McAfee Security Suite for Virtual Desktop Infrastructure

La sécurité et la flexibilité indispensables à votre entreprise

L'adoption de postes de travail virtuels est en plein essor. La solution privilégiée doit néanmoins intégrer des fonctionnalités de sécurisation des postes de travail robustes, qui protègent votre entreprise sans compromettre les performances ou affecter la densité de serveurs souhaitée. Les antivirus traditionnels ne fonctionnent pas bien sur les infrastructures virtualisées. La réponse ? McAfee® Security Suite for Virtual Desktop Infrastructure, qui offre une protection complète optimisée pour les postes de travail virtuels.

Principaux avantages

- Fonctionnalités de découverte et de visibilité pour les environnements VMware vSphere grâce au logiciel McAfee ePO et à la solution McAfee Data Center Connector for VMware vSphere. Combinaison unique de listes noires et de listes blanches qui assurent la protection des actifs physiques et virtuels contre les logiciels malveillants (*malware*)
- Sécurisation des environnements virtualisés, optimisée de façon à limiter l'impact sur les performances
- Protection contre les menaces inconnues grâce au blocage de l'exécution d'applications indésirables sur les postes de travail virtuels
- Protection de l'environnement web et défense contre les intrusions grâce à un pare-feu pour postes de travail, la protection de la mémoire et la protection des applications web
- Exploitation du logiciel McAfee ePO afin d'offrir une visibilité, un contrôle et une génération de rapports instantanés sur l'ensemble des terminaux

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 (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 garantit l'absence d'interférences avec les performances de l'hyperviseur.

intel Security

Configuration de McAfee Security Suite for Virtual Desktop Infrastructure

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus
  - Déploiement de plusieurs hyperviseurs
  - Déploiement sans agent
- McAfee Data Center Connector for vSphere
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- Technologie McAfee SiteAdvisor® Enterprise
- McAfee ePolicy Orchestrator

Gestion granulaire des stratégies

La console du logiciel McAfee® ePolicy Orchestrator® (McAfee ePO™) bien connue vous permet de configurer les stratégies et les contrôles prescrivant le comportement de 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 McAfee Data Center Connector. Ils adaptent ainsi leurs paramètres de sécurité à la configuration et aux besoins spécifiques du centre de données.

Déploiement sans agent tirant parti de VMware vShield pour une efficacité accrue

Dans les déploiements sans agent, VMware vShield Endpoint utilise l'hyperviseur comme connexion haut débit pour permettre à McAfee MOVE AntiVirus Security Virtual Appliance (SVA) d'analyser les machines virtuelles depuis un point extérieur à l'image du système invité. Au fur et à mesure de l'analyse, SVA indique à vShield de mettre les fichiers corrects en cache et de supprimer les fichiers malveillants, de les mettre en quarantaine ou d'empêcher leur consultation.

Une fois SVA et les composants vShield requis installés et configurés sur les serveurs ESX, parallèlement à l'installation du pilote vShield sur les machines virtuelles invitées, chaque image est automatiquement protégée à sa création. Il n'est pas nécessaire d'installer le logiciel McAfee sur toutes les machines virtuelles clientes. Notre prise en charge de vMotion signifie que les machines virtuelles peuvent passer d'un hôte à un autre en étant toujours protégées par SVA sur l'hôte cible et ce, sans impact négatif sur les analyses ou sur l'expérience utilisateur. L'intégration McAfee permet de surveiller l'état SVA au sein de vCenter et de recevoir des alertes en cas de perte de connectivité par le SVA. Le logiciel McAfee ePO reçoit des données sur les événements, détaillant la machine virtuelle spécifiquement concernée en cas d'infection d'une machine virtuelle.

Prise en charge multi-hyperviseur pour le respect des normes et une plus grande facilité

Dans les installations comportant plusieurs hyperviseurs, 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 au nom de chaque poste de travail virtuel. 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.

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 logicielle McAfee ePO. L'ensemble des machines virtuelles peut également être géré en tant que groupe.

En savoir plus

Les solutions McAfee vous assurent la sécurité et la flexibilité dont votre entreprise a besoin. Consultez notre site : **www.mcafee.com/fr/products/data-center-security-suite-for-vdi.aspx**.

Fonctionnalité	Avantage pratique
Sécurité de la virtualisation	• Amélioration de la sécurité des charges de traitement déployées dans les infrastructures virtuelles, sans préjudice en termes de performances et d'utilisation des ressources • Options de déploiement sans agent et multi-hyperviseur : déploiement pour les environnements virtualisés associant les produits de plusieurs fournisseurs (VMware, Citrix; Hyper-V) • Déploiement sans agent optimisé pour les environnements VMware pour des performances et une densité de machines virtuelles hors pair. Aucune installation ou mise à jour d'agents McAfee sur les postes de travail virtuel individuels, pour une complexité réduite et une convivialité nettement améliorée
Protection de base des terminaux	• Protection antivirus pour les serveurs physiques classée numéro un par NSS Labs pour ses performances contre les exploits « jour zéro » et les attaques par contournement • Grâce à la fonction de prévention des intrusions, protection des entreprises contre les menaces complexes susceptibles d'être introduites ou autorisées involontairement • Grâce à McAfee SiteAdvisor® Enterprise, Blocage des interactions utilisateurs avec les sites web dangereux et personnalisation des stratégies afin de limiter l'accès aux sites web potentiellement nuisibles, garantissant ainsi la conformité aux stratégies
Listes blanches d'applications	• Réduction considérable de l'impact sur les performances des hôtes par rapport aux contrôles de sécurité appliqués aux terminaux traditionnels • Protection contre les attaques de type « jour zéro » et les menaces persistantes avancées sans mise à jour des signatures pour un délai de protection réduit • Charge opérationnelle réduite des listes blanches dynamiques par rapport aux anciennes techniques de listes blanches
Visibilité complète sur les machines virtuelles au sein des clouds privés	• Découverte automatique des machines virtuelles dans le cloud privé (VMware vSphere)
Protection des fichiers et des supports amovibles (chiffrement)	• Déploiement du chiffrement plus simple et sûr grâce à la protection des fichiers et des supports amovibles • Performances quasi natives sur les hôtes chiffrés grâce à une implémentation optimisée de la technologie Intel AES-NI • Chiffrement des fichiers et des dossiers transparent et automatique mis en œuvre par des stratégies, et chiffrement des supports amovibles (clés USB, CD, DVD) • Possibilité de chiffrement des supports USB amovibles et de transfert sécurisé des informations par les utilisateurs • Accès sécurisé au données sur les partages réseau
Gestion centralisée à l'aide du logiciel McAfee ePO	• Gestion unifiée via une seule console pour les machines physiques et virtuelles, y compris celles hébergées dans des clouds privés et publics, pour une visibilité accrue de la sécurité • Processus opérationnels simplifiés et investissement en temps réduit pour le personnel administratif • Coûts en matériel réduits en raison du nombre de serveurs nécessaires réduit

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com