RÉSUMÉ

Modernisez la gestion et la sécurité de Windows 10 avec la solution de gestion unifiée des terminaux VMware AirWatch

L'évolution de l'espace de travail moderne

Dans un monde du travail EN CONSTANTE ÉVOLUTION, les entreprises d'aujourd'hui emploient des individus plus mobiles et autonomes que jamais. Avec la prolifération des appareils mobiles, les collaborateurs s'appuient sur un large éventail d'applications, de terminaux et de services Cloud dans le cadre de leurs activités. Ils sont de plus en plus nombreux à effectuer des tâches personnelles et professionnelles sur le même terminal, et valorisent les critères de choix, de libre-service et de confidentialité. Les départements informatiques incapables de satisfaire ces besoins déploient des environnements utilisateur peu satisfaisants, ce qui démotive les collaborateurs, qui se tournent alors vers une offre de services informatiques « fantôme » (non officielle).

En outre, les départements informatiques eux-mêmes sont fortement cloisonnés avec d'un côté les silos de gestion des postes de travail et de l'autre, les silos de gestion de la mobilité. Les équipes informatiques répondent aux besoins en gestion des terminaux mobiles par l'utilisation de solutions EMM modernes (Enterprise Mobility Management ou gestion de la mobilité d'entreprise). Jusqu'à présent cependant, les ordinateurs de bureau ont été gérés de manière indépendante au moyen d'outils de gestion du cycle de vie des PC.

Ce modèle de gestion fragmentée ne répond pas du tout aux attentes en matière de coûts et de sécurité informatiques. Les utilisateurs étant de moins en moins sédentaires, et les outils classiques de gestion du cycle de vie du parc de PC nécessitant que les terminaux appartiennent au domaine et au réseau d'entreprise pour être associés aux stratégies informatiques et bénéficier de mises à jour de système d'exploitation et de correctifs, le risque de non-conformité augmente ainsi que les vecteurs d'attaque potentiels.

Pour répondre aux besoins de ces travailleurs de la nouvelle génération, il est nécessaire de commencer par éliminer les silos de gestion, puis d'adopter une approche cohérente et tournée vers l'utilisateur sur tous les terminaux. Selon M. Chris Silver, analyste chez Gartner, « L'avenir de la gestion des terminaux réside dans la consolidation des outils prenant en charge les PC traditionnels et les terminaux mobiles à l'heure où un cadre commun de gestion se met en place entre les deux univers. »

L'intégration de protocoles de gestion de la mobilité dans Windows 10 donne aux départements informatiques l'opportunité d'unir les différentes équipes d'administration et de consolider les outils, de réduire les coûts, d'améliorer l'efficacité informatique et de renforcer la sécurité de l'entreprise. Désormais, en s'appuyant sur une solution de gestion unifiée des terminaux, l'entreprise est en mesure de simplifier la gestion des terminaux des utilisateurs (postes de travail et appareils mobiles).

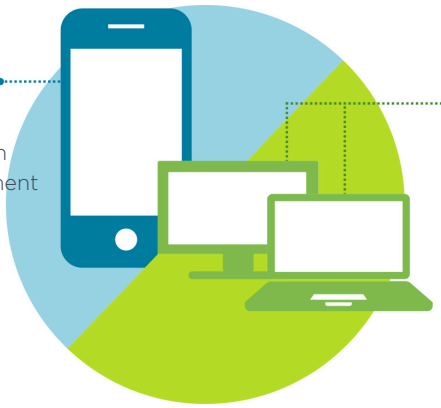
LES LIMITES DE L'APPROCHE CLASSIQUE DE LA GESTION DES PC

Les départements informatiques doivent avoir comme principal objectif d'offrir une expérience optimale à l'utilisateur final, afin de stimuler son efficacité et sa productivité. Toutefois, sur de nombreux aspects, les environnements utilisateur des appareils mobiles et des ordinateurs présentent des caractéristiques radicalement opposées. Alors que le déploiement et la configuration d'un terminal mobile est devenu un processus autonome et efficace, le déploiement d'un poste de travail ou d'un ordinateur portable peut prendre plusieurs semaines ; quant aux heures passées à la création d'image, la configuration et la gestion, elles ne se comptent plus.

Face au niveau élevé de rationalisation de la configuration et de la gestion des terminaux mobiles, la frustration des utilisateurs ne cesse d'augmenter lorsqu'ils constatent qu'à l'inverse, la configuration des PC reste un processus lent et restrictif.

Terminal mobile

L'utilisateur sort du lieu d'achat avec un téléphone entièrement configuré



Poste de travail et ordinateur portable

L'utilisateur attend pendant des semaines que son terminal soit configuré

Comment changer la donne ?

1 Le système d'exploitation

Le système d'exploitation Windows est le premier composant qui doit évoluer pour répondre aux besoins actuels des effectifs. Windows 10 est un système d'exploitation centré sur le consommateur et doté de fonctionnalités combinant liberté de choix, confidentialité et mobilité. Plus important encore : l'adoption d'une approche fondamentalement différente de la protection et de la gestion du système d'exploitation, davantage en adéquation avec les solutions EMM modernes. L'ensemble unifié de protocoles de gestion sur les PC, tablettes et téléphones Windows 10 permet désormais aux départements informatiques de consolider les outils de gestion, de provisionner les appareils prêts à l'emploi, et de publier des règles et applications over-the-air pour former les utilisateurs rapidement.

2 Les outils d'administration

Les outils de gestion des PC existants ne sont pas en mesure de répondre de manière efficace aux besoins actuels des utilisateurs, qui souhaitent travailler n'importe où, à tout moment et depuis n'importe quel terminal. En outre, les utilisateurs souhaitent retrouver un environnement identique sur tous leurs appareils pour accéder à leurs applications et données professionnelles. Satisfaire ces attentes devient plus complexe pour les équipes informatiques qui continuent à gérer les PC au moyen d'outils traditionnels, du fait que ces derniers sont :

- **Coûteux** : les approches héritées de la gestion des PC se caractérisent par une utilisation élevée des serveurs et des ressources ; elles s'appuient sur plusieurs solutions logicielles et reposent sur des méthodes complexes de création d'image et de gestion de la configuration. La gestion des mises à jour logicielles et des correctifs de système d'exploitation est un processus fastidieux, et les départements informatiques se voient contraints de développer et de gérer des compétences en interne pour répondre aux besoins d'une gestion des postes de travail et des appareils mobiles par silos.

- **Non sécurisés** : la gestion est en grande partie assurée par des stratégies de groupe (GPO) applicables uniquement aux périphériques en réseau et joints à un domaine. Avec cette approche, la mise en œuvre des politiques de sécurité, des correctifs de système d'exploitation et des mises à niveau d'application peut prendre plusieurs semaines, voire même des mois, ce qui rend l'entreprise vulnérable à des risques accrus en matière de sécurité. Avec l'apparition quotidienne de nouveaux vecteurs d'attaque, il devient encore plus difficile de bénéficier d'une visibilité adéquate sur l'état d'intégrité et de conformité des terminaux.

- **Restrictifs** : les approches héritées font monter la frustration des utilisateurs en limitant le contrôle que ces derniers peuvent avoir sur leurs appareils. En effet pour renforcer la sécurité, les départements informatiques doivent limiter les types de périphériques utilisés et autoriser uniquement les applications et les mises à jour sécurisées sur le système d'exploitation. Cela laisse peu de place à la personnalisation, avec peu ou pas de fonctionnalités en libre-service pour les utilisateurs. Résultat : ces restrictions génèrent des demandes hautement personnalisées et un nombre accru d'appels du service d'assistance, même pour des tâches aussi simples que l'installation d'une application sur un terminal.

L'AVÈNEMENT DE LA GESTION UNIFIÉE DES TERMINAUX

L'introduction d'API de gestion de la mobilité dans Windows 10 change radicalement le mode d'administration des PC en entreprise. Il n'en reste pas moins que les PC présentent des contraintes qui leur sont propres :

- La prise en charge nécessaire de scripts et de stratégies de groupe complexes
- Le packaging et la distribution d'applications Windows (Win32) classiques
- Le test des correctifs de système d'exploitation avant leur mise à disposition des utilisateurs
- La taille de ces applications et mises à jour, qui limitent la capacité du réseau

Les entreprises ont besoin d'une plateforme de gestion unifiée des terminaux qui combine l'efficacité d'une solution EMM pour les terminaux mobiles avec le niveau de granularité nécessaire dans l'approche classique de la gestion des PC.

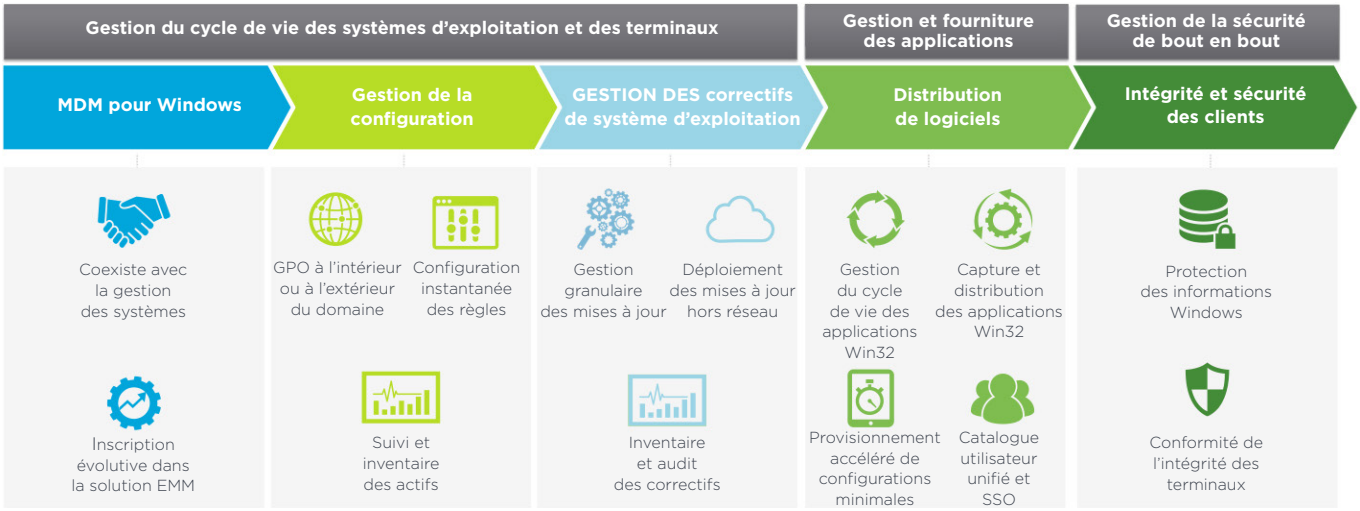
La solution de gestion unifiée des terminaux VMware AirWatch intègre un ensemble complet de fonctionnalités Windows 10 permettant le déploiement, la configuration, la distribution d'applications (y compris les applications Win32) et de mises à jour, ainsi que la protection de bout en bout du système d'exploitation. Par cette approche moderne donnant la priorité au Cloud, la solution permet d'alléger les coûts et la charge des départements informatiques, ainsi que de simplifier et de sécuriser davantage l'implémentation et la gestion de Windows 10. L'entreprise peut ainsi :

- Passer d'un processus de création d'image coûteux à un modèle de déploiement simplifié
- Prendre en charge l'application de correctifs du système d'exploitation et la distribution de logiciel en dehors du domaine et sur n'importe quel réseau
- Provisionner l'accès en libre-service et laisser aux utilisateurs le choix des fonctionnalités, périphériques et applications
- Autoriser la coexistence des données personnelles et professionnelles sur les appareils
- Garantir une visibilité instantanée, la sécurité et la conformité pour tous les terminaux au sein ou en dehors du réseau

Grâce à AirWatch UEM, la gestion Windows couvre tous les cas d'utilisation :

- Déploiement de Windows 10 pour les collaborateurs distants
- Intégration des appareils appartenant personnellement aux employés (BYOD)
- Implémentation de déploiements d'entreprise à l'échelle des succursales
- Gestion d'un terminal spécifique à une branche d'activité

AirWatch UEM assure une gestion des terminaux plus simple, plus sûre et plus économique



DÉPLOIEMENT DE FONCTIONS DE GESTION ET DE SÉCURITÉ WINDOWS ACCORDANT LA PRIORITÉ AU CLOUD

MDM pour Windows

AirWatch prend en charge des workflows homogènes d'inscription des périphériques adaptés à tous les cas d'utilisation, tels que les appareils appartenant à l'entreprise ou aux employés, qu'ils soient joints à un domaine, nouveaux ou déjà configurés. AirWatch permet de transformer intégralement un terminal OEM générique en un appareil fiabilisé et prêt à l'emploi sans qu'il soit nécessaire de créer d'image, ce qui économise du temps et de l'argent. Outre les workflows des départements informatiques, AirWatch prend également en charge les besoins des utilisateurs en intégrant les terminaux de manière intuitive, en libre-service.

Pour les utilisateurs de terminaux personnels ou les sous-traitants, AirWatch prend également un processus d'inscription avancé qui repose sur le degré de sensibilité des applications et les exigences de sécurité. Par exemple, l'accès aux applications de productivité de base peut être octroyé via un catalogue d'applications d'entreprise personnalisé en fonction de l'identité et des droits de l'utilisateur. L'accès aux applications contenant des données sensibles peut être réservé aux terminaux intégralement gérés avec AirWatch.

AirWatch peut tirer parti de ce cadre moderne du Cloud mobile pour gérer les terminaux Windows intégrés et configurer des règles instantanément over-the-air. Avec chaque nouvelle mise à niveau de Windows 10, Microsoft met à la disposition des fournisseurs de solutions EMM un ensemble commun de protocoles de gestion toujours plus étendu. Ainsi la gestion repose sur un modèle s'inspirant davantage des profils et paramètres utilisateur utilisés aujourd'hui dans le cadre de la gestion des terminaux mobiles. Ainsi l'utilisation de règles de mot de passe, la configuration d'une messagerie, l'accès à l'environnement d'entreprise par le Wi-Fi et un VPN, ou l'application de restrictions au niveau des terminaux et des applications par exemple, visent à simplifier la configuration du système d'exploitation et à renforcer la sécurité.

Gestion de la configuration

Pour les PC Windows, les départements informatiques sont souvent soumis à des exigences d'automatisation complexes qui les obligent à utiliser des scripts complexes, des règles d'objet de stratégie de groupe (GPO), ainsi que d'autres paramètres d'administration propres aux PC traditionnels. Certaines entreprises souhaitent par exemple personnaliser leurs postes de travail avec l'affichage d'un papier peint spécifique, supprimer les logiciels encombrants et définir des règles de pare-feu et d'antivirus. Les fonctionnalités de gestion de la configuration d'AirWatch permettent aux départements informatiques de créer des « produits » qui incluent ces fichiers, applications ou paramètres personnalisés. Ces produits peuvent ensuite être déployés instantanément sur n'importe quel réseau ; ils peuvent également être associés à une séquence plus complexe de tâches et de conditions d'installation.

Gestion des correctifs du système d'exploitation

En proposant les mises à jour de Windows sous forme de service, Microsoft distribue les mises à jour cumulées du système d'exploitation en mode over-the-air. Les mises à jour qui ont subi un cycle de test étendu sont disponibles sous forme de service de maintenance directement exploitable. Bien que ce modèle de déploiement dans le Cloud et de mise en service présente des avantages, les départements informatiques redoutent toujours de perdre le contrôle sur :

- Les mises à jour qui sont distribuées
- Le risque d'altération du système d'exploitation dont les mises à jour n'ont pas été rigoureusement testées en interne
- Les contraintes de réseau, étant donné que la taille de ces mises à jour se chiffre désormais en plusieurs giga-octets

Wi-Fi | VPN | Certifications | Messagerie | Codes d'accès | Conformitéet restrictions | Cryptage | Pare-feu et antivirus | Gestion des licences de système d'exploitation

AirWatch simplifie la configuration et la gestion des terminaux en mode over-the-air.

AirWatch permet aux départements informatiques de déployer et/ou de reporter les mises à jour et correctifs de système d'exploitation en fonction d'une échelle de priorité pour les terminaux et des fenêtres de maintenance choisies. Les équipes informatiques peuvent approuver automatiquement ou refuser certains groupes de mises à jour (applications, développement, sécurité, etc.), sur la base du niveau de sensibilité des utilisateurs par rapport aux mises à jour de fonctionnalités et de sécurité. En exploitant la mise en cache pair à pair, AirWatch garantit l'optimisation du déploiement des mises à jour et évite la saturation du réseau. Les départements informatiques peuvent recevoir un inventaire détaillé et effectuer un audit de la conformité des mises à jour Windows spécifiques, tout en surmonter les défis posés par l'application de correctifs hors réseau.

Distribution de logiciels

Avec sa plateforme Windows universelle (UWP), Microsoft a unifié l'environnement applicatif sur tous les terminaux équipés de Windows 10. Les applications UWP publiques sont désormais disponibles sur le Windows Store (qui propose une expérience de magasin en ligne similaire à celle des autres plateformes de systèmes d'exploitation pour mobile) ou via un magasin interne personnalisable pour chaque entreprise. AirWatch s'intègre à la fois au Windows Store et au Windows Store pour Entreprise, permettant ainsi de rationaliser la fourniture de ces applications modernes.

Toutefois, la plupart des logiciels d'entreprise Windows sont toujours des applications Win32 classiques volumineuses qui peuvent s'avérer complexes à packager, déployer et gérer. En conséquence, la distribution de logiciels constitue l'une des principales difficultés inhérentes à la gestion de Windows avec des solutions EMM. AirWatch surmonte cet obstacle en éliminant les lacunes dans la gestion du cycle de vie des applications UWP et Win32.

Grâce à AirWatch, les départements informatiques peuvent consolider la gestion des applications mobiles et le déploiement des logiciels Win32 traditionnels via une console d'administration unique. Les administrateurs peuvent gérer les correctifs des applications tierces, transférer les dépendances, et même définir les conditions ou les éventualités liées à l'installation des applications.

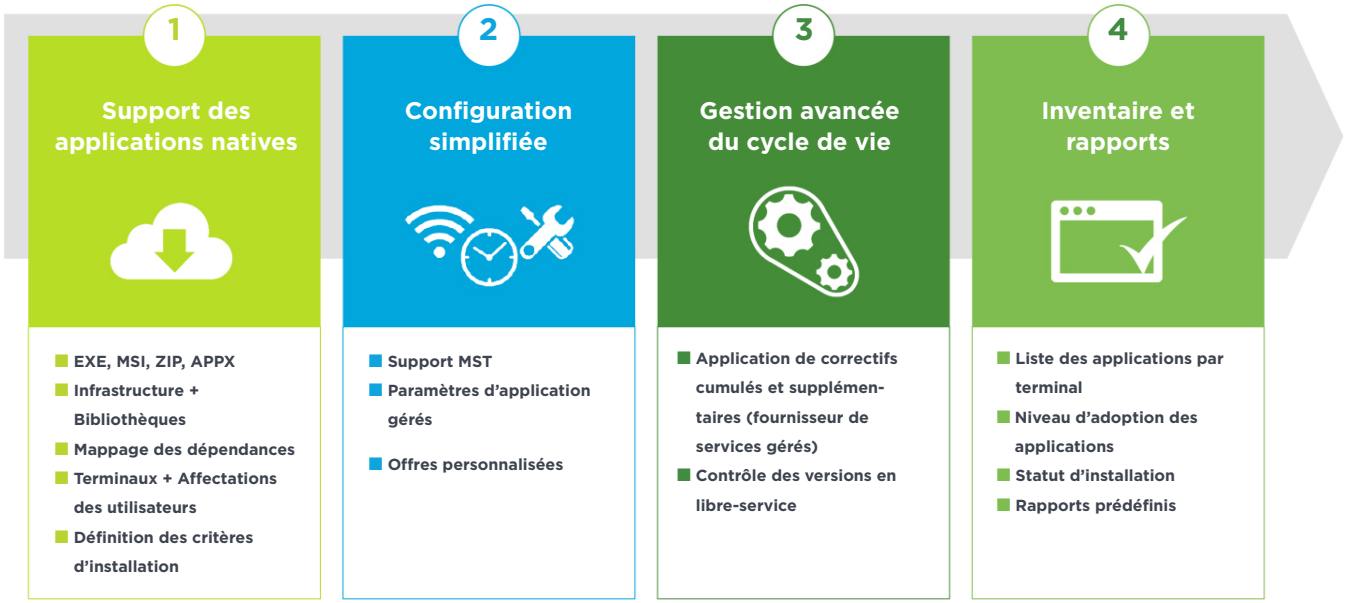
Avec la fonctionnalité App Stacks, AirWatch introduit une nouvelle approche de la distribution de logiciels qui passe outre les problèmes relatifs au packaging d'application et aux installations non fiables. Les applications Win32 peuvent également être déployées plus rapidement sur n'importe quel terminal Windows, de manière aussi fiable et facile que le déploiement d'une application mobile. Pour l'utilisateur final, AirWatch propose un catalogue en libre-service et un accès unique sécurisé à toutes les applications Windows, qu'elles soient natives, SaaS ou distantes.

Intégrité et sécurité des clients

Aujourd'hui les nouveaux défis en matière de cybersécurité imposent également l'application d'une politique de sécurité de bout en bout. AirWatch gagne la confiance des utilisateurs, renforce la protection du système d'exploitation contre les nouvelles menaces, et assure la séparation des données professionnelles et personnelles afin de protéger les données d'entreprise inactives, en cours d'utilisation et en transit.

- **Confiance des utilisateurs** : même les mots de passe les plus sécurisés restent vulnérables et peuvent être piratés de nombreuses

Fonctionnalités de gestion des applications Win32



manières (attaque d'hameçonnage, enregistrement de frappe, logiciel malveillant, etc.). AirWatch s'intègre avec les fonctions de gestion des identités de Windows 10 pour définir des règles d'authentification sans mot de passe, via des gestes ou l'utilisation d'un code PIN. Une fonction d'authentification multifacteur prête à l'emploi peut être mise en place afin d'aider les entreprises à se protéger des attaques de type « Pass-The-Hash ».

■ **Renforcement du système d'exploitation** : AirWatch permet aux départements informatiques d'adopter des mesures de sécurité proactives en empêchant le téléchargement ou l'exécution d'applications non sécurisées ou non approuvées. AirWatch vérifie l'état d'intégrité et de conformité des terminaux en temps réel, et bloque automatiquement l'accès aux applications et services d'entreprise pour les terminaux non conformes.

■ **Protection des données** : avec la multiplication actuelle des terminaux mobiles, qui s'accompagne d'une augmentation des risques de perte ou de vol, la prévention des pertes de données est devenue une priorité majeure. En outre, les utilisateurs utilisent souvent une même machine pour leurs activités professionnelles et personnelles. AirWatch définit des stratégies de chiffrement des données, permet aux administrateurs et utilisateurs d'effacer le contenu d'un terminal en cas de perte ou de vol, et tire parti des fonctionnalités natives de conteneurisation du système d'exploitation Windows pour séparer les données professionnelles et personnelles.

AirWatch UEM aide l'entreprise à gérer la sécurité de bout en bout et de manière rentable.

SÉCURISATION DE N'IMPORTE QUEL TERMINAL À PARTIR D'UNE PLATE-FORME UNIQUE

De par sa conception, UEM est indépendant de la plate-forme et procure une solution unique pour gérer chaque terminal et chaque système d'exploitation, quel que soit le cas d'usage au sein de l'organisation. Ainsi, les utilisateurs bénéficient d'une expérience cohérente sur tous les terminaux grâce auxquels ils accèdent à l'environnement de l'entreprise.

AirWatch UEM offre une approche globale et centrée sur l'utilisateur conçue pour gérer et sécuriser n'importe quel terminal à partir d'une plate-forme unique. La solution prend en charge le déploiement mondial d'une entreprise à l'échelle des divisions, des régions et des départements dans une console unique avec une architecture à locataires multiples. AirWatch UEM s'intègre aux systèmes d'entreprise pour optimiser les investissements dans l'infrastructure existante et étendre ces services à tous les terminaux.

Avec VMware AirWatch UEM, les départements informatiques sont en mesure d'automatiser les processus sur les plates-formes Windows 10 par le biais de moteurs de règles dynamiques et intelligents. Cette configuration permet de minimiser les tâches manuelles et d'activer des fonctions en libre-service, d'où une réduction des coûts de support technique.

Êtes-vous prêt à repenser votre approche de la gestion des terminaux ? Nous vous invitons à inscrire jusqu'à 100 terminaux pour une évaluation gratuite d'une durée de 30 jours. Pour en savoir plus, visitez le site Web.