Sécuriser les applications dans les environnements virtualisés et de Cloud via VMware AppDefense

Alors que les budgets consacrés à la sécurité informatique ne cessent d'augmenter dans le monde entier, la probabilité pour une entreprise d'être victime d'une violation de données s'est envolée pour s'établir à 1 sur 4[1]. En dépit des milliers de produits de sécurité disponibles sur le marché et des budgets conséquents qui leur sont alloués, les données ne sont pas mieux protégées que par le passé. Pour les responsables de la sécurité informatique chargés de protéger les applications et les données dans des environnements de plus en plus dynamiques et distribués, le défi est considérable. L'adoption de modèles de développement d'applications modernes et agiles par un nombre croissant d'entreprises ne fait qu'exacerber le problème consistant à implémenter la sécurité au même rythme que l'activité, si bien que la sécurité fait souvent figure d'entrave au progrès.

Dans leur mission de sécurisation des données et des applications, le responsable de la sécurité informatique et son équipe se heurtent à deux grands types obstacles :

Les menaces non détectées et les fausses alertes

Les solutions de sécurité des terminaux déclenchent des taux élevés de fausses alertes, de sorte que l'équipe responsable des opérations de sécurité perd un temps considérable à enquêter sur des menaces fictives. Mais le risque le plus grave est de passer complètement à côté de menaces réelles.

Des environnements hautement dynamiques

Les solutions de sécurité existantes n'ont pas été conçues pour répondre à l'accélération actuelle des processus de développement et de déploiement d'applications, si bien que la sécurité ne peut plus suivre le rythme auquel les applications sont lancées ou mises à jour.

Transformer la sécurité via la virtualisation

VMware AppDefense est idéalement positionné pour résoudre ces deux problématiques. VMware AppDefense est un produit de sécurité des terminaux du Data Center qui intègre les fonctions de détection et de réponse dans la couche de virtualisation occupée par vos applications et vos données. Fondé sur VMware vSphere®, AppDefense offre trois avantages décisifs par rapport aux solutions de sécurité des terminaux existantes :

Une connaissance de première main de l'état attendu des applications : savoir ce qui convient permet de détecter à coup sûr ce qui n'est pas conforme

Postée au cœur de l'hyperviseur vSphere, la solution AppDefense sait parfaitement comment les terminaux du Data Center sont censés se comporter, et est la première informée des modifications apportées. Cette veille contextuelle lui permet de départager sans hésitation les changements légitimes des menaces réelles.

Une réaction précise et automatisée aux menaces : la bonne réponse au bon moment

Lorsqu'une menace est détectée, AppDefense peut déclencher vSphere et VMware NSX® afin d'orchestrer la réponse adaptée à cette menace sans aucune intervention manuelle. AppDefense peut notamment assurer l'exécution automatique des actions suivantes :

- Bloquer la communication de processus
- Prendre un snapshot d'un terminal pour analyse technique
- Suspendre un terminal
- Fermer un terminal

EN BREF

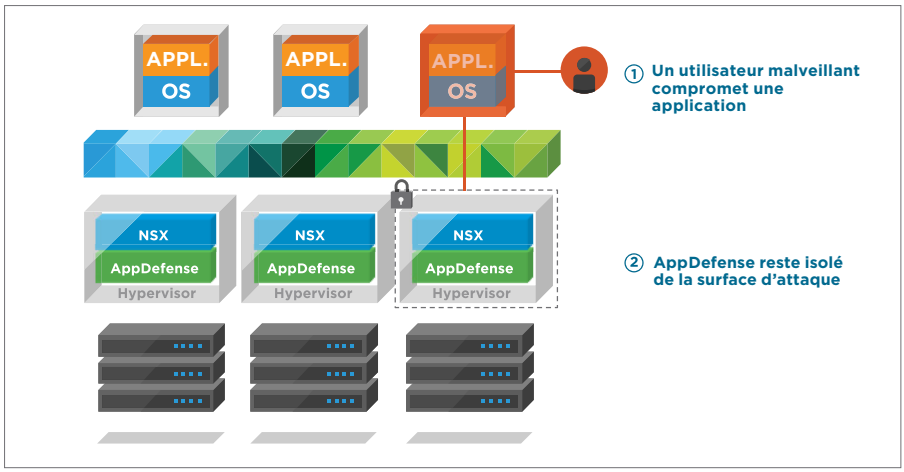
VMware AppDefense™ est une solution de sécurité des terminaux du Data Center qui protège les applications exécutées dans les environnements virtualisés. À la différence des solutions de sécurité existantes qui visent à traquer les menaces, AppDefense surveille les applications en fonction de leur état attendu (qui définit leur comportement légitime) et réagit automatiquement à tout écart pouvant indiquer une menace. Cette solution permet ainsi d'optimiser l'efficacité et l'efficience des opérations de sécurité, mais aussi de simplifier le processus d'examen du niveau de préparation de la sécurité des applications.

POINTS CLÉS

- Simplifiez la sécurité des terminaux du Data Center
- Améliorez la détection des menaces au sein du centre d'opérations de sécurité
- Automatisez la réponse aux incidents
- Rationalisez l'évaluation de la sécurité des applications

Isolation par rapport à la surface d'attaque : protéger le dispositif de protection

La première chose que font la plupart des variantes de logiciels malveillants lorsqu'elles atteignent un terminal est de désactiver l'antivirus et les autres solutions de sécurité des terminaux basées sur un agent. L'hyperviseur permet à AppDefense d'opérer depuis un emplacement protégé, si bien que sa sécurité reste garantie même si un terminal est compromis.



AppDefense en action

AppDefense est un produit de sécurité fondamental qui influe en profondeur sur la stratégie de sécurité de l'entreprise.

Alertes axées sur les applications pour le centre d'opérations de sécurité

AppDefense génère peu d'alertes, mais celles-ci sont importantes. La combinaison entre les alertes fiables générées par AppDefense et les fonctionnalités de réponse automatique permet aux administrateurs de la sécurité de se concentrer sur la détection et l'éradication des menaces dans leur environnement, plutôt que de passer au crible des données foisonnantes et d'enquêter sur des menaces inexistantes.

Transformation du processus d'évaluation du niveau de préparation de la sécurité des applications

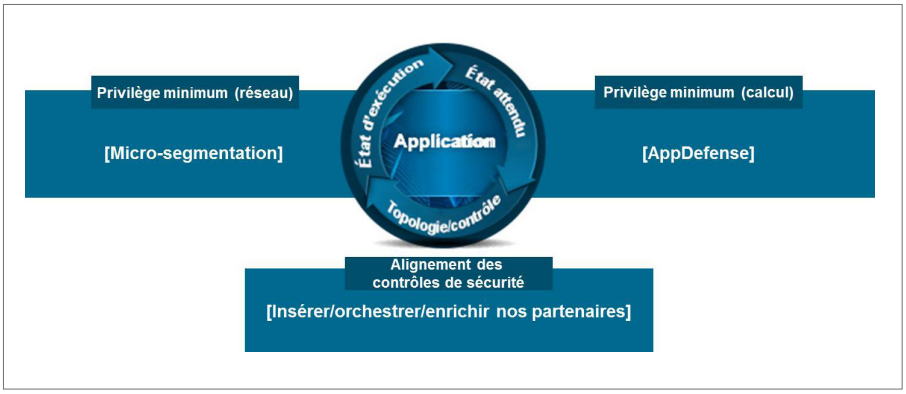
Dans les environnements de développement d'applications modernes, le lancement, la modification et la mise hors-service des applications s'effectuent à un rythme élevé. Au moment où l'équipe de sécurité apprend l'existence d'une nouvelle application, celle-ci a probablement déjà été modifiée. AppDefense crée une source fiable commune aux équipes chargées des applications et de la sécurité, ce qui rationalise le processus d'évaluation de la sécurité.

VMware et la sécurité axée sur les applications

Avec sa plate-forme de virtualisation de réseau VMware NSX et la capacité d'activer la micro-segmentation à l'échelle du Data Center, VMware a révolutionné la sécurité réseau. L'architecture de NSX intègre les services de réseau et de sécurité – tels que le pare-feu – directement dans l'hyperviseur, ce qui permet d'appliquer au réseau un modèle de sécurité basé sur le principe du privilège minimum. Résultat : l'équipe de sécurité réseau est capable d'empêcher la propagation latérale des menaces au sein de son environnement.

EN SAVOIR PLUS

Pour en savoir plus ou pour acheter VMware AppDefense, visitez le site http://www.vmware.com/fr/appdefense et testez ce produit dans le cadre de notre laboratoire d'essai en ligne.



AppDefense introduit des fonctionnalités de détection et de réponse aux menaces dans un autre domaine clé de l'infrastructure, ce qui permet d'appliquer aux terminaux du Data Center un modèle de sécurité basé sur le principe du privilège minimum. Si une menace parvient à atteindre un terminal, AppDefense la détecte immédiatement et réagit automatiquement avec précision. Ensemble, NSX et AppDefense constituent une robuste solution de sécurité pour l'infrastructure applicative et, par conséquent, pour les applications et les données qui y sont exploitées.

[1] Ponemon Institute, juin 2017, « 2017 Cost of a Data Breach Study: Global Overview »

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.com/fr