FICHE TECHNIQUE

McAfee Security Suite for Virtual Desktop Infrastructure

Une sécurité rigoureuse avec un impact minimal sur les performances

L'adoption des postes de travail virtuels est en plein essor. Pour les protéger efficacement, veillez à choisir une solution de sécurité conçue pour ce type d'architecture, pour ne pas compromettre les performances ou affecter la densité de serveurs. Les antivirus traditionnels ne fonctionnent pas bien sur les infrastructures virtualisées. La réponse ? McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), qui offre une protection complète optimisée pour les postes de travail virtuels.

McAfee Security Suite for Virtual Desktop Infrastructure comprend une protection antimalware optimisée pour les environnements virtualisés, des listes blanches pour mettre en échec les attaques de type « jour zéro », une protection contre les intrusions sur les postes de travail et une protection des données. La solution avertit également les utilisateurs du caractère malveillant de certains sites web et/ou les empêche d'y accéder.

Architecture d'analyse optimisée

La nature dynamique des postes de travail virtuels nécessite une administration rigoureuse. Les images doivent être libres de tout logiciel malveillant lorsqu'elles sont hors ligne et analysées sans aucun délai à l'ouverture de session. La protection antimalware n'est cependant pas l'unique service exécuté au démarrage et les utilisateurs commencent souvent leur travail en groupe, ce qui génère des pics de demandes et donc des « bombardements antivirus » qui consomment toutes les ressources et bloquent les ouvertures de session.

Pour éliminer les goulots d'étranglement et les retards d'analyse, McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) transfère les opérations d'analyse, de configuration et de mise à jour des fichiers DAT depuis les images des systèmes invités vers une appliance virtuelle renforcée ou vers un serveur d'analyse de déchargement. McAfee conçoit et entretient un cache global de fichiers analysés pour garantir qu'une fois un fichier contrôlé et son absence de contamination confirmée, les machines virtuelles qui y accéderont par la suite seront dispensées d'attendre l'exécution d'une analyse. Les ressources de mémoire allouées à chaque machine virtuelle sont ainsi réduites et peuvent être réaffectées au pool de ressources en vue d'une utilisation plus efficace. La planification intelligente des analyses à la demande permet de préserver les performances de l'hyperviseur.

Principaux avantages

- Découverte et visibilité grâce à McAfee ePO et à Cloud Workload Discovery
- Combinaison unique de listes noires et de listes blanches pour assurer la protection antimalware
- Protection des environnements virtuels, optimisée de façon à limiter l'impact sur les performances
- Protection de l'environnement web et défense contre les intrusions grâce à la protection de la mémoire et des applications web
- Intégration à McAfee ePO pour une visibilité, un contrôle et une génération de rapports immédiats sur l'ensemble des terminaux
- Déploiement flexible sans agent et multiplate-forme
- Prise en charge du provisionnement élastique des serveurs d'analyse hors ligne, en fonction de la demande (multiplate-forme)
- Intégration avec les fonctions locales d'analyse de la réputation pour une réponse plus rapide face aux menaces (multiplate-forme)

Gestion granulaire des stratégies

La console McAfee® ePolicy Orchestrator® (McAfee ePO™) vous permet de configurer les stratégies et les contrôles régissant McAfee MOVE AntiVirus. Les données des postes de travail virtuels peuvent être cumulées avec les données d'autres systèmes dans des tableaux de bord et des rapports unifiés. Les administrateurs peuvent configurer des stratégies individualisées par machine virtuelle, pool de ressources, cluster ou centre de données grâce à l'outil Cloud Workload Discovery pour les déploiements en cloud privé. Ils adaptent ainsi leurs paramètres de sécurité à la configuration et aux besoins spécifiques du centre de données.

Déploiement sans agent pour les environnements VMware

McAfee MOVE AntiVirus tire parti de VMware NSX ou VMware vCNS pour plus d'efficacité. Dans les déploiements sans agent, l'hyperviseur est utilisé comme connexion haut débit pour permettre à la machine virtuelle de sécurité (SVM) McAfee MOVE AntiVirus d'analyser les machines virtuelles à partir d'un emplacement extérieur à l'image du système invité. À mesure de l'analyse, la SVM indique à VMware NSX à ou VMware vCNS de mettre en cache les fichiers corrects et de supprimer les fichiers malveillants, d'en interdire l'accès ou de les mettre en quarantaine.

Il suffit d'installer et de configurer la SVM VMware et les composants VMware NSX/vCNS sur les serveurs VMware ESX, et les pilotes pour terminaux VMware NSX/vCNS sur les machines virtuelles invitées. Chaque image est alors automatiquement protégée sans qu'il soit nécessaire d'installer le logiciel sur chaque machine virtuelle cliente. Notre prise en charge de vMotion signifie que vos machines virtuelles peuvent passer d'un hôte à un autre en restant protégées par la SVM sur l'hôte cible, et ce sans impact négatif sur les analyses ou sur l'expérience utilisateur.

L'intégration de McAfee MOVE AntiVirus avec vCNS vous permet en outre de surveiller l'état de la SVM au sein de VMware vCenter et de recevoir des alertes en cas de perte de connectivité. Et en cas d'infection d'une machine virtuelle, le logiciel McAfee ePO reçoit des données sur les événements, détaillant la machine spécifiquement concernée. Par ailleurs, l'intégration étroite avec NSX permet de synchroniser à la fois les stratégies créées dans McAfee ePO et les règles affectées dans VMware NSX. Enfin, le marquage des machines virtuelles infectées ou dépourvues de protection antimalware permet au pare-feu VMware NSX de les placer immédiatement en quarantaine.

Multiplate-forme pour tous les hyperviseurs

Dans les installations multiplates-formes, l'agent McAfee MOVE AntiVirus, un composant de terminal léger, communique avec le serveur d'analyse de déchargement (McAfee MOVE Offload Scan Server) pour gérer le traitement antivirus à la place des postes de travail virtuels. Un agent McAfee ePO gère les stratégies et les fonctions d'analyse. Il est également possible de désigner et analyser une image étalon pour l'utiliser comme image saine de référence. L'administrateur peut ainsi préremplir les caches globaux à l'aide d'images saines pour accélérer le démarrage des machines virtuelles.

Configuration de McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Déploiement multiplate-forme
  - Déploiement sans agent
- Cloud Workload Discovery pour les déploiements en cloud privé (VMware et OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktop
- McAfee Application Control for Desktops
- McAfee SiteAdvisor® Enterprise
- McAfee ePolicy Orchestrator

Lorsqu'un utilisateur accède à un fichier, le serveur McAfee MOVE Offload Scan Server effectue une analyse à l'accès, fournissant ainsi une réponse à la machine virtuelle. Les utilisateurs peuvent être informés des problèmes grâce à une alerte pop-up et les fichiers peuvent alors être placés en quarantaine en attendant la prise de décision. Chaque poste de travail virtuel peut être configuré à l'aide de stratégies uniques et individuelles, définies dans la console McAfee ePO. L'ensemble des machines virtuelles peut également être géré en tant que groupe.

Comme les charges de travail varient dans les déploiements multiplates-formes, il est possible d'ajouter ou de supprimer automatiquement des machines virtuelles de sécurité (SVM) à partir du pool de ressources. Cette flexibilité vous permet d'augmenter ou réduire votre puissance d'analyse afin de bénéficier d'une évolutivité illimitée et d'utiliser plus efficacement les ressources. Les notifications d'événement aident les administrateurs à comprendre les tendances d'utilisation des SVM afin d'optimiser la gestion des ressources.

Dans les déploiements multiplates-formes, McAfee MOVE AntiVirus peut compléter les informations mondiales sur la réputation de McAfee Global Threat Intelligence par les données locales de McAfee Threat Intelligence Exchange (module vendu séparément). Cette complémentarité permet d'identifier et de neutraliser instantanément le nombre croissant d'échantillons de malwares uniques. Grâce à McAfee Threat Intelligence Exchange, McAfee MOVE AntiVirus peut également collaborer avec McAfee Advanced Threat Defense pour analyser de manière dynamique le comportement des applications inconnues dans un environnement sandbox. Cela permet d'immuniser automatiquement tous les postes de travail virtuels contre les nouveaux logiciels malveillants détectés.

Fonctionnalité	Avantage pratique
Sécurité de la virtualisation	▪ La sécurité des charges de travail est améliorée, sans impact sur les performances et l'utilisation des ressources. ▪ Le déploiement sans agent, optimisé pour les environnements VMware, assure d'excellentes performances et une densité de machines virtuelles hors pair. Il n'est pas nécessaire d'installer ou de mettre à jour des agents McAfee sur les postes de travail virtuels individuels, ce qui simplifie la gestion et l'utilisation. ▪ Le déploiement multiplate-forme pour tous les hyperviseurs permet de prendre en charge le provisionnement élastique des serveurs d'analyse hors ligne en fonction de la demande. De plus, il s'intègre avec les fonctions locales de réputation pour une réponse plus rapide face aux menaces.

FICHE TECHNIQUE

Fonctionnalité	Avantage pratique
Protection de base des terminaux	▪ Les analyses antivirus sont plus rapides, sollicitent moins la mémoire et le processeur et offrent une protection performante. ▪ La fonction de prévention des intrusions protège les entreprises contre les menaces complexes susceptibles d'être introduites ou autorisées involontairement. ▪ McAfee SiteAdvisor® Enterprise empêche les utilisateurs d'interagir avec les sites web dangereux et permet de limiter l'accès aux sites web potentiellement nuisibles, garantissant ainsi la conformité à la politique d'entreprise.
Listes blanches d'applications	▪ L'impact sur les performances des hôtes est très limité comparé aux mécanismes de sécurité traditionnels appliqués aux terminaux. ▪ La protection contre les attaques de type « jour zéro » et les menaces APT n'exige aucune mise à jour des signatures, ce qui réduit le délai de protection. ▪ La charge opérationnelle des listes blanches dynamiques est réduite par rapport aux techniques plus anciennes.
Cloud Workload Discovery	▪ L'administrateur dispose d'une visibilité complète sur toutes les charges de travail dans le cloud privé et sur les plates-formes sous-jacentes, pour identifier les contrôles de sécurité trop faibles.
Protection des fichiers et des supports amovibles (chiffrement)	▪ Le chiffrement est plus simple et moins risqué à déployer grâce à la fonction de protection des fichiers et des supports amovibles. ▪ Grâce à une implémentation optimisée de la technologie Intel® AES-NI, les hôtes chiffrés présentent des performances quasi natives. ▪ Le chiffrement peut être contrôlé par des stratégies et s'appliquer de manière transparente et automatique aux fichiers et dossiers, ou aux supports amovibles (clés USB, CD, DVD). ▪ Les utilisateurs peuvent chiffrer les supports USB amovibles et le transfert des informations. ▪ L'accès aux données est sécurisé sur les partages réseau.
Gestion centralisée à l'aide de McAfee ePO	▪ Les déploiements physiques, virtuels et dans le cloud sont gérés de manière centralisée pour assurer des contrôles de sécurité plus performants sur l'ensemble des plates-formes (gestion des stratégies, déploiements, visibilité, sécurité). ▪ Les aspects opérationnels sont simplifiés — un gain de temps pour le personnel administratif. ▪ Les coûts en matériel sont réduits en raison du nombre limité de serveurs requis.

En savoir plus

Les solutions McAfee vous assurent la sécurité dont vous avez besoin, avec un impact minimal sur les performances. Consultez notre site : **www.mcafee.com/fr/products/data-center-security-suite-for-vdi.aspx**.

McAfee Together is power.

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