VMware vShield Endpoint

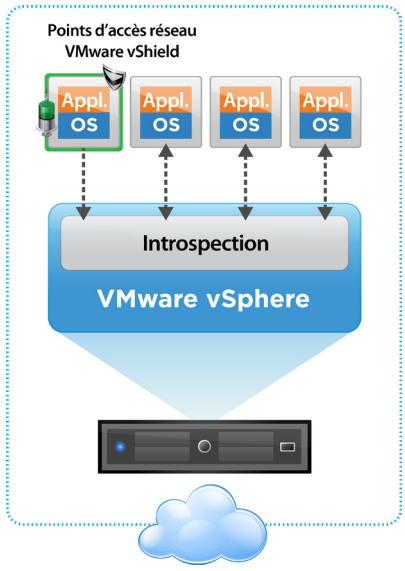
Accroître la sécurité et les performances des points limites réseau pour les datacenters virtuels

EN BREF

VMware vShield™ Endpoint renforce la sécurité des machines virtuelles tout en améliorant les performances de protection au niveau des points limites, selon différents échelons d'importance. vShield Endpoint transfère les fonctions de traitement antivirus et antimalware vers une appliance virtuelle sécurisée dédiée, fournie par les partenaires de VMware. L'objectif de cette solution est de tirer parti des investissements existants ; pour cela, elle permet à nos clients de gérer les règles appliquées aux environnements virtualisés concernant la protection contre les virus et les programmes malveillants (malware) à l'aide des mêmes interfaces que celles utilisées pour sécuriser leurs environnements physiques.

PRINCIPAUX AVANTAGES

- Amélioration des ratios de consolidation et des performances au travers de l'élimination des agents antivirus sur les machines virtuelles clientes
- Rationalisation du déploiement et du contrôle des fonctions antivirus et antimalware au sein des environnements VMware
- Amélioration de la sécurité par la consolidation des agents logiciels antivirus, afin de réduire la « surface d'attaque »
- Satisfaction des exigences de conformité et d'audit au travers de la journalisation des activités antivirus et antimalware



vShield Endpoint améliore les performances et les ratios de consolidation des fonctions antivirus et antimalware au sein des environnements virtualisés.

Présentation de vShield Endpoint

vShield Endpoint révolutionne l'approche adoptée en matière de protection des machines virtuelles clientes contre les virus et les programmes malveillants. Cette solution optimise les fonctions de sécurité au point limite réseau, telles que les fonctions antivirus, en vue d'une utilisation au sein des environnements VMware vSphere® et VMware View™.

vShield Endpoint améliore les performances en transférant les activités de détection de virus exécutées sur chaque machine virtuelle vers une appliance virtuelle sécurisée, dotée d'un moteur d'analyse antivirus et d'une base de signatures connues. Pour les fonctions antivirus et antimalware, ce type d'architecture élimine l'encombrement lié aux agents logiciels sur les machines virtuelles clientes, libère des ressources système, améliore les performances et écarte le risque de « tempêtes » d'antivirus (surcharge des ressources lors des analyses programmées et des mises à jour de signatures). Étant donné que l'appliance virtuelle sécurisée n'est jamais hors ligne, contrairement à une machine virtuelle cliente, elle peut constamment mettre à jour les signatures d'antivirus, garantissant ainsi une protection permanente pour les machines virtuelles présentes sur l'hôte. En outre, dès qu'elles sont en ligne, les nouvelles machines virtuelles (ou celles qui étaient hors ligne) bénéficient immédiatement de la même protection, avec les signatures d'antivirus les plus à jour.

vShield Endpoint accroît le niveau de sécurité au moyen d'une appliance virtuelle sécurisée, renforcée et inviolable (fournie par les partenaires de VMware) qui exploite les fonctions sûres et robustes d'introspection de l'hyperviseur de vSphere, et réduit ainsi le niveau de vulnérabilité du service antivirus et antimalware lui-même.

vShield Endpoint offre également aux sociétés partenaires de VMware des interfaces permettant d'effectuer l'analyse des fichiers, des mémoires et des processus. Les entreprises peuvent avoir recours à plusieurs solutions de sécurité simultanément ; par exemple, elles peuvent exploiter la fonction d'identification des données sensibles fournie par VMware vShield App with Data Security au sein d'une appliance virtuelle sécurisée, tout en mettant en œuvre un autre type de solution antivirus sur une autre appliance virtuelle sécurisée.

Elles peuvent, de plus, satisfaire aux exigences d'audit et prouver leur conformité par le biais d'une journalisation détaillée des activités du service antivirus ou antimalware.

Les administrateurs gèrent vShield Endpoint de façon centralisée, via la console vShield Manager fournie. Intégrée en toute transparence à VMware vCenter™ Server, cette console permet une gestion unifiée de la sécurité des datacenters virtuels.

Fonctionnement de vShield Endpoint

vShield Endpoint s'intègre directement à vSphere et repose sur trois composantes :

- Appliances virtuelles sécurisées renforcées, fournies par les partenaires de VMware
- Agent léger permettant aux machines virtuelles de se délester des événements de sécurité (inclus avec VMware Tools)
- Module hyperviseur VMware Endpoint ESX® permettant la communication entre les deux premières composantes, au niveau de la couche hyperviseur

Par exemple, dans le cas d'une solution antivirus, vShield Endpoint surveille les événements portant sur les fichiers des machines virtuelles et en informe le moteur antivirus, lequel effectue une analyse et renvoie un résultat. La solution prend en charge à la fois les analyses de fichiers en accès et à la demande (planification) lancées par le moteur antivirus dans l'appliance virtuelle sécurisée.

Si un problème doit être résolu, les administrateurs peuvent indiquer les actions correctives à effectuer à l'aide des outils de gestion antivirus et antimalware existants. vShield Endpoint gère alors ces actions au sein des machines virtuelles concernées.

Utilisation de vShield Endpoint

La console de gestion fournie par le partenaire de VMware sert à configurer et à contrôler le logiciel partenaire hébergé sur l'appliance virtuelle sécurisée. Certains partenaires de VMware fournissent une interface permettant à l'utilisateur de bénéficier de fonctions de gestion (notamment pour les règles) identiques à celles d'un logiciel hébergé sur une appliance de sécurité physique dédiée.

Le travail des administrateurs de l'infrastructure virtuelle est nettement simplifié, puisque les machines virtuelles n'ont plus d'agent antivirus à gérer. Il suffit aux administrateurs d'utiliser la console de gestion du partenaire pour administrer l'appliance virtuelle sécurisée. Par ailleurs, avec une telle approche, il n'est plus nécessaire de gérer les fréquentes mises à jour à effectuer sur chaque machine virtuelle. Pour le déploiement, VMware Tools inclut l'agent léger et le module VMware ESX assure la fonction d'introspection de l'hyperviseur.

Les administrateurs de l'infrastructure virtuelle peuvent facilement contrôler les déploiements et déterminer, par exemple, si une solution antivirus fonctionne correctement.

Fonctionnalités clés

Transfert des activités de protection contre les virus et les programmes malveillants

- vShield Endpoint améliore les performances en utilisant le module vShield Endpoint ESX pour transférer les activités d'analyse antivirus vers une appliance virtuelle sécurisée au sein de laquelle l'analyse antivirus est exécutée.
- Les tâches telles que l'analyse des fichiers, des mémoires et des processus sont transférées des machines virtuelles vers une appliance virtuelle sécurisée par le biais d'un agent client léger et du module VMware ESX fourni par le partenaire.
- L'API EPSEC (Endpoint Security) de vShield Endpoint gère la communication entre les machines virtuelles et l'appliance virtuelle sécurisée, à l'aide d'un processus d'introspection au niveau de la couche hyperviseur.
- La mise à jour du moteur antivirus et des fichiers de signatures s'effectue exclusivement au niveau de l'appliance virtuelle sécurisée, mais les règles peuvent être appliquées à l'ensemble des machines virtuelles d'un hôte vSphere.

Actions correctives

- vShield Endpoint met en application les règles antivirus qui déterminent si un fichier malveillant doit être supprimé, mis en quarantaine ou autre.
- Un agent léger gère les actions correctives sur les fichiers au sein de la machine virtuelle.

Intégrations de partenaires

- L'API EPSEC permet aux partenaires de VMware dans le domaine de l'analyse antivirus d'intégrer leur solution à vShield Endpoint. Pour cela, elle fournit une fonction d'introspection concernant les activités sur les fichiers de l'hyperviseur. Cette API prend en charge les principales fonctions antivirus.

vShield Manager, gestion des règles et automatisation

- vShield Manager permet un déploiement et une configuration complète de vShield Endpoint.
- Des API REST (Representational State Transfer) permettent une intégration automatisée et personnalisée des fonctionnalités vShield Endpoint au sein des solutions.
- Des rapports de surveillance sont générés.
- vShield Manager peut être exploité en tant que plug-in de vCenter.

Journalisation et audit

- La journalisation des événements repose sur le format standard syslog.

Versions prises en charge

Pour plus d'informations sur les versions prises en charge des environnements vSphere, VMware ESX et View, consultez la page http://vmware.com/fr/products.

Produits associés

Font également partie de la famille de produits de sécurité vShield : VMware vShield Edge pour la sécurité des périmètres ; vShield App with Data Security pour protéger les applications contre les attaques réseau et identifier les données sensibles ; vShield Manager ; et, enfin, vShield Bundle, qui inclut tous les produits.

En savoir plus

Pour acheter des produits VMware ou obtenir des informations sur ceux-ci, appelez le numéro international 1-650-475-5000, visitez le site Web http://www.vmware.com/fr/products ourecherchez un revendeur agréé en ligne. Pour plus d'informations sur les spécifications des versions du produit et les configurations système requises, consultez le Guide d'administration de VMware vShield : http://www.vmware.com/pdf/vshield_41_admin.pdf.

Pour plus d'informations sur les produits vShield, consultez le site Web : http://vmware.com/fr/products.

VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc. 100-101 Terrasse Boieldieu 92042 Paris La Défense France Tél. : +33 1 47 62 79 00 Fax : +33 1 47 62 79 01 www.vmware.com/fr