Les meilleures pratiques pour rendre le BYOD, le CYOD et le COPE simples et sécurisés

Une productivité mobile pour votre entreprise. La liberté de choix pour vos employés. Une sécurité et un contrôle complets pour votre direction informatique.

Définissez les stratégies BYOD (bring-your-own-device), CYOD (choose-your-own-device) et COPE (corporate-owned, personally-enabled) adaptées à votre entreprise, en bénéficiant de l'appui de technologies complètes de gestion de la mobilité d'entreprise (EMM).

CITRIX®

La liberté de choix de l'utilisateur est devenue le fondement essentiel de la plupart des stratégies informatiques. En permettant aux utilisateurs de choisir eux-mêmes les périphériques les plus adaptés à leurs besoins, les entreprises améliorent la productivité, la flexibilité d'emploi et la satisfaction de leurs employés. Durant la première vague de consumérisation, les initiatives se focalisaient essentiellement sur des stratégies et des programmes BYOD. Puis apparut très vite le CYOD (choose-your-own-device), qui permet aux utilisateurs de choisir eux-mêmes un périphérique d'entreprise dans une courte liste proposée par leur employeur. Apparus plus récemment, les programmes COPE (corporate-owned, personally-enabled) permettent aux utilisateurs de choisir un périphérique d'entreprise à partir d'une liste approuvée et d'utiliser conjointement sur ce périphérique à la fois leurs applications professionnelles et personnelles. S'il existe quelques nuances entre les programmes BYOD, CYOD et COPE, notamment dans leur approche de partage des coûts et de compensation financière, leurs principes fondamentaux demeurent relativement identiques, notamment dans leurs implications en termes de sécurité. À chaque fois que du contenu personnel et du contenu professionnel cohabitent sur un même périphérique, les directions informatiques doivent s'assurer que des stratégies et des technologies efficaces sont bien en place afin de protéger les données d'entreprise, sans que l'expérience et la productivité de l'utilisateur n'en soient impactées négativement.

Principes directeurs pour une stratégie BYOD, CYOD ou COPE réussie

Les utilisateurs doivent être libres de choisir le type de périphérique sur lequel ils souhaitent travailler, y compris les périphériques qu'ils utilisent dans leur vie personnelle, et pouvoir passer d'un périphérique à un autre pendant la journée.

L'informatique doit être en mesure de délivrer des fichiers, des applications et des postes à la demande sur tout périphérique, en tout lieu et sur n'importe quelle connexion, tout en garantissant un niveau de sécurité, de respect des stratégies, de conformité et de contrôle uniforme et efficace via un point de gestion unique.

Ce livre blanc offre aux cadres informatiques des conseils pour élaborer une stratégie BYOD, CYOD ou COPE complète, donnant aux utilisateurs la liberté de choix nécessaire, tout en répondant aux contraintes en matière de sécurité, de simplicité et de réduction des coûts. Basée sur une technologie de gestion de la mobilité d'entreprise, de virtualisation d'applications et de postes, de partage sécurisé de fichiers, ainsi que des meilleures pratiques de BYOD, CYOD et COPE, cette stratégie permet à votre entreprise :

- **De donner de l'autonomie à ses utilisateurs** en les laissant choisir leur propre périphérique pour améliorer la productivité, la collaboration et la mobilité.
- **De protéger les informations sensibles** contre la perte et le vol tout en respectant les normes de confidentialité, de conformité et de gestion des risques.
- **De réduire les coûts et de simplifier la gestion** grâce au provisioning en libre-service et à l'automatisation de l'administration et de la supervision
- **De simplifier l'informatique** grâce à une unique solution complète pour sécuriser les données, les applications et les périphériques.

Le BYOD 2.0 : de nouveaux modèles et de nouvelles technologies étendent en toute sécurité la liberté de choix des utilisateurs

Partant du postulat que les employés travaillent souvent bien mieux s'ils sont autorisés à choisir leurs propres outils, les stratégies BYOD permettent aux utilisateurs d'employer à des fins professionnelles leurs périphériques personnels, que ce soit de façon occasionnelle, prioritaire ou exclusive. Alors que la mobilité et la consumérisation continuent à transformer radicalement l'informatique, deux nouvelles approches alternatives,

le CYOD et le COPE, ont fait leur apparition. Elles associent la liberté de choix à un contrôle accru des directions informatiques. Le COPE peut également être mis en œuvre parallèlement au CYOD ou au BYOD, sous forme d'une stratégie hybride permettant d'accroître la mobilité de façon adaptée pour différents types utilisateurs et groupes d'utilisateurs. Par exemple, le COPE permet de garantir mobilité et liberté de choix aux employés qui ne pourraient ou ne souhaiteraient pas utiliser leurs périphériques personnels au travail, ou qui ne pourraient pour une quelconque raison bénéficier d'un programme BYOD ou CYOD.

Dans les faits, que cela soit autorisé ou non, les employés utilisent déjà leurs périphériques personnels au travail. Sans une stratégie BYOD, CYOD ou COPE complète et cohérente, intégrant à la fois des politiques et des technologies, l'entreprise court des risques significatifs, notamment en termes de sécurité, de conformité et de complexité informatique.

D'un point de vue technologique, la question la plus importante (surtout pour le BYOD et le CYOD) est : comment les utilisateurs pourront-ils accéder aux applications, aux fichiers et aux données d'entreprise à partir de leurs périphériques personnels ? La seule installation d'applications sur le périphérique soulèverait de sérieux risques en matière de sécurité, de confidentialité et de conformité, des problèmes de gestion des licences et une complication du support. Limiter le choix des employés aux périphériques Windows et négliger les autres poserait les mêmes problèmes. Que ce soit dans le cadre d'un programme BYOD, CYOD ou COPE, les directions informatiques doivent également faire en sorte que les applications et données d'entreprise résidant sur le périphérique ne soient pas exposées à des risques du fait de la coexistence de contenu personnel, comme par exemple lors de l'utilisation d'un service de partage de fichiers grand public pour stocker et synchroniser des données professionnelles, ou lorsqu'un virus introduit via un jeu personnel infecte les données d'entreprise stockées sur le périphérique.

C'est pourquoi, tout programme BYOD, CYOD ou COPE doit intégrer des technologies garantissant une informatique totalement indépendante vis-à-vis du périphérique, notamment l'EMM (gestion de la mobilité d'entreprise), la virtualisation de postes et d'applications Windows, le partage de fichiers sécurisé, la collaboration en ligne et les services de support technique à distance. En adoptant cette approche, l'informatique peut offrir aux utilisateurs la liberté qu'ils souhaitent tout en garantissant sécurité et contrôle. Les utilisateurs peuvent accéder en un seul clic à toutes leurs applications Windows, Web, SaaS et mobiles via une librairie d'applications unifiée, et ce sur tout périphérique et toute connexion, via un système d'authentification unique et en bénéficiant d'une reconnexion transparente de session, indépendamment du lieu, du réseau et du périphérique. L'informatique bénéficie d'un point de contrôle unique pour provisionner et déprovisionner rapidement tout type d'application, que ce soit pour fournir de nouvelles ressources ou bloquer l'accès lorsque cela n'est plus nécessaire ou souhaité. Dans la plupart des scénarios, les informations d'entreprise restent en sécurité dans le datacenter ; dans les cas où elles doivent être stockées sur le périphérique, elles sont protégées via des mécanismes de création de conteneurs, de chiffrement et de suppression à distance. Une solution EMM qui permet la gestion d'applications mobiles (MAM), la gestion de contenus mobiles (MCM) et la gestion de périphériques mobiles (MDM) permet aux directions informatiques d'adopter une approche de sécurisation granulaire et adaptée à chaque application, à la place ou en complément d'une approche uniquement axée au niveau du périphérique.

De cette façon, les directions informatiques simplifient la gestion et réduisent les coûts, tout en donnant aux utilisateurs la possibilité de travailler facilement, en toute sécurité et transparence sur tout type de périphérique, quel que soit son propriétaire. En s'appuyant sur la capacité à gérer les données et les applications de façon granulaire, elles protègent efficacement les informations sensibles tout en s'affranchissant de la nécessité de gérer les périphériques personnels des employés. Elles bénéficient d'options de provisioning et de contrôle des applications, des données et des périphériques basés sur l'identité, de déprovisioning de compte automatique pour les utilisateurs licenciés et peuvent supprimer à distance des données et applications sur les périphériques perdus.

Les stratégies BYOD, CYOD et COPE peuvent varier considérablement d'une organisation à une autre, selon les priorités et les inquiétudes, et doivent être élaborées en consultant les équipes des ressources humaines, financières, juridiques et de la sécurité informatique. Généralement, les principales différences existant entre les approches BYOD, CYOD et COPE concernent les coûts. Les utilisateurs du BYOD payent leurs périphériques et leurs abonnements, en bénéficiant parfois d'une allocation totale ou partielle versée par l'entreprise. Dans le cas du COPE et du CYOD, c'est l'entreprise qui paie directement le périphérique et les abonnements. En outre, les stratégies BYOD intègrent parfois des éléments qui dépassent le cadre des programmes COPE ou CYOD, comme par exemple la question de savoir si les employés doivent être rémunérés en heures supplémentaires lorsqu'ils consultent leur messagerie professionnelle en dehors des heures ouvrables et le week-end.

Le chapitre suivant fournit une liste de conseils et de meilleures pratiques destinés à la conception des stratégies BYOD, CYOD et COPE, ainsi qu'à leur mise en œuvre avec l'aide de solutions Citrix® (XenMobile®, XenApp®, Citrix Receiver®, NetScaler® Access Gateway, ShareFile®, GoToMeeting®, GoToAssist® et Podio®).

Les éléments constitutifs d'une stratégie BYOD, CYOD ou COPE véritablement complète	
Technologie et systèmes	• Librairie applicative en libre-service offrant un accès sécurisé et unifié, ainsi qu'une authentification unique aux applications mobiles, Web, Windows et personnalisées sur tout périphérique et tout réseau. • Gestion de la mobilité d'entreprise pour sécuriser les applications, données et périphériques mobiles. • Mise à disposition à la demande et sécurisée des applications, des données et des postes sur tout périphérique (personnel ou professionnel) avec suivi et supervision pour favoriser la conformité et la confidentialité. • Partage et synchronisation de fichiers sécurisés sur tout périphérique. • Collaboration avec réunions en ligne, vidéo en haute définition et espaces de travail collaboratifs sur tout périphérique. • Support distant aux utilisateurs et technologies en tout lieu.
Stratégies	• Admissibilité • Périphériques autorisés • Disponibilité des services • Déploiement • Partage des coûts • Sécurité • Support et maintenance

Considérations et meilleures pratiques pour le BYOD, le CYOD et le COPE

Le succès d'une initiative BYOD, CYOD ou COPE repose sur sa simplicité aux yeux des utilisateurs et son efficacité en matière de sécurité, de contrôle et de gestion aux yeux de l'informatique. Les directions informatiques peuvent être tentées d'élaborer des stratégies spécifiques pour chaque scénario envisageable ; mais, dans la réalité, la plupart des réflexions peuvent être menées en appliquant quelques principes simples et cohérents. Dans la majorité des cas, les directions informatiques peuvent réfléchir à la façon de gérer et de fournir aux utilisateurs un accès sécurisé aux applications et aux données, assorti de fonctionnalités de gestion, de configuration et de sécurité des périphériques personnels basées sur des rôles, afin de protéger l'entreprise contre les menaces, la perte de données et les utilisations non conformes.

Admissibilité et enregistrement

Les entreprises doivent identifier clairement les personnes autorisées à utiliser des périphériques personnels, que ce soit sur une base ponctuelle pour compléter un périphérique d'entreprise, pour le remplacer de façon permanente ou pour tout autre cas de figure. Cela peut être considéré comme un privilège à gagner, une réponse à la demande d'un employé, une exigence pour certains types de rôle, un risque excessif pour certains scénarios d'utilisation ou, plus vraisemblablement, une combinaison de tout cela.

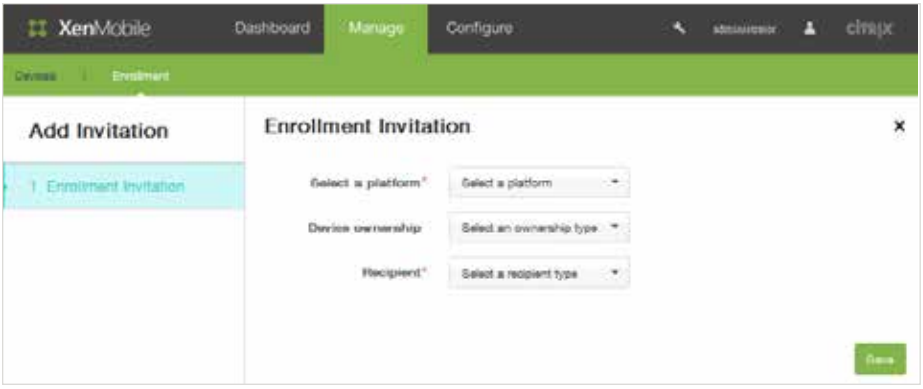

Figure 1 : XenMobile prend en charge l'enregistrement des périphériques BYOD, CYOD et COPE

Figure 2 : XenMobile simplifie l'enregistrement des périphériques. XenMobile permet aux directions informatiques d'enregistrer les utilisateurs manuellement ou via une importation de fichier. L'auto-détection simplifie significativement le processus d'enregistrement pour les utilisateurs, qui peuvent employer leurs noms d'utilisateur réseau et leurs mots de passe Active Directory pour enregistrer leurs périphériques au lieu d'avoir à saisir des informations associées au serveur.

Les programmes impliquant le remplacement d'un périphérique d'entreprise par un périphérique personnel (souvent avec une compensation financière proposée à l'employé) s'accompagnent de considérations spécifiques à prendre en compte. Une façon de déterminer qui peut participer à ce type de programme consiste à appliquer des critères, tels que le type d'utilisateur, la fréquence des déplacements ou la nécessité pour cette personne d'accéder à des données sensibles hors ligne. Bien que les conditions d'admissibilité soient assez larges, les directeurs doivent avoir le dernier mot quant aux membres du personnel considérés comme des candidats appropriés pour recevoir une compensation afin de remplacer leur périphérique d'entreprise par celui de leur choix. Les directeurs peuvent également mettre en œuvre le BYOD, le CYOD ou le COPE dans le cadre d'autres incentives, privilèges et mesures disciplinaires au sein d'un service.

Les sous-traitants sont généralement les candidats au BYOD par excellence. De nombreuses entreprises s'attendent déjà à ce que les sous-traitants apportent leur propre périphérique, et leur demander qu'ils le fassent contribue à la conformité des sous-traitants indépendants.

Périphériques autorisés

Le CYOD et le COPE permettent aux directions informatiques d'éviter une diversité ingérable de périphériques au sein de l'entreprise grâce à la limitation des types de périphériques mobiles pris en charge. La granularité de cette stratégie dépendra des besoins de vos utilisateurs, des risques encourus et des ressources de support technique disponibles. D'une manière générale, plus votre stratégie est détaillée en termes de types de périphériques, de versions de système d'exploitation et de numéros de modèles, plus les ressources nécessaires

pour tester et maintenir de façon adéquate les périphériques concernés devront être importantes. Une stratégie plus granulaire peut également s'avérer plus restrictive pour les utilisateurs, par exemple en n'autorisant qu'un modèle particulier d'iPhone ou une version bien précise du système d'exploitation Android.

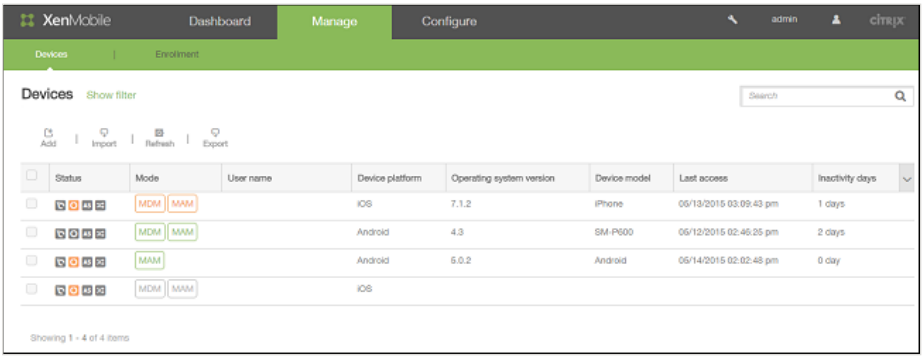

Figure 3 : La présence d'informations pré-enregistrées sur les périphériques accélère le déploiement. XenMobile fournit une base de données relative aux périphériques mobiles afin de faciliter le déploiement. Des périphériques supplémentaires peuvent être ajoutés manuellement ou via une importation de fichier.

Les participants au programme BYOD doivent être invités à acheter leur propre périphérique en passant par les circuits de consommation normaux, plutôt qu'auprès du service achats de l'entreprise. Cela permet de clarifier les choses en matière de propriété, et garantit une relation directe entre les participants et leur fournisseur de matériel. Vous pouvez faire profiter vos employés de réductions, dans le cadre de vos accords avec des fournisseurs professionnels. Certains utilisateurs peuvent avoir besoin ou envie de compléter leur périphérique par un autre, comme un moniteur ou un clavier, lorsqu'ils sont au bureau. Dans ce cas de figure, veillez à définir qui achète et possède chaque article.

Déploiement

Une fois que votre initiative BYOD, CYOD ou COPE a été élaborée, la communication est essentielle au succès de sa mise en œuvre. Les utilisateurs doivent recevoir des conseils afin de décider s'ils souhaitent participer et comment choisir le périphérique correspondant à leurs besoins. Ils doivent également parfaitement comprendre leurs responsabilités en tant qu'utilisateurs mobiles, notamment savoir exactement comment accéder aux données, les utiliser et les stocker, et connaître la façon appropriée d'installer et d'utiliser à des fins professionnelles des comptes de services ou d'applications grand public non gérés par l'entreprise. Les données professionnelles doivent être strictement séparées afin de respecter les exigences de e-Discovery et les politiques de stockage des données ; de la même façon, aucun courrier électronique professionnel ne doit être envoyé depuis un compte personnel. La politique d'utilisation doit s'appliquer de la même façon aux périphériques BYOD qu'aux périphériques d'entreprise.

Il est également important de mettre en place un programme d'aide à l'adoption qui aidera les participants à devenir opérationnels rapidement. Un email de bienvenue contenant un lien vers un portail en libre-service peut aider les utilisateurs à devenir plus productifs, plus rapidement.

Partage des coûts

L'un des principaux avantages du BYOD réside dans sa capacité à réduire les coûts en laissant à la charge des utilisateurs tout ou partie du coût de divers périphériques utilisés au travail, et en évitant aux directions informatiques d'avoir à gérer l'achat et le support d'un nombre croissant de périphériques dans l'entreprise. Cela est particulièrement vrai lorsque les entreprises ne fournissent plus de périphériques. Les entreprises accordent en moyenne une allocation représentant entre 18 et 20 % de la valeur du périphérique, même si certaines sont plus généreuses et que d'autres n'accordent rien du tout. Les participants doivent être conscients du fait que l'allocation sera considérée comme un revenu d'un point de vue fiscal. Dans les régions où l'impôt sur le revenu est plus élevé, vous pouvez envisager d'augmenter l'allocation en fonction de cela afin que le montant net des subventions soit le même pour tous les participants. Toute stratégie BYOD, avec ou sans partage des coûts, doit identifier clairement qui paiera pour l'accès au réseau en dehors du pare-feu d'entreprise, que ce soit via la 3G, un accès public à Internet sans fil ou une connexion haut débit à la maison.

Si vous choisissez d'offrir une subvention, celle-ci doit refléter l'intégralité de la participation de chaque personne. Les subventions doivent être renouvelées à intervalles réguliers afin de garantir que les périphériques personnels ne dépassent pas l'âge attendu pour un périphérique d'entreprise. Si un participant quitte l'entreprise pendant un cycle BYOD, vous pouvez réclamer une partie de l'allocation en cours.

Le partage des coûts a des conséquences sur la mise en place du BYOD dans l'entreprise. Un déploiement en une seule fois peut augmenter les coûts à mesure que les utilisateurs décident de participer au programme (et de réclamer leur allocation), et ce en tout point du cycle de rafraîchissement. Proposer le programme aux utilisateurs lorsqu'ils approchent de la fin de la durée de vie de leur périphérique permet d'étaler l'impact. Les entreprises ne proposant pas d'allocation peuvent inviter les utilisateurs à participer au programme dès sa mise en place.

Sécurité et Conformité

Un prérequis essentiel demeure, que le propriétaire du périphérique soit l'entreprise ou l'utilisateur : la protection efficace des données sans impact négatif sur l'expérience. Pour les programmes autorisant la présence d'applications et de données personnelles sur les périphériques utilisés à des fins professionnelles, la MAM permet d'assurer une séparation stricte entre les contenus personnel et professionnel.

Si l'installation directe d'applications sur des périphériques personnels peut augmenter les risques, un programme de mobilité associant la gestion de la mobilité d'entreprise, la virtualisation de postes et le partage de fichiers sécurisé permet de rendre cette installation totalement inutile. Toutes les informations d'entreprise demeurent sécurisées au sein du datacenter, et ne sont stockées sur le périphérique que sous forme chiffrée et parfaitement isolée, lorsque cela est absolument nécessaire. Dans les cas où les informations n'ont pas besoin de résider sur le périphérique mobile, les données d'entreprise peuvent être protégées via des mécanismes de création de conteneurs, de chiffrement et de suppression à distance. Pour éviter toute exfiltration, la direction informatique peut mettre en place des stratégies pour désactiver l'impression ou l'accès au stockage côté client (disques locaux, périphériques de stockage USB, etc.).

Sur les périphériques mobiles, l'accès aux données et aux applications peut être contrôlé, sécurisé et géré à l'aide de stratégies basées sur le propriétaire du périphérique, son statut et son emplacement. La direction informatique peut enregistrer et gérer tout périphérique, détecter les périphériques débridés, et supprimer tout ou partie d'un périphérique non conforme, perdu, volé ou appartenant à un employé ou un sous-traitant licencié. La sécurité des applications est garantie grâce à un accès sécurisé aux applications via des tunnels applicatifs, une liste d'applications autorisées et interdites, ainsi que des stratégies dynamiques en fonction du contexte.

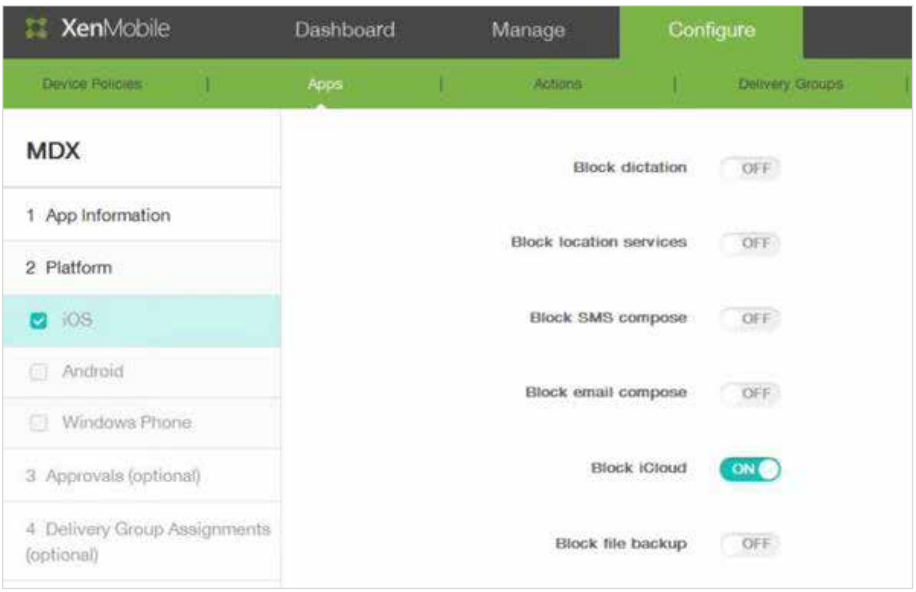

Figure 3 : La gestion d'applications mobiles (MAM) protège les données de l'entreprise. XenMobile garantit un contrôle de sécurité granulaire des stratégies applicatives en vous permettant d'ajouter des fonctionnalités à des applications mobiles internes ou tierces existantes. Notamment : provisioning, exigences d'authentification personnalisées, révocation application par application, stratégies de confinement des données, chiffrement des données et mise en réseau privé virtuel application par application.

Pour protéger le réseau de l'entreprise, certaines directions informatiques utilisent une technologie de contrôle d'accès réseau (NAC) afin d'authentifier les utilisateurs se connectant au réseau et de vérifier si leur périphérique dispose d'un antivirus et de correctifs de sécurité à jour. Une autre option consiste à utiliser Citrix NetScaler Access Gateway pour fournir des fonctionnalités d'accès sécurisé supplémentaires. NetScaler garantit un contrôle granulaire basé sur des stratégies et intégrant l'authentification unique au niveau applicatif, le micro VPN applicatif et les mots de passe forts.

En dehors du pare-feu, la virtualisation et le chiffrement peuvent dissiper la plupart des failles sécuritaires associées au Wi-Fi, au chiffrement WEP, à la connectivité sans fil ouverte, à la 3G/4G et aux méthodes d'accès grand public. Sur les périphériques mobiles, la sécurité des applications est garantie grâce à un accès sécurisé aux applications via des tunnels applicatifs, une liste d'applications autorisées et interdites, ainsi que des stratégies dynamiques en fonction du contexte. Les fonctionnalités de sécurité réseau offrent non seulement visibilité et protection contre les menaces mobiles internes et externes, en bloquant les périphériques malveillants, les utilisateurs non autorisés et les applications non conformes, mais aussi l'intégration de systèmes de gestion du système d'information (SIEM).

En cas de départ d'un participant au programme BYOD, d'une violation de la stratégie correspondante, de perte ou de vol d'un périphérique personnel, l'équipe informatique doit disposer d'un mécanisme pour résilier instantanément l'accès aux données et aux applications, notamment pour déprovisionner les comptes SaaS professionnels et supprimer à distance les données présentes sur les périphériques égarés. Cette fonctionnalité est également essentielle pour les périphériques CYOD ou COPE appartenant à l'entreprise, car elle permet de réattribuer un périphérique d'entreprise à un nouvel utilisateur sans que les données laissées sur celui-ci ne tombent entre les mains d'un utilisateur non autorisé à y accéder.

Plutôt que d'adopter une approche BYOD ouverte, permettant aux utilisateurs d'apporter n'importe quel périphérique pour accéder aux données et applications d'entreprise, certaines entreprises optent pour une approche gérée. Dans ce cas de figure, la direction informatique gère directement le périphérique personnel, y compris son enregistrement, sa validation, ses autorisations et son accès aux ressources.

Gestion et supervision

Qu'il s'agisse de BYOD, de CYOD ou de COPE, une gestion et une supervision continues sont indispensables afin de garantir la conformité de la stratégie et de permettre le calcul du retour sur investissement. Si des violations sont détectées, la direction informatique devra rappeler aux utilisateurs la politique applicable et prendre les mesures prévues. Certaines solutions EMM améliorent l'efficacité et la productivité informatiques en automatisant différents aspects de la gestion et de la supervision. Par exemple la définition des actions précises à entreprendre en cas de violations diverses. Ces actions peuvent notamment inclure la suppression totale ou partielle du périphérique, la qualification du périphérique comme non-conforme, la révocation du périphérique ou l'envoi d'une notification à l'utilisateur lui enjoignant de corriger un problème (supprimer une application interdite, par exemple) dans un certain délai avant que des mesures plus sévères ne soient appliquées.

Figure 4 : Le tableau de bord de XenMobile garantit aux directions informatiques une visibilité complète et conviviale sur son environnement mobile.

Figure 5 : XenMobile automatise les tâches de gestion et de supervision.

XenMobile contribue à alléger le travail en automatisant différents aspects de la gestion et de la supervision. Par exemple, les directions informatiques peuvent configurer XenMobile afin qu'il détecte automatiquement toute application mise sur liste noire (Words with Friends, par exemple). Il est alors possible de définir un déclencheur qui qualifie le périphérique comme non-conforme lorsque Words with Friends est détecté. Puis de notifier à l'utilisateur qu'il doit supprimer cette application s'il veut que son périphérique soit de nouveau déclaré conforme. Vous pouvez en outre définir un délai maximal accordé à l'utilisateur pour obtempérer avant que des mesures plus sévères ne soient adoptées (suppression sélective du périphérique, par exemple).

Support et maintenance des périphériques

Un programme de BYOD réduit souvent la maintenance nécessaire pour chaque périphérique, car l'utilisateur en est également le propriétaire. Cela dit, la stratégie doit préciser clairement la façon dont les activités de support et de maintenance doivent être gérées et payées. En cas d'utilisation d'un périphérique personnel à la place d'un périphérique d'entreprise, la probabilité d'un recours au support technique peut être plus élevée, mais cela doit être défini plus précisément afin d'épargner à la direction informatique une complexité et une charge de travail accrues. Dans le cadre de la plupart des programmes CYOD ou COPE, la direction informatique est entièrement responsable du support et de la maintenance des périphériques.

Une stratégie technologique sécurisée pour le BYOD, le CYOD et le COPE

Citrix permet aux entreprises de prendre en charge les initiatives BYOD, CYOD et COPE grâce à la gestion de la mobilité d'entreprise, la virtualisation d'applications et de postes Windows, le partage de fichiers sécurisé, la collaboration et le support distant. Ainsi, l'informatique peut mettre à disposition les applications d'entreprise, le partage et la synchronisation de fichiers sur tout périphérique apporté par les utilisateurs au travail, tout en garantissant sécurité et contrôle.

Les solutions Citrix offrent toutes les fonctionnalités clés nécessaires pour rendre le BYOD, le CYOD ou le COPE simple, sûr et efficace pour toute entreprise.

Gestion de la mobilité d'entreprise *fournie par Citrix XenMobile*

La direction informatique bénéficie d'options de provisioning et de contrôle des applications, des données et des périphériques basés sur l'identité, de déprovisioning de compte automatique pour les utilisateurs licenciés et de la suppression à distance des données et applications sur les périphériques perdus. En plus de la MDM qui permet de gérer les périphériques, les fonctionnalités MAM et MCM de XenMobile garantissent la sécurité et le contrôle au niveau des applications, pour protéger efficacement les données d'entreprise sans impacter l'utilisation du contenu personnel présent sur les périphériques BYOD, CYOD ou COPE.

Virtualisation de postes et d'applications Windows *fournie par Citrix XenDesktop et Citrix XenApp*

La direction informatique peut transformer des applications et des postes de travail complets en services à la demande délivrés sur tout périphérique. Les applications et les données sont gérées au sein du datacenter, ce qui permet à la direction informatique d'assurer la protection des données, la conformité, le contrôle d'accès et l'administration des utilisateurs de façon centralisée, aussi facilement sur des périphériques personnels que sur des périphériques d'entreprise, le tout dans un environnement unifié.

App store *fourni par Citrix Receiver*

Les utilisateurs sont libres de choisir leur périphérique, y compris les ordinateurs de bureau et portables Windows et Mac®, les appareils mobiles iOS, Android et Windows, ou encore les périphériques mobiles Google Chromebook et Blackberry®, le tout avec une itinérance et une expérience haute définition sans accroc entre les différents périphériques, lieux et réseaux. Les utilisateurs bénéficient d'un accès en un seul clic aux applications mobiles, Web, Windows et du datacenter à partir d'une librairie applicative unifiée, y compris à des applications de productivité intégrée, en offrant une formidable expérience utilisateur.

Accès sécurisé *fourni par Citrix NetScaler Access Gateway*
Un cadre de gestion unifié permet à la direction informatique de sécuriser, de contrôler et d'optimiser l'accès à des applications, des postes de travail et des services sur tout périphérique. Le contrôle d'accès, l'audit et les rapports assurent la conformité et la protection des données.

Partage de fichiers sécurisé *fourni par Citrix ShareFile*
Les utilisateurs peuvent partager des fichiers en toute sécurité avec n'importe qui au sein de l'entreprise ou à l'extérieur, et synchroniser leurs fichiers sur tous leurs périphériques. Le contrôle d'accès basé sur des stratégies, l'audit, la création de rapports et la suppression à distance permettent de sécuriser le contenu de l'entreprise.

Collaboration sociale *fournie par Citrix GoToMeeting et Citrix Podio*
Les utilisateurs peuvent organiser ou rejoindre des réunions en quelques secondes depuis n'importe quel lieu et n'importe quel périphérique, grâce à des vidéos en haute définition pour de véritables interactions en face à face. Les flux d'activités sociales, les applications personnalisées et les espaces de travail collaboratifs aident les personnes à travailler ensemble de façon plus efficace.

Support à distance *fourni par Citrix GoToAssist*
La direction informatique peut fournir un support centralisé aux utilisateurs et technologies en tout lieu, afin de garantir la disponibilité des PC, Mac, périphériques mobiles, serveurs et réseaux au sein de l'organisation.

Conclusion

Stratégie étroitement liée à de puissantes tendances informatiques comme la consumérisation, la flexibilisation de l'environnement de travail (télétravail, stratégies de reconception de l'espace de travail, etc.), la mobilité et le cloud computing, le BYOD, le CYOD et le COPE continueront à transformer la façon dont les utilisateurs et les organisations travaillent. Sous la forme de la mise à disposition à la demande de données, d'applications et de postes sur tout périphérique, la bonne stratégie permettra :

- **De donner de l'autonomie à ses utilisateurs** en les laissant choisir leur propre périphérique pour améliorer la productivité, la collaboration et la mobilité.
- **De protéger les informations sensibles** contre la perte et le vol tout en respectant les normes de confidentialité, de conformité et de gestion des risques.
- **De réduire les coûts et de simplifier la gestion** grâce au provisioning en libre-service et à l'automatisation de l'administration et de la supervision
- **De simplifier l'informatique** grâce à une solution complète unique pour sécuriser les données, les applications et les périphériques.

Leader en matière de modes de travail mobiles et flexibles, Citrix propose des technologies complètes, fondées sur une expérience concrète et les meilleures pratiques pour la mise en œuvre réussie de programmes BYOD, CYOD et COPE. Les solutions Citrix aident déjà de nombreuses entreprises de toutes tailles à profiter pleinement des avantages de la mobilité et de la liberté de choix.

Pour en savoir plus, visitez www.citrix.fr/byod ou consultez nos autres livres blancs sur le sujet.

Ressources supplémentaires

Délivrer des informations d'entreprise en toute sécurité sur les tablettes et smartphones Android, Apple iOS et Microsoft

Éviter les pièges sécuritaires dans le cadre d'une stratégie BYOD

Siège social
Fort Lauderdale, Floride, États-Unis

Siège Silicon Valley
Santa Clara, Californie, États-Unis

Siège Europe, Moyen-Orient, Afrique
Schaffhausen, Suisse

Centre de développement Inde
Bangalore, Inde

Siège Division en ligne
Santa Barbara, Californie, États-Unis

Siège Pacifique
Hong Kong, Chine

Siège Amérique latine
Coral Gables, Floride, États-Unis

Centre de développement Royaume-Uni
Chalfont, Royaume-Uni

CITRIX®

À propos de Citrix
Citrix (NASDAQ : CTXS) est à la pointe de la transition vers le bureau logiciel. En combinant virtualisation, gestion de la mobilité, solutions networking et SaaS, Citrix offre aux entreprises et aux utilisateurs de nouveaux moyens pour mieux travailler. Les solutions Citrix favorisent la mobilité professionnelle grâce à des espaces de travail mobiles et sécurisés offrant aux utilisateurs un accès instantané aux applications, postes de travail, données et communications sur tout périphérique, tout réseau et dans le cloud. Le chiffre d'affaires annuel de l'entreprise a atteint 3,14 milliards de dollars en 2014. Les produits Citrix sont utilisés dans le monde entier par plus de 330 000 entreprises et plus de 100 millions d'utilisateurs. Pour en savoir plus : www.citrix.fr

Copyright © 2015 Citrix Systems, Inc. Tous droits réservés. Citrix, XenMobile, XenApp, Citrix Receiver, NetScaler, ShareFile, GoToMeeting, GoToAssist et Podio sont des marques commerciales de Citrix Systems, Inc. et/ou de l'une de ses filiales, et peuvent être enregistrées aux Etats-Unis et dans d'autres pays. Tous les autres noms de produit et d'entreprise mentionnés ici sont des marques commerciales de leurs propriétaires respectifs.