LIVRE BLANC – FÉVRIER 2017

CINQ ÉTAPES ESSENTIELLES POUR MODERNISER VOTRE ENVIRONNEMENT WINDOWS

Découvrez comment tirer le meilleur parti de vos investissements existants dans Windows et faciliter la migration de vos déploiements virtuels et physiques vers Windows 10.

vmware®

Le monde entier fonctionne sous Windows

Plus de 1,5 milliard de terminaux exécutent Windows*. Au cours des 30 dernières années, la plupart des organisations dans le monde ont adopté Windows de façon généralisée, réalisant des investissements considérables dans leurs environnements Windows : acquisition de licences, configuration, services professionnels et infrastructure pour Active Directory, Microsoft Exchange, gestion du cycle de vie des PC, etc. Microsoft continue également de développer des solutions destinées à aider les organisations à mener à bien leur transition vers le Cloud avec des produits tels que Microsoft Office 365 et Azure Active Directory, et avec la création d'un cadre de gestion moderne du Cloud mobile dans Windows 10.

Dans le même temps, les départements informatiques sont contraints en permanence de réussir le tour de force de réduire les coûts tout en renforçant la sécurité et en améliorant la productivité des collaborateurs à l'aide des dernières technologies. Windows 10 assure une meilleure expérience utilisateur et offre aux départements informatiques la possibilité d'adopter une approche fondamentalement différente de la gestion et de la sécurité pour se simplifier la tâche. Cependant, pour véritablement optimiser leur environnement Windows et en tirer ainsi le meilleur parti, les organisations doivent :

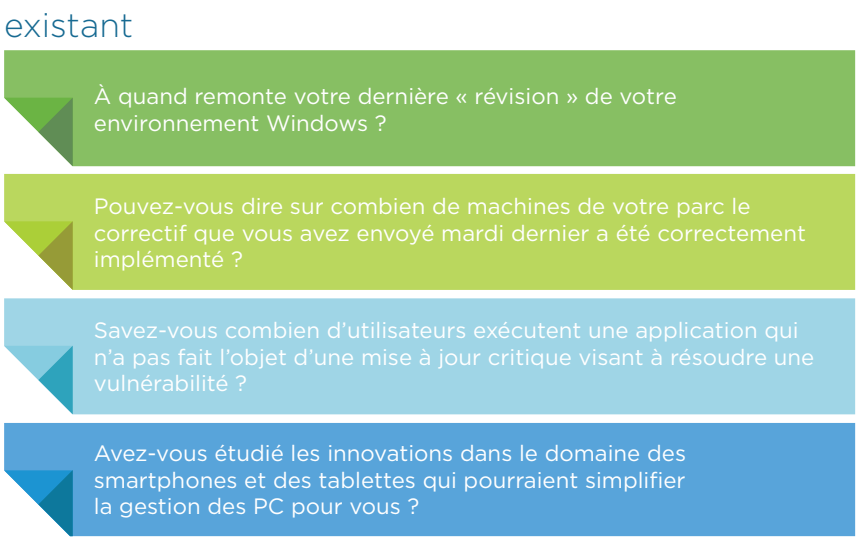
- Améliorer l'environnement existant en renforçant la sécurité et l'intégrité des terminaux.
- Évaluer et tester la compatibilité des terminaux, des applications et des processus avec Windows 10.
- Déterminer le chemin de migration optimal vers Windows 10 en fonction des cas d'usage.
- Moderniser la gestion des environnements Windows 10.
- Sécuriser l'environnement Windows 10 grâce à une visibilité et à des actions correctives en temps réel.

Dans ce livre blanc, nous nous pencherons sur cinq étapes que les organisations peuvent suivre pour optimiser leurs investissements existants dans Windows et adopter une approche moderne de la gestion et de la sécurité dans leur transition vers Windows 10.

Étape 1 : Procéder à une « révision » de votre environnement Windows pour prolonger sa durée de vie

Les propriétaires de voiture responsables font faire réviser leur véhicule pour inspecter, réparer ou remplacer des bougies, des filtres à air ou d'autres pièces qui ne fonctionnent pas de manière optimale. Des solutions complémentaires sont parfois utilisées : remplacement de l'huile par une formule pour moteur à kilométrage élevé, utilisation d'un additif pour éliminer l'accumulation de carbone dans les circuits de carburant, etc. Tout cela permet d'optimiser la consommation du carburant et la durée de vie du véhicule.

À quand remonte votre dernière « révision » de votre environnement Windows ? Le premier pas vers un environnement Windows moderne consiste à améliorer vos processus, vos technologies et votre reporting existants pour vous simplifier la vie et celle de vos utilisateurs. Pouvez-vous dire sur combien de machines de votre parc le correctif que vous avez envoyé mardi dernier a été correctement implémenté ? Savez-vous combien d'utilisateurs exécutent une application qui n'a pas fait l'objet d'une mise à jour critique visant à résoudre une vulnérabilité ? Avez-vous étudié les innovations dans le domaine des smartphones et des tablettes qui pourraient simplifier la gestion des PC pour vous ?



Les commentaires que nous recevons des clients sont à chaque fois similaires. Les utilisateurs veulent pouvoir rester productifs partout et sur n'importe quel terminal. Ils accèdent souvent aux ressources de l'entreprise hors du réseau sur un large éventail de terminaux, ce qui multiplie les vecteurs de menace pour l'organisation. Les départements informatiques ont besoin d'une visibilité en temps réel sur leur environnement Windows pour identifier les terminaux qui ne sont pas à jour avec les derniers correctifs, qui exécutent des applications non signées ou encore qui exécutent des versions obsolètes de dépendances d'application (Java, .NET, etc.), exposant le terminal et le réseau de l'entreprise à des attaques potentielles. Ils doivent avoir la possibilité d'exécuter des actions spécifiques en fonction de ces informations, comme déployer un correctif, mettre fin à un processus non autorisé ou effacer à distance le contenu d'un terminal qui représente une menace pour la sécurité.

Une visibilité et une protection en temps réel de votre environnement

Imaginez si vous pouviez obtenir une vue complète de tous vos terminaux en 15 secondes maximum. Imaginez si vous pouviez saisir une question simple, comme vous le faites dans Google, pour interroger l'ensemble de votre environnement, obtenir des résultats en quelques secondes (même si des millions de terminaux sont impliqués) et collecter des informations critiques exploitables sur-le-champ. C'est désormais chose possible. Compatible avec les versions poste de travail et serveur de Windows 7, 8.1 et 10, aussi bien pour les environnements virtuels que physiques, VMware® vous permet de :

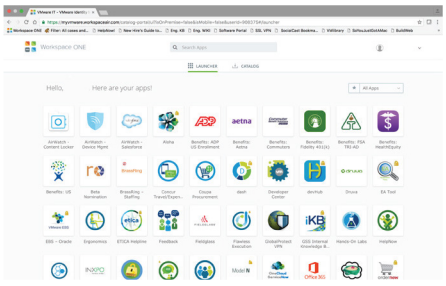
- détecter et contrôler les terminaux non gérés ;
- détecter les menaces avancées en quelques secondes sur plusieurs millions de terminaux ;
- corriger rapidement et à grande échelle les terminaux présentant une faille ;
- restaurer une image maître sur les terminaux Windows dont la sécurité a été compromise.

La plate-forme s'étend à toute l'entreprise pour sécuriser les terminaux, offrir au département informatique une visibilité sur l'inventaire des logiciels actifs et des informations détaillées sur l'utilisation des ressources, et distribuer les applications et les correctifs à grande échelle. Dans le cadre de la planification d'une migration vers Windows 10, VMware permet de prendre le pouls de l'environnement existant afin de corriger les éventuels problèmes et de simplifier la transition.

VMware dote également les clients d'un moyen moderne de protéger et gérer leurs terminaux mobiles, ainsi que leurs terminaux et serveurs Windows. L'intégration avec l'écosystème VMware assure une conformité renforcée, un confinement plus rapide des menaces et des actions correctives personnalisables basées sur le niveau de menace, le tout via des règles de configuration et de gestion dynamiques.

Par exemple, vous pouvez utiliser VMware pour exécuter des requêtes destinées à détecter les terminaux non conformes, puis placer ces derniers en quarantaine. Une fois la menace confinée, VMware peut informer les utilisateurs du problème de conformité et les administrateurs informatiques peuvent apporter les corrections nécessaires pour ramener les terminaux à un état conforme.

Configuration « over-the-air » et catalogue d'applications consolidé



Vous rappelez-vous la dernière fois où vous avez reçu un appel d'un cadre en déplacement qui avait malencontreusement « égaré » son ordinateur portable ? À moins que vous ayez appliqué au préalable un chiffrement BitLocker, des informations sensibles de votre entreprise se sont retrouvées dans la nature et vous n'avez rien pu y faire. Mais si vous aviez déployé une solution de gestion unifiée des terminaux, vous auriez pu effacer le contenu de l'ordinateur à distance pour empêcher la perte de données.

Les solutions de gestion de la mobilité d'entreprise (EMM) ont traditionnellement donné aux organisations la possibilité de configurer des réseaux Wi-Fi et des VPN, d'accéder à un magasin d'applications professionnelles et d'effectuer un effacement du contenu à distance sur les systèmes d'exploitation mobiles iOS, Android et autres. Grâce au déploiement de solutions EMM compatibles avec les environnements Windows traditionnels, les organisations peuvent étendre les fonctionnalités des systèmes d'exploitation mobiles à leurs outils de gestion du cycle de vie des PC afin d'offrir une meilleure expérience aux utilisateurs, d'améliorer la sécurité et de faire gagner un temps précieux à leur département informatique.

Prendre en charge le travail à distance et déployer des applications avec la virtualisation

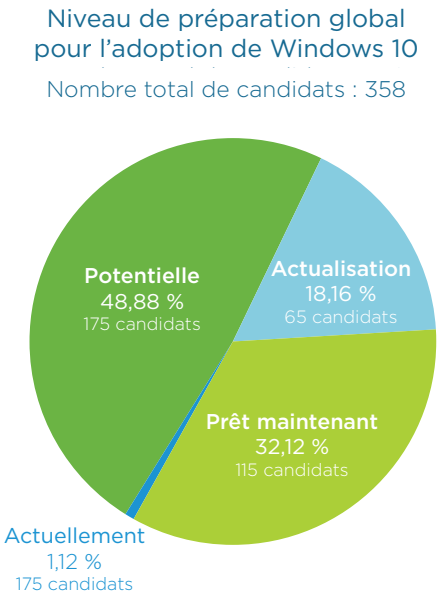
À quand remonte votre dernière évaluation des besoins de vos utilisateurs et des cas d'usage ? Alors certes, il se peut très bien que vous ayez des postes de travail virtuels en place pour des scénarios courants comme les centres d'appels et le développement à distance, mais avez-vous réfléchi à d'autres moyens d'étendre les ressources à vos collaborateurs, vos sous-traitants et vos partenaires ? Avec la virtualisation des postes de travail et des applications, vous pouvez fournir les ressources dont les utilisateurs ont besoin sur leur terminal personnel, ou sur n'importe quel terminal à vrai dire. Certaines de vos applications peuvent nécessiter une version spécifique d'un système d'exploitation, d'un navigateur ou d'un plug-in, et avoir besoin d'être virtualisées pour pouvoir s'exécuter indépendamment du système d'exploitation des utilisateurs.

VMware vous permet de déployer des postes de travail de façon centralisée et à grande échelle, d'adopter le BYOD, d'éliminer les interruptions de service causées par la perte ou l'endommagement de terminaux et d'améliorer la sécurité en conservant vos données à l'abri dans le Data Center. Par ailleurs, vous pouvez potentiellement doper votre chiffre d'affaires en éliminant les renouvellements de matériel ou en réduisant les coûts liés aux terminaux. Vous bénéficiez d'une stratégie simplifiée, sécurisée et évolutive en matière d'informatique pour l'utilisateur.

Découvrez un nouveau monde dans votre transition vers Windows 10

Henry Ford aurait dit : « Si j'avais demandé à mes concitoyens ce qu'ils voulaient, ils m'auraient répondu : de meilleurs chevaux. » L'automobile de Ford a révolutionné le problème en abordant le problème sous un angle complètement différent. De la même manière, Windows 10 s'écarte de façon spectaculaire de ses prédécesseurs, redéfinissant la manière dont les départements informatiques gèrent l'ensemble du cycle de vie des PC, des smartphones, des tablettes et de tout autre terminal qui exécute le dernier système d'exploitation de Microsoft.

Avant que Windows 10 voit le jour, les départements informatiques devaient aborder leur environnement comme un centre commercial, en assemblant des technologies disparates qui ne fonctionnent pas bien ensemble pour répondre à différentes problématiques liées à la configuration, à la distribution des logiciels, aux correctifs, aux logiciels malveillants et à la sécurité.



Avec Windows 10, Microsoft a introduit une nouvelle possibilité comparable au e-commerce : ce système d'exploitation est pratique, les technologies fonctionnent bien ensemble et elles ouvrent de nouvelles opportunités qui n'existaient pas auparavant. En échangeant avec des centaines de clients qui ont migré vers Windows 10 ou qui planifient leur déploiement, nous avons découvert qu'après l'amélioration de la sécurité au sein de l'environnement existant, il reste quatre étapes clés pour mener à bien un déploiement Windows 10 :

Évaluer ▸ Migrer ▸ Gérer ▸ Sécuriser

Étape 2 : Évaluer votre environnement existant pour éliminer toute incertitude de vos déploiements physiques et virtuels

De nombreuses organisations ont bien du mal à savoir par où commencer dans leur transition vers Windows 10, qu'il s'agisse de déterminer quelles machines existantes peuvent prendre en charge Windows 10 ou d'identifier les cas d'usage les mieux adaptés pour la virtualisation des postes de travail. Avec l'outil d'évaluation des postes de travail adéquat, les organisations peuvent bénéficier de recommandations intelligentes concernant les machines et les cas d'usage les plus appropriés pour une migration physique sur place vers Windows 10 et ceux plus adaptés pour l'exécution d'un poste de travail virtuel on-premise ou dans le Cloud. Elles acquièrent ainsi une compréhension de base de leur environnement existant, qui leur permet de savoir comment aborder leur migration vers Windows 10. Pour en savoir plus sur l'outil d'évaluation, consultez la page assessment.vmware.com.

Tout comme avec les précédentes mises à niveau vers des nouvelles versions de Windows, les administrateurs informatiques chargés des environnements de postes de travail physiques ou virtuels devront tester les applications afin de détecter les éventuels problèmes de compatibilité avant de migrer leur parc vers Windows 10. Si les applications ne fonctionnent pas sous Windows 10, l'équipe informatique peut les déployer sous forme d'applications virtuelles pour qu'elles continuent de fonctionner après la migration vers Windows 10 et que les utilisateurs puissent mener à bien leurs tâches malgré tout. Les applications « legacy » telles qu'Internet Explorer 6 en sont un exemple.

Étape 3 : Élaborer votre plan de migration des machines virtuelles et physiques

Selon Microsoft, 96 % des entreprises testent actuellement Windows 10. Cependant, nombre d'entre elles n'en sont encore qu'au stade de la planification de leur migration. Afin de donner aux clients un point de départ pour leur transition vers Windows 10, nous leur posons les questions suivantes :

- Prévoyez-vous d'adopter Windows 10 dans les 3 ou 4 ans à venir en même temps que vous renouvelez vos PC ?
- Envisagez-vous d'effectuer une migration d'image en place ou personnalisée de toutes les machines existantes ?
- Comptez-vous virtualiser les terminaux qui ne prennent pas en charge Windows 10 ?
- Prenez-vous en compte les cas d'usage au sein de votre entreprise où les postes de travail et les applications virtuels procurent des gains d'efficacité ?
- Prévoyez-vous de mettre en œuvre l'ensemble des éléments ci-dessus ?

Les organisations devront déterminer quel chemin de migration est le plus approprié pour elles, mais voici quelques-uns des moyens que nous mettons en œuvre pour les aider dans leur approche :

Actualisation

En même temps qu'elles renouvellent leurs terminaux dans les 3 ou 4 ans à venir, les organisations peuvent effectuer leur transition vers Windows 10 et gérer les nouveaux terminaux à l'aide de la structure moderne de gestion unifiée des terminaux, qui permet de simplifier l'informatique, de réduire les coûts de gestion et d'optimiser l'expérience utilisateur.

Migration

- En place : les organisations tirent parti des outils de migration en place pour migrer les machines des versions de système d'exploitation précédentes vers une image de base Windows 10 et provisionnent les règles recommandées et les applications à l'aide de la solution de gestion unifiée des terminaux.
- Image personnalisée : au lieu de l'image de système d'exploitation de base, les organisations peuvent aussi effectuer une migration vers une image recommandée pour les entreprises avec des applications et des données personnalisées, et inscrire automatiquement les terminaux dans la solution de gestion unifiée.

Virtualisation

- Les postes de travail et les applications virtuels sont mis à niveau de façon centralisée et fournis aux utilisateurs sur leurs terminaux existants. Cela permet de prendre en charge différents cas d'usage, par exemple :
  - Les machines existantes qui ne prennent pas en charge Windows 10 reçoivent un poste de travail virtuel.
  - Les organisations envisagent de déployer des postes de travail virtuels pour les scénarios d'utilisation d'ordinateurs portables personnels (BYO).
  - Virtualiser les applications stratégiques qui ne sont pas compatibles avec Windows 10.
  - Les organisations créent un isolement d'Internet ou des données pour les déploiements sensibles à la sécurité.

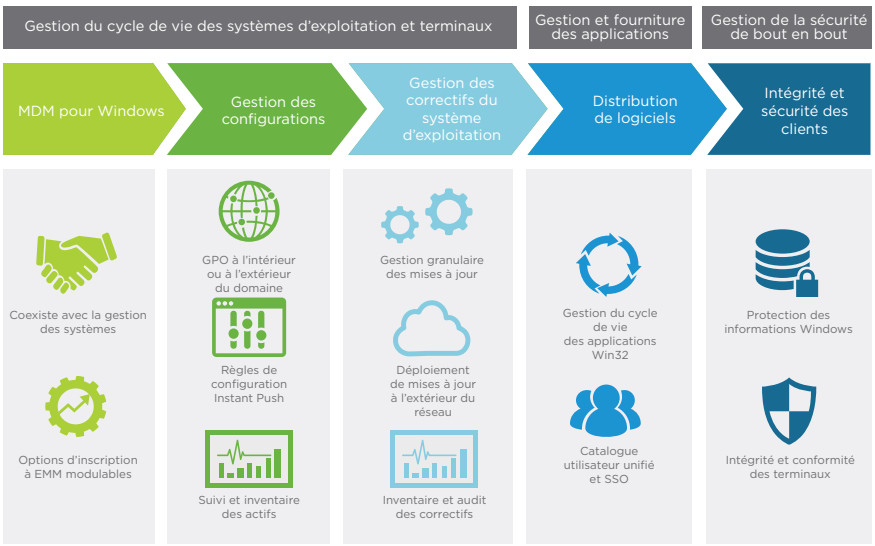
Étape 4 : Évaluer la gestion unifiée des terminaux pour les machines physiques dans la nouvelle infrastructure Windows

Les processus traditionnels mis en œuvre pour imager, déployer et configurer entièrement un PC physique peuvent demander plusieurs heures. Avec le temps, les données résiduelles des applications et du registre ralentissent les performances système, provoquant une dérive des images. Cela entraîne des problèmes de performances pour les utilisateurs et oblige souvent les départements informatiques à réintervenir et à passer plusieurs heures à réimager les terminaux, ce qui nuit à la productivité des utilisateurs.

La plupart des organisations s'appuient sur des outils de gestion du cycle de vie des PC avec des centaines d'objets de stratégie de groupe (GPO), de scripts personnalisés et des outils plus sommaires pour gérer leur environnement Windows. Malheureusement, les outils de gestion du cycle de vie des PC legacy présentent plusieurs limites, dont l'impossibilité d'exécuter des actions sur les terminaux qui se trouvent en dehors du domaine et du réseau de l'entreprise, une infrastructure coûteuse à entretenir et des processus demandant beaucoup de travail, comme la création d'images.

Le grand avantage des smartphones modernes est que vous pouvez entrer dans un magasin, acheter un terminal, saisir vos informations d'authentification et accéder ensuite automatiquement à l'ensemble de vos applications et services over-the-air en quelques minutes. Pourquoi les utilisateurs de PC ne peuvent-ils pas bénéficier de la même expérience ? Eh bien, avec Windows 10, ils le peuvent. Assorti d'une solution de gestion unifiée des terminaux, Windows 10 dote les organisations d'un nouveau moyen de prendre en charge leur parc de postes de travail et d'offrir aux utilisateurs une expérience comparable à celle d'un smartphone ou d'une tablette. Il suffit à ces derniers de saisir leur adresse e-mail professionnelle et leur mot de passe, et leur terminal est alors configuré over-the-air en quelques minutes, avec l'ensemble des applications, services et règles d'entreprise requis pour travailler. Cette nouvelle approche redéfinit la manière dont le département informatique gère l'intégralité du cycle de vie des PC, des smartphones, des tablettes et de tout autre terminal, de façon homogène à partir d'une console unifiée.

Gestion et sécurité de Windows modernes accordant la priorité au Cloud



Fini les heures passées à réimager chaque machine. Fini les Patch Tuesday. Fini l'impossibilité d'exécuter des actions sur les terminaux qui se trouvent à l'extérieur de l'entreprise. En déployant une solution de gestion unifiée des terminaux sur les machines Windows 10, le département informatique peut consacrer plus de temps au soutien de l'activité, tout en disposant d'un environnement beaucoup plus sécurisé. Les utilisateurs bénéficient d'un catalogue d'applications unifié sur leur PC Windows 10, leur tablette et leur smartphone. En outre, un portail en libre-service leur permet de résoudre les problèmes courants par eux-mêmes plutôt que d'accaparer le temps du département informatique.

Étape 5 : Renforcer la sécurité grâce à une visibilité en temps réel sur votre environnement

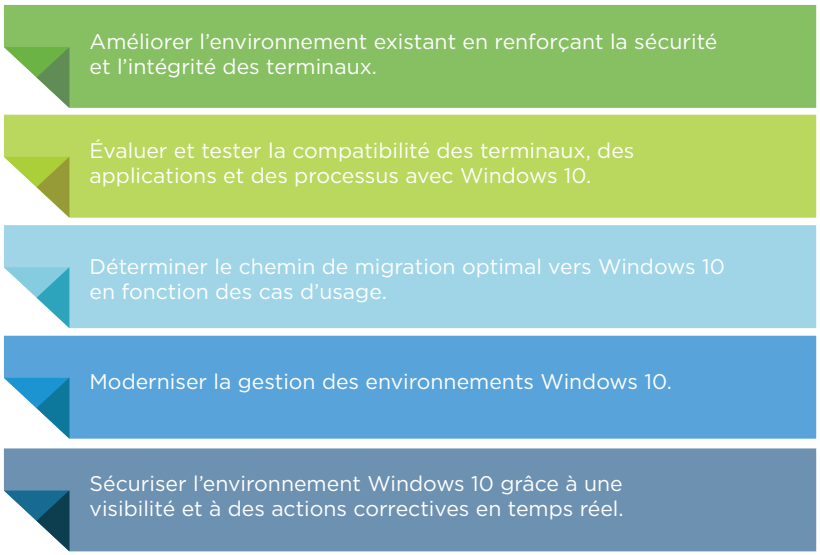
Andrew Grove, cofondateur et ancien CEO d'Intel Corporation, vivait sa vie selon une devise simple : Seuls les paranoïaques survivent. Ce principe, qui a guidé Intel vers la réussite, doit être suivi par l'ensemble du personnel informatique. Par le passé, les organisations possédaient un environnement d'exploitation standard : un seul type de terminaux exécutant un même système d'exploitation avec un ensemble d'applications pré-approuvées sur un réseau spécifique. Aujourd'hui, les départements informatiques doivent prendre en charge plusieurs types de systèmes d'exploitation exécutés sur toutes sortes de terminaux avec des ensembles uniques d'applications aussi bien sur le réseau de leur entreprise qu'en dehors.

Devant cet environnement d'exploitation dynamique et les attaques de cybersécurité toujours plus variées et nombreuses, les départements informatiques ont dû adopter un modèle « zéro confiance » pour protéger les données d'entreprise. Avec VMware, ils peuvent renforcer le système d'exploitation en mettant en œuvre les authentifications sans mot de passe, en interdisant les applications non approuvées et non signées, en surveillant la présence de terminaux dont la sécurité a été compromise et en exécutant des actions correctives automatisées qui éliminent la nécessité de créer des tickets informatiques. Ces actions peuvent inclure la restriction immédiate de l'accès aux ressources de l'entreprise lorsqu'un système d'exploitation a été identifié comme compromis ou même l'exécution d'une commande d'effacement du contenu à distance en cas de perte ou de vol d'un terminal. VMware fournit également les fonctionnalités de visibilité et de protection en temps réel mentionnées précédemment pour les terminaux exécutant Windows 10.

Pour en savoir plus sur la façon dont VMware peut vous aider à moderniser votre environnement Windows et à rentabiliser pleinement vos investissements auprès de Microsoft, consultez le site www.WindowsUEM.com/fr.

Tirez pleinement parti de votre environnement

Nous ne vous avons offert qu'un aperçu de ce que vous pouvez faire pour rentabiliser vos investissements dans Microsoft avec VMware. Si vous envisagez d'ajouter des fonctionnalités supplémentaires à votre environnement existant en migrant vers Windows 10, voici un récapitulatif rapide des cinq façons principales dont VMware peut soutenir vos initiatives :



Outre vos déploiements Windows, vous réalisez peut-être d'autres investissements auprès de Microsoft, en ayant par exemple choisi de passer à Office 365 ou à Azure Active Directory. Les solutions informatiques pour l'utilisateur de VMware peuvent vous aider à déployer et à configurer plus facilement vos applications et services Office, et à connecter vos informations d'authentification et vos règles Active Directory afin de profiter d'une identité fédérée et d'une authentification unique pour vos applications.

1,5 milliard de terminaux : http://www.computerworld.com/article/2919104/windows-pcs/where-will-microsoft-find-1-billion-devices-for-windows-10.html

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