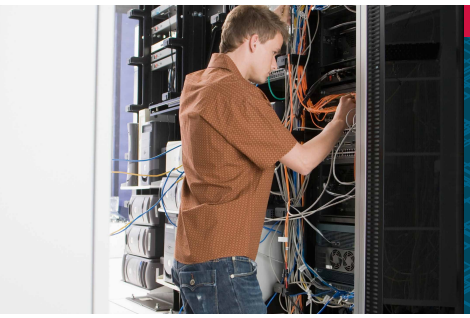

Etendre la virtualisation en préservant la sécurité

Des choix de sécurité essentiels pour l'infrastructure virtualisée

Dans la mesure où la virtualisation des serveurs et des postes de travail devient une proccupation stratégique pour de plus en plus d'entreprises, les équipes informatiques doivent faire face à l'augmentation du nombre d'utilisateurs finaux, davantage répartis géographiquement, et supporter une charge de travail accrue tout en répondant à de nouvelles exigences, telles que l'allocation « à la volée » et le libre-service. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) adapte les systèmes de sécurisation aux exigences spécifiques de la virtualisation en matière technique et de gestion. Cette solution vous permet d'atteindre les résultats escomptés en matière de virtualisation, tout en offrant une expérience positive à vos utilisateurs et ce, en toute sécurité.

Les technologies de virtualisation sont en tête des priorités des directeurs informatiques pour 2012[1]. Grâce à la prise en charge de programmes clés tels que l'informatique dématérialisée (cloud), l'utilisation des équipements personnels sur le lieu de travail et la consolidation des serveurs et des centres de données, elle permet aux entreprises de réaliser des économies et de gagner en flexibilité. Mais si la virtualisation revêt une importance stratégique pour la réussite de l'entreprise, elle lance également certains défis spécifiques, par rapport aux installations de sécurité physiques traditionnelles, en termes d'opérations et de gestion des risques. Le nouveau modèle opérationnel de virtualisation impose une réévaluation des processus opérationnels, des stratégies et des décisions de déploiement traditionnels en matière de sécurité informatique.

Dégradation des performances

Le problème apparaît clairement au niveau des performances d'analyse. Dans un déploiement traditionnel, chaque système (poste de travail ou serveur) exécute localement un antimalware, celui-ci réalisant une analyse à l'accès ou planifiée pour veiller à ce que l'hôte ne soit pas infecté. Toutefois, ce modèle « par poste » consomme trop de ressources pour les environnements virtuels. En cas de « bombardement d'analyses », les opérations d'analyse peuvent consommer l'intégralité de la mémoire et des ressources de traitement disponibles de l'hyperviseur et, par conséquent, empêcher les utilisateurs d'ouvrir de nouvelles sessions. De nombreux administrateurs ont tenté de résoudre le problème en désactivant les analyses ou en ignorant les mises à jour logicielles.

De par leur popularité en tant que plates-formes d'entreprise, les environnements virtualisés sont désormais le nouveau terrain de chasse des cybercriminels, qui exploitent les vulnérabilités logicielles et de configuration. Sans analyse de sécurité à jour et active, l'infrastructure virtualisée offre une mine d'opportunités aux voleurs de données et aux pirates.

Solution de sécurité obsolète

Les cybercriminels s'attaquent en priorité aux images s'exécutant sans protection antimalware ou dont la protection n'est pas à jour. Il faut donc veiller à ce que le logiciel de sécurité analyse les images en cours d'exécution et hors ligne, ainsi que les modèles d'image (ou images de référence). Pour être efficaces contre les pirates, les fonctionnalités de sécurisation des systèmes et de protection antimalware doivent être constamment à jour.

Dans une infrastructure de postes de travail virtualisés (VDI) de grande envergure, prenant en charge des milliers de machines virtuelles allouées et mises hors service au quotidien, la gestion de la sécurité devient moins prévisible. Pour les serveurs physiques en exécution permanente, il suffit de programmer les mises à jour de sécurité au moment le plus opportun, c.-à-d. en période de faible utilisation. Par contre, en ce qui concerne les utilisateurs des postes de travail, les mises à jour de sécurité doivent tenir compte des workflows dynamiques des machines virtuelles. Les images en ligne passent hors ligne, sont enregistrées et désactivées pour la nuit, ou parfois pendant quelques heures seulement, et les utilisateurs s'attendent à pouvoir accéder rapidement à leurs systèmes virtualisés — sans délai lié au démarrage ou à l'analyse.

Des ressources variées

Les centres de données compliquent encore la donne. Le rassemblement des ressources — serveur, stockage et réseau — permet une utilisation optimale mais présente également deux inconvénients majeurs. En termes de sécurité, l'avantage de la séparation physique des bases de données, des serveurs d'application, des serveurs web et des autres logiciels disparaît. En effet, l'isolement physique constitue un frein aux activités malveillantes. Il est donc essentiel de concevoir une sécurité plus forte pour les systèmes virtualisés.

Ensuite, la centralisation des fonctions liées au serveur, au stockage et au réseau — auparavant distinctes — au sein d'une même console de gestion oblige à modifier les processus de gestion. Ces ressources traditionnellement associées à des stratégies et à des administrateurs différents doivent à présent coexister au sein d'un seul environnement de procédures et de stratégies, souvent géré par un administrateur de virtualisation exclusif, un « superutilisateur ». Cette situation engendre une réelle concurrence entre les processus et les alertes en termes de visibilité, et il est possible que les stratégies doivent être normalisées. Les administrateurs doivent trouver les moyens de collaborer sur le plan opérationnel.

Multiplication des fournisseurs

En plus des changements mentionnés ci-dessus, beaucoup d'entreprises doivent relever le défi de la diversité des fournisseurs. Chaque fournisseur de solutions de virtualisation a des atouts spécifiques, ce qui pousse les entreprises à faire appel à plusieurs d'entre eux, notamment pour des logiciels stratégiques. Ce type de déploiement comprenant un mélange d'hyperviseurs multiplie les contraintes : vous devez sécuriser les images et veiller à la conformité tout en tenant compte des différents attributs de chaque produit.

« McAfee MOVE [AntiVirus] AV assure une protection cohérente et complète de l'environnement virtuel de McKesson contre les codes malveillants. Au fil de l'adoption des technologies émergentes, particulièrement des solutions de cloud, l'implémentation de McAfee MOVE [AntiVirus] AV renforce la sécurisation de notre environnement virtuel. Cette solution simplifie le dimensionnement et le déploiement et garantit que chaque système déployé bénéficie du même niveau de protection. »

— Patrick Enyart
Directeur
McKesson Information Security

Conformité

Pour ajouter à la complexité, vous êtes tenu de prouver que vos systèmes virtualisés répondent aux exigences de conformité visant (hier comme aujourd'hui) vos systèmes physiques. Les réglementations actuelles exigent une maintenance régulière de la protection antimalware. Par exemple, la réglementation 201 CMR 17.00 de l'Etat du Massachusetts sur la protection des données personnelles exige « des versions raisonnablement à jour du logiciel de sécurisation des systèmes comprenant une protection antimalware et des correctifs et définitions de virus raisonnablement à jour ou une version dudit logiciel pouvant être prise en charge par les correctifs et définitions de virus à jour et pour lequel des mises à jour de sécurité régulières sont prévues ».

Tous ces problèmes, placés dans le contexte d'un paysage de menaces dynamique, compliquent au quotidien les opérations de sécurisation des systèmes virtualisés. Les modèles traditionnels de sécurité issus du monde physique doivent être étendus, voire remplacés, en faveur d'une sécurité optimisée pour le monde de la virtualisation.

Optimisation des opérations avec McAfee MOVE

Dès le début de sa collaboration avec la communauté des spécialistes de la virtualisation, il y a de cela plusieurs années, McAfee a été témoin de l'émergence de ces difficultés opérationnelles. Pour les résoudre, nous avons conçu une technologie spécialisée permettant à nos meilleures fonctionnalités de sécurité de fonctionner de manière optimale au sein des déploiements de serveurs et de postes de travail virtualisés. McAfee MOVE AntiVirus garantit une protection antimalware et une sécurisation efficaces sans nuire aux performances. Ainsi, vous gagnez sur les deux tableaux : vous bénéficiez de la puissance de la virtualisation tout en assurant la productivité des utilisateurs et la sécurité du système d'exploitation invité de la machine virtuelle.

Notre solution vous offre la possibilité de choisir votre modèle de déploiement préféré : multiplate-forme ou sans agent (API VMware vShield). Les deux options tirent pleinement parti de la solution antimalware éprouvée et à la pointe du secteur[2] de McAfee. Elles offrent en outre des fonctionnalités de prévention des intrusions et de sécurisation des applications web pour une couche de protection supplémentaire contre les attaques.

Des analyses opportunes

McAfee MOVE AntiVirus libère les ressources des hyperviseurs pour d'autres fonctions, tout en veillant à l'exécution d'analyses à jour conformément aux stratégies. Une appliance virtuelle ou physique renforcée prend en charge le traitement des analyses, la maintenance des configurations et la mise à jour des signatures .DAT, de sorte que l'hyperviseur reste dédié à la prise en charge des images invitées.

L'intégration de McAfee MOVE AntiVirus avec le logiciel de gestion de la virtualisation nous permet d'éviter les « bombardements d'analyses » provoqués lorsque de nombreuses images demandent simultanément des allocations et des analyses. Par ailleurs, McAfee MOVE AntiVirus for Virtual Servers peut planifier les analyses de manière intelligente en fonction de la disponibilité des ressources et de l'hyperviseur. Plutôt que d'exiger la mise hors ligne des machines virtuelles actives pour procéder à l'analyse, la solution attend que les images soient hors ligne pour les analyser et les mettre à jour, de manière à ce qu'elles soient toujours prêtes à l'emploi.

Les renseignements les plus récents

McAfee MOVE AntiVirus protège les machines virtuelles à l'aide du moteur McAfee VirusScan®, également présent dans nos produits antivirus physiques leaders du marché. Pour que les analyses restent à jour sans nuire aux performances, l'appliance télécharge et applique les dernières signatures sur le serveur d'analyse de déchargement (McAfee MOVE Offload Scan Server) et non sur les machines virtuelles. Si des fichiers inconnus semblent suspects, McAfee MOVE AntiVirus interroge McAfee Global Threat Intelligence™ pour connaître leur réputation en temps réel.

Outre les fonctionnalités d'analyse antimalware, McAfee MOVE AntiVirus for Virtual Desktops comprend un pare-feu pour postes de travail et un système de protection avancée de la mémoire pour limiter les activités malveillantes et préserver l'intégrité des fichiers. Pour aider les utilisateurs à éviter les sites web dangereux susceptibles d'introduire un logiciel malveillant dans l'image active, la solution prévoit également des alertes de réputation des sites web et des contrôles de l'utilisation du Web basés sur les stratégies. L'action combinée de ces outils diminue les risques d'attaque de vos systèmes virtualisés. Pour une protection optimale, d'autres outils, tels que des listes d'autorisation d'applications, peuvent être ajoutés à la solution (par exemple, pour empêcher des applications indésirables ou des logiciels malveillants de perturber les activités de l'entreprise).

Sécurisation du réseau

La virtualisation modifie également la manière dont les organisations envisagent la sécurisation de leur réseau. En effet, la virtualisation de l'infrastructure physique requiert de nouvelles stratégies pour établir et maintenir les frontières de la sécurité en l'absence de silos physiques. Par ailleurs, la portabilité des machines virtuelles a un impact sur les stratégies de sécurisation du réseau. Les organisations doivent pouvoir sécuriser leur réseau de manière cohérente, quel que soit l'emplacement physique des applications et des serveurs virtualisés.

McAfee propose une sécurisation des réseaux intégrée pour les environnements physiques et virtuels. McAfee Network Security Platform assure l'inspection native des environnements virtuels grâce à son intégration complète avec l'API de sécurité réseau VMware vShield. Elle vous permet d'inspecter le trafic et de mettre en œuvre des stratégies sur et entre les machines virtuelles, quel que soit leur emplacement physique. Par ailleurs, grâce à l'accès natif aux outils VMware vCenter, vous pouvez intégrer la sécurisation du réseau dans les environnements virtuels.

Gestion tout-en-un

McAfee MOVE AntiVirus utilise McAfee ePolicy Orchestrator® (McAfee ePO™). Cet environnement de gestion est bien connu des administrateurs, qui l'utilisent déjà avec les outils physiques de McAfee pour la sécurisation des postes clients, des informations et des réseaux. Cette console unique permet à chaque administrateur de créer des tableaux de bords personnalisés pour surveiller les données et autres éléments dont il est responsable et générer des rapports sur des actifs spécifiques, mêmes variés (hôtes physiques/virtuels, postes clients/serveurs). La prise en charge des rôles est un facteur crucial pour la sécurisation de l'environnement de gestion collaborative propre aux centres de données virtualisés. Le logiciel McAfee ePO s'intègre également avec plus de 100 autres produits des partenaires McAfee Security Innovation Alliance, ce qui permet aux services informatiques de rationaliser les workflows dans toute l'infrastructure informatique.

Normalisation ou spécialisation

Le choix d'une implémentation multiplate-forme ou sans agent signifie que vous pouvez envisager sereinement vos relations actuelles ou à venir avec vos fournisseurs. La solution multiplate-forme utilise un agent léger dans chaque image invitée pour gérer les stratégies et les analyses, en s'appuyant sur un serveur d'analyse de déchargement pour les analyses à l'accès. Cette approche permet de combiner des hyperviseurs Citrix, Microsoft et VMware pour une flexibilité accrue ou pour répondre aux besoins de différentes communautés d'utilisateurs.

L'option de déploiement sans agent s'intègre très étroitement avec VMware pour exploiter au mieux votre investissement dans cette technologie basée sur l'hyperviseur. McAfee MOVE AntiVirus fonctionne par l'intermédiaire de VMware vShield Endpoint pour analyser les machines virtuelles à partir d'un emplacement extérieur aux images invitées, sans logiciel McAfee au sein de l'image elle-même. Grâce à VMware vMotion, les machines virtuelles analysées peuvent migrer d'un hôte à un autre sans affecter ni l'utilisateur ni les systèmes d'analyse. L'intégration du logiciel McAfee ePO avec vCenter rationalise le contrôle et la gestion des incidents.

Conformité continue

La plate-forme McAfee ePO vous permet de veiller à ce que les stratégies soient cohérentes sur les systèmes physiques et virtuels. Pour prendre en charge les processus de conformité, vous pouvez créer une vue de l'auditeur rassemblant les données pertinentes et exécuter des rapports ponctuels ou planifiés conformément aux réglementations.

Un avenir serein

Vous pouvez désormais disposer d'une sécurité qui correspond aux spécificités de la virtualisation. McAfee a optimisé ses solutions antimalware et de protection des postes clients de manière à ce qu'elles agissent tant au cœur qu'à la périphérie de la structure et des processus qui font l'efficacité de la virtualisation. L'analyse ne vient pas perturber les utilisateurs actifs. Les solutions de sécurisation et les processus de mise à jour des signatures respectent les cycles de mise en ligne/hors ligne des images des postes de travail et des serveurs.

Nos options de déploiement flexibles vous permettent de travailler avec vos fournisseurs favoris tout en ayant la certitude de respecter les normes de sécurité et de conformité. McAfee vous permet de bénéficier de tous les avantages de la virtualisation, sans laisser vos utilisateurs et vos données à la merci des cybercriminels. Nous ne cessons d'investir dans l'intégration et l'optimisation de notre vaste gamme de produits pour vous permettre de déployer une sécurité robuste et efficace à mesure que vous étendez votre utilisation de la virtualisation.

Pour en savoir plus sur McAfee MOVE AntiVirus, consultez notre site à l'adresse www.mcafee.com/fr/solutions/virtualization/virtualization.aspx ou contactez votre revendeur ou représentant McAfee local.

McAfee
An Intel Company

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

[1] http://www.informationweek.com/news/storage/virtualization/232400150
[2] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf

45601brf_virtualization_0512_fnl_ETMG