



Guide Enjeux & Perspectives

Les meilleures pratiques pour optimiser le déploiement, la gestion et la sécurité des environnements Office 365 & Windows 10 avec VMware Workspace ONE

Facilitateur de la transformation numérique, VMware Workspace ONE unifie la gestion de tous les terminaux, qu'ils soient mobiles ou non, sécurise les applications et données de l'entreprise dans un univers devenu essentiellement mobile et transfigure les expériences utilisateurs en entreprise.

Moteurs de la transformation numérique des entreprises, la mobilité et le Cloud ont, considérablement, redessiné le rôle des IT et les prérogatives de la DSI.

Une DSI qui a dû apprendre à dire « oui » et à s'aligner sur les besoins métiers et qui doit désormais apprendre à évoluer dans des environnements toujours en mouvement et aux changements incessants.

Windows 10 et Office 365 sont deux éléments très caractéristiques de cette transformation.

Le premier a complètement transformé la gestion des mises à jour et le rythme d'évolution du système. Il a introduit une nouvelle génération de PC (Always Connected PCs, 2 en 1 hybride, Hololens, lunettes de réalité mixtes) aux interactions incroyablement plus riches à même de servir de nouveaux scénarios jusqu'ici impossibles.

Le second a, totalement, transfiguré le travail collaboratif permettant à tous

les collaborateurs de rester efficaces et productifs où qu'ils soient et quel que soit l'appareil entre leurs mains.

Ces nouveaux environnements, ces nouveaux outils, ces nouvelles interactions et ces nouveaux scénarios sont, autant, de challenges à relever par les IT pour permettre à l'entreprise d'être agile et réactive tout en restant sécurisée, fiable, et cohérente.

Le premier rôle de la DSI est, aujourd'hui, de permettre la concrétisation de ces nouveaux usages et scénarios. Ce qui impose de repenser des process IT parfois ancestraux et de trouver des solutions originales à des problèmes d'intégration parfois très complexes.

Avec **Workspace ONE**, VMware introduit une nouvelle génération d'outils pour aider les DSI à gagner en agilité et à concrétiser cette transformation digitale nécessaire aux métiers.

1/ Adopter l'agilité du numérique

L'agilité numérique commence par ne pas laisser l'utilisateur attendre pendant plusieurs jours voire plusieurs semaines que son nouveau terminal soit configuré, que celui-ci soit un nouveau PC fourni par l'entreprise ou un appareil mobile personnel. Dès qu'il sort du magasin avec son matériel, l'utilisateur s'attend à pouvoir accéder immédiatement et en libre-service aux données, applications et services de l'entreprise. C'est, exactement, le type de scénario que permet **VMware Workspace ONE** tout en assurant aux IT visibilité et contrôle sur ces appareils, sans pour autant nuire à la sécurité de l'entreprise ni envahir l'espace privé et personnel de l'utilisateur.

Il ne s'agit, d'ailleurs, pas seulement d'accepter l'usage professionnel d'un terminal personnel (BYOD) mais, bien au-delà, de permettre à l'entreprise d'adopter la multiplicité des terminaux, des systèmes et des usages sous toutes leurs formes dans un cadre facilitateur et sécurisant. En effet, dans ce nouvel âge numérique, la plupart des entreprises du monde entier sont bien contraintes d'accepter le fait que nombre de leurs collaborateurs passent 50 à 60% de leur temps hors de leur bureau. La DSI se retrouve, donc, confrontée à devoir repenser l'idée même du poste de travail en acceptant la diversité des outils et des lieux. Quels que soient les scénarios d'acceptation envisagés (BYOD, CYOD, COPE, etc.), **VMware Workspace ONE** est la plateforme qui permet leur mise en œuvre rapide et sécurisée.

Elle combine la livraison d'apps et de services depuis un catalogue unifié défini par l'entreprise, à une puissante gestion des identités, des outils innovants de supervision et d'analytique, et une gestion mature et éprouvée des terminaux et de leur diversité. Elle permet de pousser à distance, « over the air », à tous types

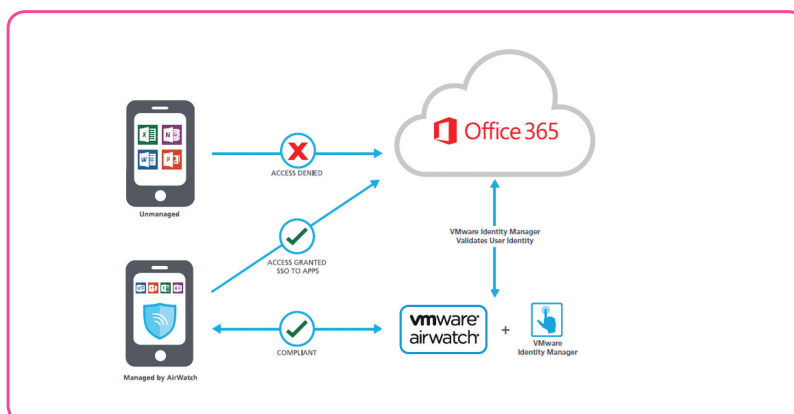
de terminaux des configurations et des politiques d'entreprise qui permettent de, dynamiquement, contrôler et adapter les droits d'accès en fonction de l'état du terminal et de son niveau de sécurisation. Dès lors, elle procure à l'entreprise l'agilité réclamée à la fois par les métiers et par les collaborateurs.

2/ Gérer la mobilité sous toutes ses formes

La DSI ne peut aller à l'encontre des nouveaux usages. Une étude récente démontrait que 60% des employés préféreraient utiliser un appareil personnel pour travailler (mais aussi se distraire chez lui) et que 30% des collaborateurs utilisaient quand même leurs appareils personnels pour travailler, quitte à aller à l'encontre des politiques dédiées par l'entreprise.

Contrairement à ce que l'on pourrait croire, le "Non" des DSI à ces nouveaux usages n'est jamais un gain de sécurité : c'est, au contraire, l'assurance à brève échéance de perdre de plus en plus de contrôle sur l'usage des informations et des applications.

Bien sûr, la fragmentation des systèmes d'exploitation et des types de terminaux mobiles (n'oublions pas qu'un notebook PC ou Mac est, par nature, lui aussi mobile) est un challenge : elle rend complexe la gestion et la sécurisation des données sur les multiples points d'accès de l'entreprise. C'est justement cette complexité que **VMware Workspace ONE** prend en charge pour la masquer aux IT et leur permettre de définir des **règles universelles**. Parmi ces règles, la possibilité de définir et forcer des autorisations d'accès en fonction d'un très grand nombre de critères comme la force de l'authentification,



le réseau, l'emplacement géographique, la conformité du matériel (pour éviter, par exemple, que la connexion d'appareils rootés ou jailbrakés, vulnérables à toutes sortes d'attaques).

3/ Unifier la gestion des appareils

Pour satisfaire les scénarios évoqués plus haut, l'entreprise doit intégrer le fait qu'un PC Windows n'est plus ce qu'il était. Des tablettes 2 en 1 aux lunettes Hololens, en passant par les Ultrabooks super « sexy » et les nouveaux Always Connected PC sous ARM à l'autonomie renversante (plus de 20 heures en conditions réelles), Windows 10 a changé le visage du PC... Il en a, aussi, profondément bouleversé la gestion. Grâce à **Workspace ONE**, un appareil Windows peut s'administrer comme un smartphone ou une tablette. L'acceptation des terminaux personnels dans le système d'information se réalise dans un environnement totalement sécurisé, contrôlé et sans surcharge pour les équipes IT.

C'est l'utilisateur lui-même qui introduit et déclare son nouveau matériel au travers d'un portail en Self-Service. Une fois déclaré, le terminal devient bicéphale : usages personnels et usages professionnels sont disjoints, isolés, et tout l'univers professionnel peut, aisément, être éradiqué à distance en cas de perte du matériel ou de départ du collaborateur. Mais, au-delà de ces fonctionnalités BYOD/CYOD désormais matures et bien maîtrisées, **Workspace ONE simplifie grandement l'administration de Windows 10**. On le sait, avec son concept de « Windows as a Service » et ses multiples branches de déploiement (CB, CBB, LTSB), le nouveau Windows nécessite des processus d'administration, radicalement, différents notamment pour maîtriser les impacts de mises à jour rendues plus fréquentes, mais surtout obligatoires.

VMware Workspace ONE permet une simplification de ces processus en introduisant des groupes de mises à jour approuvées, un contrôle centralisé des fenêtres de maintenance, un mécanisme d'approbation automatique ou par l'utilisateur des phases de mise à jour, etc.

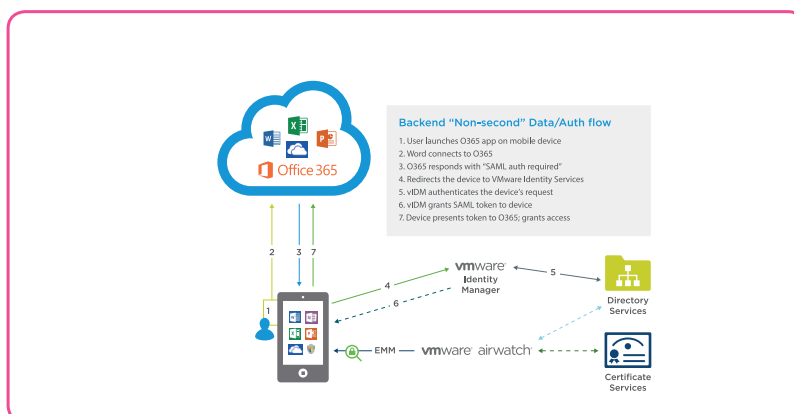
4/ Optimiser les expériences utilisateurs

La solution **VMware Workspace ONE** propose un espace de travail numérique unifié, quel que soit le terminal utilisé. Les départements informatiques peuvent, ainsi, fournir aux utilisateurs les mêmes services et applications sur tous les appareils et proposer à la fois une expérience simplifiée et une sécurité de classe d'entreprise.

Typiquement, **les anciennes applications Windows « métier » peuvent être exécutées sur tout terminal**. Grâce à un mécanisme de streaming, elles ne sont pas physiquement installées sur les terminaux non autorisés, de sorte que leur usage et leurs données restent « dans l'entreprise ».

Les nouvelles applications mobiles et SaaS sont exposées au travers d'un catalogue unifié utilisant une authentification forte, un environnement d'authentification unique, ainsi que des contrôles d'accès conditionnel.

La DSI peut alors établir des règles d'accès pour n'importe quelle application. Toutes les données et tous les points d'accès bénéficient d'un environnement sécurisé. Enfin, les nouvelles applications et nouveaux services développés en interne peuvent, également, être distribués via ce catalogue unifié sans que l'entreprise n'ait à passer par une diffusion sur les stores de chaque environnement.



Par-delà ce catalogue unifié et cet accès universel à toutes les applications **quel que soit l'appareil, Workspace ONE** transfigure l'expérience utilisateur au quotidien **au travers de sa fonctionnalité de "Single Sign-On" (SSO), intégrée à sa fonction de gestion des identités (Identity Manager).**

Les utilisateurs sont automatiquement authentifiés sur la multiplicité des services qu'ils utilisent au travers de leur authentification à **Workspace ONE.**

5/ Superviser tous les usages, y compris ceux du Cloud

Cette facilité de « Single Sign-On » s'applique à tous les appareils (mobiles ou non) et à tous les services y compris Office 365. Typiquement, quand Office 365 reçoit une requête d'authentification, il la redirige à **Workspace ONE** qui l'analysera en fonction du type d'appareil et de sa conformité avant de la retourner à Office 365.

Ce mécanisme permet aux DSI de définir des politiques d'accès à Office 365 plus contraignantes et plus sécurisées sans pour autant impacter l'expérience utilisateur.

C'est important parce qu'avec Office 365, les voies d'accès à l'email et aux données se sont multipliées : applications Mac/Windows, apps mobiles, navigateurs Web. Chaque voie ayant son propre mécanisme d'authentification, il en résulte une complexité accrue et des risques de sécurité nouveaux.

Workspace ONE masque cette complexité tout en renforçant le niveau de sécurité global. Il assure le déploiement automatique des applications sur les appareils personnels enregistrés avec les politiques d'utilisation

associées. Il protège les informations de l'entreprise stockées via OneDrive dans un conteneur isolé du reste de l'appareil.

Enfin, il offre un client email d'entreprise, convivial et intuitif, s'exécutant dans une bulle sécurisée, un conteneur, isolé du reste du système mobile.

De plus, la nouvelle fonctionnalité **Workspace ONE Intelligence** invite désormais les IT à une approche plus efficace de l'administration. **Elle met l'analytique et le Machine Learning au service de l'IT.**

Grâce à la collecte et l'analyse de données provenant des terminaux, applications et utilisateurs d'un déploiement **Workspace ONE**, elle trouve des corrélations, détecte des anomalies et fournit des recommandations.

Elle met à disposition des outils de recherche et d'investigation. Elle offre, surtout, aux IT une vision étendue de tout ce qui se passe et permet de définir des réactions automatisées à toutes sortes d'événements et incidents, y compris en matière de sécurité. Très visuels, les tableaux de bord peuvent d'intégrer à d'autres outils comme ServiceNow.

En intégrant la gestion des identités, le SSO, la gestion de la mobilité d'entreprise, la livraison d'applications en temps réel sur tous les appareils et l'automatisation de processus IT à travers une analytique avancée, VMware Workspace ONE transfigure la gestion des ordinateurs, tablettes et smartphones au sein de l'entreprise. La solution déploie et gère n'importe quelle app sur n'importe quel dispositif tout en sécurisant et simplifiant l'intégration d'appareils personnels dans l'environnement professionnel.

Elle contribue à changer l'image de la DSI auprès des autres entités et permet à tous les collaborateurs d'être productifs et mobiles en toute sécurité.

Insight, un partenaire innovant

Des entreprises privées aux organisations gouvernementales, Insight apporte à ses clients des Solutions Technologiques Intelligentes afin de réaliser leurs objectifs. En tant que fournisseur mondial, classé Fortune rang 500, de Hardware, Software, Cloud et Services, les 5 400 collaborateurs offrent aux clients les conseils et l'expertise nécessaires pour sélectionner, mettre en œuvre et gérer des solutions technologiques complexes pour les conduire aux meilleurs résultats commerciaux possibles. Grâce au réseau international, à ses partenaires, services et solutions, Insight aide les entreprises à fonctionner plus efficacement. Découvrez-en plus sur [Insight.com](https://www.insight.com).