KASPERSKY SECURITY FOR VIRTUALIZATION ET VMWARE NSX

PROTECTION SUPÉRIEURE POUR LES SOFTWARE-DEFINED DATACENTERS

Les données représentent le bien le plus précieux de votre entreprise. Donc, la façon de les stocker et l'endroit où les données sont conservées, traitées et transmises sont essentiels, non seulement pour parvenir à un meilleur avantage concurrentiel, mais aussi pour augmenter l'efficacité opérationnelle et maintenir la continuité de l'activité.

Il existe de nombreuses solutions de traitement, de stockage et de mise en réseau de données. Cependant, les solutions de mise en réseau peuvent être complexes, sans aucune flexibilité et donc trop souvent limitées par la plate-forme du matériel informatique à laquelle elles sont intégrées. En conséquence, cela freine l'agilité de votre data center ainsi que votre capacité à satisfaire rapidement des exigences professionnelles changeantes.

Ensemble, VMware® et Kaspersky Lab traitent ces problèmes au moyen d'une solution commune, élaborée autour d'un software-defined datacenter hautement efficace et doté de capacités de sécurité avancées, qui assurent une protection de haut niveau contre les menaces internes ou externes.

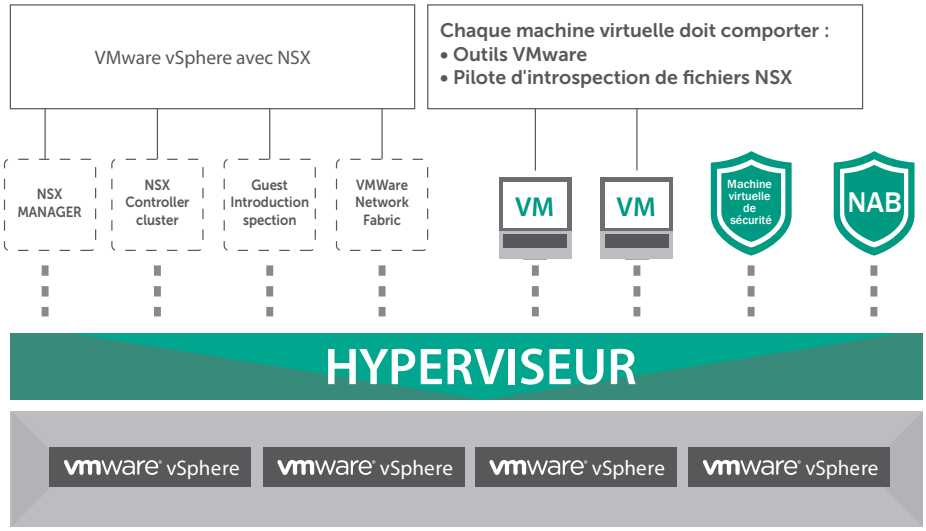
SERVICES VMWARE NSX INTÉGRÉS	
Pare-feu distribué	Réseaux virtuels (VXLAN)
Surveillance de l'activité du serveur	VPN (IPSec, SSL L2VPN)
KASPERSKY SECURITY FOR VIRTUALIZATION	
Protection contre les programmes malveillants	Prévention et détection des intrusions (IDS/IPS) sur un réseau virtuel
Automatisation de la sécurité	Intégration des politiques de sécurité
Intégration des balises de sécurité	Analyse complète de l'infrastructure, même sur les machines virtuelles déconnectées

Kaspersky Security for Virtualization Agentless a été spécifiquement développé pour protéger les data software-defined datacenters reposant sur VMware vSphere avec technologies NSX. Notre solution de sécurité intègre des fonctionnalités avancées qui n'affectent quasiment pas les performances de la plate-forme. Vous pouvez ainsi profiter d'une solution de protection contre les programmes malveillants leader du secteur tout en maintenant des taux de consolidation élevés.

FONCTIONNEMENT DE L'INTÉGRATION À LA PLATE-FORME

VMware NSX® reproduit le réseau de votre data center en utilisant un modèle géré par logiciel, vous permettant de travailler avec différents groupes de ressources de réseau, créant ou reconfigurant de façon dynamique toute votre topologie de réseau en quelques secondes, à l'aide d'une approche de sécurité « Confiance zéro ».

L'intégration solide entre la plate-forme VMware NSX et Kaspersky Security for Virtualization offre une protection automatisée pour chaque machine virtuelle et chaque réseau virtualisé contre les menaces les plus avancées. Une protection constante et générale est assurée, sans nécessiter l'installation d'un agent de sécurité dans une machine virtuelle et sans provoquer d'impact sur les ressources de votre plate-forme virtualisée.



SVM

MACHINE VIRTUELLE DE SÉCURITÉ
- Intégration native à VMware NSX
- Prise en charge de NSX et de vShield Endpoint
- Faible impact sur les ressources système
- Analyse des machines en ligne et hors ligne

NAB

PRÉVENTION DES INTRUSIONS
- Puissante protection des réseaux
- Contrôle du trafic Web avec analyse des URL
- Moteur d'analyse heuristique pour protéger les applications
- Protection immédiate de toute l'infrastructure

L'intégration native entre votre plate-forme de virtualisation et son dispositif de sécurité permet à votre software-defined datacenter de réagir en temps réel à n'importe quel incident de sécurité sur l'ensemble de votre infrastructure.

CONÇUE SPÉCIFIQUEMENT POUR LA SÉCURITÉ DES ENVIRONNEMENTS VMWARE NSX

- Le moteur de protection contre les programmes malveillants le plus récompensé identifie et bloque les cybermenaces connues, inconnues et même « zero-day ».
- Le déploiement automatisé pour VMware NSX permet à la SVM (Security Virtual Machine) d'apparaître automatiquement sur l'hyperviseur, en fonction des exigences des machines virtuelles protégées abritées par cet hôte.
- L'intégration des politiques de sécurité de permet l'envoi fonctionnalités de sécurité précises vers chaque machine virtuelle, comme défini dans vos politiques d'entreprise, en fonction du rôle individuel de chaque machine.
- L'intégration des balises de sécurité NSX permet à votre software-defined datacenter de réagir en temps réel aux incidents de sécurité, en reconfigurant automatiquement l'ensemble de l'infrastructure virtuelle si nécessaire.
- La défense proactive contre les menaces avancées est fournie par le réseau basé dans le Cloud Kaspersky Security Network.
- La prise en charge simultanée de NSX et vShield Endpoint garantit que vos stratégies informatiques et de sécurité sont entièrement adaptées aux besoins de votre entreprise.

KASPERSKY

SÉCURITÉ ET SURVEILLANCE AUTOMATISÉES

- L'analyse complète de l'infrastructure protège toutes les machines virtuelles, en ligne ou hors ligne, pour renforcer encore plus la sécurité sur toute votre infrastructure.
- L'analyse standard de toutes les machines virtuelles peut être programmée à l'avance à un niveau granulaire, afin d'organiser les tâches de sécurité selon vos besoins.
- L'auto-protection et la surveillance avancée reposant sur le protocole SNMP garantissent que les SVM sont opérationnelles immédiatement et fournissent des informations exhaustives aux outils de surveillance tiers pour renforcer le contrôle.
- La protection avancée n'est jamais interrompue, même lorsqu'une charge de travail est déplacée d'un hôte à un autre ; les fonctionnalités de VMware vMotion et Disaster Recovery sont entièrement prises en charge.
- L'intégration native à VMware vCenter Server et à NSX Manager permet de toujours communiquer les éventuels changements au niveau de l'infrastructure à votre système de sécurité.

LE JUSTE ÉQUILIBRE ENTRE PROTECTION ET PERFORMANCES

- Le moteur de protection primé contre les programmes malveillants permet de délocaliser les tâches d'analyse des fichiers d'une machine virtuelle vers une SVM dédiée pour plus d'efficacité.
- La prévention et détection des intrusions (IDS/IPS) sur un réseau virtuel fonctionne en mode sans agent pour protéger l'ensemble de votre infrastructure virtualisée des menaces basées sur le réseau.
- L'optimisation fondée sur le cache s'assure que les fichiers récemment analysés ne sont pas à nouveau pris en compte lors de l'analyse standard.
- Efficace en termes de ressources, notre solution de sécurité améliore les performances et réduit la charge imposée à votre infrastructure informatique.

FIABILITÉ ET SIMPLICITÉ DE GESTION RENFORCÉES

- Une console d'administration unique pour les appareils virtuels, physiques et mobiles vous permet d'imposer des politiques de sécurité cohérentes sur l'ensemble de votre infrastructure informatique.
- Le déploiement sans indisponibilité signifie qu'il n'est pas nécessaire de redémarrer les machines virtuelles ou de placer l'hôte en mode « maintenance ».
- L'orchestration intelligente des tâches d'analyse et l'automatisation éliminent les pics de consommation au niveau des ressources de l'hyperviseur afin de préserver l'efficacité globale de la plate-forme.
- Les rapports et la surveillance dotés de nombreuses fonctionnalités facilitent la gestion et le contrôle de la sécurité dans l'ensemble de votre organisation.

Le résultat est un environnement d'entreprise virtualisé flexible qui offre des performances exceptionnelles ainsi qu'une sécurité de premier plan.

SÉCURITÉ OPTIMALE POUR VOTRE SOFTWARE-DEFINED DATACENTER

Les infrastructures, qu'elles soient virtuelles ou physiques, sont confrontées aux mêmes menaces de sécurité, les cybercriminels ne faisant pas la différence. Vous ne pouvez pas vous permettre de faire des compromis sur la sécurité. Ni sur la performance.

1 LES CYBERMENACES SONT EN PASSE DE DEVENIR UN LOINTAIN SOUVENIR

Kaspersky Security for Virtualization, reposant sur le moteur de sécurité le plus primé du secteur, permet de lutter contre les menaces et les vulnérabilités les plus avancées sur l'ensemble de votre parc informatique virtualisé. Notre solution de sécurité a été spécialement conçue pour exploiter les avantages technologiques qu'offrent les plates-formes de virtualisation, assurant ainsi une sécurité puissante avec une rapidité et une efficacité optimales.

2 CONÇUE ET OPTIMISÉE POUR LA PLATE-FORME VMWARE NSX

Grâce à l'intégration native de notre solution sans agent à la plate-forme VMware NSX, votre infrastructure virtuelle est tout simplement plus performante et rentable. Désormais, votre plate-forme VMware vSphere avec infrastructure NSX et ses couches de sécurité fonctionnent de concert. Vous bénéficiez ainsi de nouveaux niveaux d'automatisation et de sécurité basée sur les politiques, notamment d'opérations améliorées grâce à la protection automatisée et renforcée par des fonctionnalités de sécurité granulaires, disponibles rapidement grâce à l'intégration des politiques et balises de sécurité.

3 VISIBILITÉ ET FACILITÉ D'ADMINISTRATION AU NIVEAU DE L'ENTREPRISE

Une console d'administration unique permet à votre équipe informatique de gérer de manière centralisée la sécurité de l'ensemble de vos machines virtuelles et des autres produits de protection de Kaspersky Lab fonctionnant sur votre infrastructure physique et vos appareils mobiles. En facilitant la gestion des environnements hybrides (combinaison de plates-formes virtualisées, physiques et mobiles) par votre équipe, Kaspersky Lab vous aide à déployer les projets de virtualisation à votre propre rythme, tout en réduisant la pression sur les ressources informatiques et le risque d'erreurs humaines.

Kaspersky Security for Virtualization assure les fonctionnalités de sécurité les plus avancées pour les environnements d'entreprise hybrides reposant sur la plate-forme VMware NSX, tout en conservant une efficacité optimale sans influer sur les performances du système. Dotée d'une architecture virtualisée, la solution de sécurité de Kaspersky Lab offre un ensemble complet de technologies de protection qui peuvent être facilement intégrées et fonctionner de pair avec l'infrastructure informatique au niveau central. Les infrastructures hybrides bénéficient d'avantages supplémentaires en travaillant de concert avec la solution Kaspersky Security for Virtualization.

Plus d'informations sur : http://www.kaspersky.fr/enterprise-security/data-center

KASPERSKY lab