de données

Une sécurisation performante n'est véritablement possible que lorsque les opérations s'exécutent de manière efficace et que la protection des bases de données est intégrée de façon cohérente et transparente. En d'autres mots, les responsables informatiques doivent mettre en place les outils nécessaires pour identifier et protéger les actifs et disposer d'une vue complète de tous les recoins de l'entreprise, en temps quasi réel et à partir d'une plate-forme unique. Cette plate-forme logicielle doit permettre la gestion et la surveillance de tous les postes clients, réseaux et bases de données.

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.

La solution emploie des sondes non intrusives, agissant en mémoire vive, pour surveiller localement l'activité sur chaque serveur de base de données et identifier les comportements malveillants que le vecteur d'attaque soit le réseau, un utilisateur local avec privilèges ou une procédure stockée au sein de la base de données elle-même. Des fonctions de surveillance en temps réel et de prévention des intrusions bloquent les tentatives d'attaques avant tout dommage. 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 faciliter la correction. En cas d'infractions à la sécurité à haut risque, il est possible de fermer automatiquement la session et de mettre en quarantaine les utilisateurs malveillants.

McAfee ePolicy Orchestrator[®] (McAfee ePO[™]) est réputé pour être la plate-forme de gestion de la sécurité la plus avancée et évolutive du marché. Grâce à McAfee ePO, les entreprises de toutes tailles peuvent gérer efficacement un nombre illimité de périphériques, à partir d'une console web personnalisée. Cette dernière constitue une « vitrine » unique et interactive pour l'administration, l'analyse et la gestion des stratégies, des rapports et des alertes. Pierre angulaire de la plate-forme McAfee Security Management, McAfee ePO administre la protection de tous les postes clients, réseaux et données. Il intègre les solutions d'éditeurs tiers et automatise les workflows et les rapports axés sur les rôles pour accroître l'efficacité, optimiser la conformité et assurer une visibilité totale sur l'état de conformité et de protection de l'entreprise.

McAfee : le partenaire idéal en matière de sécurisation des bases de données

Les bases de données stratégiques constituent la force vitale de la plupart des entreprises. Leur stabilité et leurs performances sont depuis toujours une priorité majeure pour les départements informatiques. La sécurité constitue également une considération importante. Toutefois, à l'heure actuelle, ces bases de données sont des cibles de prédilection pour les cybercriminels. Cette évolution du paysage des menaces signifie que les défenses conventionnelles sont inadéquates face à la puissance intellectuelle déployée par les nouveaux génies du cybercrime.

Pour mieux sécuriser vos données d'entreprise critiques, McAfee propose une solution de sécurisation des bases de données complète, qui protège l'environnement de bases de données avec efficacité et pour un coût mesuré, tout en préservant une disponibilité et des performances optimales. Cette solution protège l'ensemble des bases de données principales ainsi que des serveurs, composants réseau et octets de données qui les touchent. Ses composants intégrés mettent en jeu la gamme de technologies et de services de sécurisation des informations la plus complète du marché, par ailleurs pleinement intégrée, en la combinant au système de collecte mondiale de renseignements sur les menaces de McAfee Labs[™]. Leur objectif commun : protéger au mieux vos données sensibles. Ils constituent en outre des composants essentiels du cadre McAfee Security Connected, qui permet d'optimiser la sécurité au quotidien, de favoriser la performance de l'entreprise tout en réduisant les risques, d'assurer la conformité et d'améliorer l'efficacité opérationnelle.

Pour plus d'informations, consultez notre site à la page www.mcafee.com/dbsecurity ou contactez votre revendeur ou représentant local McAfee.

A propos des produits McAfee de gestion des risques et de la conformité

Les produits McAfee de gestion des risques et de la conformité vous aident à réduire les risques, à automatiser la mise en conformité et à optimiser la sécurité. Nos solutions diagnostiquent l'état de votre environnement afin que vous disposiez d'informations pertinentes en temps réel sur vos vulnérabilités et stratégies et que vous puissiez protéger vos actifs les plus critiques en concentrant vos investissements de sécurité là où ils sont indispensables. Pour en savoir plus, visitez notre site à l'adresse www.mcafee.com/fr/products/risk-and-compliance/index.aspx.

A propos de McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC) est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. Elle propose dans le monde entier des solutions et des services proactifs et réputés, qui assurent la sécurisation des systèmes, des réseaux et des périphériques mobiles et qui permettent aux utilisateurs de se connecter à Internet, de surfer ou d'effectuer leurs achats en ligne en toute sécurité. Grâce au soutien de son système hors pair de renseignement sur les menaces, Global Threat Intelligence, McAfee crée des produits innovants au service des particuliers, des entreprises, du secteur public et des fournisseurs de services, pour les aider à se conformer aux réglementations, à protéger leurs données, à prévenir les perturbations dans le flux des activités, à identifier les vulnérabilités ainsi qu'à surveiller et à améliorer en continu leurs défenses. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable. www.mcafee.com/fr

