PRINCIPES FONDAMENTAUX D'UNE INFRASTRUCTURE D'APPLICATIONS SÉCURISÉE

La sécurité, première préoccupation de tous les secteurs d'activité

Alors que les personnes, les terminaux et les objets sont de plus en plus connectés, la protection de l'ensemble de ces environnements et connexions est devenue plus essentielle que jamais. Dans le même temps, c'est aujourd'hui la plus importante problématique du département informatique. Pourquoi ? Parce que les départements informatiques de tous les secteurs d'activité doivent, par nécessité, sécuriser chaque interaction entre les utilisateurs, les applications et les données, quels que soient le mode et le lieu de connexion. De plus, ils doivent le faire dans des environnements en constante évolution et de plus en plus dynamiques.

Alors comment réduire les risques dans un monde où la complexité informatique et les interactions numériques « partout, tout le temps » augmentent de façon exponentielle ? Pour les entreprises qui adoptent les environnements de Cloud et virtualisés, une visibilité et un contrôle maximum sont essentiels pour limiter ce risque.

L'évolution des menaces exige de nouveaux modèles de sécurité

Au cours des dernières années, les entreprises de pratiquement tous les secteurs d'activité ont été au cœur de cas très médiatisés de violation des données d'entreprise et de clients, avec pour conséquence des milliards de dollars en coûts de résolution, dommage pour la marque, perte de confiance et perte de revenus. Même si les méthodes d'attaque varient, la plupart des failles exploitent (et mettent en évidence) la faiblesse inhérente de la sécurité de réseau axée sur le périmètre, qui se concentre généralement sur la protection du trafic nord-sud via des pare-feu de périmètre. Mais que se passe-t-il lorsqu'une menace parvient à contourner ces pare-feu de périmètre ? Dans ce cas, très peu de contrôles au sein du Data Center l'empêchent de se propager au trafic est-ouest (à savoir, de serveur à serveur). Les menaces modernes étant de plus en plus sophistiquées, c'est malheureusement devenu monnaie courante.

Pour tenter de résoudre ce problème, de nombreuses entreprises ont déployé un arsenal de produits ponctuels, créant un réseau complexe et déconnecté de systèmes rigides, difficiles à provisionner et loin d'être adaptés aux applications qu'ils sont sensés protéger. Pire encore, les outils disponibles pour lancer ces attaques malicieuses sont devenus extrêmement puissants et simples d'utilisation, permettant à un plus grand nombre d'attaquants d'atteindre leur cible.

L'informatique a besoin de sécurité et d'agilité

Pour répondre aux attentes des dirigeants et parties prenantes de l'entreprise, les départements informatiques doivent pouvoir fournir les services et applications critiques rapidement et sans faire de compromis sur la sécurité. Or, dans leurs efforts de sécuriser l'entreprise, les équipes informatiques font face à de nombreux obstacles, notamment :

- Évolution des architectures d'applications, qui passent d'applications monolithiques sur site à des applications distribuées et des microservices
- Manque de visibilité et de contexte sur le trafic du réseau
- Modèles et règles de sécurité rigides et axés sur le périmètre
- Difficulté à atteindre, conserver et prouver la conformité

Les entreprises doivent être agiles pour favoriser la croissance

Alors que les entreprises cherchent à accélérer les délais de mise sur le marché et le retour sur investissement des branches d'activité et autres parties prenantes internes, elles doivent aussi contrôler la sécurité et gérer le risque plus efficacement. Il s'agit de réduire non seulement le risque de faille de sécurité, mais aussi l'impact de telles failles. Or cela engendre une difficulté : renforcer considérablement la sécurité et la conformité à l'aide d'outils conventionnels peut souvent avoir un impact négatif sur l'agilité. Alors comment offrir aux équipes informatiques les solutions et ressources dont elles ont besoin pour suivre le rythme de l'entreprise tout en garantissant la sécurité de l'infrastructure ?

Avantages de l'isolation des applications de l'infrastructure

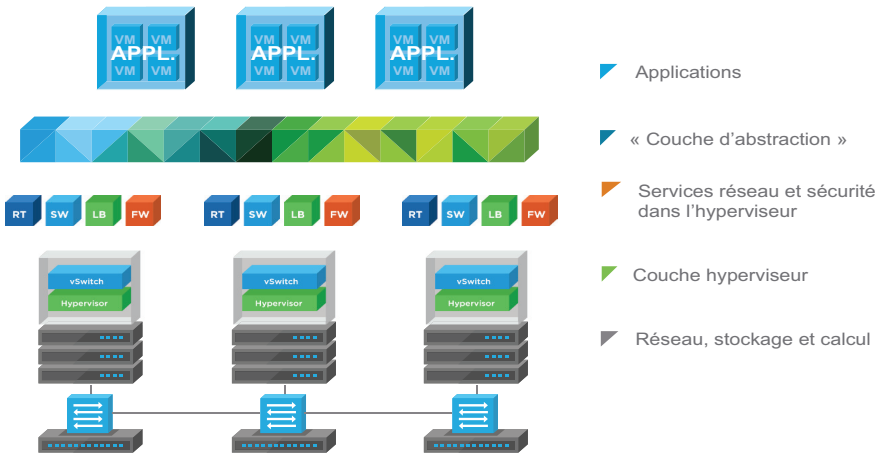
Pour résoudre ce problème, les entreprises doivent transformer radicalement la méthode de protection de l'infrastructure d'applications. La gamme complète de solutions VMware permet aux équipes informatiques de déployer une plate-forme virtualisée qui dissocie les applications de l'infrastructure sous-jacente, peu importe où se trouve cette infrastructure : sur site ou dans le Cloud public. Avec VMware vSphere® et VMware NSX®, les entreprises peuvent profiter de plates-formes de virtualisation flexibles et puissantes pour exécuter leurs applications nouvelles et existantes, et ce, sans compromis sur la sécurité et la conformité. VMware vRealize® Network Insight™ améliore leurs fonctionnalités grâce à une gestion du Cloud adaptée aux besoins des entreprises pour une visibilité et une protection renforcées.

Trois principes fondamentaux pour sécuriser une infrastructure d'applications

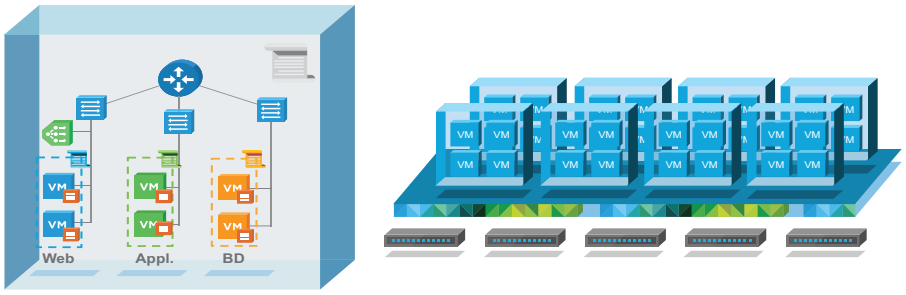
Appliquer une toute nouvelle approche pour sécuriser l'infrastructure d'applications permet aux départements informatiques de profiter de plusieurs fonctionnalités puissantes :

Isolation des applications de l'infrastructure

Isoler les applications de l'infrastructure offre une visibilité complète sur le chemin de données des applications afin de mieux comprendre les schémas de trafic. Cela permet au département informatique de mieux appréhender le contexte de l'interaction entre l'infrastructure et les applications, et entre ses deux dernières et les données. Grâce à une vue complète et unifiée sur les données, les applications et l'infrastructure, les entreprises peuvent créer des règles et répondre aux menaces plus efficacement.



Règle de sécurité granulaire orientée applications
Une approche virtualisée permet aux entreprises d'adapter parfaitement les règles de sécurité aux applications à protéger, ainsi que de les suivre lorsqu'elles se déplacent entre les Cloud privés et publics. Elle offre la micro-segmentation de réseau qui permet d'empêcher la propagation latérale (est-ouest) des menaces entre les charges de travail et les applications. De plus, elle facilite l'intégration intelligente de services de sécurité tiers dans la plate-forme pour ajouter des fonctionnalités.



Protection de l'infrastructure basée sur hyperviseur
Un modèle qui isole les applications de l'infrastructure sous-jacente fournit aussi un point idéal au sein de l'infrastructure pour protéger cette dernière. Les entreprises peuvent protéger les données inactives via le cryptage au niveau des charges de travail sur chaque hôte d'hyperviseur. Elles peuvent aussi chiffrer les données en transit pour réduire le risque de compromettre des composants de réseau comme les routeurs et les commutateurs.

Un portefeuille de fonctionnalités pour sécuriser l'infrastructure d'applications

Peu importe leur niveau de virtualisation, VMware offre aux entreprises des technologies leaders qui améliorent les environnements de sécurité d'applications.

VMware vSphere
Pour protéger leurs ressources critiques dans un environnement virtualisé, les entreprises ont besoin de fonctionnalités de gestion rationalisée et d'une sécurité suivant des règles prédéfinies simple à exploiter.

Plate-forme de virtualisation leader du marché, VMware vSphere constitue la base puissante, flexible et sécurisée offrant à l'entreprise l'agilité nécessaire pour accélérer sa transformation numérique vers le Cloud Computing. La solution prend en charge les applications existantes et de nouvelle génération grâce à son expérience client simplifiée permettant l'automatisation et la gestion à grande échelle, sa sécurité intégrée complète assurant la protection des données, de l'infrastructure et des accès, et sa plate-forme applicative universelle qui permet d'exécuter toutes les applications, en tout lieu. Avec vSphere, les entreprises peuvent exécuter, gérer, connecter et sécuriser leurs applications dans un environnement d'exploitation commun, sur l'ensemble des Clouds et terminaux.

VMware vSphere inclut des fonctions de sécurité complètes pour protéger les environnements et réduire les problèmes en cas de faille :

- Sécurité à grande échelle : sécurité suivant des règles prédéfinies qui simplifie la sécurisation de l'infrastructure.
- Chiffrement : le chiffrement au niveau des VM protège les données, aussi bien inactives qu'en transit, contre tout accès non autorisé.
- Consignation des audits : journalisation améliorée fournissant des informations utiles sur les actions des utilisateurs.

VMware NSX
Pour offrir une protection contre les menaces sophistiquées d'aujourd'hui, les entreprises ont besoin d'un environnement de réseau virtuel qui leur permet de diviser le Data Center en segments logiques.

Si une personne malveillante traverse les défenses du périmètre du Data Center, il est essentiel d'empêcher cette menace de se propager latéralement à l'intérieur de ce dernier. Avec une approche virtualisée, les équipes informatiques peuvent définir des règles de sécurité pour chaque charge en fonction de groupes de sécurité dynamiques, et ce, pour pouvoir réagir immédiatement aux menaces à l'intérieur du Data Center. VMware NSX fournit une plate-forme de virtualisation du réseau qui distribue le modèle opérationnel d'une machine virtuelle pour le réseau du Data Center. Avec VMware NSX, les entreprises peuvent créer, stocker, déplacer, supprimer et restaurer des réseaux entiers et en réaliser des snapshots, le tout par programme et en un clic. Vous bénéficiez ainsi de la simplicité et de la rapidité d'une machine virtuelle, avec un niveau de sécurité, d'agilité et de disponibilité impossible avec les approches matérielles ou opérationnelles classiques. La solution leur permet d'appliquer des règles de sécurité jusqu'au niveau de chaque machine virtuelle.

VMware NSX permet aux entreprises de profiter des avantages de la virtualisation en matière de sécurité et de performance. Les principales fonctionnalités incluent :

- Sécurité : des fonctions de sécurité intégrées à l'hyperviseur offrent micro-segmentation et sécurité granulaire au niveau des charges de travail.
- Automatisation : les services de réseau et de sécurité sont reliés aux charges de travail selon une approche suivant des règles prédéfinies, pour offrir automatisation et amélioration des performances.
- Disponibilité permanente des applications : le réseau est isolé du matériel sous-jacent et les règles de réseau et de sécurité sont reliées à leurs charges de travail associées.

vRealize Network Insight

Pour gérer un environnement de Cloud hybride hétérogène, les entreprises ont besoin d'une plate-forme de gestion du Cloud adaptée à leurs besoins et spécifiquement conçue à cet effet.

vRealize Network Insight offre des opérations intelligentes pour la sécurité et le réseau du Software-Defined Data Center, avec une visibilité convergée sur l'ensemble des réseaux virtuels et physiques, ainsi que des recommandations de planification de la micro-segmentation et la gestion des opérations pour VMware NSX. vRealize Network Insight offre une large gamme de fonctions d'optimisation de la sécurité :

- Visibilité : offre une visibilité convergée sur les couches superposées et sous-jacentes, les réseaux virtuels et physiques, les Clouds privés et publics grâce à l'intégration des couches virtuelles et physiques.
- Modélisation du comportement des applications par la micro-segmentation : permet aux utilisateurs d'être facilement informés sur qui parle avec qui et de savoir quels flux doivent être autorisés ou bloqués.
- Audit et conformité : permet d'établir le suivi de tous les changements à des fins d'audit et de conformité.

Sécurisez votre infrastructure d'applications avec VMware dès aujourd'hui

Les départements informatiques modernes font face à une problématique sans précédent induite par la transformation numérique et un paysage de menaces à évolution rapide. Dans cet environnement dynamique, il est plus important que jamais de collaborer avec un fournisseur de technologies reconnu afin de garantir la sécurité des opérations d'entreprise. VMware aide les entreprises à transformer leur approche de la sécurité grâce à une couche logicielle omniprésente sur l'infrastructure d'applications. En isolant l'infrastructure des applications qu'elle exécute, VMware permet au département informatique d'étendre sa visibilité au chemin de données pour une meilleure analyse et un meilleur contrôle. Associée à la micro-segmentation, la solution permet aux entreprises de simplifier les règles de sécurité et de mieux adapter la protection aux besoins applicatifs spécifiques. Pour cela, VMware propose un large choix de solutions de sécurité et de virtualisation, appuyé par un écosystème de partenaires étendu. Grâce à une solution de sécurité et de conformité puissante, les entreprises peuvent réaffecter leurs équipes informatiques à la croissance et l'innovation.

DÉMARRER AUJOURD'HUI

Sécuriser votre infrastructure d'applications

EN SAVOIR PLUS >

Rejoignez-nous en ligne :

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Global Inc. Tour Franklin 100-101 Terrasse Boieldieu 92042 Paris La Défense 8 Cedex France Tél. +33 1 47 62 79 00 www.vmware.fr