# VMware vShield App

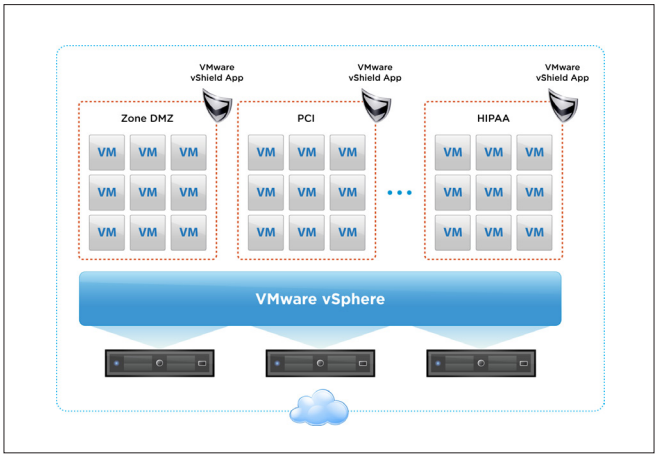
Protéger les applications contre les attaques réseau

## EN BREF

Appartenant à la gamme VMware vShield de produits de sécurité de la virtualisation, VMware vShield App protège les applications au sein du datacenter virtuel contre les attaques réseau. vShield App assure une visibilité étendue sur les communications réseau entre les machines virtuelles et permet d'appliquer des règles précises en utilisant des groupes de sécurité. Cette solution permet également d'éviter la prolifération de matériel et de règles inhérente aux mesures classiques, offrant un moyen économique de dépasser les limites de la sécurité physique.

## AVANTAGES

- Visibilité et contrôle améliorés des communications réseau entre les machines virtuelles.
- Absence de matériel et de VLAN dédiés pour séparer les groupes de sécurité les uns des autres.
- Meilleure utilisation des ressources matérielles et sécurité élevée.
- Conformité simplifiée par la journalisation exhaustive de l'activité réseau de l'ensemble des VM.




VMware vShield App permet d'appliquer des règles précises en utilisant des groupes de sécurité.

# Présentation de VMware vShield App

VMware vShield App est un pare-feu de type hyperviseur orienté applications pour les datacenters virtuels. S'intégrant directement à VMware vSphere™, vShield App assure la protection contre les menaces réseau internes et limite le risque de violation des règles dans le périmètre de sécurité de l'entreprise. Cette solution de pare-feu de protection orientée applications effectue une vérification poussée des paquets et contrôle les connexions en fonction des adresses IP sources et cibles.

En accélérant la création de groupes de sécurité opérationnels et en assurant la surveillance du flux, vShield simplifie le contrôle des règles. Il permet ainsi d'analyser le trafic réseau des machines virtuelles et d'appliquer de façon dynamique les règles des groupes de sécurité. Les administrateurs gèrent vShield App de façon centralisée, via la console vShield Manager fournie. Intégrée en toute transparence à VMware vCenter™ Server, cette console facilite une gestion unifiée de la sécurité des datacenters virtuels.

# Fonctionnement de VMware vShield App

vShield App s'installe sur tous les hôtes vSphere pour en contrôler et en surveiller le trafic réseau, même les paquets qui ne transitent jamais par une carte réseau physique. vShield App peut créer et appliquer des règles basées sur les groupes de sécurité opérationnels que définit l'administrateur plutôt que sur les limites physiques ou des hypothèses statiques sur les déploiements d'applications.

L'interface centralisée de vShield App utilise vCenter Server pour appliquer ces règles de façon uniforme sur plusieurs hôtes vSphere dans le datacenter virtuel.

# Utilisation de VMware vShield App

- **Suppression des zones cachées** : vShield App aide les administrateurs à définir et appliquer des règles précises pour l'ensemble du trafic passant par une carte réseau virtuelle, ce qui permet d'améliorer la visibilité sur le trafic interne du datacenter virtuel tout en contribuant à éviter le passage par des pare-feu physiques.

- **Protection garantie au fil des modifications** : avec vShield App, la topologie réseau peut changer sans incidence sur la sécurité des applications, car la protection par pare-feu des machines virtuelles est assurée tout le temps de leur migration d'un hôte à l'autre.
- **Gestion efficace des règles dynamiques** : vShield App permet de simplifier la définition des règles et offre aux administrateurs un contexte riche pour créer et améliorer des règles de pare-feu internes à mesure que les besoins de l'entreprise évoluent.
- **Réduire le risque d'attaques par botnets** : vShield App aide les administrateurs de la sécurité à prévenir les attaques réseau, notamment les attaques par botnets, en attribuant dynamiquement des ports aux applications fiables.
- **Contrôle des accès aux ressources partagées** : vShield App permet aux administrateurs de la sécurité de limiter l'accès aux services partagés tels que le stockage et la sauvegarde sur les hôtes vSphere, d'après l' adresse IP.
- **Mise en conformité informatique accélérée** : vShield App renforce la visibilité et le contrôle sur la sécurité réseau des machines virtuelles en fournissant les outils de journalisation et d'audit nécessaires pour respecter les règles internes et les directives officielles.

# Fonctionnalités clés

### Pare-feu de niveau hyperviseur

- Contrôle des connexions entrantes/sortantes au niveau de la carte réseau virtuelle par vérification de l'hyperviseur, avec prise en charge des machines virtuelles (VM) multi-hébergées
- Application possible en fonction du réseau, du port, du type de protocole (TCP, UDP), du type d'application
- Protection dynamique pendant la migration des VM
- Pare-feu IP dynamique et passerelle intervenant au niveau application pour une large gamme de protocoles, dont Oracle, Sun Remote Procedure Call (RPC), Microsoft RPC, LDAP et SMTP. La liste complète des protocoles pris en charge figure dans le Guide d'administration de VMware vShield App

### Surveillance du flux

- Possibilité d'observer l'activité réseau entre les VM pour faciliter la création et l'amélioration des règles de pare-feu, identifier les attaques par botnets et sécuriser les processus métier par le reporting détaillé du trafic des applications (applications, sessions, octets)

### Groupes de sécurité

- Regroupements opérationnels de machines virtuelles définis par l'administrateur en fonction de leurs cartes réseau virtuelles

### Gestion des règles

- Gestion complète via vShield Manager. De nombreuses fonctions sont également accessibles via l'interface de vCenter Server
- Application des règles aux groupes de sécurité, aux regroupements vCenter et au tuple TCP à 5 éléments (adresse IP source, adresse IP cible, port source, port cible, protocole)
- Interface programmable pour la gestion et l'application des règles avec les API REST
- Prise en charge de l'intégration aux outils de gestion de la sécurité informatique de l'entreprise

### Journalisation et audit

- Format syslog standard
- Accessible via les API REST et vShield Manager
- Activation/désactivation de la journalisation pour les pare-feu au niveau des règles définie par l'administrateur

# En savoir plus

Pour acheter les produits VMware ou obtenir des informations sur ceux-ci, appelez le 01 47 62 79 00, visitez le site Web www.vmware.com/fr/products ou recherchez un revendeur agréé en ligne. Pour connaître les caractéristiques du produit et la configuration système requise, consultez le Guide d'administration de VMware vShield App.

**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