LIVRE BLANC

DES APPLICATIONS SÉCURISÉES POUR L'ENTREPRISE

Guide pratique relatif à la sécurisation et à la mobilisation des applications d'entreprise

vmware®

Sommaire

De nouveaux défis pour le département informatique

Dans le monde actuel, caractérisé par sa mobilité, les employés peuvent travailler partout en utilisant n'importe quel terminal, ou presque. L'époque où la plus grande partie des employés travaillait au sein des locaux de l'entreprise en utilisant des systèmes de bureau fixes, dotés d'applications et de systèmes d'exploitation installés par les administrateurs, est révolue.

Pour le département informatique, cette transition vers l'ère de la mobilité et du travail à distance se traduit par de nouveaux défis. Le modèle prescriptif et descendant adopté jusque-là, qui consistait à transférer des images universelles aux employés, au moyen de configurations matérielles standard, n'est désormais plus applicable. Vous devez à présent vous pencher sur la sécurisation et la mobilisation des applications d'entreprise. Il est donc nécessaire de modifier les outils et processus de gestion utilisés de longue date, et de tenir compte du fait que, désormais, les employés n'utilisent pas tous les mêmes terminaux.

Nombre d'entre eux utilisent leurs propres terminaux sur leur lieu de travail. Qui plus est, un nombre croissant de départements et de branches d'activité souhaitent choisir le type de format le plus récent d'un terminal, quelle que soit la plate-forme. Suite à l'apparition de ces tendances, le département informatique doit pouvoir gérer de nombreux terminaux, systèmes d'exploitation et modèles de propriété, qu'il s'agisse de terminaux partagés et verrouillés appartenant à l'entreprise ou de terminaux personnels appartenant aux employés. En parallèle, la mobilité croissante du personnel et l'application d'un modèle qui ne tient pas compte du terminal donnent lieu à de nouveaux processus, requis pour la fourniture d'applications et de données permettant aux employés de réaliser leurs tâches, où qu'ils se trouvent.

La sécurité est également un problème important lorsque le département informatique fournit des services aux employés mobiles et travaillant à distance. Vous devez définir des stratégies permettant de protéger les données d'entreprise inactives et en transit, ou encore placées en mémoire cache ou stockées sur des terminaux mobiles.

La question se pose : comment faire pour sécuriser et mobiliser les applications d'entreprise dans ce nouveau contexte ? Dans ce document, vous découvrirez l'approche unique qui permet à VMware de sécuriser la gestion des applications et des accès.

Sécurisation et mobilisation des applications d'entreprise

Supprimer les barrières entre les composants existants et les nouvelles technologies

Une plate-forme d'espace de travail numérique fournit les outils nécessaires à votre département informatique pour gérer et sécuriser les différents terminaux des utilisateurs, mais également fournir des applications et des données aux employés à distance et mobiles.

Une plate-forme d'espace de travail numérique ne se contente pas de fournir les fonctionnalités legacy d'une infrastructure de postes de travail virtuels (VDI), de services RDS ou d'instances XenApp, ni de fournir des applications virtualisées aux utilisateurs distants. Elle combine la fourniture d'applications et de postes de travail virtualisés avec une expérience alliant simplicité pour les utilisateurs et sécurité de classe d'entreprise. Par ailleurs, elle aide l'organisation à faire le lien entre les applications client/serveur legacy, conçues pour l'ère du PC, et les nouvelles applications Cloud, ou natives, mobiles et hétérogènes, qui dépendent peu du point d'accès.

L'ESPACE DE TRAVAIL NUMÉRIQUE

Une stratégie axée sur l'espace de travail numérique permet à votre département informatique de fournir les applications et les données aux employés et ce, quel que soit le terminal. Grâce à cette nouvelle méthode de fourniture des services destinés à l'utilisateur, vous disposez des possibilités suivantes :

- Vous pouvez permettre l'accès aux terminaux verrouillés et partagés appartenant à l'entreprise, ainsi qu'aux terminaux personnels des employés, tout en protégeant efficacement la confidentialité des données.
- Vous avez la possibilité de protéger les données professionnelles inactives et en transit, notamment des e-mails, fichiers et états d'application qui peuvent être placés en mémoire cache ou stockés sur les terminaux.
- Vous pouvez fournir des applications natives aux terminaux et jouer le rôle de gestionnaire d'accès en contexte pour les applications Cloud et sur site.
- Vous avez la possibilité de simplifier l'intégration des employés et de réduire le nombre d'appels au support.

Prendre le contrôle de la sécurité

Tout arsenal de sécurité devrait être à même de centraliser et de fournir des applications virtuelles, afin de s'assurer que les données sensibles ne sont pas stockées sur des terminaux non sécurisés, et que ces terminaux ne sont pas connectés aux réseaux de l'entreprise. Cela permet de supprimer les risques liés aux réseaux VPN, par ailleurs complexes à gérer. Toutefois, les meilleures pratiques modernes en matière de sécurité ne peuvent pas reposer uniquement sur une approche caractérisée par l'isolement et la protection renforcée des ressources. Dans le cadre d'une méthode de sécurité moderne, les planificateurs doivent partir du principe que du code malveillant et des tricheurs parviendront à contourner les pare-feu, que les applications soient exécutées on premise ou dans le Cloud.

Grâce aux fonctionnalités intégrées dans les solutions VMware Horizon® and VMware Workspace ONE™, vous pouvez surmonter ces défis. Utilisées de concert, ces dernières vous permettent de conserver vos données les plus sensibles sur des terminaux qui ne sont pas compromis, et d'éviter la connexion de terminaux compromis au réseau.

Avantages de la plate-forme VMware :

- **Elle supprime la nécessité de configurer des réseaux VPN.** Seul le trafic relatif à l'expérience utilisateur (graphismes, frappes de touches, etc.) peut traverser un proxy inverse, ce qui permet de limiter l'exposition d'éventuels programmes malveillants se trouvant sur des terminaux locaux au réseau de l'entreprise.
- **Elle renforce le réseau dans le cas du trafic est-ouest.** Vous pouvez exploiter la virtualisation de réseau offerte par VMware NSX® pour isoler les applications individuelles, ce qui réduit le risque de dégâts entraînés par l'exécution de programmes malveillants.
- **Elle implémente des règles de sécurité à granularité fine.** Utilisez différentes options d'activation ou de restriction, notamment en matière d'impression ou de sauvegarde sur des disques locaux, qui sont basées sur des propriétés telles que le type et le niveau de fiabilité du terminal et l'emplacement du réseau.
- **Elle augmente le niveau de sécurité dans l'ensemble de l'entreprise.** Vous pouvez considérer chaque terminal comme éventuellement malveillant, et sécuriser les applications de la même manière pour tous les employés.

En s'assurant que les données ne sont pas placées sur des terminaux non sécurisés, et en appliquant une fonction de micro-segmentation du réseau à chaque charge de travail virtuelle, VMware aide votre entreprise à limiter les risques relatifs aux attaques et à empêcher les pertes de données, tout en répondant aux besoins d'un personnel toujours plus mobile en matière d'accès à distance.

Une solution complète

Vous pouvez opter pour une solution d'espace de travail numérique VMware en toute sérénité, car vous savez qu'elle sera gérée de bout en bout. Cela inclut une intégration étroite avec votre Data Center, des technologies de gestion avancées et une plate-forme de gestion intervenant au moment adéquat.

Intégration étroite avec le Software-Defined Data Center

Pour tirer pleinement parti de l'automatisation et de la portabilité des charges de travail entre les différents Data Centers et avec le Cloud, vous devez disposer d'une base exhaustive, associant des fonctions de traitement, de stockage et de virtualisation de réseau avec des outils de gestion capables d'administrer la pile dans son intégralité.

En tant que leader mondial en matière d'infrastructure du Cloud et d'environnements d'espace de travail numérique, VMware intègre les fonctionnalités de gestion de la virtualisation des applications et postes de travail de VMware Horizon avec les technologies de virtualisation du réseau (via VMware NSX), du stockage (grâce à VMware vSAN™) et du traitement (avec VMware vSphere®), afin de constituer la base de son Software-Defined Data Center.

Technologies de gestion avancées

La plate-forme d'espace de travail numérique de VMware inclut des technologies de gestion avancées, qui offrent une flexibilité et une personnalisation maximales, pour un TCO supérieur en matière de fourniture de postes de travail et d'applications. Par ailleurs, elle divise par deux le temps consacré à la gestion et le nombre de tâches fréquentes par rapport à ses principaux concurrents.

Une plate-forme intervenant au moment adéquat, leader sur le marché

VMware Horizon est une plate-forme de gestion intervenant au moment adéquat, qui comprend trois technologies clés capables de répondre aux défis associés à la personnalisation des applications, des systèmes d'exploitation et utilisateur, à savoir : Clones VMware Instant Clones, VMware App Volumes™ et VMware User Environment Manager™. Lorsqu'elles fonctionnent de concert, ces technologies offrent une flexibilité et une personnalisation maximales, pour un TCO supérieur en matière de fourniture de postes de travail et d'applications. Par ailleurs, elle divise par deux le temps consacré à la gestion et le nombre de tâches fréquentes par rapport à ses principaux concurrents.[1]

> **VMware Workspace ONE** est une plate-forme d'entreprise simple et sécurisée, qui fournit et gère n'importe quelle application, que ce soit sur smartphone, tablette ou ordinateur portable. Intégrant la gestion des identités, la fourniture d'applications en temps réel et la gestion de la mobilité d'entreprise, Workspace ONE répond aux attentes des employés numériques, réduit la menace de fuite de données et adapte les opérations informatiques traditionnelles à l'ère du Cloud mobile.
>
> **La solution VMware NSX** est une plate-forme de gestion de la sécurité et de virtualisation de réseau permettant de créer des réseaux entiers sous forme logicielle et de les intégrer dans la couche hyperviseur, laquelle est isolée du matériel physique sous-jacent. Tous les composants réseau peuvent être provisionnés en quelques minutes, sans que vous soyez contraint de modifier l'application.
>
> **VMware Horizon** fournit aux utilisateurs des applications et des postes de travail virtualisés ou hébergés, via une plate-forme unique. Ces services applicatifs et de poste de travail (notamment les applications RDS publiées, les applications packagées avec VMware ThinApp®, les applications SaaS et même les applications Citrix virtualisées) sont tous accessibles à partir de l'espace de travail numérique unique VMware Workspace ONE, quels que soient le terminal, le lieu, le support et le type de connexion, sans aucun compromis sur la qualité, ni sur l'expérience utilisateur.

1. Selon le résultat de tests effectués par des tiers indépendants à la demande de VMware lors de la sortie de la solution VMware Horizon 7.1, en février 2017.

Grâce à VMware Workspace ONE, les clients bénéficient de tous les avantages offerts par les récentes innovations et intégrations apportées à chaque gamme de produits (Horizon, VMware AirWatch® et Identity Manager™), mais peuvent également acheter une SKU présentant l'ensemble de solutions répondant le mieux à leurs besoins.

2. IDC MarketScape : évaluation 2016 des fournisseurs sur le marché mondial des logiciels d'exécution de clients virtuels, novembre 2016.

Points à retenir

- La plate-forme d'espace de travail numérique de VMware vous permet de surmonter les défis informatiques entraînés par le nombre croissant d'employés mobiles et travaillant à distance.
- Cette plate-forme d'espace de travail numérique fournit les outils nécessaires à votre département informatique pour gérer et sécuriser les différents terminaux des utilisateurs, mais également fournir des applications et des données aux employés à distance et mobiles.
- En s'assurant que les données ne sont pas placées sur des terminaux non sécurisés, et en appliquant une fonction de micro-segmentation du réseau à chaque charge de travail virtuelle, VMware limite les risques relatifs aux attaques et empêche les pertes de données.

DÉMARRER AUJOURD'HUI

Informez-vous sur la sécurisation et la mobilisation de vos applications.

Inscrivez-vous à la formation VMware Workforce Mobility Fundamentals (Principes de base de la technologie VMware de mobilité du personnel).

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