McAfee Application Data Monitor

Détection des menaces cachées grâce à l'inspection de la couche Application

Avec l'appliance McAfee® Application Data Monitor, la sécurité et la conformité vont au-delà de la simple gestion des journaux grâce à une surveillance réalisée à tous les niveaux, jusqu'à la couche Application. Vous pouvez inspecter le contenu des applications en profondeur pour bénéficier d'une visibilité sans précédent sur l'utilisation de votre réseau.

L'appliance McAfee Application Data Monitor décode toute une session applicative jusqu'à la couche 7 et fournit une analyse complète de tous les éléments, de l'intégrité de la session et des protocoles sous-jacents au contenu de l'application (par exemple le texte d'un e-mail ou ses pièces jointes). Un tel niveau de détail permet d'effectuer une analyse précise de l'utilisation de l'application tout en permettant de mettre en œuvre des stratégies d'utilisation et de détecter le trafic clandestin ou malveillant.

Cette inspection approfondie favorise la conformité puisque l'appliance effectue un suivi de toutes les utilisations des données sensibles sur le réseau. Lorsque l'appliance McAfee Application Data Monitor détecte une violation, elle conserve tous les détails de cette session applicative afin de pouvoir les utiliser dans les réponses aux incidents, les investigations numériques ou les audits de conformité.

Parallèlement, l'appliance offre une visibilité sur les menaces susceptibles de prendre l'apparence d'applications légitimes :

- Menaces évoluées au niveau de la couche Application
- Utilisation non autorisée ou vol d'informations confidentielles
- Attaques visant les « angles morts » de la sécurité
- Utilisation de code plus ancien à risque
- Vol ou utilisation abusive des informations d'identification des utilisateurs
- Transmission de données sensibles par l'intermédiaire d'une application quelconque
- Failles au niveau des processus d'entreprise

Principaux avantages

- Décodage de toute la session applicative, jusqu'à la couche 7, pour des centaines d'applications
- Règles de détection prédéfinies pour les données sensibles et réglementées
- Prise en charge de dictionnaires définis par l'utilisateur et de règles personnalisables
- Génération d'une piste d'audit complète des événements applicatifs à des fins de conformité
- Mode de fonctionnement passif pour éviter toute interférence avec les applications
- Intégration avec McAfee Enterprise Security Manager pour assurer la corrélation des données des applications avec les événements et d'autres flux de données
- Options de déploiement hybrides et flexibles comprenant des appliances physiques et virtuelles

Fuites de données et violations de conformité

L'appliance McAfee Application Data Monitor peut détecter la transmission de données sensibles au sein des pièces jointes aux e-mails, des messages instantanés, des transferts de fichiers, des messages HTTP ou de toute autre application, et vous en informe immédiatement afin de limiter les fuites.

Vous pouvez identifier les informations sensibles, notamment les numéros de carte de crédit et de sécurité sociale dès la première utilisation ou personnaliser les fonctionnalités de détection de l'appliance McAfee Application Data Monitor en définissant vos propres dictionnaires d'informations sensibles et confidentielles. L'appliance détecte ces types de données sensibles, avertit le personnel concerné et enregistre l'infraction afin de conserver une piste d'audit.

Découverte de documents

L'appliance McAfee Application Data Monitor est capable de détecter plus de 500 types de documents lors de leur transmission sur le réseau sous la forme d'e-mails, de conversations, de partages peer-to-peer, de partages de fichiers et autres. Elle identifie les documents quelle que soit leur extension, et notamment les documents qui se présentent sous un autre type et tentent de contourner les passerelles de messagerie et les systèmes IDS/IPS. Même les documents incorporés à d'autres documents ainsi que les fichiers archivés, compressés et codés sont découverts grâce à des informations pertinentes telles que le nom de fichier et l'opération effectuée.

Menaces visant la couche Application

De nouvelles menaces sophistiquées exploitent les vulnérabilités présentes dans les applications d'entreprise les plus répandues afin de s'introduire dans votre réseau et d'en extraire abusivement les données sensibles. Alors que ces menaces de la couche Application sont difficiles à détecter à l'aide de pare-feux et de systèmes de détection et de prévention des intrusions (IDS/IPS) classiques, l'appliance McAfee Application Data Monitor est en mesure d'analyser tout le contenu d'une application, y compris les protocoles sous-jacents, afin de détecter les charges actives cachées, les logiciels malveillants et même les canaux de communication clandestins (par exemple, un fichier exécutable incorporé à un document PDF).

Anomalies de protocoles

La détection des anomalies permet d'identifier de façon proactive les menaces imminentes afin de réduire les risques et les fuites. Alors que certaines solutions de sécurité classiques sont limitées à l'analyse des flux réseau, l'appliance McAfee Application Data Monitor va bien plus loin. Son analyse dépasse le simple comportement réseau pour détecter des anomalies au sein des applications et des protocoles et offre ainsi une méthodologie de détection des risques plus efficace et proactive.

Aucun impact sur les performances des applications

Dans la mesure où l'appliance McAfee Application Data Monitor fonctionne sur un port SPAN, elle n'a aucune incidence sur les performances des applications, leur fiabilité ou leur latence.

Prise en charge de plus de 500 applications et protocoles

- **Protocoles réseau de bas niveau :** TCP/IP, UDP, RTP, RPC, SOCKS, DNS, etc.
- **Messagerie électronique :** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Messagerie web :** AOL Webmail, Hotmail, Yahoo! Mail, Gmail et messageries Facebook et MySpace
- **Messagerie instantanée :** AOL, ICQ, Jabber, MSN, SIP et Yahoo!
- **Protocoles de transfert des fichiers :** FTP, HTTP, SMB et SSL
- **Protocoles de compression et d'extraction :** BASE64, GZIP, MIME, TAR, ZIP, etc.
- **Fichiers archives :** archives RAR, ZIP, BZIP, GZIP et archives codées au format UU et BinHex
- **Packages d'installation :** packages Linux, fichiers CAB InstallShield, fichiers CAB Microsoft
- **Fichiers image :** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW et icônes Windows
- **Fichiers audio :** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, SHOUTCast, etc.
- **Fichiers vidéo :** AVI, Flash, QuickTime, RealMedia, MPEG-4, Vivo, Digital Video (DV), Motion JPEG, etc.
- **Autres applications et fichiers :** bases de données, feuilles de calcul, télécopies, applications web, polices, fichiers exécutables, applications Microsoft Office, jeux et outils de développement de logiciels

Intégration avec l'infrastructure de votre entreprise

Alors que la plupart des solutions de surveillance des réseaux fonctionnent de façon isolée, McAfee Application Data Monitor opère en étroite collaboration avec les autres systèmes de sécurité des informations. En effet, l'intégration avec McAfee Enterprise Security Manager permet à la solution de se connecter au reste de votre infrastructure de sécurité, ce qui présente de nombreux avantages : simplification des opérations de sécurité, amélioration de l'efficacité globale et réduction des coûts. Vous pouvez intégrer la détection des fraudes et des fuites avec des outils puissants d'analyse, d'inspection réseau, de surveillance des événements de base de données et d'autres fonctions.

Exemples d'utilisation

L'appliance McAfee Application Data Monitor est capable de détecter un large éventail d'activités non autorisées, de violations de stratégies, de vols et de fraudes. En voici quelques exemples :

Vol d'informations confidentielles

Un employé connecté sous le nom de jdupont@une-entreprise.com envoie un e-mail à complice@gmail.com. L'e-mail contient un fichier shoo.doc qui comprend les mots « formule secrète ». Il a été envoyé à 12h20 du poste hôte 0232 (192.168.0.36) à l'aide du serveur SMTP (10.0.2.13) avec la ligne d'objet suivante : je l'ai.

Utilisation d'applications non autorisées

Un employé a transgressé une stratégie en transférant de la musique à l'aide d'une application de partage de fichiers peer-to-peer qu'il a installée. Il a envoyé des fichiers volumineux pendant ses heures de travail et donc consommé une bande passante importante. Une investigation plus approfondie révèle que l'employé n'en est pas à son premier méfait. Il utilise Jabber et IRC en plus d'exécuter un serveur web non autorisé sur son poste de travail.

Le « cyberslacking » ou l'utilisation abusive d'Internet sur le lieu de travail

Une employée effectue en secret des opérations de courtage. Au cours de sa journée de travail, elle se connecte pendant une heure environ à des sites de courtage boursier tous les matins et après-midi. Elle utilise également le système VoIP (SIP) de la société pour effectuer six appels par jour en moyenne et passe des heures sur Yahoo! Messenger sous le nom de « traderjean » pour parler à « traderlouis » et à « tradermarie ».

Utilisation de mots de passe faibles

La stratégie de sécurité de votre entreprise exige l'utilisation de mots de passe forts pour accéder à tous les comptes d'application et système des utilisateurs. Les comptes Microsoft Active Directory sont gérés de façon stricte. En revanche, des dizaines de mots de passe faibles sont utilisés sur les serveurs FTP accessibles au public, les serveurs de messagerie et d'autres applications web critiques qui n'utilisent pas Active Directory.

Prise en charge de plus de 500 applications et protocoles (suite)

- **Autres protocoles :** imprimantes réseau, accès SSH, VoIP et peer-to-peer

En savoir plus

Pour en savoir plus, visitez notre site à l'adresse : **www.mcafee.com/fr/products/siem/index.aspx**.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr

61322ds_app-data-monitor_0914
SEPTEMBRE 2014