MDM : un levier pour le BYOD

Présentation

De plus en plus, les entreprises se laissent séduire par les systèmes et les architectures convergées, des systèmes informatiques qui promettent une plus grande simplicité et surtout un déploiement accéléré.

Si mobilité a longtemps rimé avec déferlement incontrôlé des terminaux personnels des employés dans l'entreprise, ce n'est plus aujourd'hui le cas.

Les craintes souvent évoquées et liées à ce phénomène dit de BYOD apparaissent largement dépassés. Au même titre que les discours encourageant à interdire à tout prix ces nouveaux usages technologiques.

Désormais, il est question de chercher à retirer des gains de productivité et des économies de ces nouveaux usages. Mais également d'en aborder d'autres, en passant notamment par les applications métiers.

Il s'agit désormais d'aller au-delà d'une simple gestion des terminaux mobiles pour s'intéresser à celle des applications mobiles, et plus loin, à la gestion d'une véritable mobilité d'entreprise.

Les outils sont là. Les projets aussi.

VALERY MARCHIVE

Rédacteur en chef adjoint,

TechTarget / LeMagIT

Comment le MDM affecte la gestion des politiques de sécurité des terminaux mobiles

Face à la montée en puisse du phénomène BYOD, les entreprises doivent trouver des solutions adéquates pour sécuriser réseaux et applications. MAM, MDM en réseau ou pas, les solutions commencent à abonder sur le marché. Mais quel est finalement leur impact pour les entreprises ?

Nul doute qu'avec les appareils mobiles, les professionnels de la sécurité IT chargés de garantir la protection des informations d'entreprise font face à de nouveaux défis. À mesure que le rôle joué par ces appareils, leur évolution et leurs exigences spécifiques gagnent en importance dans l'entreprise, le contrôle nécessaire à la sécurisation des données doit progresser de concert.

Or, pour assurer la protection des données d'entreprise, les responsables de la sécurité ont besoin d'une vue d'ensemble précise de l'évolution des préférences des salariés en matière d'équipements et de modes de travail. BYOD, utilisation de contenus axés sur les applications mobiles, de tablettes ou encore usage exclusif du sans-fil, ces nouvelles préférences modifient les actifs IT traditionnels par un glissement vers le domaine public. Les plus grandes organisations IT doivent donc faire appel aux professionnels de la sécurité de l'information. Pour garantir la protection d'une flotte d'appareils mobiles en pleine expansion, elles recourent à une large palette de technologies qui prennent en charge une politique d'utilisation reposant sur les identifications.

La technologie SMDM (gestion logicielle des terminaux mobiles) reste incontournable pour sécuriser les terminaux mobiles grand public qui font florès dans les entreprises. Selon le Nemertes Research Group, 46 % des entreprises ont mis en œuvre une politique de gestion des terminaux mobiles (MDM), et 84 % ont l'intention de le faire d'ici à fin 2014. Au vu des tendances de convergence des appareils mobiles, il est grand temps : dans les entreprises qui confirment ces tendances, un quart (25 %) des salariés devraient utiliser une tablette comme outil de travail d'appoint d'ici fin 2014 et un nombre encore faible mais croissant de salariés (10 %) ont déjà remplacé leurs ordinateurs portables par des tablettes.

Les fournisseurs, de leur côté, font assaut d'inventivité pour mettre en avant les fonctionnalités MDM de leurs produits. Nombre d'entre eux ont désormais recours à des

outils de gestion de terminaux natifs ou en conteneurs, voire à une infrastructure de poste de travail virtuelle (VDI). Par ailleurs, la plupart – pour ne pas dire tous – proposent une bonne partie des technologies suivantes :

- Une gestion des applications mobiles (MAM) ou une boutique d'applications d'entreprise
- Des conteneurs ou des espaces de travail sécurisés pour les documents, applications mobiles et de gestion des informations personnelles
- Un système de partage de documents sécurisé (SDS) intégré au terminal, des partenariats ou des services dans le Cloud ou des interfaces de programmation d'applications (API) autorisant une intégration aux plates-formes les plus connues, telles que Microsoft SharePoint, Dropbox ou encore Google Drive.
- Une intégration WLAN ou une fonctionnalité de gestion MDM en réseau (NMDM)
- Des fonctionnalités avancées telles que le gardiennage virtuel (geo-fencing), l'encapsulation d'applications (app-wrapping), l'intégration d'une autorité de certification et la prévention de fuites ou de perte de données par e-mail.

Actuellement utilisée par 29 % des entreprises, la gestion des applications mobiles (MAM) est la fonctionnalité MDM la plus répandue et la plus incontournable. Tout comme les terminaux grand public stimulent l'adoption des technologies de gestion des terminaux mobile en entreprise, l'expansion des initiatives de développement applicatif des entreprises ne peut se faire sans outil MAM et boutique d'applications mobiles d'entreprise. Le MAM présente en effet aux utilisateurs le visage familier d'une boutique au service des applications de l'entreprise. Les politiques de gestion des licences, de distribution et de mise à jour sont régulées par l'IT grâce à un service d'annuaire de type Active Directory ou Apple Open Directory.

Structuré selon une approche de service d'annuaire, le partage de documents sécurisé (SDS) est le même que celui du contrôle et du partage de documents. Cette technologie SDS pour terminaux mobiles diffère de celle pour points d'accès mieux contrôlés tels que les ordinateurs portables. En effet, les systèmes

d'exploitation mobiles présentent peu d'options d'administration natives similaires à celles conçues pour les entreprises. Les fournisseurs de solutions MDM qui veulent mettre les terminaux mobiles à égalité avec les points d'accès plus traditionnels proposent donc des API pour les systèmes de partage de documents d'entreprise les plus utilisés et pour le contrôle des pièces jointes aux e-mails ou aux applications. La plupart des MDM offrent également des solutions combinant coffres-forts de documents embarqués sur le terminal, intégration SDS dans le Cloud et accès aux documents à distance par VDI.

La technologie MDM prend aussi de l'envergure : même si 11 % seulement des entreprises y ont recours aujourd'hui, Nemertes Research pointe un chiffre en augmentation. Une grande partie de l'intérêt des solutions NMDM pour les entreprises provient du fait qu'elles permettent d'identifier des indicateurs clés pour ces terminaux et de mettre en œuvre des politiques qui, à l'aide de logiciels d'administration réseau, font essentiellement appel aux protocoles réseau standards. La plupart des fonctionnalités du MDM en réseau (NMDM) ne sont pas propriétaires. Il n'est donc nul besoin d'investir ou de prévoir du matériel réseau supplémentaire pour les faire fonctionner de manière autonome, ou en tandem avec une solution MDM logicielle. Ainsi, les professionnels de la sécurité peuvent rentabiliser des fonctionnalités telles que la reconnaissance d'empreintes digitales, les rapports sur la configuration de sécurité, la qualité de service des applications mobiles ou les réseaux privés virtuels de niveau application, sans que l'utilisateur n'ait besoin d'être connecté au préalable à un point d'accès. En résumé, la technologie NMDM fournit aux professionnels de la sécurité les outils pour bloquer, réorienter ou classer par ordre de priorité le trafic réseau généré par les terminaux mobiles et leurs applications, ce qui est particulièrement adapté aux environnements BYOD.

Comment l'évolution MDM influe sur les politiques de sécurité mobile

Même pour les praticiens les plus aguerris de la sécurité IT, écumer le paysage en constante évolution des fonctionnalités MDM n'est pas une sinécure.

À l'aide de la liste des fonctionnalités disponibles établies ci-dessus, il est néanmoins recommandé aux entreprises de réfléchir aux éléments suivants au moment d'élaborer ou d'affiner leur politique de sécurité mobile :

- Révisez votre politique de mise à disposition de terminaux mobiles et décidez dans quelles limites autoriser le BYOD. Les fonctionnalités indiquées ci-dessus permettent d'utiliser une palette d'applications mobiles plus large et de les utiliser de manière plus souple afin d'améliorer la productivité des collaborateurs.

- De même, déterminez avec soin vos attentes actuelles et vos attentes de court terme en matière d'équipements mobiles (smartphones et tablettes), ainsi que leur configuration de sécurité et leur configuration par défaut.

- Recensez le nombre de terminaux mobiles des salariés au sein de votre entreprise : ceux qui sont connus/administrés par l'IT et ceux qui ne le sont pas. Puis :

- Étudiez comment déployer l'outil NMDM quand le BYOD est intense ; par exemple, quand les collaborateurs apportent des appareils qui demandent différents niveaux d'accès aux e-mails, à la gestion d'agenda et à d'autres données d'entreprise plus sensibles. Assurez-vous que votre politique vous apporte le bon équilibre entre sécurité et facilité d'usage.

- Cette politique devrait stipuler que les utilisateurs doivent être formés, en fonction de votre niveau de sécurité et de vos règles de conformité, soit à ne pas introduire le BYOD dans l'entreprise, soit à s'assurer qu'ils le font en utilisant la procédure d'inscription du système MDM (généralement par une URL spécifique ou un portail d'accès).

Enfin, les outils MDM (MDM logiciel ou MDM réseau), MAM et SDS devraient être les principaux outils de sécurisation des terminaux mobiles.

Si votre entreprise ne les a pas encore mis en place, évaluez les produits nécessitant des demandes d'informations (RFI) ou des demandes de propositions (RFP), et ceux pour lesquels des projets pilotes sont nécessaires.

Reste ensuite à se poser les questions suivantes :

- Déployez-vous des applications développées sur mesure, en interne ou en externe ? Si oui, évaluez votre gestion MAM pour bloquer et classer les applications publiques, et en améliorer la sécurité.

- Étudiez les capacités SDS actuellement utilisées : sont-elles adaptées aux appareils mobiles ou sont-elles à la traine par rapport aux solutions SDS des postes de travail ? Évaluez les produits d'administration de terminaux mobiles applicables dans le Cloud, dans l'entreprise ou embarqués sur le terminal lui-même. Sont-elles en phase avec l'objectif de venir en appui d'une politique homogène applicable à l'échelle de tous les points d'accès.

– Philip Clarke, analyste chercheur pour le Nemertes Research Group

Renault mise sur la conteneurisation pour sa mobilité

Historiquement, mobilité rimait avec BlackBerry, chez Renault, explique Damien Martayan, responsable du domaine poste de travail et mobilité, au sein de la DSI du constructeur automobile. On en comptait quelque 6 000 début 2012.

Mais voilà, la pression des utilisateurs s'est faite sentir, certains ayant trouvé les moyens de connecter leur smartphone personnel au réseau et aux systèmes de l'entreprise, pour gérer e-mails, agenda et contacts : « ce n'était ni préconisé, ni prévu, et nous avons identifié un risque potentiel », relève Damien Martayan.

Un début de BYOD non encadré qui est survenu alors que se posaient des questions sur l'avenir même de la flotte de BlackBerry, et plus largement sur « les services à mettre en place pour la mobilité ». Mi-2012, Renault a donc lancé un projet de BYOD piloté et sécurisé. Aujourd'hui, le programme ne concerne rien moins que 5 000 terminaux.

Prendre en compte la composante légale

Dès le début, Renault a impliqué ses équipes RH pour étudier différents aspects juridiques liés au BYOD. La solution technique recherchée devait de fait intégrer les spécificités de chacun des pays dans lequel le constructeur est présent. D'où une conclusion : « la seule solution pour faire du BYOD efficacement sur smartphone ou tablette, c'est un mode conteneur », explique Damien Martayan. L'isolation complète des composants liés à l'entreprise permet ainsi d'éviter la confusion chez l'utilisateur entre ce qui est du domaine professionnel et du domaine personnel. « Cela nous permet aussi d'assurer que, en cas de problème, nous sommes capables d'effacer uniquement les données d'entreprise et pas le reste. » Et de relever que « d'autres entreprises n'ont pas la même prudence et font signer un accord aux utilisateurs. Mais notre service juridique a jugé cela risqué, notamment en l'absence de recul et de jurisprudence sur ces sujets ».

Un accueil enthousiaste

Sans trop de surprise, alors qu'ils poussaient à cela, les utilisateurs ont bien accueilli le programme de BYOD du constructeur, démontrant « une véritable appétence pour des mobiles autres que les BlackBerry. Majoritairement, des iPhone, et puis des appareils Samsung ». De là, les

équipes de Damien Martayan ont étendu leur offre de mobilité à la flotte de smartphones corporate – « essentiellement des iPhone » - en optant pour une sécurisation plus forte, avec un contrôle complet sur le terminal. Là, le message aux utilisateurs est clair : l'entreprise peut effacer à distance tout le contenu du terminal ; si des données personnelles s'y trouvent, elles relèvent de la seule responsabilité de l'utilisateur.

C'est une solution double qu'à finalement retenu Renault, déployant initialement les outils de Good Technology pour le BYOD, puis s'orientant vers XenMobile de Citrix, ce dernier s'appuyant notamment sur les outils de Zenprise, racheté par Citrix fin 2012.

Si cela se traduit par une surcharge de travail, liée à l'utilisation de deux consoles, la solution permet, dans son ensemble, à chaque région, chaque pays où est présent Renault, de « mettre en place une politique spécifique suivant les recommandations que l'on a émises. Nous autorisons un certain nombre de smartphones et de systèmes d'exploitation, mais chaque pays peut choisir de mettre l'accent sur le BYOD, ou le COPE ». Et cela notamment en fonction de contraintes légales locales : en France, fournir une enveloppe aux salariés pour qu'ils achètent un équipement peut être considéré comme un avantage en nature. Et se pose aussi la question du seuil à partir duquel l'utilisateur peut être considéré comme propriétaire du terminal, en fonction de la part qu'il a payé de sa poche.

Des usages qui se découvrent

La flotte de terminaux BlackBerry décroît progressivement alors que la flotte corporate se renouvelle. « Mais certains utilisateurs passés sur le programme de BYOD expriment désormais le souhait de revenir à la flotte corporate pour renouveler leurs terminaux », souligne Damien Martayan, tout en précisant que le BYOD est également ouvert à des populations qui n'étaient pas éligibles à la flotte corporate.

Mais pour l'heure, les utilisateurs concernés par le BYOD restent limités au courrier électronique, à l'agenda et aux contacts. Certains souhaiteraient toutefois accéder à la messagerie instantanée… pour l'heure encore réservée à la flotte corporate. Surtout, les demandes d'ouverture de nouveaux usages commencent à émerger.

« Des utilisateurs veulent faire avec leur tablette comme avec leur PC », explique ainsi Damien Martayan. Mais ceux-ci ne sont pas virtualisés. Certaines applications le sont toutefois avec XenApp, « notamment pour des raisons de compatibiltié Windows 7 ». Alors, « nous réfléchissons à la mettre à disposition sur des tablettes avec Citrix Receiver ».

Ce n'est toutefois pas la principale priorité. Outre l'accès à la messagerie instantanée, les demandes touchent surtout l'accès aux fichiers partagés ou encore à des applications de workflow. Et pour les fichiers, Citrix a déjà une réponse : ShareFile. Mais pour de nombreux utilisateurs, le chiffrement est impératif. D'où un travail avec le partenaire chargé de ce volet : Prim'X, qui réfléchit à un certificat embarqué sur le terminal et qui permettrait de déchiffrer à la volée.

De nouveaux projets à venir

Mais la mobilité ne s'arrête pas aux cols blancs. La réflexion s'étend désormais aux centres logistiques et aux usines : « nous commençons à réfléchir à des applications métiers de bord de chaîne, sur tablette durcie, notamment », explique Damien Martayan, évoquant à nouveau la conteneurisation, mais soulignant la problématique de la couverture Wi-Fi dans ces espaces. Côté commercial, en revanche, le sujet a déjà bien avancé, avec des tablettes permettant, dans les concessions, d'accéder aux configurateurs de véhicules. L'accueil atelier devrait suivre.

Pour résumer, Damien Martayan, rappelle que « l'on vient d'un monde centré sur l'organisation personnelle, mâtiné d'un tout petit peu d'intranet. Et maintenant, on tire la pelote du poste de travail au sens large. Mais il est aujourd'hui très industrialisé et l'on veut atteindre le même niveau sur les terminaux mobiles corporate. »

Mobilité d'entreprise : au-delà du MDM et du BYOD

La mobilité est devenue l'une des principales préoccupations des DSI. Et cela se traduit par des investissements de plus en plus conséquents dans les solutions d'administration des parcs de terminaux mobiles (MDM) et dans les autres composants nécessaires à la construction d'une stratégie complète de gestion de la mobilité d'entreprise (EMM).

De fait, le MDM est le premier composant à avoir fait son apparition. Et ce n'est pas une surprise : il s'agit d'une simple extension de la méthodologie de gestion élémentaire qui domine depuis longtemps l'administration d'infrastructure, en se concentrant sur des éléments faciles à identifier, à savoir les composants matériels tels que routeurs, commutateurs, et PC. L'administration des terminaux mobiles étend ce modèle et s'intègre facile dans une doctrine éprouvée de l'administration IT.

Mais l'approche du MDM souffre de limites qui sont rapidement apparues. Tout d'abord, la gestion de la mobilité doit aller au-delà du seul terminal mobile. Les éléments additionnels – tels que la gestion des applications, des données et des informations, des stratégies et de l'exploitation, et même des dépenses opérationnelles – sont tout aussi importants. Et cela vaut aussi pour des domaines qui s'étendent bien au-delà du terminal mobile. Vient ensuite une conséquence de l'essor rapide du BYOD :Les entreprises ne possédent plus forcément les terminaux utilisés par les utilisateurs à des fins professionnelles. Et certaines capacités des systèmes de MDM, telles que l'effacement à distance, sont complètement inappropriées pour des terminaux qui sont la propriété des utilisateurs et contiennent donc aussi des données privées.

Cette situation a conduit à l'émergence de solutions dédiées à l'administration des autres éléments évoqués plus haut : applications, informations, accès réseau, et application des stratégies de sécurité.

Le MAM (administration des applications mobiles) recouvre des fonctions telles que la mise d'applications en liste blanche et noire, ou encore la mise en place de magasins applicatifs d'entreprise, et le support technique pour l'utilisateur final.

L'administration des informations mobiles (MIM) touche à la conteneurisation, parfois présentée comme du sandboxing, pour isoler, chiffrer, superviser, et contrôler la distribution et l'utilisation de données sensibles de l'entreprise sans interférer avec la nature fondamentale d'un terminal propriété de son utilisateur.

La gestion des stratégies mobiles (MPM), et celle des dépenses mobiles (MEM), visent à assurer que les politiques opérationnelles de maîtrise des dépenses de télécommunications sont en place et effectives.

Que reste-t-il alors au MDM ? En fait, les logiciels de gestion de terminaux restent incontournables pour la supervision de problèmes essentiels liés aux terminaux et pour assurer le respect des règles opérationnelles relatives aux configurations. Les réglages de pare-feu, d'anti-virus, et de protection contre les logiciels malveillants, l'activation (ou non) de certaines capacités matérielles, etc. sont autant de fonctionnalités essentielles des outils de MDM dans un monde du BYOD.

Pour résumer, le MDM est nécessaire, mais pas suffisant pour assurer une gestion efficace de la mobilité. Les autres domaines d'administration évoqués plus haut vont jouer un rôle de plus en plus important alors que la gestion de la mobilité d'entreprise gagne en maturité, tout particulièrement dans les grandes organisations. Et les éditeurs de solutions de gestion de la mobilité travaillent désormais d'arrache-pied à la construction de solutions combinant l'ensemble de ces fonctionnalités au sein de suites intégrées à console unique.

Et qu'en est-il alors du BYOD ? Le BYOD a avant tout un impact sur les politiques internes et l'authentification, renvoyant naturellement à la gestion des identités et des accès (IAM).

Et justement, l'IAM a rapidement évolué, notamment sous l'effet des efforts de la communauté des équipementiers WLAN, et représente le futur de l'authentification et du contrôle d'accès pour définir qui peut faire quoi, à partir de quel terminal, où et quand, sur quels réseaux, et avec quel niveau de supervision et de contrôle. Le contrôle de la conformité des configurations via MDM restant ici complémentaire, on peut s'attendre à ce que des solutions futures d'IAM intègrent des capacités de MDM.

Ainsi, alors que MDM et BYOD sont des concepts distincts, ils requièrent des techniques et des solutions d'administration complémentaires.

Heureusement, l'industrie progresse régulièrement sur les deux domaines. Et comme souligné plus haut, les évolutions futures des fonctionnalités de gestion de la mobilité d'entreprise promettent une administration toujours plus légère.

– Craig Mathias, associé du cabinet de conseil en mobilité et connectivité sans fil Farpoint Group

BYOD ou COPE : quelle stratégie de mobilité pour l'entreprise ?

Le modèle COPE - pour Corporate Owned, Personally Enabled, ou acquis par l'entreprise mais individualisé - offre une alternative aux organisations dans lesquelles le BYOD n'a pas tenu ses promesses. Cet autre modèle vise à offrir une expérience mobile pensée pour l'utilisateur final, mais offrant un niveau d'administration plus élevé.

La différence clé tient à la propriété du terminal : dans le BYOD, le terminal appartient à l'utilisateur; avec le COPE, tablettes et smartphones restent la propriété de l'entreprise mais les utilisateurs peuvent s'en servir pour accomplir également des tâches personnelles. Mais comme le BYOD, le COPE n'est pas exempt de défauts et ne conviendra pas à toutes les DSI.

Le BYOD peut limiter l'autonomie de la DSI

Les programmes de BYOD sont apparus alors que les smartphones et tablettes des utilisateurs sont devenus des outils populaires au travail. Les DSI, peut-être plus rapidement que d'autres, ont réalisé que lutter pour empêcher l'entrée sur le réseau de ces terminaux n'est pas le meilleur moyen d'utiliser leur temps et leurs ressources. Ils ont donc commencé à agir pour supporter et intégrer ces terminaux à l'environnement corporate.

Le BYOD peut apporter des bénéfices significatifs en termes de productivité des employés, parce que les terminaux et applications mobiles modernes offrent une expérience utilisateur bien supérieure à celle des PC traditionnels et des suites logicielles d'entreprise monolithiques.

La flexibilité qui apparaît lorsque les utilisateurs ne sont plus enchaînés à leurs bureaux peut également faire des merveilles pour le moral des effectifs et l'équilibre vie privée/vie professionnelle.

Certaines organisations adoptent les règles de BYOD dans l'espoir de réaliser des économies. Mais cela n'est souvent pas le cas. Certaines économies peuvent survenir, notamment sur le coût du matériel, et si le programme de BYOD s'inscrit en remplacement d'un programme de fourniture d'équipement, mais il faut généralement dépenser plus en support.

Déployer une solution de gestion de la mobilité d'entreprise (EMM) pour sécuriser et configurer un large éventail de terminaux d'employés peut être significativement pénalisant.

Les organisations peuvent circonscrire ce phénomène en limitant le nombre de terminaux autorisés dans le cadre d'un programme de BYOD, mais les utilisateurs risquent de rejeter l'initiative si l'éventail est trop restreint.

Qui plus est, le BYOD peut limiter ce que l'IT entend faire avec sa plateforme d'EMM. Les employés peuvent refuser à offrir un contrôle complet de leur terminal à l'EMM - avec notamment les fonctions d'effacement à distance ou de suivi de la localisation.

La gestion des applications mobiles demande une approche plus légère, ne laissant à l'IT que le contrôle des actifs informationnels de l'entreprise, ce qui peut remporter plus aisément l'adhésion des utilisateurs. Mais si des fonctionnalités de MDM sont nécessaires, comme c'est souvent le cas dans les industries les plus régulées, le BYOD risque de ne pas être la solution.

La combinaison de terminaux personnels et d'un contrôle par l'entreprise peut également s'avérer délicate, en raison de problèmes de vie privée et de législation. Du point de vue de l'IT, ce n'est pas parce que les administrateurs pourraient accéder à des données personnelles des utilisateurs qu'ils le devraient. Et pour les utilisateurs, la ligne entre univers personnel et professionnel n'est pas toujours claire. Des règles de BYOD claires et précises peuvent aider à définir et à faire appliquer des usages acceptables pour tous.

Une approche différente

Le modèle COPE diffère de cela, mais également des programmes de fourniture de terminaux par l'entreprise en reconnaissant aux utilisateurs le droit d'utiliser ces terminaux à des fins personnelles.

Ce qui doit être verrouillé l'est, ce qui doit être administré l'est, et tout le reste est laissé au libre arbitre de l'utilisateur. Et parce que l'entreprise est propriétaire du terminal, l'IT peut se permettre d'être plus autoritaire quant à son contrôle.

COPE est plus simple à supporter que le BYOD, parce que l'IT peut mettre en place des processus industrialisés d'enrôlement de terminal et de déploiement d'applications, au lieu de peiner à supporter les terminaux apportés par les employés.

L'IT devrait continuer de donner aux utilisateurs des

options, mais les administrateurs ne devraient pas se sentir l'obligation de supporter tous les terminaux disponibles sur le marché, comme c'est plus ou moins le cas avec le BYOD.

Les organisations pourraient également tirer profit des économies d'échelle liées au COPE. Certains employeurs offrent une participation financière dans le cadre de leurs programmes de BYOD.

Mais acheter des terminaux via les processus d'achat en volume des constructeurs, et payer à l'usage suivant des forfaits partagés d'opérateurs mobiles peut s'avérer bien plus économique. Cela dit, l'investissement immédiat lié au modèle COPE peut s'avérer rédhibitoire pour certaines entreprises.

Mais l'une des missions de la DSI est aujourd'hui de trouver un équilibre acceptable pour toutes les parties concernées entreprise contrôle et vie privée. La ligne désormais floue entre actifs personnels et professionnels existe dans tous les scenarios. Et si l'utilisateur final se sent espionné, la stratégie de mobilité de l'entreprise échouera, quelle qu'elle soit.

.

AUTEURS

.

Le document consulté provient du site www.lemagit.fr

Cyrille Chausson | *Rédacteur en Chef*

Valéry Marchive | *Rédacteur en Chef Adjoint*

Linda Koury | *Directeur Artistique*

Neva Maniscalco | *Designer*

TechTarget
22 rue Léon Jouhaux, 75010 Paris
www.techtarget.com