vmware®

Conseils techniques

# 10 bons conseils pour renforcer la sécurité de votre déploiement VMware Horizon

**Protégez votre environnement informatique à l'ère de la virtualisation**

Séduites par les avantages de la mobilité d'entreprise, les équipes informatiques sont naturellement impatientes de franchir les limites de l'architecture propriétaire pour choisir en toute liberté les postes de travail de la nouvelle génération. Grâce à la transformation du poste de travail avec VMware® Horizon®, l'utilisateur final peut désormais bénéficier de la flexibilité nécessaire pour accéder aux applications et postes de travail virtualisés via une plate-forme unique.

Mais cette flexibilité accrue pour l'utilisateur, avec notamment la possibilité d'utiliser son propre matériel (stratégie BYOD), présente de nouvelles difficultés en matière de sécurité informatique. La diversité des accès nécessite une vigilance renforcée pour assurer la protection des données. Et dans un monde où la sécurité informatique de l'entreprise exige une attention de tous les instants — le nombre d'incidents enregistre un taux de croissance annuel composé (CAGR) de 66 %, avec un coût par faille de sécurité qui atteint 5,9 millions de $[1] — vous devez obtenir l'assurance que la transformation de vos postes de travail est à la fois efficace et sûre.

## QU'EST-CE QUE VMWARE HORIZON ?

VMware Horizon renforce la puissance de la virtualisation des postes de travail et des applications en fournissant aux utilisateurs des applications et postes de travail virtuels via une plate-forme unique. Ces services applicatifs et de poste de travail, notamment les applications hébergées par RDS et les applications packagées avec VMware ThinApp®, sont tous accessibles à partir d'un espace de travail unifié, quels que soient le terminal, le support, le type de connexion et le lieu. Pour en savoir plus sur Horizon, visitez le site vmware.com/go/horizon.

**Comment la virtualisation des postes de travail des utilisateurs entraîne de nouvelles considérations en matière de sécurité informatique**

Même si la transformation des postes de travail offre de très nombreux avantages pour les utilisateurs et les départements informatiques (réduction des coûts d'exploitation et dépenses d'investissement, gestion simplifiée, productivité accrue des utilisateurs, disponibilité élevée, etc.), il est important de bien comprendre les défis qu'elle pose aux responsables du secteur.

- Avec la fourniture de postes de travail et d'applications en temps réel, les administrateurs informatiques peuvent rendre opérationnels les nouveaux utilisateurs rapidement, en déployant des postes réellement sans état en quelques secondes. Comment assurerez-vous rapidement l'évolutivité horizontale des déploiements sans perdre la visibilité ni le contrôle de votre réseau ?
- Votre service gère peut-être des milliers, voire des centaines de milliers, d'utilisateurs à proximité de l'infrastructure stratégique. Si les postes de travail virtuels sont menacés, la faille de sécurité risque de coûter cher.
- Les flux de trafic est-ouest, qui correspondent au trafic interne entre les serveurs ou les postes de travail, peuvent vous fragiliser. Les actions quotidiennes effectuées par des utilisateurs de confiance présentent des menaces pour le réseau, notamment via l'envoi d'e-mails infectés par des virus ou une navigation imprudente sur Internet.

Sachant cela, voici 10 conseils techniques qui vous permettront de sécuriser davantage votre déploiement Horizon :

### 1 Utiliser des images de référence

Avec une image de référence, un modèle pour les postes de travail virtuels, les équipes informatiques peuvent personnaliser les postes de travail virtuels des utilisateurs de manière à ce qu'ils n'aient accès qu'à des activités pertinentes dans le cadre de leurs fonctions. Ainsi le département informatique peut s'attacher à maintenir l'intégrité de l'image de référence qui se trouve en lieu sûr dans le Data Center. Lorsqu'un poste virtuel est menacé, il peut supprimer l'image et redéployer un nouveau poste de travail.

### 2 Mettre en place une approche de sécurité par couches

Dans un environnement virtualisé, il vaut mieux faire face aux risques de sécurité sur plusieurs fronts. En prenant des mesures de sécurité renforcées, telles que l'établissement de listes blanches d'applications via VMware NSX™, vous pouvez approuver les applications qui s'exécutent sur votre réseau. Ce mécanisme garantit la sécurité du réseau et oblige les utilisateurs à respecter la conformité, dans la mesure où les entreprises sont confrontées à la réalité de l'informatique parallèle ; en effet certains utilisateurs et responsables des branches d'activité optent pour des applications et services professionnels sans passer par leur département informatique. Les méthodes de distribution des applications, avec l'utilisation d'outils tels que VMware App Volumes™, permettent également d'assurer l'intégrité des applications.

1. PwC, PwC, « Managing cyber risks in an interconnected world », septembre 2014

## À PROPOS DE VMWARE APP VOLUMES

VMware App Volumes permet aux administrateurs informatiques de distribuer des applications et des données aux utilisateurs ou postes de travail en quelques secondes et à grande échelle. Avec App Volumes, l'utilisation de volumes gérés permet de réduire les coûts d'infrastructure et de gestion. Ces applications fonctionnent comme si elles étaient installées en natif et suivent les utilisateurs de manière transparente d'une session ou d'un périphérique à un autre.

Principaux avantages :

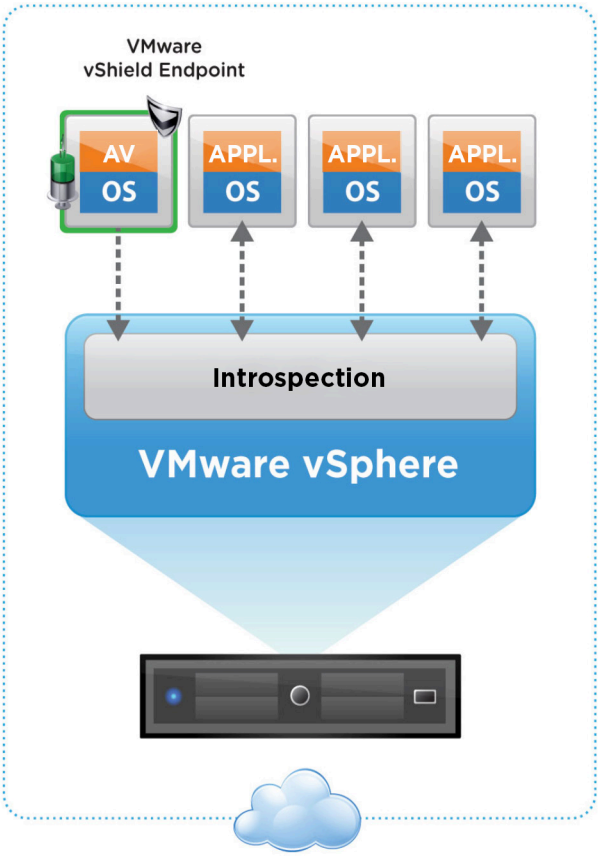
- Applications gérées de manière centralisée
- Facilité de déploiement des applications
- Applications distribuées par utilisateur

Pour plus d'informations sur App Volumes, rendez-vous sur le site https://www.vmware.com/fr/products/appvolumes/.

## 3 Assurer une protection adéquate des terminaux

En investissant dans des fonctionnalités matérielles et logicielles, vous pouvez renforcer la sécurité de vos terminaux Horizon. En cas de perte ou de vol d'un périphérique par exemple, des fonctions matérielles telles que le module TPM (Trusted Platform Module) activent un mécanisme d'authentification qui empêche l'appareil de démarrer. Veillez aussi à ce que les définitions des antivirus et les outils anti logiciels malveillants soient à jour, et à ce que le pare-feu du terminal soit actualisé et actif.

Vous connaissez peut-être des administrateurs informatiques qui se passent d'antivirus pour leurs postes de travail virtuels afin d'en minimiser l'impact sur la mémoire, les processeurs et les disques. Mais les dégâts provoqués par un virus sur un poste de travail virtuel peuvent être aussi graves que ceux d'un virus affectant un poste physique, notamment si vous négligez de réactualiser les machines virtuelles à intervalles réguliers. VMware vShield Endpoint™, qui transfère le logiciel de traitement antivirus et anti-programme malveillant des machines virtuelles vers un boîtier virtuel sécurisé, offre une excellente alternative.




Enfin vous pouvez renforcer encore davantage la sécurité des terminaux avec des solutions de fournisseurs tiers. Trend Micro Deep Security, par exemple, propose les fonctionnalités avancées suivantes : protection contre les logiciels malveillants, systèmes de détection/prévention des intrusions, contrôle d'intégrité, filtrage d'URL et application de correctifs. Les puissantes fonctions de sécurité s'exécutent au niveau de l'hyperviseur et assurent instantanément la protection d'un nouveau poste de travail virtuel au moment où il est mis en service. En outre, la règle de sécurité suit automatiquement le terminal où qu'il se trouve dans le Data Center.

## À PROPOS DE VMWARE VSHIELD ENDPOINT

VMware vShield Endpoint renforce la sécurité des machines virtuelles tout en optimisant la protection au niveau des terminaux, selon différents échelons d'importance ; vShield Endpoint est conçu pour exploiter les investissements existants en permettant aux clients de gérer les règles de traitement antivirus et antimalware pour les environnements virtualisés avec les mêmes interfaces d'administration qu'ils utilisent pour sécuriser les environnements physiques. La solution s'intègre aux produits des fournisseurs suivants : Trend Micro, Intel Security, Symantec, Sophos et Kaspersky.

## 4 Appliquer des règles de groupe et des règles étendues

En cas de violation d'un terminal, lorsque l'antivirus ou la protection contre les logiciels malveillants n'est pas mis à jour sur un périphérique par exemple, les règles de groupe peuvent vous aider à empêcher les attaques. Une règle de groupe vous permet également d'assurer la cohérence sur les postes de travail virtuels, de désactiver les services inutiles pour l'utilisateur et d'interdire l'accès à certaines parties du poste de travail ou du réseau. Les paramètres de règle empêchent également les utilisateurs d'apporter des modifications qui peuvent rendre les postes de travail vulnérables.

Envisagez d'utiliser VMware User Environment Manager™, une solution de gestion de l'environnement utilisateur puissante, simple et évolutive, qui facilite l'administration des applications, des utilisateurs et la configuration de règles dynamiques. Les paramètres de règle et d'application qui suivent les utilisateurs quel que soit leur emplacement et le périphérique utilisé, et la gestion des accès selon que les utilisateurs utilisent un poste de travail interne ou un périphérique externe, permettent de gagner en efficacité et de renforcer la sécurité des opérations au quotidien.

En outre, l'utilisation de fichiers de modèles d'administration (ADM) de stratégie de groupe Horizon, qui étend la stratégie de groupe Active Directory, vous permet de contrôler les informations qui circulent vers et depuis le poste de travail (en désactivant le presse-papier par exemple).

## 5 Maintenir une architecture adéquate

Avec Horizon, la sécurisation d'un déploiement nécessite de porter une étroite attention à la configuration du pare-feu et de la DMZ, ainsi qu'à la séparation des pools de postes de travail. Commencez par installer un pare-feu entre le réseau du Data Center et le réseau du bureau. Si vous utilisez des LAN virtuels ou des pare-feu pour segmenter les serveurs et les postes de travail, vérifiez que votre environnement VDI se situe côté postes de travail du pare-feu.

Pour assurer la sécurité des utilisateurs distants, il est nécessaire de configurer le serveur de sécurité ou le point d'accès à la DMZ. Il s'agit de fournir un point de connexion aux utilisateurs sans autoriser l'accès direct au réseau. Pour bénéficier d'une fonction de passerelle, il est temps de vous pencher sur les avantages offerts par Access Point par rapport à un serveur de sécurité. Avec Access Point par exemple, vous mettez en place une machine virtuelle Linux renforcée, verrouillée et préconfigurée, et non pas simplement un logiciel qui s'exécute sur un système d'exploitation Windows générique. Vous pouvez également connecter Access Point à un serveur View Connection Server spécifique, ou connecter l'appliance via un équilibreur de charge devant plusieurs View Connection Servers pour renforcer la disponibilité.

Il est recommandé de séparer les pools de postes de travail lorsque les postes doivent être isolés du reste de l'entreprise, comme c'est le cas pour les postes dédiés aux ressources humaines, aux sous-traitants ou aux développeurs. L'utilisation de VMware NSX comme module complémentaire de la plate-forme VMware vSphere® permet d'effectuer cette opération.

## 6 Utiliser l'authentification multifacteur et l'authentification en mode pass-through

Compatible avec les principales solutions d'authentification multifacteur telles que RSA SecurID, VASCO DIGIPASS, SMS Passcode et SafeNet, Horizon fournit les bases d'une stratégie efficace de sécurité des postes de travail. En outre, Horizon s'appuie sur la technologie d'authentification en mode pass-through, qui exige que les utilisateurs saisissent deux fois leurs informations d'identification, ou qu'ils se connectent à leur poste de travail via un compte distinct.

Il est utile également d'envisager l'utilisation de VMware Identity Manager™. Cette solution de gestion des identités fournit un accès conditionnel et un mécanisme d'authentification unique, afin de simplifier la mobilité d'entreprise et d'assurer une expérience utilisateur homogène sur tous les périphériques sans compromettre la sécurité de votre environnement.

## 7 Protéger les terminaux

Les lecteurs externes sont en mesure d'introduire des virus nuisibles et permettent le vol de propriété intellectuelle. Avec Horizon, vous pouvez empêcher la copie de données en local sur des dispositifs de stockage portables tels que les clés USB et les imprimantes non sécurisées. En outre, lorsque la fonction de redirection de lecteur client est installée sur le poste de travail virtuel, elle permet aux utilisateurs d'accéder à distance aux fichiers stockés sur leurs ordinateurs locaux. La compression et le chiffrement ont lieu lors du transfert des fichiers depuis le terminal vers le poste de travail virtuel.

## 8 Effectuer des opérations de maintenance/analyses périodiques

Une diligence raisonnable en matière de sécurité se manifeste idéalement par l'attention portée à la maintenance. Lorsque vous êtes confronté à un risque de faille de la sécurité, adoptez la stratégie suivante :

- Mettez à jour le logiciel avec des fonctionnalités d'anti-virus et de protection anti-logiciels malveillants qui informent le personnel responsable lorsque des attaques sont imminentes.
- Définissez une stratégie acceptable pour reconstituer ou réactualiser les postes de travail Horizon à intervalles réguliers pour tenir compte des correctifs de sécurité, des correctifs et mises à jour d'applications, et des mises à jour de système d'exploitation.
- Appliquez régulièrement les correctifs de sécurité et les mises à jour, non seulement pour le système d'exploitation mais aussi pour les applications dans l'image de référence.
- Analysez périodiquement les ports des pare-feu principaux et secondaires afin de garantir que les règles de pare-feu sont correctement mises en œuvre et empêchent les accès non autorisés à la zone DMZ.
- Analysez les schémas de trafic pour identifier le trafic autorisé à l'intérieur des pare-feu et de la DMZ, et surveillez les ports non utilisés.

## POURQUOI UNE TELLE REFONDATION ? OPTIMISER LA SÉCURITÉ ET LES PERFORMANCES

En réactualisant vos postes de travail virtuels à la déconnexion, vous garantissez à chaque utilisateur de toujours disposer d'un poste intègre et fonctionnel. Non seulement vous améliorez la sécurité avec la suppression des virus potentiels et des logiciels malveillants du poste virtuel, mais vous offrez la même convivialité à l'utilisateur et renforcez les performances.

### 9 Sécuriser le réseau

L'association de VMware NSX et d'Horizon fournit les bases de l'automatisation et de la micro-segmentation. Avec VMware NSX, vous pouvez déployer un pare-feu distribué par port, qui vous offre la possibilité de contrôler le trafic entrant sur un poste de travail et avec qui le poste peut communiquer. Vous pouvez également créer des zones pour isoler les sous-traitants et protéger le réseau d'une navigation Web à haut risque.

Grâce à la micro-segmentation, chaque machine virtuelle est dotée de son propre périmètre de défense. Un pare-feu distribué surveille le trafic qui entre et sort de chaque VM, empêchant les accès non autorisés et l'infiltration de menaces au sein du Data Center. Il est possible d'automatiser le provisionnement de la sécurité et de micro-segmenter les charges de travail, ce qui permet d'évoluer plus rapidement et de manière sécurisée tout en dopant les performances du poste de travail virtuel.

### 10 Limiter l'exposition au strict nécessaire

Ne laissez jamais de failles pouvant être exploitées par n'importe qui, ce qui souligne l'importance de la granularité des autorisations. Dans votre environnement par défaut, les applications peuvent accéder à d'autres applications. Un logiciel malveillant, par exemple, peut faire en sorte qu'une application écrase la mémoire d'une autre application que vous exécutez. Les risques de nuisance deviennent ainsi importants, étant donné que tout ce à quoi l'application a accès est menacé. Dans le cadre de la virtualisation des applications avec VMware ThinApp, chaque application reçoit son propre sandbox de système d'exploitation virtuel. Résultat : les applications ne peuvent plus voir les autres ni leurs fichiers, et certaines parties du système d'exploitation peuvent même être isolées de l'application. En conséquence, vous limitez l'étendue des infections potentielles et êtes en mesure de supprimer facilement ces infections en cas de violation de la sécurité.

## CONSIDÉRATIONS COURANTES SUR LA SÉCURITÉ MAIS SOUVENT IGNORÉES :

- Autant que possible, évitez d'octroyer des droits d'administration aux utilisateurs.
- En termes de sécurité, gérez les postes de travail virtuels comme des postes traditionnels par l'application de règles et en utilisant des applications antivirus et des outils de verrouillage.
- Remplacez les certificats auto-signés par défaut pour sécuriser les canaux SSL par un certificat créé par une autorité de certification de confiance pour réduire les attaques d'intercepteur.
- Lorsque les utilisateurs exécutent un second poste de travail virtuel pour bénéficier d'un accès à distance ou dans le cadre du télétravail, limitez leur possibilité d'accéder à des données sensibles.
- Utilisez VMware vRealize® Operations Manager™ pour surveiller les pics de trafic.
- Pour les déploiements externes, déployez des serveurs de sécurité ou des serveurs Access Point dans la zone DMZ.

# Conclusion

En dépit de toutes les promesses de flexibilité pour l'utilisateur et de gestion efficace, la transformation des postes de travail ne renforcera pas d'elle-même la sécurité du département informatique. En fait, comme vu précédemment, elle peut au contraire présenter de nouvelles difficultés en matière de sécurité si vous n'êtes pas proactif. Avec une mise en œuvre adéquate, et en respectant les conseils prodigués dans ce document, vous pouvez améliorer la sécurité de votre réseau tout en bénéficiant des avantages informatiques offerts par la transformation des postes de travail.

Vous pouvez tester gratuitement Horizon dans le cadre d'un laboratoire d'essai en ligne. Il est accessible en quelques minutes depuis votre navigateur et ne requiert aucune installation. Inscrivez-vous dès maintenant : https://www.vmware.com/horizon-hol-labs.

Rejoignez-nous en ligne

**Blog :** https://blogs.vmware.com/euc

**Twitter :** @vmwarehorizon

**Facebook :** https://www.facebook.com/vmwarehorizon

**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