Projet technologique

PROTECTION DES BASES DE DONNÉES

Renforcement de la sécurité contre les attaques et les vecteurs de fuites actuels

ARCHITECTURE DE RÉFÉRENCE SECURITY CONNECTED

NIVEAU 1 2 **3** 4 5

McAfee Security Connected

Le cadre d'implémentation McAfee Security Connected permet l'intégration de plusieurs produits, services et partenariats dans le but d'assurer une réduction des risques efficace et centralisée. Fondée sur plus de vingt ans de pratiques éprouvées en matière de sécurité, l'approche Security Connected apporte une assistance précieuse à toutes les entreprises, indépendamment de leur taille, de leur secteur d'activités ou de leur situation géographique. Ainsi, elle permet d'améliorer l'état de sécurisation général, d'optimiser les systèmes de protection pour une meilleure rentabilité de l'investissement en sécurité et d'aligner les stratégies de sécurité sur les initiatives d'ordre commercial. L'architecture de référence McAfee Security Connected vous mène des idées jusqu'à l'implémentation. Faites-en bon usage et adaptez ses concepts aux risques, à l'infrastructure et aux objectifs spécifiques de votre entreprise. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable.

Renforcement de la sécurité contre les attaques et les vecteurs de fuites actuels

Les faits

En 2010, le nombre de divulgations de données a atteint un niveau record et 47 % des attaques n'ont mis que quelques minutes ou quelques heures pour passer du point d'entrée à la compromission des données. 44 % ont pu réaliser leur objectif en quelques jours, d'après le rapport d'enquête sur les divulgations de données rédigé par les services de renseignement américains et Verizon en 2011. Le constat est simple : il faut très peu de temps aux cybercriminels pour s'introduire dans les systèmes, alors que, côté défense, la réaction est lente. Il a fallu des semaines (dans 38 % des cas) ou des mois (36 %) pour découvrir la compromission[1], ce qui laisse largement le temps aux criminels de s'emparer de leur butin et de s'évanouir dans la nature.

Les cybercriminels opèrent en quelques minutes ou jours, tandis que du côté des responsables de la sécurité, ce délai se compte en semaines, voire en mois. Comment expliquer une telle rapidité ? Par un simple changement de tactique. Le piratage (50 %) et les logiciels malveillants (49 %) sont les nouvelles tactiques de prédilection des cybercriminels. Toujours selon le rapport, ces derniers s'en prennent à des cibles plus vulnérables, à savoir des organisations de plus petite taille avec des systèmes moins bien protégés, plutôt qu'à des serveurs gigantesques contenant des millions d'enregistrements.

Il n'est pas rare non plus que les auteurs d'attaques bénéficient de l'aide involontaire des employés. Grâce à des manœuvres d'ingénierie sociale ou au vol d'informations d'identification, ces cybercriminels trouvent facilement le moyen de se faire passer pour des utilisateurs « internes » dotés de droits d'accès légitimes. Compte tenu de la valeur des actifs conservés dans les bases de données et de la conjoncture économique difficile, il est logique que la corruption gagne du terrain. Toujours selon le même rapport, la sollicitation et la corruption ont été les deux tactiques d'ingénierie sociale les plus utilisées l'année dernière. Au bout du compte, vous ne pouvez ni faire confiance au système de défense de votre périmètre pour protéger votre base de données ni compter sur vos employés pour toujours agir de façon appropriée.

Les problèmes

Les bases de données ne servent pas uniquement à stocker des informations critiques ; elles sont souvent reliées à de multiples systèmes chargés de fournir des services métier essentiels. Toute interruption, divulgation accidentelle ou fuite de données peut perturber le fonctionnement de l'entreprise toute entière et porter préjudice à sa réputation. Sans compter que les bases de données contiennent généralement des données sensibles et réglementées. Par conséquent, leur compromission constitue généralement une infraction majeure à la conformité réglementaire, avec les coûts de nettoyage élevés, la perte de confiance des clients, voire la baisse importante de la capitalisation boursière que cela suppose.

Pour protéger les données sensibles contre les menaces internes et externes, les entreprises ont besoin d'une visibilité en temps réel sur les activités liées à la base de données. La plupart des organisations ont aujourd'hui recours à des outils de journalisation et d'audit intégrés à la base de données pour assurer cette protection, mais ces derniers sont malheureusement inefficaces contre les tactiques de piratage et d'ingénierie sociale actuelles. Pour protéger correctement une base de données contre le code malveillant et les fuites de données, vous devez résoudre les problèmes suivants :

- **Surveillance des activités et des modifications**. Toutes les bases de données répondent à des commandes. Pour autant que l'utilisateur à l'origine de la demande de données soit autorisé à utiliser la commande, il obtiendra ce qu'il veut. La sophistication croissante des attaques et des outils permet aux cybercriminels d'échapper aux techniques de détection classiques et d'élever leurs privilèges. Des contrôles d'accès insuffisants simplifient la tâche des pirates. En général, les droits d'accès accordés aux utilisateurs sont très supérieurs à ceux dont ils ont besoin pour utiliser le système ou s'acquitter de leurs tâches. Les comptes expirés et le contrôle trop laxiste de la création de nouveaux comptes ouvrent de nombreuses portes aux cybercriminels, qui ciblent d'abord les mots de passe faibles ou par défaut, puis élèvent leurs privilèges. Le suivi des activités réseau s'est avéré inapproprié face à ce problème dans la mesure où les méthodes d'accès local peuvent contourner les systèmes de surveillance du réseau.

- **Outils d'audit**. Les fonctions de journalisation et d'audit natives des bases de données n'offrent pas une visibilité suffisante, loin s'en faut. La plupart ne capturent pas les modifications effectuées, les privilèges utilisés, les administrateurs concernés ou les changements introduits au niveau du système. En outre, les activités de journalisation et d'audit intégrées à la base de données peuvent dégrader les performances de celle-ci. Conçues à des fins de surveillance et non de sécurisation, ces fonctions peuvent en outre être désactivées par les administrateurs, ce qui leur ôte leur utilité première.
- **Elimination des interruptions liées à l'application de patchs**. Les revenus, le temps de fonctionnement et la disponibilité priment sur la sécurité. Certaines organisations ont un cycle d'application de patchs supérieur à 12 mois. Des centaines de nouvelles menaces voient chaque année le jour, mais en raison de la nature critique des bases de données, tout arrêt de celles-ci est exclu. Les entreprises veulent être protégées en permanence mais sans appliquer de patchs à la base de données.
- **Transition vers le Cloud**. Face à l'adoption progressive du Cloud par les organisations, il devient impératif d'adapter la base de données afin qu'elle soit accessible et puisse être surveillée par l'intermédiaire de services dématérialisés et pas uniquement via le réseau local.
- **Démonstration de la conformité aux normes internes, gouvernementales et sectorielles**. Selon le rôle de votre base de données, il se peut que vous deviez vous conformer à une série de réglementations (PCI DSS, Sarbanes-Oxley, HIPAA, SAS 70, GLBA et FERPA, par exemple), ce qui exige de gérer des stratégies et de générer des rapports démontrant votre conformité. Et si vous entretenez des relations commerciales avec d'autres pays, vous serez généralement tenu de respecter les obligations de contrôle financier et de confidentialité en vigueur dans ces nations. Enfin, si votre entreprise a développé ses propres pratiques et normes d'exploitation, il se peut que la direction veuille avoir accès à des tableaux de bord reflétant l'état de conformité aux normes de gouvernance.

Description de la solution

Les opérations de toutes les organisations reposent sur des bases de données. Nous ne confions pas aux éditeurs de systèmes d'exploitation le soin de protéger leurs systèmes. Alors pourquoi nous contentons-nous des outils fournis par les fournisseurs de bases de données pour sécuriser les ressources les plus précieuses contenues dedans ? Les bases de données présentent des défis uniques et leur protection est généralement confiée à des administrateurs chargés de mettre en œuvre des normes et des stratégies de sécurité. Face au nombre de violations de bases de données relayées par les médias, il faut envisager une nouvelle approche pour garantir la protection de l'intégrité des bases de données contre le code malveillant et, même si c'est regrettable, contre notre propre personnel.

Pour résoudre ces problèmes, la solution choisie doit satisfaire les exigences suivantes :

- **Surveillance des activités et des modifications**. La solution doit être en mesure de surveiller toutes les activités et le comportement de la base de données depuis un poste d'observation extérieur à la base de données. Si cette surveillance était effectuée exclusivement par une fonction intégrée à la base de données, les administrateurs pourraient la désactiver (de façon délibérée ou non). La solution doit pouvoir interrompre une session non conforme à une stratégie, envoyer des alertes à une console de gestion centralisée et mettre en quarantaine un utilisateur non conforme ou malveillant. Elle doit également être en mesure de détecter et de neutraliser les techniques de dissimulation.

- **Outils d'audit**. A l'instar de la fonction de surveillance, les outils d'audit sont inefficaces s'ils peuvent être désactivés par un administrateur. La solution doit fournir des fonctions de journalisation et d'audit protégées extérieures à la base de données afin de garantir la capture des enregistrements à des fins d'analyse. Lors de l'analyse post-mortem réalisée après un incident, cette piste d'audit peut vous aider à déterminer la quantité de données perdues et à vous faire une idée plus précise de l'activité malveillante. La solution doit fournir une piste et des rapports d'audit répondant aux critères SOX et PCI, ainsi qu'à d'autres exigences en matière d'audit de la conformité.

- **Elimination des interruptions liées à l'application de patchs**. La solution doit être capable de détecter les attaques qui tentent d'exploiter les vulnérabilités connues ainsi que les vecteurs de menaces habituels. Elle doit être configurée pour générer une alerte ou interrompre la session en temps réel. Si vous attendez que le fournisseur de bases de données vous fournisse des patchs ou si vous négligez de les appliquer pour éviter toute perte de productivité, vous exposez vos bases de données à de nombreux vecteurs de menaces. Les patchs virtuels peuvent vous aider à vous protéger contre les vulnérabilités « jour zéro » et récemment découvertes et 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 et puisse être appliqué.

Facteurs décisionnels

Les facteurs ci-dessous sont susceptibles d'influencer votre architecture :

- Quelles obligations réglementaires votre organisation est-elle tenue de respecter ?
- Quelles sont les procédures en place pour évaluer la conformité réglementaire de votre base de données et générer des rapports de conformité ?
- Possédez-vous des bases de données exécutées sur des systèmes d'exploitation 64 bits ? Lesquelles ?
- Connaissez-vous le niveau de sécurité de votre base de données ?
- A quelle fréquence appliquez-vous des patchs à vos bases de données ?

- **Transition vers le Cloud**. Une solution se fondant sur l'analyse du trafic réseau pour identifier les infractions aux stratégies est inefficace, voire impossible à appliquer, dans les architectures distribuées et hautement dynamiques utilisées pour la virtualisation des centres de données et l'informatique dématérialisée. Il doit être possible de configurer la solution afin qu'elle soit automatiquement mise en service chaque fois qu'une nouvelle base de données vient s'ajouter au réseau, qu'elle demande la stratégie de sécurité applicable en fonction des données hébergées, puis qu'elle commence à envoyer des alertes au serveur de gestion. Même si la connexion au réseau est interrompue, les données doivent rester protégées par des stratégies mises en œuvre au niveau local.
- **Conformité aux normes internes, gouvernementales et sectorielles**. Toute modification des normes et des réglementations entraîne inévitablement celle des rapports à soumettre. La solution doit fournir des modèles réglementaires et de conformité gérés conformément aux contrôles et directives en matière d'infraction les plus récents. Elle doit pouvoir identifier les menaces au moment où elles apparaissent et générer des rapports sur la prévention, de manière à réduire les risques et la responsabilité légale. Elle doit comprendre des modèles PCI-DSS, Sarbanes-Oxley, HIPAA et SAS 70 préconfigurés, tous accessibles depuis une plate-forme gérée de façon centralisée.

Technologies utilisées par la solution McAfee

McAfee propose deux produits spécialement conçus pour la protection des bases de données : McAfee® Vulnerability Manager for Databases et McAfee Database Activity Monitoring. La gestion centralisée assurée par McAfee ePolicy Orchestrator® (McAfee ePO™) permet de combiner ces deux produits au sein d'une plate-forme unifiée de gestion de la conformité et de la sécurité pour l'ensemble de votre infrastructure.

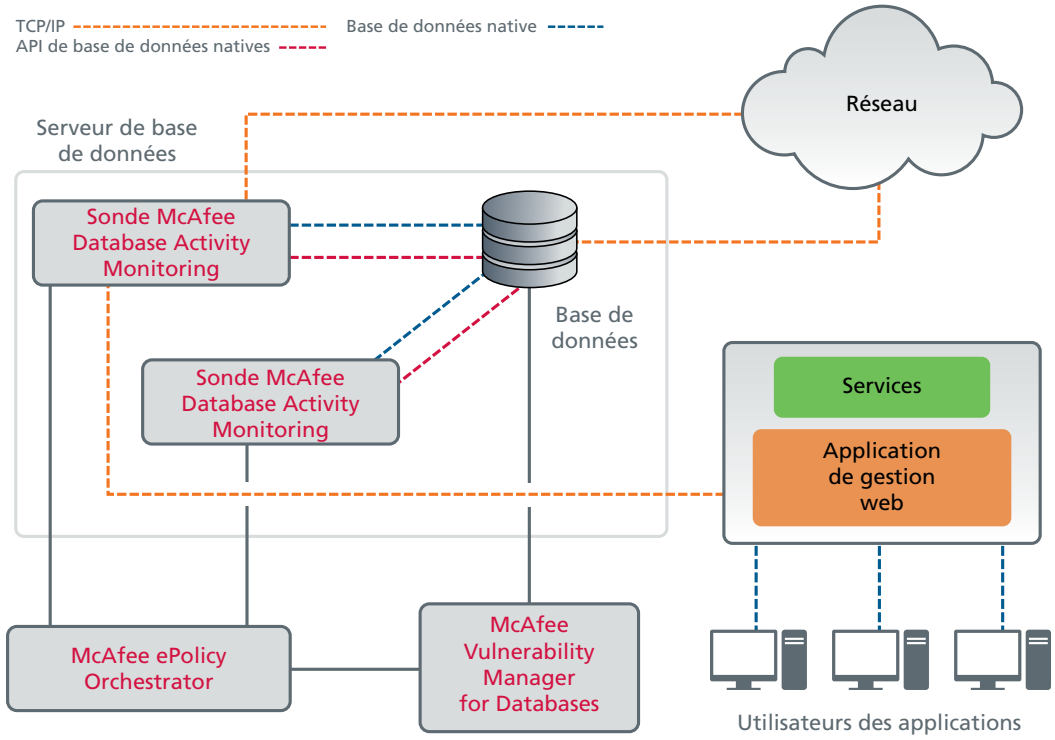
McAfee Vulnerability Manager for Databases effectue plus de 3 000 contrôles de vulnérabilités sur les principaux systèmes de base de données, dont Microsoft SQL Server, IBM DB2 et MySQL. En améliorant la visibilité sur les vulnérabilités des bases de données et en fournissant des recommandations de correction élaborées par des experts, McAfee Vulnerability Manager for Databases réduit le risque de divulgation préjudiciable et permet de réaliser des économies grâce à une meilleure préparation des audits et au respect des obligations réglementaires. McAfee Vulnerability Manager for Databases permet également de réduire la surface d'attaque en identifiant les vulnérabilités types ciblées par les pirates et les attaques, notamment les mots de passe faibles ou partagés et les comptes par défaut. Pour vous aider à repérer les événements suspects et à y répondre par des mesures appropriées, il génère des rapports sur la version, le niveau de patch, les objets et les privilèges modifiés, ainsi que les traces analysables laissées par les outils de piratage courants.

Contrairement à un audit et à une analyse des journaux élémentaires, qui ne vous informent des faits qu'a posteriori, McAfee Database Activity Monitoring offre une visibilité en temps réel ainsi que des fonctions de prévention qui bloquent les infractions avant que celles-ci ne provoquent des dégâts. Plus de 380 règles prédéfinies permettent de résoudre des problèmes spécifiques corrigés au moyen de patchs publiés par les fournisseurs de bases de données, ainsi que de nombreux profils d'attaque génériques. Les modèles de stratégie prédéfinis peuvent être personnalisés pour prendre en charge des règles définissant les processus et les types d'accès à la base de données conformes et appropriés.

Par ailleurs, des alertes sont directement envoyées au tableau de bord de surveillance, avec des détails complets concernant toute infraction aux stratégies, 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, pour donner le temps à l'équipe de sécurité d'enquêter sur l'intrusion.

Les attaques ciblant les données précieuses stockées dans les 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 surveiller les activités et intercepter ces trois types de menaces au moyen d'une solution unique non intrusive. Des patchs virtuels sont par ailleurs régulièrement distribués afin de couvrir les nouvelles vulnérabilités découvertes et 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 puisse être appliqué. Les informations sur les activités et les événements peuvent également servir à démontrer la conformité à des fins d'audit et à améliorer la sécurité globale.



Des systèmes de protection spécialisés permettent à McAfee d'évaluer les vulnérabilités des bases de données et de surveiller les actions malveillantes et dangereuses.

McAfee Vulnerability Manager for Databases

Conçu pour accélérer les analyses initiales et fort de modèles de rapport prêts à l'emploi répondant à la plupart des exigences en matière de conformité, McAfee Vulnerability Manager for Databases est à même de découvrir et d'analyser plusieurs bases de données à partir d'une seule console. Il localise et identifie les tables contenant des informations sensibles et effectue une analyse rapide des ports précisant la version de la base de données et l'état d'application des patchs. Outre la détection de base des mots de passe faibles (mots de passe simples, partagés et par défaut), il peut analyser les mots de passe hachés enregistrés, par exemple, au format SHA-1, MD5 ou DES. Il teste également 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. Il présente ensuite ses conclusions dans des rapports préconfigurés pour diverses normes de conformité courantes.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring est une sonde de petite taille et plus précisément un agent logiciel installé sur le serveur hôte de la base de données et chargé de surveiller toutes les activités. La sonde est un processus autonome écrit en C++ et exécuté sur l'ordinateur hôte de la base de données. Elle est installée à l'aide des outils standard de la plate-forme (RPM, PKG, DEPOT, BFF ou EXE) dans un compte d'utilisateur distinct du système d'exploitation. La sonde identifie automatiquement toutes les instances de base de données sur le serveur et peut en surveiller plusieurs, même de types différents, sur le même hôte.

Lors de son exécution, la sonde se fixe à la zone de mémoire de l'instance dans le cache SQL, à l'aide de mécanismes en lecture seule et d'interfaces de programmation d'application (API), puis démarre la surveillance au moyen d'une boucle d'interrogation d'un échantillonnage de la mémoire. Lors de chaque cycle d'échantillonnage, la sonde analyse les instructions antérieures et en cours d'exécution pour chaque session de l'instance de base de données et, à l'aide d'une stratégie prédéfinie envoyée par le serveur, détermine les instructions à bloquer ou pour lesquelles elle doit générer une alerte. Les instructions contraires à la stratégie sont envoyées en temps réel à la console de gestion sous la forme d'alertes. La sonde peut également être configurée pour interrompre les sessions en cas d'infractions spécifiques ou pour mettre des utilisateurs en quarantaine. Non intrusive, elle utilise très peu de ressources du processeur (moins de 5 % d'un processeur monocœur, même sur les ordinateurs multiprocesseurs). Les fonctionnalités de prévention de la sonde sont mises en œuvre à l'aide d'API de base de données natives qui lui permettent d'interrompre des sessions de base de données sans jamais mettre en péril l'intégrité des données.

McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO permet de gérer des stratégies et de distribuer des logiciels de façon automatique et centralisée. McAfee Vulnerability Manager for Databases est intégré au tableau de bord de McAfee ePO afin de fournir des rapports centralisés et des informations récapitulatives sur toutes vos bases de données. McAfee ePO travaille également en tandem avec McAfee Database Activity Monitoring afin d'offrir une visibilité complète et unique sur l'ensemble des systèmes et de générer des rapports optimisés.

Impact de la solution

En ajoutant un système de protection spécialisé contre les attaques ciblant les bases de données et les vecteurs de fuites de données, vous pouvez améliorer votre capacité à détecter et à neutraliser les attaques externes, mais aussi diminuer le risque de compromission ou d'interruption au sein du réseau.

McAfee offre une visibilité en temps réel sur toutes les sources d'attaques et vous en protège grâce à des fonctions de surveillance et de génération d'alertes en cas d'événements suspects. Que la menace émane du réseau, d'utilisateurs locaux connectés au serveur ou de la base de données elle-même, McAfee vous aide à réduire les risques et à limiter votre responsabilité légale en bloquant les attaques avant qu'elles provoquent des dégâts. L'application de patchs virtuels aux nouvelles vulnérabilités de base de données découvertes vous offre en outre une protection immédiate, sans temps d'arrêt de la base de données.

Des modèles et règles prédéfinis, des vérifications mises à jour et automatisées ainsi que des interfaces basées sur des Assistants permettent d'accélérer le déploiement et vous aident à mettre en place une architecture de sécurité des bases de données efficace et facile à contrôler en cas d'audit.

Ressources supplémentaires

www.mcafee.com/fr/solutions/database-security/database-security.aspx
www.mcafee.com/fr/products/vulnerability-manager-databases.aspx
www.mcafee.com/fr/products/database-activity-monitoring.aspx
www.mcafee.com/fr/products/epolicy-orchestrator.aspx

Pour en savoir plus sur l'architecture de référence McAfee Security Connected, consultez le site www.mcafee.com/fr/enterprise/reference-architecture/index.aspx.

L'auteur

Uy Huynh est Directeur de l'ingénierie commerciale de McAfee. A ce titre, il supervise une équipe chargée de fournir aux clients les solutions de sécurité et les modèles de conception appropriés ainsi que les meilleures pratiques afin de les aider à améliorer leur niveau de sécurité et à protéger leurs actifs numériques les plus précieux. Uy Huynh est un expert en sécurité qui a travaillé avec d'importants clients du classement Fortune 100 tels que HP, Oracle, ATT, McKesson et d'autres afin de les aider à sélectionner les produits de sécurité les mieux adaptés à leurs besoins complexes.

Avant de rejoindre McAfee, il a créé et dirigé le service d'ingénierie commerciale de Foundstone. Il a contribué à l'élaboration des meilleures pratiques en matière de gestion des vulnérabilités et des risques pour des réseaux et des systèmes de grande taille. Avant cela, il était consultant pour ISS, où il a participé au déploiement d'un large éventail de solutions, stratégies et technologies de sécurité au sein de grandes entreprises.

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

Les renseignements contenus dans le présent document ne sont fournis qu'à titre informatif, au bénéfice des clients de McAfee. Les informations présentées ici peuvent faire l'objet de modifications sans préavis et sont fournies sans garantie ni représentation quant à leur exactitude ou à leur adéquation à une situation ou à des circonstances spécifiques.

McAfee, McAfee Database Activity Monitoring, McAfee ePolicy Orchestrator, McAfee ePO, McAfee Vulnerability Manager for Databases et le logo McAfee sont des marques commerciales déposées ou des marques commerciales de McAfee, Inc. et/ou de ses sociétés affiliées aux Etats-Unis et/ou dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs. Les plans de développement des produits, les spécifications et les descriptions sont fournis à titre indicatif uniquement. Ils sont susceptibles d'être modifiés sans préavis et sont fournis sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Copyright © 2012 McAfee, Inc.
38600bp_protecting-databases-L3_1111