



VMware vShield

Sécurité orientée virtualisation pour le cloud

BROCHURE

En bref

Pour les entreprises qui souhaitent bénéficier des avantages du Cloud Computing sans risque pour la sécurité, le contrôle ou la conformité, la gamme de solutions de sécurité VMware vShield assure une protection complète des datacenters virtuels et des environnements de Cloud Computing. vShield permet aux clients de renforcer la sécurité de leurs applications et données, d'améliorer la visibilité, le contrôle et d'accélérer le rythme de la mise en conformité informatique à l'échelle globale de leur entreprise.

Défis soulevés par la sécurité au niveau du cloud

De nombreuses entreprises considèrent les solutions et services de Cloud Computing comme un moyen d'améliorer la réactivité et de réduire les coûts de possession et d'exploitation de leur environnement informatique. Toutefois, toutes les études récentes sur le Cloud Computing réalisées auprès des clients révèlent que la sécurité, le contrôle et la conformité représentent les principaux obstacles à son adoption. Ils recherchent par conséquent des solutions leur permettant de tirer avantage du Cloud Computing sans compromettre la sécurité, le contrôle et la gestion de la conformité.

Problèmes de sécurité liés au Cloud Computing

- **Sécurité des applications et des données** - Les solutions de Cloud Computing actuelles ne proposent pas les outils avancés dont les entreprises ont besoin pour sécuriser leurs applications ou empêcher les pertes et les fuites de données.
- **Visibilité et contrôle** - Les solutions de Cloud Computing actuelles n'assurent pas la visibilité dont les responsables de la sécurité ont besoin pour contrôler les règles de sécurité pendant toute la durée des cycles de vie, de la définition à la mise en œuvre, en passant par l'application et l'audit.
- **Gestion de la conformité** - La plupart des entreprises disposent déjà d'outils, de technologies et de processus pour la gestion de la conformité réglementaire et recherchent des solutions de Cloud Computing qui ne constituent pas un obstacle dans leur démarche.

Protéger le cloud avec VMware vShield

Non seulement la virtualisation s'avère indispensable pour la transition des applications existantes vers la nouvelle infrastructure de Cloud Computing, mais elle constitue aussi un vecteur de sécurité essentiel pour ce type d'environnement. En tant que leader mondial de la virtualisation, VMware fournit des solutions fiables et sécurisées depuis plus d'une décennie.

Aujourd'hui, avec la nouvelle gamme VMware vShield de produits de sécurité pour datacenters virtuels et clouds privés, VMware aide ses clients à tirer le maximum du Cloud Computing.

Principaux avantages

Dépasser les limites de la sécurité physique

vShield assure une sécurité évolutive : les machines virtuelles sont protégées durant leur migration d'un hôte à l'autre, ce qui permet aux clients de les exploiter en toute sécurité dans des environnements de cloud dynamiques. Cette stratégie permet également de garantir le fonctionnement optimal des applications au sein des environnements de Cloud Computing tout en préservant la fiabilité et la segmentation réseau des utilisateurs et des données sensibles.

Améliorer et simplifier la gestion de la sécurité dans une infrastructure unique

vShield offre une infrastructure complète unique pour la sécurisation des datacenters virtuels et des environnements de Cloud Computing à tous les niveaux : hôte, réseau, applications, données et points d'accès réseau. vShield garantit un niveau de fiabilité et de segmentation adéquat pour tous les déploiements d'applications sur les clouds VMware. vShield fournit également un ensemble complet de fonctionnalités pour l'introspection et la protection des hôtes et des machines virtuelles. Ces fonctionnalités, conjuguées aux solutions sécurisées des partenaires de VMware, garantissent une protection optimale des applications et des données dans les clouds VMware.

Réduire la complexité et supprimer les congestions

vShield contribue à réduire la complexité liée à la sécurité de la virtualisation en permettant aux clients de regrouper leurs infrastructures de sécurité et d'éviter la prolifération des agents logiciels, règles de sécurité, appliances dédiées et solutions d'isolation. vShield élimine également les congestions associées aux agents de sécurité sur les points d'accès en supprimant le besoin d'installer un antivirus sur chaque machine virtuelle.

Améliorer la visibilité et accélérer la mise en conformité

vShield exploite les fonctionnalités exclusives d'introspection de la plate-forme VMware vSphere™ pour permettre l'identification précise et efficace de problèmes difficiles à détecter. vShield offre également des options de contrôle, telles que la surveillance de l'intégrité des fichiers, la protection contre les outils de piratage et la prévention des fuites

de données. Il permet en outre d'accélérer la mise en conformité grâce à une journalisation détaillée qui peut être élargie aux solutions d'audit et de gestion de la conformité informatique existantes.

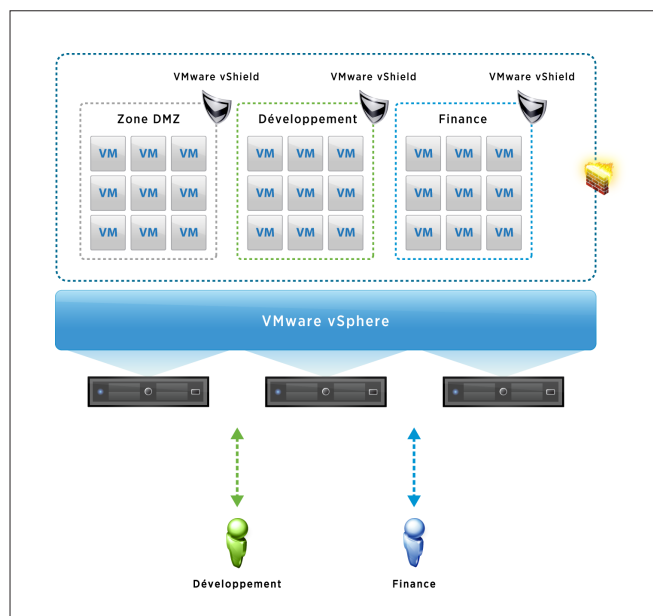
Exploiter les solutions de sécurité existantes

vShield fonctionne en toute transparence avec les mesures de sécurité informatique existantes des entreprises grâce à des API REST qui permettent l'intégration personnalisée de ses fonctions à des solutions de sécurité tierces. En outre, vShield comprend une API de sécurité pour les points d'accès réseau qui s'intègre aux solutions antivirus et antimalware existantes. Cette API interagit également avec des solutions de sécurité plus globales pour la gestion des informations et des événements de sécurité, la protection contre les fuites de données, la gestion des modifications et des configurations et l'audit.

Utiliser VMware vShield

Sécuriser les applications stratégiques

Les solutions vShield simplifient la prise en charge d'applications représentant différents niveaux de confiance dans le même datacenter virtuel (production et développement, finance et ventes, applications classifiées et non classifiées, etc.). vShield intègre un pare-feu au niveau de l'hyperviseur qui garantit la fiabilité et la segmentation adéquates pour tous les déploiements d'applications.

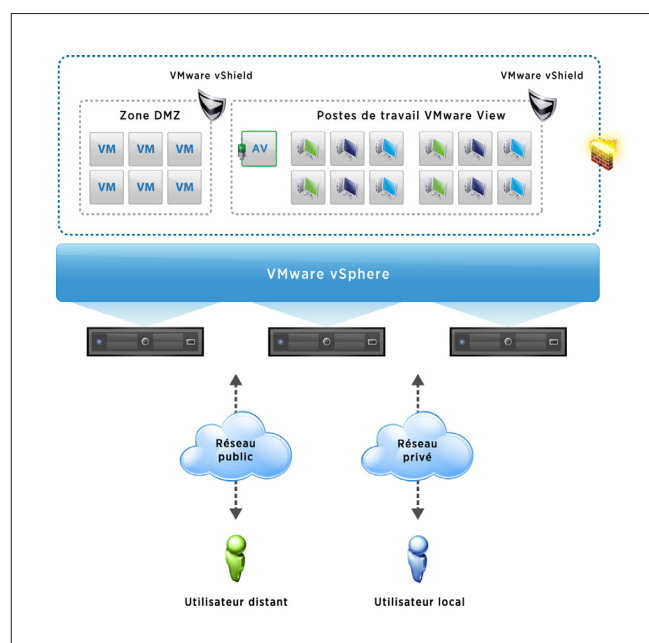


VMware vShield permet aux clients de créer des groupes de sécurité fonctionnels et de protéger les applications vitales contre les menaces du réseau.

Sécuriser les déploiements de postes de travail virtuels

Intégré à VMware View™, vShield offre une protection antivirus et antimalware plus efficace pour les points d'accès réseau et applications virtuels en déléguant les machines virtuelles de ces fonctions au profit d'une seule machine sécurisée qui protège l'hôte et l'ensemble de ses machines virtuelles. Cette méthode simplifie la gestion de la sécurité et offre une protection renforcée contre les attaques de virus, les problèmes de performances et les attaques de réseaux de bots (botnet).

vShield aide également les entreprises à mettre en place des périmètres de sécurité logiques autour des infrastructures de postes de travail virtuels en isolant entièrement le réseau et en proposant un ensemble de services de passerelle, tels que les pare-feu, VPN et DHCP.



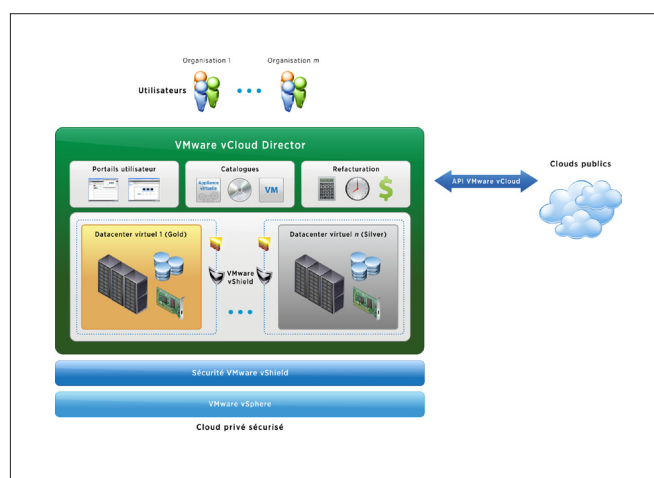
Avec VMware vShield, les programmes antivirus et antimalware assurent une sécurité optimale pour les environnements virtualisés grâce à une machine virtuelle de sécurité (fournie par les partenaires de VMware).

Réseaux extranet des partenaires

vShield permet aux entreprises d'étendre leurs réseaux et applications aux succursales, aux domiciles de leurs employés et aux sites des partenaires commerciaux grâce à des services de VPN intersites qui simplifient le provisionnement et les tâches administratives et améliorent l'évolutivité. L'ensemble du trafic entre les sites est crypté via le protocole IPsec afin de garantir la confidentialité et l'intégrité de l'ensemble des communications.

Sécuriser les environnements à utilisateurs multiples

Les solutions vShield facilitent la tâche des entreprises et fournisseurs de services de cloud pour gérer des environnements informatiques multi-utilisateurs et garantissent le partage sécurisé des ressources réseau en créant des périmètres de sécurité logiques qui isolent complètement le réseau des datacenters virtuels. vShield garantit également un contrôle et une visibilité granulaires sur le trafic des passerelles du réseau, en combinaison avec des services VPN pour protéger la confidentialité et l'intégrité des communications entre les datacenters virtuels.



Intégré à VMware vCloud Director, VMware vShield garantit la sécurité et l'isolation du réseau dans les clouds privés multi-utilisateurs.

Solutions vShield

VMware vShield App

VMware vShield App protège les applications du datacenter virtuel contre les menaces du réseau. vShield App permet de créer et de gérer des règles d'entreprise qui s'adaptent aux environnements de Cloud Computing dynamiques. Il offre en outre une entière visibilité sur les communications réseau entre les machines virtuelles et permet l'application de règles précises grâce à des groupes de sécurité.

VMware vShield Edge

Solution de passerelle réseau, vShield Edge protège la périphérie du datacenter virtuel grâce au protocole DHCP, à la traduction d'adresse réseau, au pare-feu, à l'équilibrage des charges, au VPN intersites, à l'isolation des groupes de ports et à d'autres fonctionnalités qui aident les entreprises à maintenir une segmentation adéquate entre les différentes unités organisationnelles.

VMware vShield Endpoint

vShield Endpoint offre une protection antivirus et antimalware sur l'hôte qui réduit la latence en matière de performances et évite l'utilisation de différents agents de sécurité sur chaque machine virtuelle, simplifiant ainsi la gestion de la sécurité tout en minimisant le risque d'infection par des logiciels malveillants.

VMware vShield Manager

Fourni avec tous les produits vShield, vShield Manager offre un point de contrôle unique pour la gestion, le déploiement, la génération de rapports, la journalisation et l'intégration de services de sécurité tiers. Utilisé de concert avec vCenter Server, vShield Manager permet également un contrôle d'accès basé sur les rôles, ainsi que la délégation administrative au sein d'une infrastructure unifiée pour gérer la sécurité des opérations de virtualisation.

VMware vShield Zones

Fourni avec vSphere, VMware vShield Zones offre une protection de base contre les menaces du réseau dans les datacenters virtuels, avec un pare-feu d'application et une gestion des règles basée sur des zones définies par l'administrateur à l'aide des informations sur le trafic (adresse IP source, port de destination, etc.).

Procédure d'achat

vShield App, vShield Edge et vShield Endpoint sont disponibles à l'achat séparément. vShield Manager est inclus dans les trois solutions. VMware vShield Zones est disponible sous forme de module intégré à VMware vSphere.

Services et support

VMware propose des contrats de support et d'abonnement (SnS) de type Basic et Production à tous les clients VMware vShield. Le support des solutions antivirus et antimalware tierces qui exploitent VMware vShield Endpoint est assuré par les fournisseurs de ces solutions.

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 obtenir le détail des spécifications et de la configuration système requise, reportez-vous à la documentation fournie avec VMware vShield.

