Meilleures pratiques en matière de mobilité d'entreprise :

gestion des terminaux mobiles, conteneurisation ou les deux ?

LIVRE BLANC

vmware®

Présentation

Introduction

Il y a moins d'un an, les prévisions des analystes avaient laissé croire aux fervents défenseurs de la mobilité qu'une catastrophe allait toucher de plein fouet le secteur de la gestion des terminaux mobiles. Lors d'un événement réservé aux analystes qui s'est tenu en 2013, un panel de spécialistes indiquait que l'utilisation des terminaux personnels allait aboutir à une réduction des prix et faire chuter les ventes. Ils annonçaient la mort de cette industrie. « La gestion des terminaux mobiles est actuellement totalement chaotique et je pense que ce marché est en train de mourir. » déclarait l'analyste Gartner John Girard (CRN.com). John Girard avait prévu une nouvelle orientation dans la gestion de niveau application qui était liée à l'utilisation de terminaux personnels et à la résistance que montraient les employés devant la gestion par l'entreprise de leurs terminaux personnels.

Au cours de la même session, un autre analyste indiquait « entrevoir la fin d'une époque, car ils construisent des conteneurs. Ils créent une solution de gestion des applications sur mobile pour s'engager sur cette nouvelle voie. » Les analystes avaient prévu une nouvelle orientation du paradigme : les directeurs informatiques et les spécialistes de la mobilité allaient abandonner totalement la gestion au niveau du terminal, et choisir une gestion des données et applications plus granulaire, par l'intermédiaire d'un conteneur d'entreprise crypté. Selon leurs prévisions, la mobilité d'entreprise allait s'orienter vers la gestion des données et non du terminal.

Aujourd'hui, le marché ne correspond pas exactement à ces prévisions. D'après un rapport Technavio, la gestion des terminaux mobiles reste la méthode favorite pour sécuriser l'utilisation de terminaux personnels. La gestion de niveau application par la conteneurisation gagne en popularité tandis que la gestion des terminaux mobiles suit son rythme. Au lieu de remplacer une méthode par une autre, les entreprises ont réalisé que la gestion des terminaux mobiles et la gestion de niveau application restent toutes deux pertinentes selon les différents déploiements de terminaux. Dans certains cas, elles offrent même des fonctionnalités supplémentaires et renforcent la sécurité si elles coexistent sur le même terminal.

Au lieu de faire le choix de la gestion des terminaux mobiles ou de la conteneurisation, les entreprises doivent définir des cas d'utilisation de terminaux et des exigences en matière de sécurité, afin de choisir les solutions qui correspondent le mieux à leurs besoins. Quel que soit leur type de déploiement (terminaux appartenant à l'entreprise, utilisation de terminaux personnels ou combinaison des deux), les entreprises estiment que l'association de la gestion des terminaux mobiles et la conteneurisation apporte de la flexibilité, offre d'autres possibilités aux utilisateurs et renforce la sécurité. De nombreuses organisations choisissent de déployer conjointement un système de gestion des terminaux mobiles et un autre de conteneurisation sur les mêmes terminaux afin de gérer les questions de sécurité par une approche en couches. Nous verrons plus loin des cas d'utilisation d'entreprise courants et définirons les avantages de la gestion des terminaux mobiles, de la conteneurisation et de l'approche en couches de la sécurité qu'offrent ces deux systèmes.

Gestion des terminaux mobiles

La gestion des terminaux mobiles apporte de la sécurité au niveau le plus fondamental : le terminal proprement dit. De nouveaux types de terminaux pour les utilisateurs arrivent en permanence sur le marché. Ils ne concernent pas seulement les téléphones portables, mais également les tablettes, ordinateurs de bureau et autres « accessoires » dans le secteur de l'IdT. Grâce à la gestion des terminaux mobiles, le département informatique est en mesure de configurer des paramètres avancés de gestion et de surveillance des terminaux par l'intermédiaire de profils applicables en fonction du système d'exploitation ou du propriétaire du terminal. Les entreprises bénéficient ainsi d'un meilleur contrôle des terminaux déployés dans l'entreprise. La gestion des terminaux mobiles protège les données stockées sur le terminal ou dans les applications au niveau du terminal, car elle interdit toute opération non autorisée telle que les tentatives de « rootage » (suppression des limitations liées à l'opérateur) ou de débridage, le téléchargement ou l'installation d'applications et de logiciels malveillants. Grâce à AirWatch® Mobile Device Management, les entreprises peuvent effectuer différentes opérations au niveau des terminaux :

- Chiffrement obligatoire des données
- Exigence d'un code d'accès sur le terminal
- Réinitialisation à distance du code d'accès
- Verrouillage à distance du terminal
- Application de restrictions d'utilisation du terminal
- Suivi de la localisation du terminal
- Définition de restrictions en matière d'itinérance visant à réduire les frais de télécommunications
- Effacement des données professionnelles ou de l'intégralité du terminal
- Envoi de notifications

Une fois le terminal enregistré dans AirWatch Mobile Device Management, les profils prédéfinis par l'administrateur en fonction du type de terminal, du modèle de propriété ou du groupe de l'organisation commencent à se télécharger automatiquement. Dans la console AirWatch, les administrateurs créent des profils qui déploient les applications d'entreprise, permettent la surveillance et l'application d'une mise en conformité automatisée par l'intermédiaire du moteur de conformité AirWatch. Si un utilisateur télécharge une application classée par l'administrateur en liste noire, AirWatch peut envoyer automatiquement à l'utilisateur une notification lui demandant de supprimer cette application. Si l'application n'a pas été supprimée après une période prédéfinie, l'administrateur peut définir des actions de remontée d'informations qui limiteront automatiquement l'accès à des ressources telles que des contenus ou la messagerie de l'entreprise jusqu'à la suppression de l'application. Les administrateurs peuvent également définir des restrictions concernant les fonctionnalités et les applications natives des terminaux.

Ils ont également la possibilité de limiter la durée pendant laquelle le terminal reste déverrouillé sans que l'utilisateur doive ressaisir le code d'accès, et peuvent verrouiller à distance un terminal qui a été perdu ou dérobé. Ils peuvent appliquer des profils qui limitent le nombre de tentatives infructueuses de saisie du code d'accès. Une fois la limite prédéterminée atteinte, un profil prédéfini peut réinitialiser le mot de passe ou effectuer un effacement des données professionnelles. Certains systèmes d'exploitation proposent des modes Kiosque avancés, l'installation et la suppression silencieuses des applications ou même le contrôle à distance.

AirWatch s'intègre dans les services d'annuaire existants tels que LDAP et Active Directory. Les administrateurs peuvent importer la structure de répertoires existante afin que les utilisateurs bénéficient d'un accès approprié, en fonction du groupe de l'organisation, et puissent s'enregistrer dans AirWatch à l'aide de leurs informations d'identification professionnelles existantes.

Dans le cadre d'un déploiement en entreprise, les terminaux peuvent recevoir différents profils de gestion et accéder aux ressources de l'entreprise en fonction du poste, de la région, de la propriété du terminal et d'autres facteurs. Tous les terminaux d'un déploiement en entreprise peuvent être surveillés depuis une même console d'administration Web, quels que soient les paramètres de gestion, le type du terminal, le groupe d'organisation, la langue, l'emplacement ou le modèle de propriété.

La gestion des terminaux mobiles offre des avantages exclusifs par rapport à d'autres modèles de gestion. AirWatch Mobile Device Management permet aux employés de se connecter automatiquement aux réseaux Wi-Fi et VPN (Virtual Private Network) de l'entreprise, sans aucune interaction. Grâce à AirWatch, les administrateurs peuvent configurer des profils Wi-Fi et VPN qui permettent d'effectuer des téléchargements automatiques ou à la demande sur les terminaux utilisateur. Les profils peuvent être attribués en fonction du groupe d'utilisateurs, de sa localisation dans un périmètre géographique défini ou de l'heure du jour. Par exemple, si les employés ne peuvent accéder au réseau Wi-Fi ou VPN que pendant les heures normales de bureau définies, AirWatch permet aux administrateurs informatiques de configurer cette restriction.

AirWatch permet également de provisionner un profil VPN sur les terminaux afin que l'accès aux réseaux et systèmes de fichiers des entreprises soit configuré automatiquement. Grâce à la fonctionnalité avancée de VPN à la demande, les utilisateurs mobiles peuvent accéder en toute sécurité à des sites Web spécifiques par l'intermédiaire d'un tunnel VPN. Ce processus est fluide et invisible pour l'utilisateur qui peut continuer à travailler sans interruption. Les fonctionnalités de VPN au niveau des applications pour les terminaux Apple iOS permettent désormais aux administrateurs de connecter des applications au réseau VPN.

Cas d'utilisation de la gestion de terminaux mobiles : Propriété de l'entreprise

L'approche de niveau terminal est une solution très simple pour les organisations qui distribuent des terminaux à leurs employés. La gestion de l'intégralité du terminal permet d'effectuer le suivi de l'inventaire des ressources et de le gérer en temps réel. Les terminaux appartenant à l'entreprise étant généralement dédiés à une utilisation strictement professionnelle, la plupart des entreprises choisissent la gestion des terminaux mobiles, car elle offre des contrôles supplémentaires au niveau du terminal (effacement des données professionnelles ou du contenu complet du terminal, verrouillage à distance du code d'accès) et permet de surveiller en temps réel un parc complet de terminaux.

La gestion des terminaux mobiles permet également aux organisations de limiter les dépenses de télécommunications. AirWatch permet aux entreprises de réduire les frais de connexion sans fil grâce à la surveillance des données en temps réel. Les administrateurs peuvent définir un profil qui désactive automatiquement l'utilisation des données ou les appels en situation d'itinérance.

Cas d'utilisation de la gestion de terminaux mobiles : utilisation de terminaux personnels

Cependant, le marché perçoit également une certaine lourdeur dans la gestion des terminaux mobiles dans le cas où les employés utilisent leur propre terminal pour accéder aux contenus de l'entreprise. Les plates-formes Apple® et Microsoft™ sont conçues pour accepter la gestion au niveau du terminal tout en laissant le contrôle ultime à l'utilisateur. Dans les paramètres, les utilisateurs peuvent voir tous les profils installés sur le terminal, notamment ceux installés par le département informatique. En revanche, aucune des plates-formes Apple® iOS ou Microsoft ne permet d'accéder au contenu des SMS, appels téléphoniques ou messages personnels. Les administrateurs ne peuvent ni lire, ni écouter, ni enregistrer les conversations échangées sur le terminal. Plus ouverte, la plate-forme Android permet des contrôles supplémentaires de gestion des terminaux, si bien que de nombreuses organisations choisissent de fournir l'option de conteneurisation sur les terminaux Android appartenant à leurs employés.

De nombreux utilisateurs ne souhaitent pas autoriser le département informatique à effacer à distance les données de leur terminal, car ils craignent de perdre des contenus personnels importants. AirWatch offre une option d'effacement à distance des données professionnelles qui permet au département informatique de n'effacer du terminal que le contenu appartenant à l'entreprise, sans intervenir sur le contenu personnel. Pour rassurer les employés, de nombreuses entreprises choisissent de déployer le contenu appartenant à l'entreprise dans un conteneur distinct sur les terminaux gérés, ce qui permet d'avoir un espace clairement défini sur les terminaux appartenant aux employés. Il revient alors à l'organisation de créer une politique concernant l'utilisation de terminaux personnels qui définit clairement les données pouvant être collectées et surveillées. AirWatch recommande d'utiliser des politiques concernant l'utilisation de terminaux personnels qui empêchent tout accès du département informatique au contenu personnel. AirWatch fournit également différentes politiques relatives à la confidentialité qui peuvent être personnalisées pour les terminaux appartenant aux employés.

Conteneurisation

Grâce à la conteneurisation, les entreprises peuvent déployer et gérer en toute sécurité les contenus leur appartenant, dans un espace crypté sur le terminal. Toutes les ressources d'entreprise, y compris les applications propriétaires, la messagerie, l'agenda et les contacts professionnels, résident dans cet espace géré. Le conteneur protégé par un mot de passe permet aux utilisateurs d'accéder à toutes les applications de l'entreprise par l'intermédiaire d'une connexion SSO (Single Sign On), ce qui simplifie l'accès à l'espace géré. Grâce à la conteneurisation, le département informatique peut non seulement sécuriser les données de l'entreprise sur le terminal, mais également contrôler les applications pouvant accéder aux données, ainsi que le mode de partage de ces données. Si la sécurité des données est compromise, il est possible de supprimer à distance une application spécifique ou l'intégralité du conteneur.

Le déploiement d'applications gérées à l'extérieur d'un conteneur crypté rend vulnérables les données hébergées dans les applications, car le département informatique ne peut pas contrôler la communication de ces applications avec d'autres applications non gérées du terminal. Prenons l'exemple d'une application sécurisée de partage de fichiers qui utilise une application partenaire pour effectuer des opérations telles que la modification et l'annotation. Si un fichier est modifié dans les deux applications, les données peuvent être copiées depuis l'application sécurisée de partage de fichiers vers le Cloud public de l'application de modification : le département informatique n'a alors plus le contrôle.

AirWatch® Content Locker est un conteneur sécurisé de partage de fichiers intégrant des fonctionnalités de modification et d'annotation, si bien que les utilisateurs peuvent effectuer ces opérations sans que les données quittent l'application. AirWatch® Inbox est un conteneur sécurisé de messagerie qui permet aux organisations de séparer la messagerie professionnelle des utilisateurs et de la stocker dans un conteneur géré et crypté. Il est possible de restreindre les hyperliens figurant dans les fichiers ou les messages pour qu'ils ne puissent s'ouvrir que dans le navigateur sécurisé AirWatch® Browser. Toutes les applications peuvent être hébergées dans AirWatch® Container afin de permettre une connexion SSO. Grâce aux solutions AirWatch® Application Management telles que le kit de développement de logiciel AirWatch® ou le regroupement d'applications AirWatch®, les applications internes de l'organisation peuvent fonctionner en toute sécurité dans le conteneur AirWatch.

Disponible pour iOS et Android, AirWatch Container est un conteneur pouvant héberger toutes les applications de l'entreprise sur un terminal et permettant d'accéder en toute sécurité aux données de l'entreprise, y compris la messagerie, les applications et les contenus, un navigateur sécurisé et des applications personnalisées. L'hébergement dans AirWatch Container d'applications telles que Content Locker, AirWatch Inbox ou d'autres applications d'entreprise n'autorise ces applications à partager des données qu'avec d'autres applications gérées et sécurisées. Toutes les applications à l'intérieur du conteneur sont accessibles par connexion SSO.

Cas d'utilisation : utilisation de terminaux personnels

La conteneurisation est couramment référencée comme étant une solution pour les terminaux appartenant aux employés. Elle offre un espace géré sur le terminal, si bien que les employés souhaitant utiliser leur propre terminal pour accéder aux contenus de l'entreprise sont généralement plus confiants en ce qui concerne le respect de la confidentialité, qu'ils soient enregistrés dans la gestion des terminaux mobiles ou pas.

Cas d'utilisation : collaboration dans l'entreprise étendue

La conteneurisation permet également de partager en toute sécurité dans l'entreprise étendue des contenus et des applications avec les utilisateurs non inscrits dans la gestion des terminaux mobiles. Les administrateurs peuvent déployer un conteneur sécurisé pour les consultants, sous-traitants, fournisseurs, partenaires, membres du conseil d'administration et autres collaborateurs sans gérer leur terminal.

AirWatch Container peut être personnalisé en fonction de la marque pour que les utilisateurs puissent partager des documents et des données avec des membres de l'entreprise étendue dans un conteneur conforme à l'identité de l'entreprise, distinct des applications tiers. En regroupant toutes les applications et données de l'entreprise dans AirWatch Container, AirWatch offre aux administrateurs un contrôle supplémentaire et une sécurité renforcée pour les données d'entreprise sur les terminaux non gérés. Grâce à AirWatch Container, les données professionnelles ne quittent jamais le réseau géré par l'entreprise, même si elles sont partagées avec des collaborateurs de l'entreprise étendue. Si la sécurité d'un terminal non géré hébergeant des données professionnelles est compromise, AirWatch Container permet

aux administrateurs d'effacer et de supprimer toutes les données professionnelles en une seule opération tout en laissant les données personnelles intactes.

Approche en couches : gestion des terminaux mobiles + conteneurisation

Les processus d'entreprise sont de plus en plus étendus vers les terminaux mobiles et de nombreuses entreprises recherchent d'autres utilisations pour la gestion des terminaux mobiles et la conteneurisation, à déployer sur différents terminaux ou sur le même terminal.

Déploiements sur différents terminaux

Dans les grandes entreprises, les administrateurs chargés du déploiement des terminaux de l'entreprise et des terminaux personnels peuvent envisager la gestion des terminaux mobiles pour les terminaux appartenant à l'entreprise, et la conteneurisation pour les terminaux appartenant aux employés, et pour d'autres cas d'utilisation ne nécessitant pas de gestion des terminaux, tels que la collaboration dans l'entreprise étendue.

Déploiement sur le même terminal de la gestion des terminaux mobiles et de la conteneurisation

Les organisations dont les contenus propriétaires sont sensibles ou dont le secteur d'activité est strictement réglementé préféreront la sécurité renforcée qu'offrent la gestion des terminaux mobiles et la conteneurisation sur un même terminal. Un conteneur d'entreprise déployé sur un terminal géré constitue une barrière supplémentaire de protection pour le contenu appartenant à l'entreprise. Les utilisateurs doivent saisir un code d'accès au niveau du terminal et un autre au niveau du conteneur. Quant aux administrateurs, ils disposent d'un contrôle au niveau du terminal et au niveau des applications qui permet la collaboration des applications avec d'autres applications gérées et sécurisées stockées dans le conteneur. Par exemple, un lien envoyé dans un e-mail sécurisé peut être ouvert dans le navigateur sécurisé AirWatch Browser, et une pièce jointe sensible peut être ouverte et modifiée dans Content Locker.

La gestion des terminaux mobiles et la conteneurisation sont souvent perçues comme étant des solutions de sécurité qui s'excluent mutuellement, mais les entreprises les plus innovantes utilisent aujourd'hui une approche en couches de la sécurité en utilisant ces deux solutions conjointement. Le département informatique d'une entreprise peut choisir d'adopter un modèle hybride, avec plusieurs approches différentes de la gestion. Cela peut s'avérer nécessaire si certains terminaux appartiennent à l'entreprise et d'autres aux employés. Dans les entreprises utilisant des terminaux personnels et d'autres appartenant à l'entreprise, les administrateurs peuvent toujours surveiller et gérer de manière efficace les terminaux sécurisés par la gestion des terminaux mobiles, la conteneurisation ou les deux approches, dans une plate-forme unique et intégrée.

Une plate-forme complète et intégrée pour les terminaux mobiles

Chaque solution de la plate-forme de gestion de la mobilité d'entreprise AirWatch® a été spécifiquement conçue à partir de la même structure de sécurité. La console d'administration permet d'avoir une vision globale de tous les terminaux d'un déploiement. Que les terminaux soient gérés par la gestion des terminaux mobiles ou par la conteneurisation, les administrateurs informatiques peuvent gérer l'intégralité du déploiement par l'intermédiaire de la seule console Web AirWatch. La solution AirWatch est réputée pour la simplicité de sa gestion de tous les terminaux de l'entreprise. Une même plate-forme répondant à tous les besoins en matière de terminaux mobiles simplifie réellement la gestion. Et une gestion simplifiée signifie que les administrateurs informatiques sont plus à même d'identifier les failles de sécurité potentielles avant qu'elles se transforment en problèmes réels.

L'utilisation de terminaux mobiles dans l'entreprise est de plus en plus stratégique, et les cas d'utilisation sont toujours plus complexes. Les entreprises ajoutent des utilisateurs, et déploient des contenus et des applications en permanence dans l'entreprise étendue. Si une organisation souhaite réellement s'ajuster à cette nouvelle ère, elle doit impérativement trouver une solution de gestion de la mobilité d'entreprise qui soit conçue avec la même architecture et sur une même plate-forme. AirWatch offre une plate-forme mobile intégrée qui permet de gérer les contenus et la collaboration, et sécurise les applications, la navigation et la messagerie dans l'entreprise étendue. AirWatch exploite également l'infrastructure existante des organisations afin d'autoriser l'accès aux ressources de l'entreprise. AirWatch pérennise les investissements informatiques dans un réseau VPN, la sécurité sur le réseau Wi-Fi, SharePoint® et d'autres référentiels de contenus, ainsi que dans les systèmes de planification d'entreprise et de gestion de la relation client. En étendant ces ressources aux terminaux mobiles, AirWatch étend également la sécurité et permet aux employés de gagner en productivité grâce à la mobilité.

Lorsqu'elles choisissent une plate-forme de mobilité d'entreprise, les organisations doivent prendre en compte non seulement leurs besoins actuels en matière de mobilité, mais également un plan d'évolution étendu qui intègre les projets de développement d'applications, d'extension d'autres processus aux terminaux mobiles ou de collaboration avec l'entreprise étendue. Afin de se préparer à l'ère de la mobilité, les organisations d'aujourd'hui ont besoin d'une plate-forme flexible et ajustable, moteur de leur évolution.

Qu'elles choisissent la gestion des terminaux mobiles, la conteneurisation ou l'approche en couches, AirWatch a créé une plate-forme qui permet l'exécution des processus d'entreprise et garantit la sécurité que les départements informatiques attendent, avec une interface utilisateur conviviale, l'intégration profonde de l'entreprise et la flexibilité nécessaire à la collaboration et à la croissance.

Ressources complémentaires

Inscrivez-vous à des laboratoires d'essai pratique
http://vmware.com/go/try-airwatch-hol

Visitez notre site Web
www.vmware.com/enterprise-mobility-management

À propos d'AirWatch
AirWatch® est la solution leader de gestion de la mobilité d'entreprise, avec une plate-forme incluant un terminal mobile leader du marché, ainsi que des solutions de gestion de la messagerie, des applications, des contenus et des navigateurs. Acquise en février 2014 par VMware, la société AirWatch est située à Atlanta ; vous pouvez consulter son site Web à l'adresse suivante : www.air-watch.com.

vmware®

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 Fax +33 1 47 62 79 01 www.vmware.fr