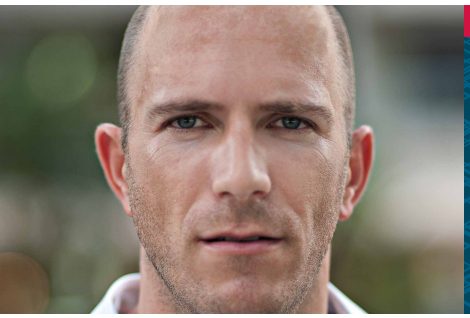

Cinq raisons de déployer une solution de sécurisation des bases de données dédiée

Une dernière ligne de défense critique

Avantages de McAfee Vulnerability Manager

- Visibilité complète sur l'état de protection des bases de données
- Analyse de nombreuses bases de données de l'entreprise au départ d'une console unique
- Délais de mise en conformité écourtés et réduction des cycles d'audit avec, pour résultat, des économies de coûts substantielles
- Déploiement rapide qui n'exige pas de connaissances approfondies des systèmes de base de données
- Génération rapide de rapports personnalisés dans un format compréhensible pour divers rôles d'utilisateurs

Avantages de McAfee Database Activity Monitoring

- 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 provoquent des dégâts
- Gain de temps et d'argent grâce à un déploiement plus rapide et à une architecture plus efficace
- Déploiement aisé sur l'infrastructure informatique de votre choix

La protection des informations précieuses et confidentielles hébergées dans les bases de données est indispensable pour protéger l'intégrité et la réputation des entreprises et assurer leur conformité réglementaire. Toutefois, bon nombre de sociétés comptent toujours sur des solutions de sécurité inefficaces ou lacunaires. Face à la complexité des plates-formes de base de données actuelles et au vu de la sophistication des cybercriminels modernes, il est impératif de déployer une solution de sécurisation des bases de données dédiée et complète. En voici les cinq raisons principales.

1. Vous ne pouvez pas protéger une ressource si vous ignorez son existence.

Même dans les environnements informatiques d'entreprise bien organisés, il n'est pas rare d'avoir des centaines ou des milliers d'instances de base de données contenant des informations très sensibles. Et les équipes informatiques seraient bien en peine de donner le nombre exact de bases de données ainsi que leur emplacement, la sensibilité des données et le niveau de protection de celles-ci. Malheureusement, les cybercriminels en sont parfaitement conscients et s'efforcent constamment de trouver des failles. Ils disposent du temps et des ressources techniques nécessaires pour exploiter des bases de données que vous pensiez protégées ou dont vous ignoriez l'existence. Ils profitent pleinement de votre manque de visibilité.

Pour jouir d'une visibilité complète sur votre environnement de bases de données, vous devez posséder les outils nécessaires pour détecter toutes les bases existantes et les analyser afin d'identifier celles contenant des données sensibles telles que des informations de cartes de paiement, des dossiers du personnel, des chiffres de vente etc. En outre, il est essentiel de pouvoir effectuer des tests de vulnérabilités approfondis et automatisés pour déterminer la nature exacte des risques. Seule une solution de sécurisation de bases de données dédiée peut vous offrir les informations détaillées et pertinentes vous permettant de hiérarchiser et de corriger des failles de sécurité tout en évitant à votre entreprise de faire appel aux coûteux services d'un consultant externe.

McAfee® Vulnerability Manager for Databases découvre automatiquement les bases de données présentes sur votre réseau, détermine si les derniers patchs disponibles ont été appliqués et recherche les vulnérabilités potentielles. En fait, cette solution effectue plus de 4 200 contrôles de vulnérabilités sur les principaux systèmes de base de données et classe les menaces selon différents niveaux de priorité, en proposant des scripts de correction ainsi que des recommandations. Elle nécessite peu de connaissances en systèmes de base de données, génère des rapports personnalisés dans des formats compréhensibles pour différents rôles d'utilisateurs, le tout à partir d'une console de sécurité centralisée.

2. La sécurisation du périmètre ne vous protège pas contre les menaces internes.

Vous avez consacré beaucoup de temps, d'argent et d'efforts à sélectionner et à déployer des pare-feux et d'autres technologies de sécurisation des réseaux. Malheureusement, comme vous le savez, les compromissions de bases de données ne sont pas toutes imputables à des menaces externes au périmètre du réseau. De fait, les recherches annuelles menées par le CERT (Computer Emergency Response Team) révèlent que près de la moitié de ces compromissions sont le fait d'utilisateurs internes. Par conséquent, vous devez protéger vos données stratégiques contre des ennemis encore plus insidieux : des utilisateurs internes avec privilèges dont la plupart ont les moyens de contourner les fonctions de sécurité natives des systèmes de gestion des bases de données, de modifier les journaux d'accès et d'effacer toute trace de leurs activités.

La solution de sécurisation des bases de données idéale détecte et bloque les menaces, quel qu'en soit le vecteur : menaces externes et surtout internes. En outre, elle propose un cadre destiné à simplifier la configuration et la mise en œuvre des stratégies d'accès à la base de données conformément à des exigences de conformité spécifiques afin de garantir en permanence un véritable cloisonnement des responsabilités et des tâches.

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. Vous bénéficiez d'une meilleure visibilité sur toutes les activités liées aux bases de données, et notamment les accès locaux privilégiés et les attaques sophistiquées émanant de la base de données. McAfee Database Activity Monitoring protège vos données contre toutes les menaces en surveillant l'activité en local sur chaque serveur de base de données, indépendamment de son emplacement, et en envoyant des alertes ou en fermant automatiquement les sessions suspectes ou contraires à la stratégie de sécurité. La solution sécurise même vos bases de données et met en œuvre vos stratégies dans des environnements virtualisés ou dématérialisés (cloud).

3. Il faut moins de temps pour lancer une attaque que pour appliquer des correctifs.

Le deuxième mardi du mois est jour de fête pour les pirates. C'est le jour où les éditeurs de bases de données publient leurs correctifs et révèlent donc les cibles les plus intéressantes à exploiter. Les criminels bénéficient en outre d'une longueur d'avance car ils sont conscients de la difficulté que présentent, pour les équipes de gestion des bases de données, la mise hors ligne des bases puis l'application et le test des correctifs. Ils comptent sur le fait que la procédure sera considérée comme une telle source de perturbation pour les activités de l'entreprise qu'elle sera retardée le plus longtemps possible, ce qui leur donne ainsi tout le temps de trouver et d'exploiter les failles.

Il n'y a aucun moyen d'éviter cette procédure de correction ni les possibilités d'exploitation qu'elle offre aux criminels, à moins de posséder une solution de sécurisation des bases de données dédiée. Cette dernière doit en outre vous permettre de mettre à jour le niveau de protection de vos bases de données en temps réel, sans compliquer la tâche de votre personnel ni interrompre vos activités.

McAfee Virtual Patching for Databases protège les bases de données contre les risques liés aux vulnérabilités non corrigées par un patch : il détecte et prévient les tentatives d'attaques et d'intrusions en temps réel, sans exiger la mise hors ligne de la base de données ou des tests sur les applications. Il vous donne l'assurance d'être protégé contre les menaces même dans les périodes d'extrême vulnérabilité, à savoir entre le moment où l'éditeur publie les mises à jour correctives et celui de leur installation.

McAfee Database Activity Monitoring est une autre solution non intrusive, qui ne nécessite aucune interruption et offre un niveau de protection supplémentaire le mardi de la publication des correctifs et les jours suivants. Ses sondes basées sur la mémoire interceptent les attaques visant les bases de données, qu'elles proviennent 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.

4. Vous ne pouvez pas continuer à sacrifier votre conformité au profit de la continuité.

Les impératifs de conformité réglementaires applicables à différents secteurs, tels que les soins de santé, la vente au détail et la finance ne cessent d'évoluer et deviennent de plus en plus stricts. Assez logiquement, les bases de données stratégiques sont directement concernées par les dispositions en matière de conformité, qui exigent la mise à jour de ces bases avec les derniers correctifs fournis par les éditeurs. Toutefois, compte tenu de la lourdeur du cycle complet de correction (mise hors ligne de la base, application du patch et tests des diverses bases de données de types différents), la plupart des entreprises privilégient la continuité de leurs activités au détriment de la conformité. Sans compter que certaines possèdent encore des versions anciennes des bases de données pour lesquelles les éditeurs ne fournissent même plus de correctifs.

Avec McAfee Virtual Patching for Databases, vous pouvez assurer la continuité de vos activités sans mettre en péril votre conformité réglementaire. Il vous permet d'appliquer les correctifs à votre propre rythme, en sachant que vos bases de données sont protégées et conformes. McAfee Virtual Patching for Databases vous fait gagner un temps considérable et constitue un contrôle compensatoire tout à fait valable aux yeux des auditeurs de conformité. En outre, il peut même étendre la protection la plus récente aux anciennes bases de données dont les éditeurs ont décidé d'abandonner le support.

Avantages de McAfee Virtual Patching

- Protection contre les menaces avant même l'installation des patchs d'éditeurs
- Aucune connaissance spécifique des systèmes de gestion des bases de données nécessaire pour le personnel informatique et de la sécurité
- Fonctionnement ininterrompu des bases de données de production grâce à une conception non intrusive du logiciel
- Protection transparente des bases de données avec distribution automatique et continue des mises à jour
- Respect plus facile des normes (PCI DSS, HIPAA, etc.) et autres réglementations en vigueur

Avantages de McAfee ePolicy Orchestrator

- Visibilité de bout en bout sur la sécurité et la conformité des bases de données à partir d'une console de gestion centralisée
- Console unique qui vous permet d'intégrer les bases de données au sein d'un programme de gestion de la sécurité unifié sur site, dans des succursales distantes et même dans le cloud
- Architecture ouverte et extensible qui connecte les solutions de sécurité de McAfee et d'autres éditeurs à vos outils de gestion des configurations, des opérations informatiques et LDAP, en toute simplicité

5. Lorsque les données sont hébergées dans le cloud, la visibilité est extrêmement limitée.

L'informatique dématérialisée (cloud computing) présente des avantages considérables d'un point de vue opérationnel et financier, mais aussi un inconvénient majeur : votre personnel peut perdre le contrôle des données sensibles et n'avoir pratiquement aucune visibilité sur les utilisateurs qui y accèdent. Toutefois, en mettant en place une solution de sécurisation des bases de données efficace, vous pouvez protéger vos données tant dans les environnements physiques que virtuels. Une solution adéquate peut bloquer les activités de base de données non autorisées et les signaler à la console de gestion, même si la base de données est virtualisée et dématérialisée.

Grâce à une implémentation unique de sondes basées sur la mémoire, McAfee Database Activity Monitoring peut être configuré pour être automatiquement mis en service sur chaque nouvelle machine virtuelle. En même temps, il peut demander les stratégies de sécurité applicables en fonction des données hébergées, puis commencer à envoyer des alertes au serveur de gestion. En outre, ses sondes peuvent fonctionner de façon autonome, même lorsqu'elles sont déconnectées du serveur. Ainsi, les données sensibles sont protégées et préservées en permanence, que la base de données soit connectée ou non et quel que soit son emplacement. 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.

Enfin, l'accès aux bases de données dématérialisées peut être surveillé via McAfee® ePolicy Orchestrator® (McAfee ePO™), une console de gestion de la sécurité d'entreprise qui vous permet de disposer d'une visibilité complète sur la conformité et la sécurité des bases de données et de l'entreprise.

En d'autres termes, qu'elles soient hébergées sur site ou dans le cloud, votre personnel et vous-même bénéficiez du plus haut niveau de visibilité sur vos bases de données. A l'évidence, McAfee offre la solution de sécurisation des bases de données la mieux adaptée à votre environnement informatique, même si vous possédez des sites d'exploitation très éloignés les uns des autres, ou des données extrêmement sensibles.

Découvrez comment garantir la sécurité et la disponibilité de vos bases de données

McAfee n'ignore pas que les bases de données abritent les ressources les plus critiques des entreprises. Leur disponibilité est indispensable au bon déroulement des activités de l'entreprise. Tout comme vos bases de données fonctionnent sans interruption, nous sommes constamment à pied d'œuvre pour les protéger. Les menaces informatiques ne connaissent pas de répit. De même, notre équipe d'experts en sécurité des bases de données met tout en œuvre pour protéger et garantir la disponibilité de vos informations sensibles et aider votre entreprise à respecter les stratégies internes et les réglementations sectorielles.

Pour découvrir comment la gamme de solutions de sécurisation des bases de données McAfee peut vous aider à protéger vos bases de données stratégiques, visitez notre site à l'adresse http://www.mcafee.com/fr/products/database-security/index.aspx ou contactez votre revendeur ou représentant McAfee local.

Suivez-nous sur Twitter : @McAfee_DBSecure.

A propos de la protection des postes clients McAfee

McAfee, filiale à part entière d'Intel Corporation (NASDAQ : INTC), est la plus grande entreprise au monde entièrement dédiée à la sécurité informatique. Les solutions de protection des postes clients McAfee de nouvelle génération 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. Elles conjuguent parfaitement l'analyse antimalware intelligente classique, les listes d'autorisation d'applications dynamiques, la prévention des intrusions « jour zéro » basée sur les comportements, la gestion unifiée et un système de renseignements sur les menaces intégré. Pour en savoir plus, consultez notre site à l'adresse www.mcafee.com/fr/products/endpoint-protection/index.aspx.

Avantages des solutions de sécurisation des bases de données McAfee

- Déploiement et gestion aisés
- Visibilité complète sur l'état de protection des bases de données
- Harmonisation des procédures d'administration des stratégies de sécurité au sein des équipes chargées de la sécurité et de la gestion des bases de données
- Gestion efficace et démonstration de la conformité réglementaire
- Limitation des risques et de la responsabilité grâce au blocage des attaques avant qu'elles provoquent des dégâts
- Gestion de la sécurité des bases de données à partir d'une console centralisée

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

41903brf_top5-db-sec_0212_fnl_ASD