FICHE TECHNIQUE

McAfee Management for Optimized Virtual Environments AntiVirus

Protégez votre cloud privé sans sacrifier les performances

Les antivirus traditionnels ne fonctionnent pas bien sur les infrastructures virtualisées. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) offre à vos postes de travail et serveurs virtuels une protection avancée et optimisée contre les logiciels malveillants. La solution est flexible : vous pouvez opter pour une implémentation sur plusieurs hyperviseurs ou pour une option personnalisée sans agent pour VMware NSX ou VMware vCNS. Dans tous les cas, vous bénéficiez d'une sécurité de premier plan garantissant la détection et la neutralisation immédiates des menaces, avec un impact minimal sur les performances des machines virtuelles. McAfee MOVE AntiVirus optimise la protection antimalware des déploiements virtualisés et libère les ressources des hyperviseurs, tout en assurant l'exécution d'analyses de sécurité conformément aux stratégies.

Contrôle optimisé des analyses

La nature dynamique des serveurs virtuels et des postes de travail invités nécessite une administration rigoureuse. Les images doivent être libres de tout logiciel malveillant à l'ouverture d'une session utilisateur. Cela pose dès lors quelques difficultés, car les utilisateurs commencent souvent leur travail en groupe : cela génère des pics de demandes appelés « 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 MOVE AntiVirus transfère les opérations d'analyse, de configuration et de mise à jour des fichiers DAT, normalement exécutées sur les systèmes invités, vers un serveur d'analyse de déchargement. McAfee crée et conserve 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.

Principaux avantages

- **Transfert de la charge de l'analyse antimalware :** Protection instantanée, avec impact minimal sur la mémoire et le temps de traitement
- **Prévention des bombardements antivirus :** Options incluant notamment les analyses à l'accès et à la demande
- **Déploiement flexible :** Architecture multiplate-forme (principaux hyperviseurs et machines virtuelles Windows) ou sans agent (machines virtuelles VMware, Windows et Linux)
- **Meilleure optimisation des ressources :** Provisionnement élastique des serveurs d'analyse hors ligne avec notifications d'événements (multiplate-forme)
- **Blocage des menaces inconnues de type « jour zéro » en quelques secondes :** Combinaison d'informations locales sur la réputation avec des analyses comportementales en sandbox (multiplate-forme, module complémentaire vendu séparément)

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.

McAfee MOVE AntiVirus permet de définir des stratégies distinctes pour l'analyse à la demande et à l'accès, pour mieux contrôler l'exécution des opérations de sécurité. Par exemple, les administrateurs peuvent accepter un niveau raisonnable de risque pour les analyses à l'accès en temps réel, afin de limiter l'impact sur les performances. En revanche, pendant les périodes d'activité réduite où l'impact sera moindre, ils pourront exécuter des analyses à la demande associées à des stratégies sont plus strictes.

Visibilité de bout en bout sur l'ensemble des clouds

La mise en œuvre de bonnes stratégies de sécurité dans les environnements virtuels passe par une bonne visibilité. McAfee Cloud Workload Discovery, un outil destiné aux déploiements de clouds privés, offre une vue complète sur les centres de données virtuels et prend en charge VMware et OpenStack. Il transmet à la console McAfee ePO des propriétés essentielles telles que les serveurs, les hyperviseurs et les machines virtuelles. Grâce à cette visibilité sur l'état de sécurité des machines virtuelles et à la surveillance en temps quasi réel des relations entre ces dernières et les hyperviseurs, la protection de vos centres de données virtuels est grandement simplifiée. Un tableau de bord personnalisable affiche l'état des analyses de sécurité, des vues d'ensemble sur divers facteurs et des données historiques sur la sécurité des ressources.

Les suites McAfee Server Security Suite Essentials et McAfee Server Security Suite Advanced étendent la visibilité et le contrôle aux clouds publics Amazon Web Services (AWS) et Microsoft Azure, ainsi qu'aux serveurs physiques.

Gestion granulaire des stratégies

La console McAfee ePO vous permet de configurer les stratégies et les contrôles régissant McAfee MOVE AntiVirus. Vous pouvez d'ailleurs cumuler les données virtuelles avec les données de vos systèmes physiques et clouds publics afin de disposer de tableaux de bord et de rapports unifiés. En outre, les administrateurs peuvent configurer des stratégies individualisées par machine virtuelle, cluster ou centre de données grâce à McAfee Cloud Workload Discovery ; ils peuvent ainsi adapter ainsi leurs paramètres de sécurité à la configuration du centre de données.

Fonctions supplémentaires de McAfee MOVE AntiVirus

Gestion et visibilité

- Planification instantanée d'analyses à la demande sur une machine virtuelle ou un groupe de machines virtuelles
- Analyses à la demande ciblées pour plus de précision
- Déploiement automatique d'un serveur d'analyse de déchargement sur chaque hyperviseur grâce à l'intégration avec VMware NSX Service Composer
- Vue sur tout l'environnement grâce aux tableaux de bord, rapports et alertes par e-mail

Principaux avantages (suite)

- **Console McAfee® ePolicy Orchestrator® (McAfee ePO™) :** Visibilité de bout en bout et contrôle de l'ensemble des déploiements physiques, virtuels et dans le cloud

Configurations de McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus :
  - Déploiement multiplate-forme
  - Déploiement sans agent
- Cloud Workload Discovery pour les déploiements en cloud privé (VMware et OpenStack)
- McAfee ePO

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus :
  - Déploiement multiplate-forme
  - Déploiement sans agent
- Cloud Workload Discovery pour les déploiements en cloud privé (VMware et OpenStack)
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Protection de la mémoire et des applications web
- McAfee ePO

Déploiement et configuration simplifiés

- Déploiement et configuration d'un serveur d'analyse de déchargement sur plusieurs hyperviseurs (sans agent)
- Restauration des fichiers mis en quarantaine à l'aide de la console McAfee ePO (multiplate-forme)
- Diagnostics détaillés pour l'optimisation des performances antivirus
- Gestion des stratégies transparente, sans agent et multiplate-forme

Option 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 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 sur les analyses ou sur l'expérience utilisateur.

L'intégration des solutions McAfee avec VMware 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. De plus, en cas d'infection d'une machine virtuelle, la console McAfee ePO reçoit des données sur les événements, détaillant la machine spécifiquement concernée. Par ailleurs, l'intégration étroite avec VMware 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.

McAfee MOVE AntiVirus sans agent peut être déployé simultanément avec VMware vCNS et VMware NSX, de sorte qu'il est très facile pour les clients possédant déjà VMware vCNS d'effectuer la transition vers VMware NSX.

Multiplate-forme pour tous les principaux hyperviseurs

Dans les installations multiplates-formes (dont vSphere, Hyper-V, KVM et XenServer), l'agent McAfee MOVE AntiVirus, un composant de terminal léger, communique avec la SVM pour gérer le traitement antivirus au nom de chaque machine virtuelle. L'agent McAfee MOVE AntiVirus conserve un cache local, et gère les stratégies

et les fonctions d'analyse. Vous pouvez désigner et analyser une image étalon pour l'utiliser comme image saine de référence. Grâce au préremplissage de caches locaux à l'aide d'images saines, le démarrage des machines virtuelles est aussi rapide que possible.

Lors de l'accès 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 sont informés des problèmes par une alerte pop-up et peuvent alors décider de supprimer les fichiers malveillants, d'en interdire l'accès ou de les mettre en quarantaine.

Comme les demandes d'analyse varient dans les déploiements multiplates-formes, il est possible d'ajouter ou de supprimer automatiquement des SVM à partir du pool de ressources. Cela vous permet d'augmenter ou de diminuer 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 (McAfee GTI) par les données locales de McAfee Threat Intelligence Exchange (module vendu séparément). Cette complémentarité permet d'identifier et de neutraliser instantanément les nouveaux malwares. 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 et immuniser automatiquement tous les terminaux contre les nouveaux logiciels malveillants détectés. L'intégration de McAfee MOVE AntiVirus avec McAfee Network Security Platform via la solution McAfee Threat Intelligence Exchange garantit une approche de sécurité multiniveau pour une protection unifiée du périmètre et des machines virtuelles.

Gestion unifiée des stratégies pour les déploiements sans agent et multiplates-formes

Il peut être intéressant de tirer parti de la capacité de McAfee MOVE AntiVirus à prendre en charge à la fois les déploiements multiplates-formes et sans agent. McAfee MOVE AntiVirus permet aux administrateurs de définir et de gérer des stratégies de sécurité cohérentes à l'aide d'un point d'extension de la console McAfee ePO, de sorte que la gestion de ces différentes méthodes soit simple et transparente.

Architecture	Déploiement multiplate-forme	Déploiement sans agent
Prise en charge des plates-formes et des hyperviseurs	Tous les principaux hyperviseurs, dont VMware, Citrix, Hyper-V et KVM	VMware
Plate-forme d'analyse	Windows 2008, Windows 2012 R2, Windows Server 2016	Linux Ubuntu 16.04
Évolutivité du déploiement	Une SVM peut assurer la protection des machines virtuelles de plusieurs hyperviseurs. Les SVM permettent un provisionnement élastique.	Une SVM par hôte ESX
Communication avec les machines virtuelles	Via le réseau	Via l'hyperviseur
Protection des machines virtuelles	Windows	Windows et Linux

En savoir plus

Les solutions McAfee vous assurent la sécurité et la flexibilité dont votre entreprise a besoin.

Pour en savoir plus, consultez notre site web à l'adresse **www.mcafee.com/fr/products/move-anti-virus.aspx**.

McAfee
Together is power.

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