VMware NSX for Horizon

EN BREF

VMware NSX™ for Horizon® confère rapidité et simplicité à la mise en réseau VDI. En quelques secondes, les administrateurs informatiques peuvent créer des règles qui suivent dynamiquement les postes de travail virtuels, sans qu'il soit nécessaire d'avoir recours à un provisionnement réseau fastidieux. En étendant les règles de sécurité du data center aux postes de travail et applications, cette solution conjointe fournit également une plate-forme évolutive qui s'intègre parfaitement aux meilleures solutions de sécurité du marché.

AVANTAGES

- Amélioration de la sécurité des postes de travail virtuels résidant parmi d'autres charges de travail du data center
- Simplification et accélération de l'administration des règles de sécurité et réseau appliquées aux utilisateurs en fonction des regroupements logiques, des rôles ou des balises
- Association automatique de règles à un poste de travail dès sa création, qui suivent la VM quelle que soit l'infrastructure sous-jacente
- Intégration aux meilleures solutions du marché en matière de services antivirus, de protection contre les logiciels malveillants, de prévention des intrusions et de sécurité de nouvelle génération

Mise en réseau et sécurité des applications et postes de travail virtuels : rapides, simples et évolutives

De nombreuses entreprises mettent en œuvre la virtualisation des postes de travail et des applications pour améliorer la sécurité informatique des clients et offrir une plus grande mobilité d'entreprise. La centralisation des postes de travail et des applications protège les données inactives, empêche les accès non autorisés aux applications et fournit un moyen plus efficace de corriger, gérer et mettre à niveau les images.

Cependant, avec la virtualisation des postes de travail et des applications, de nouveaux risques de sécurité peuvent survenir derrière le pare-feu du data center, là où des centaines, voire des milliers, de postes de travail résident. Ces postes de travail sont très proches d'autres utilisateurs et d'autres charges de travail stratégiques, ce qui les rend beaucoup plus vulnérables face aux logiciels malveillants et à d'autres attaques. Ces attaques peuvent progresser du poste de travail au serveur en exposant une large surface d'attaque au sein du data center. Ce scénario de menace « est-ouest » est courant et affecte de nombreux clients aujourd'hui, en particulier ceux ayant des obligations de sécurité et de conformité strictes.

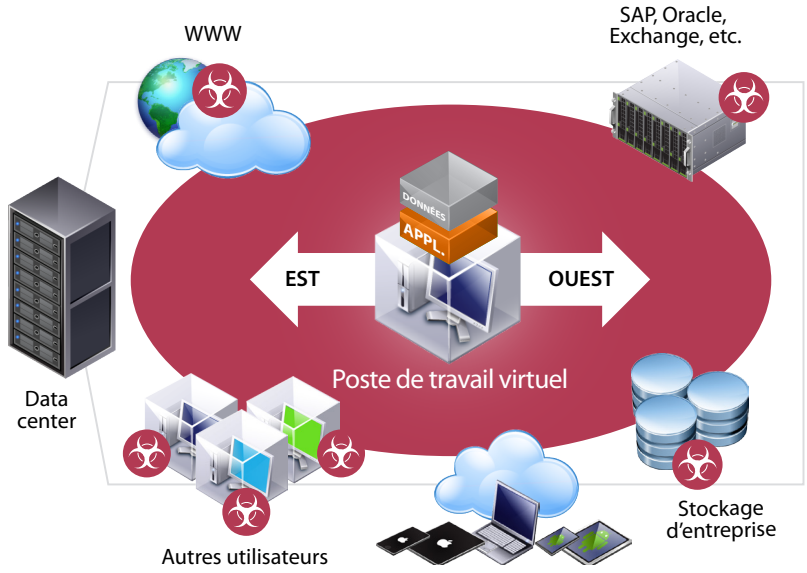

Figure 1 : Problèmes de sécurité est-ouest dans le data center

Généralement, les entreprises qui cherchent à administrer des règles de sécurité et réseau qui suivent les utilisateurs et les charges de travail en permanence ont également réalisé un investissement important dans une architecture reposant sur une approche matérielle qui implique de lourdes dépenses d'investissement et qui s'avère complexe à gérer et lente à s'adapter à un environnement d'entreprise résolument dynamique.

VMware NSX for Horizon

VMware NSX for Horizon sécurise efficacement le trafic est-ouest au sein du data center, tout en permettant au département informatique d'administrer rapidement et facilement des règles de sécurité et réseau qui suivent dynamiquement les postes de travail virtuels et les applications des utilisateurs, quels que soient l'infrastructure, le terminal et le lieu.

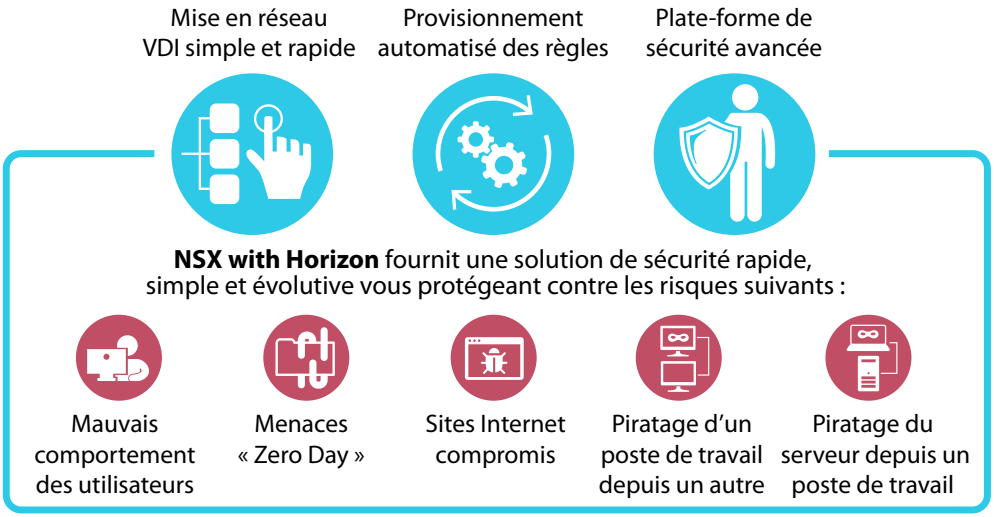

Figure 2 : NSX for Horizon garantit une mise en réseau et une sécurité VDI rapides, simples et évolutives

Avec cette solution, les entreprises bénéficient d'une mise en réseau et d'une sécurité VDI simples et rapides. En quelques secondes, les administrateurs informatiques peuvent créer des règles qui suivent dynamiquement les postes de travail virtuels, sans qu'il soit nécessaire d'avoir recours à un provisionnement réseau fastidieux.

En étendant les règles de sécurité du data center aux postes de travail et applications, cette solution fournit également une plate-forme évolutive qui peut s'intégrer à l'écosystème VMware de partenaires de sécurité leaders du secteur pour offrir aux clients une défense approfondie qui protège le poste de travail complet.

Fonctionnement

VMware NSX for Horizon améliore la sécurité de la virtualisation des postes de travail et contribue à traiter les menaces est-ouest en permettant aux administrateurs de définir des règles de façon centralisée. Ces règles sont ensuite distribuées à la couche de l'hyperviseur de chaque hôte vSphere et automatiquement associées à chaque poste de travail virtuel dès sa création. Pour sécuriser les postes de travail virtuels et les charges de travail adjacentes dans le data center, VMware NSX met en œuvre une « micro-segmentation » en garantissant à chaque poste de travail la défense de son propre périmètre. Cette « sécurité prête à l'emploi » exploite la fonctionnalité de protection par pare-feu virtuel distribué de VMware NSX pour réglementer le trafic en provenance et à destination de chaque VM, supprimant ainsi les accès non autorisés entre les postes de travail et les charges de travail adjacentes. Si le poste de travail virtuel passe d'un hôte à un autre ou se déplace dans le data center, les règles le suivent automatiquement.

Fonctionnalités et avantages

VMware NSX for Horizon garantit la rapidité et la simplicité de la mise en réseau VDI grâce à des règles de sécurité qui suivent dynamiquement les utilisateurs quels que soient l'infrastructure, le terminal et le lieu.

Mise en réseau VDI simple et rapide

Avec VMware NSX for Horizon, les administrateurs, peuvent créer, modifier et gérer les règles de sécurité sur tous les postes de travail virtuels en quelques clics. Les règles de sécurité peuvent être rapidement associées à des groupes d'utilisateurs pour accélérer l'intégration des postes de travail virtuels. Ayant la possibilité de déployer des fonctions réseau virtualisées (telles que la commutation, le routage, la protection par pare-feu et l'équilibrage de charge), les administrateurs peuvent créer des réseaux virtuels pour VDI sans avoir recours à une syntaxe complexe de configuration de VLAN, de listes de contrôle d'accès ou de matériel.

Règles automatisées suivant dynamiquement les utilisateurs et les postes de travail

Les administrateurs peuvent configurer des règles qui s'adaptent dynamiquement à l'environnement informatique de l'utilisateur, avec des services de sécurité réseau qui sont associés à chaque utilisateur en fonction de son rôle, de son regroupement logique, du système d'exploitation de son poste de travail, etc., quelle que soit l'infrastructure réseau sous-jacente. Les règles gérées de façon centralisée sont automatiquement associées à chaque poste de travail virtuel dès la création de celui-ci, ce qui permet aux entreprises de se développer en toute confiance en bénéficiant d'une solution de sécurité qui suit en permanence le poste de travail virtuel dans le data center.

Plate-forme de sécurité avancée

VMware NSX offre une plate-forme évolutive qui peut être intégrée aux fonctionnalités de pointe proposées par un écosystème établi de partenaires de sécurité. Grâce à l'ajout dynamique de services, la sécurité des postes de travail virtuels peut être étendue du data center aux postes de travail et applications. Cet écosystème de partenaires, incluant notamment Trend Micro, Intel Security et Palo Alto Networks, offre des solutions qui protègent le système d'exploitation, le navigateur, la messagerie, etc. grâce à des services antivirus, de protection contre les logiciels malveillants, de prévention des intrusions et de sécurité de nouvelle génération.

En savoir plus

Pour plus d'informations sur Horizon et VMware NSX, consultez le site Web VMware et suivez-nous sur Twitter.

Ressources VMware Horizon

Web : http://www.vmware.com/fr/products/horizon-view

Blog : http://blogs.vmware.com/euc/

Twitter : @VMwareHorizon

Ressources VMware NSX

Web : http://www.vmware.com/fr/products/nsx/

Blog : http://blogs.vmware.com/networkvirtualization/

Twitter : @VMwareNSX

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 Fax +33 1 47 62 79 01 www.vmware.fr