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 avancée, qui assure 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 des intrusions (IPS)
Intégration des politiques de sécurité	Intégration des balises de sécurité
Déploiement automatisé	... une sécurité multi-niveaux pour les software-defined datacenters

Kaspersky Lab propose une large gamme de solutions de sécurité pour les entreprises. Pour votre data center, il est essentiel de choisir une solution de sécurité qui s'intègre aux autres technologies tout en maintenant une efficacité optimale et en préservant la performance des systèmes.

DESCRIPTION

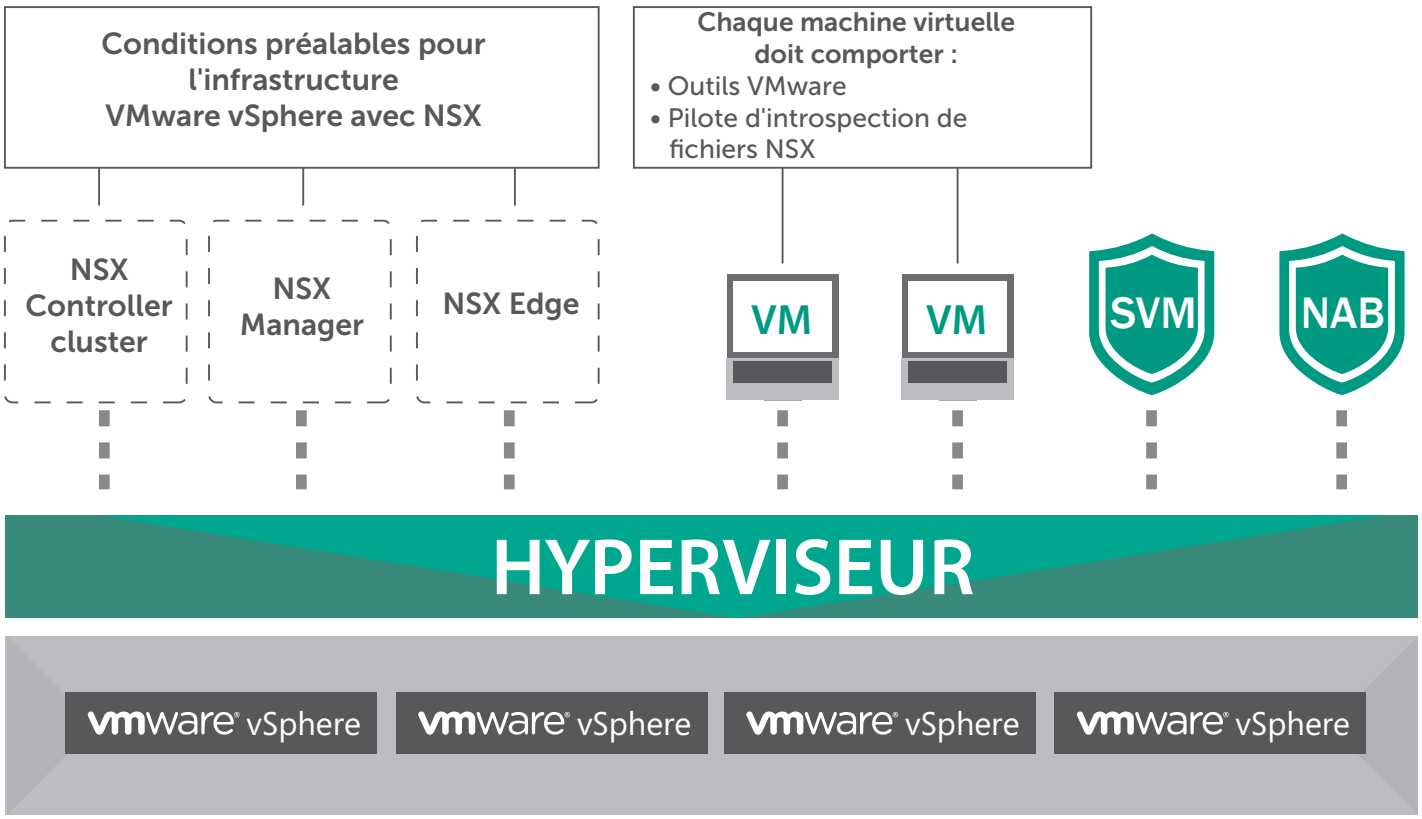
VMware NSX® reproduit le réseau de votre data center en utilisant un modèle géré par logiciel, vous permettant de travailler avec différents groupes de ressources de réseau, créant ou reconfigurant de façon dynamique toute votre topologie de réseau en quelques secondes, à l'aide d'une approche de sécurité « 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, sans impact sur la performance de la plate-forme de virtualisation.

Ensemble, Kaspersky Lab et VMware offrent une base solide et sécurisée pour les software-defined datacenters de toute taille, sans impact sur l'efficacité ou la performance.

INTÉGRATION À LA PLATE-FORME

L'intégration de Kaspersky Security for Virtualization à votre plate-forme VMware NSX permet une protection optimale de l'infrastructure de tout votre software-defined datacenter. 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.



MACHINE VIRTUELLE DE SÉCURITÉ
- Protection contre les programmes malveillants pour chaque machine virtuelle
- Aucun agent (« lourd ») traditionnel sur la machine virtuelle
- Préserve l'efficacité et les performances

PRÉVENTION DES INTRUSIONS
- Prévention des intrusions avancée (IPS)
- Protection du trafic Web et URL
- Analyseur de réseau heuristique

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

PROTECTION COMPLÈTE DE L'INFRASTRUCTURE AVEC KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization élargit les capacités de sécurité de la plate-forme VMware, en introduisant des niveaux avancés de protection contre les programmes malveillants et de protection de réseau.

PROTECTION PERMANENTE

- Protection contre les programmes malveillants en temps réel pour tous vos serveurs virtuels et ordinateurs de bureau.
- L'IDS/IPS virtualisé performant reconnaît et bloque des menaces de réseau avancées, connues et inconnues.
- Le déploiement de la solution sans interruption vous permet d'exécuter et de protéger constamment les charges de travail essentielles à votre activité.

PERFORMANCE

- Sécurité conçue spécialement pour la virtualisation, permettant d'économiser des ressources d'hyperviseur précieuses pour conserver des ratios de consolidation élevés.
- Une machine virtuelle de sécurité dédiée (SVM) installée sur un hyperviseur permet d'alléger les tâches d'analyse, afin de minimiser l'incidence sur le fonctionnement et les performances de la machine virtuelle.
- Notre conception innovante et brevetée utilise une optimisation basée sur le cache, afin de réduire autant que possible les ressources utilisées, pour bénéficier d'une densité maximale.

EFFICACITÉ ET PROTECTION

- Les blitz de mise à jour et d'analyse, ainsi que les fenêtres de vulnérabilité ou les clichés instantanés sont éliminés.
- La prévention des intrusions (Network Attack Blocker), un appareil IDS/IPS compact mais puissant, reconnaît et bloque les attaques réseau, à la fois connues et inconnues, y compris celles qui exploitent des failles spécifiques.
- L'intégration solide avec VMware NSX permet à la solution de suivre de façon ininterrompue les changements de topologie de l'infrastructure et du réseau, sans restriction.
- Les capacités de sécurité proactive protègent l'ensemble de votre data center contre des menaces émergentes, grâce à l'intégration au réseau Kaspersky Security Network (KSN) basé dans le Cloud.

FLEXIBILITÉ ET VISIBILITÉ

- Une console unique permet de gérer simultanément toutes les machines virtuelles et physiques, les ordinateurs de bureau virtualisés, ainsi que les appareils mobiles.
- Les rapports et la surveillance dotés de nombreuses fonctionnalités facilitent la gestion et le contrôle de la sécurité au sein de votre organisation.
- Options de licences flexibles : selon le nombre de machines virtuelles (ordinateurs de bureau ou serveurs) ou de ressources matérielles (nombre de cœurs), sans tenir compte de la topologie du réseau.

TECHNOLOGIES D'AUTODÉFENSE

- La machine virtuelle de sécurité surveille constamment et de façon autonome sa propre activité pour s'assurer que le moteur d'analyse est disponible et prêt à gérer des tâches de protection contre les programmes malveillants à tout moment.
- La communication entre les composants de votre solution de sécurité et les nœuds de l'infrastructure virtualisée utilisent des certificats SSL pour empêcher les cybercriminels de tirer parti des vulnérabilités de l'infrastructure.

KASPERSKY

SÉCURITÉ OPTIMALE POUR VOTE 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.

Travaillant de pair, VMware NSX et Kaspersky Security for Virtualization offrent désormais :

- Des niveaux de sécurité renforcés pour les software-defined datacenters et leurs charges de travail, activités appuyées par un pare-feu distribué et des capacités de micro-segmentation.
- Protection permanente pour toute votre infrastructure contre les menaces de programme malveillant, de ransomware, d'attaques réseau et même d'attaques « zero-day », sans impact sur la performance ou la productivité des systèmes.
- Votre data center entièrement protégé contre les menaces réseau, grâce aux technologies de prévention et de détection des intrusions (IDS/IPS) de Kaspersky Lab.
- Politiques de sécurité entièrement intégrées et gérées à travers la console de la plate-forme NSX.
- Sécurité totalement évolutive et automatisée, fournissant encore plus de flexibilité et d'efficacité opérationnelle à votre activité.

Kaspersky Security for Virtualization s'intègre aux technologies natives de la plate-forme de virtualisation de VMware. Sans agent supplémentaire requis sur chaque machine virtuelle, l'impact des systèmes sur la performance de la plate-forme virtuelle est proche de zéro, l'administration est réduite et chaque machine virtuelle activée est protégée instantanément.

1 INFRASTRUCTURE AXÉE SUR LA TECHNOLOGIE

- Automatisation de la gestion du réseau virtuel
- Micro-segmentation dynamique dans le software-defined datacenter
- Intégration entre les composants de l'architecture du software-defined datacenter

2 SÉCURITÉ INTÉGRÉE MULTI-NIVEAUX

- Sécurité avancée pour le software-defined datacenter, ses réseaux et ses machines virtuelles
- Sécurité supérieure pour toute opération de fichier dans les machines virtuelles
- Protection contre les attaques réseau (IDS/IPS)
- Solution de sécurité automatisée et évolutive

3 PERFORMANCE ET EFFICACITÉ

- Sécurité conçue spécialement pour la virtualisation VMware
- Aucun impact sur la performance des machines virtuelles ou de l'hôte, partout dans le software-defined datacenter
- Maintient un niveau élevé de densité de la machine virtuelle et préserve l'efficacité des systèmes

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

KASPERSKY lab