Mener votre entreprise vers la mobilité : Check-list pour les cadres

Opportunités mobiles

La transformation des téléphones mobiles en véritables ordinateurs ne date pas d'hier, mais cette transition est passée à la vitesse supérieure ces deux dernières années : Les périphériques mobiles de grande consommation sont si fascinants et offrent aux utilisateurs professionnels une solution tellement puissante pour apprendre, interagir, partager et communiquer que les entreprises sont désormais disposées à chambouler leur mode d'organisation pour les adopter.

Devenir une entreprise mobile est synonyme de nouvelles opportunités pour votre organisation. Les employés sont davantage satisfaits et plus productifs lorsqu'ils bénéficient d'un accès mobile à leur messagerie, leurs applications et leurs données depuis des tablettes ou des smartphones. Les entreprises basant leur activité sur des solutions de travail mobile profitent d'un avantage concurrentiel et stimulent la croissance de leur chiffre d'affaires.

Dans un récent sondage, Aberdeen a mis en évidence que les meilleures entreprises sont trois fois plus susceptibles que les autres d'associer le flux d'activité aux périphériques mobiles de leurs utilisateurs.[1] Cependant, et la quasi totalité des études à ce sujet sont unanimes, la sécurité est le premier obstacle à la mobilité des entreprises et aux programmes BYOD. D'après des chiffres récents publiés par CSO Magazine, 17 % des entreprises ont déjà rencontré une faille de sécurité mobile.[2]

Et pourtant...

Voilà le problème. Comités d'audit, comités de direction et conseils d'administration sont tous d'accord, même s'ils continuent joyeusement à pianoter sur leurs périphériques préférés : laisser les employés choisir leur périphérique et accéder aux ressources, applications et données de l'entreprise est une proposition à risque. Contrairement aux PC verrouillés ou aux périphériques BlackBerry® rigoureusement contrôlés, les périphériques mobiles de l'entreprise d'aujourd'hui sont divers, présentent différents niveaux de vulnérabilité et ne permettent pas à l'informatique de gérer de façon unique et cohérente la stratégie de sécurité la plus fondamentale, comme l'application d'un mot de passe.

À mesure que de plus en plus d'entreprises transmettent des documents confidentiels à leur conseil d'administration via iPad® d'Apple®, les conséquences d'une violation des données sont plus faciles à imaginer. Encore marqués par les violations de données qui ont signé la fin de nombreuses entreprises au milieu des années 2000, et ayant des intérêts en jeu à la suite du passage de la loi Sarbanes-Oxley, cadres et membres du conseil d'administration ont besoin, de toute urgence, que leurs entreprises régissent et sécurisent les périphériques mobiles.

Inquiétudes relatives à la sécurité mobile

Les inquiétudes relatives à la sécurité mobile vont de l'application de mots de passe au chiffrement de périphériques, mais les violations et les fuites de données restent en tête de liste pour les personnes chargées de mettre en œuvre des programmes de travail mobile. D'après Jack Gold, expert en sécurité des entreprises, les organisations perdront trois ou quatre fois plus de smartphones que d'ordinateurs portables chaque année. Gold pose la question (rhétorique) suivante : « avec 32 ou 64 GB de mémoire, combien de fichiers un smartphone ou une tablette perdu(e) contient-il/elle ? »[3] Si l'on estime à 250 $ le coût d'un fichier perdu,[4] l'addition se révèle salée en cas de violation de données. Concrètement, certaines études estiment le coût d'une violation mobile à plus de 400 000 $ pour une grande entreprise et à plus de 100 000 $ pour une petite structure[5] et dans certains cas, ces coûts atteignent des millions.[6] Cette inquiétude se fait plus grande à mesure qu'augmente le nombre de smartphones et de tablettes se connectant non seulement au réseau d'entreprise, mais accédant également à un nombre grandissant d'applications professionnelles et d'emplacements de stockage de contenu. Au-delà des données, les services en charge de l'informatique et de la sécurité des entreprises s'inquiètent du risque associé à l'ouverture du réseau interne à un éventail divers de périphériques mobiles. Dans de nombreux cas, les périphériques mobiles ne sont ni supervisés ni surveillés, de sorte qu'ils peuvent introduire des menaces réseau et affecter de manière négative la conformité d'une entreprise.

Trois principaux facteurs sont à l'origine des inquiétudes des entreprises en matière de sécurité

1. D'après le Center for Telecom Environment Management Standards, 78 % des entreprises autorisaient les périphériques mobiles personnels des employés sur le lieu de travail[7] et les dépenses informatiques d'entreprise en tablettes iPad® d'Apple® atteignaient à elles seules 16 milliards de dollars en 2013 ;[8] le nombre de périphériques mobiles dans l'entreprise est donc en pleine explosion, et les cadres ne sont plus les seuls concernés ; le reste des troupes s'y met aussi. De plus, que les périphériques mobiles soient détenus par l'entreprise ou personnels, le nombre d'applications présentes sur ces périphériques augmente lui aussi. Asymco, société d'analyse en mobilité, fait état d'une moyenne de 60 applications par périphérique iOS®.[9] Etant donné que plus de la moitié des entreprises prennent en charge plus d'un type de périphérique,[10] l'exposition du réseau d'entreprise à des applications potentiellement non conformes ou malveillantes est considérable.

2. L'entreprise, à tous ses niveaux, souhaite fortement équiper ses utilisateurs de périphériques mobiles et leur offrir un accès mobile aux applications et données d'entreprise. Les organisations se mobilisent également à l'horizontale, au niveau de leurs différentes activités. Cela va des chaînes de restauration équipant leurs serveurs et leur personnel de cuisine de tablettes iPad aux compagnies aériennes distribuant à leur équipage des « sacs de vol », contenant manuels, plans de vol et documents de conformité, le tout au format électronique sur leur Samsung Galaxy Tab. Ce type d'accès mobile est très prometteur, mais cela signifie également qu'un grand nombre d'utilisateurs auront accès aux données et au réseau d'entreprise depuis un nombre croissant de périphériques, multipliant ainsi les risques.

3. Les solutions de sécurité pour la mobilité d'entreprise dont nous entendons le plus souvent parler privilégient le verrouillage ou la suppression à distance des périphériques perdus ou volés, mais la principale menace réside dans le partage de données non contrôlé. Des millions d'utilisateurs partagent des données depuis une infinité de points de contact connectés au cloud, et le risque d'une fuite de données éclipse celui de la perte ou du vol de périphériques. D'après le rapport de cloud sur la gestion des périphériques mobiles Citrix, certaines des applications les plus déployées, comme Dropbox ou Evernote, sont parmi les plus fréquemment interdites par les entreprises, ce qui en dit long sur leur utilité et le risque qu'elles représentent en parallèle.[11]

Ce ne sont là que quelques-unes des activités pouvant mettre en danger les données confidentielles et exposer l'entreprise aux menaces mobiles. Il est désormais temps de passer à une solution de gestion des périphériques mobiles offrant une protection en temps réel à tous les niveaux de l'entreprise mobile.

Avec Citrix, le comité d'audit peut enfin pousser un soupir de soulagement

Citrix XenMobile™ fournit la protection en temps réel dont les entreprises ont besoin pour saisir les opportunités professionnelles qu'offre l'activité mobile tout en sauvegardant les données des entreprises, des clients et des employés, les informations financières non publiques et de Business Intelligence. Grâce à ses offres basées dans le cloud et sur site, Citrix permet à vos équipes informatiques de sécuriser et de gérer l'éventail le plus vaste de périphériques mobiles, de gagner en visibilité et en contrôle sur les applications mobiles, et de protéger le réseau d'entreprise contre les menaces mobiles.

XenMobile offre à votre organisation :

- **MDM d'entreprise.** Offrez aux utilisateurs la liberté de choisir leur périphérique sans affecter les exigences en matière de conformité.
- **Sécurisez les applications de messagerie, de navigateur et de partage de données.** Productivité applicative que les utilisateurs apprécient et que les équipes informatiques adoptent.
- **Conteneurs d'applications mobiles.** Les utilisateurs bénéficient des applications dont ils ont besoin, tandis que l'informatique respecte les normes de conformité.
- **Magasin d'applications unifié.** Stimulez l'activité en offrant un accès aux applications en tout lieu.
- **Administration avancée et accès utilisateur simplifié.** Gérez l'accès des utilisateurs et simplifiez considérablement l'expérience utilisateur.

Votre rôle dans la stratégie mobile de votre entreprise

Vous êtes conscient des risques, et vous connaissez Citrix et XenMobile, notre solution de gestion de la mobilité d'entreprise sécurisée. Vous êtes désormais armé et dangereux, vous pouvez donc aider votre équipe informatique, et l'ensemble de votre entreprise, à adopter la mobilité et à saisir les nombreuses opportunités professionnelles qu'elle offre. Partez en vainqueur.

Check-list pour les cadres

☑ Considérations relatives aux périphériques

- **Objectifs de l'entreprise :** Définissez les objectifs de votre entreprise en matière de mobilité. Précisez si vous souhaitez privilégier l'amélioration de la productivité, les opportunités commerciales et/ou le choix du périphérique des utilisateurs. Veillez à ce que la stratégie mobile de votre entreprise reflète ces objectifs.
- **Choix du périphérique vs cohérence des périphériques :** Veillez à ce que votre équipe informatique ait bien réfléchi aux compromis associés à la prise en charge des périphériques, entre liberté et choix des périphériques, ou cohérence et contrôle. Veillez à ce que tout le monde, vous y compris, soit à l'aise avec la variété des types de périphériques, ainsi que la gouvernance et la sécurité offertes à l'informatique par ces périphériques.
- **BYOD ou périphériques d'entreprise :** Si vous n'arrivez pas à choisir entre un programme 100 % périphériques d'entreprise ou 100 % périphériques personnels, réfléchissez à un scénario hybride susceptible de mieux convenir à votre entreprise. Par exemple, vous pouvez décider d'autoriser certains utilisateurs à choisir leur périphérique (à partir d'une liste définie) et limiter le choix des autres utilisateurs à un seul type de périphérique. Dans cette optique, un hôpital peut choisir de déployer un programme BYOD pour ses médecins permanents et son personnel administratif, tout en distribuant à ses infirmières des tablettes d'entreprise devant rester sur place.

☑ Considérations relatives aux utilisateurs

- **Gestion de la mobilité et éligibilité :** Déterminez les utilisateurs autorisés à être mobiles (les cadres ? le service des ventes ? les travailleurs temporaires ? tout le monde ?). Si la réponse est tout le monde, décidez des services, postes (responsables et supérieurs, par ex.) et/ou motifs professionnels donnant droit à la mobilité. Décidez également si votre politique en matière de mobilité doit être différente pour les utilisateurs intervenant sur le terrain ou ne travaillant pas à temps plein.
- **Qui finance le BYOD ? :** Décidez si votre entreprise optera pour un programme de BYOD et si vous choisirez de tolérer, d'encourager voire de subventionner tout ou partie des dépenses en périphériques et/ou en mobilité sans fil.
- **Nombre de périphériques par utilisateur :** Décidez si, oui ou non, tout ou partie des utilisateurs pourront posséder plusieurs périphériques équipés d'une solution de mobilité d'entreprise. Par exemple, l'équipe des ventes peut-elle utiliser des tablettes personnelles pour les démos en plus de téléphones ?

☑ Considérations relatives aux applications

- **Quelles applications autoriserez-vous ?** Assurez-vous que votre service informatique ait bien réfléchi aux applications mobiles auxquelles votre entreprise donnera accès (messagerie, contacts et calendrier uniquement ? automatisation de l'activité ? ERP ? applications personnelles ?). Veillez à ce que leur plan de déploiement des applications soit cohérent en termes de besoins et de risques pour votre activité. Veillez à ce que l'accès permis par l'informatique aux applications puisse varier en fonction des rôles, des groupes, des périphériques et selon que le périphérique appartient à l'entreprise ou à l'utilisateur.
- **Comment allez-vous sécuriser les applications ?** Veillez à ce que l'informatique ait la possibilité de restreindre l'accès aux applications et ressources mobiles, quel que soit le type d'utilisateur ou de périphérique choisi. Dans ce conteneur, l'informatique peut sécuriser les applications et les données grâce à des contrôles complets basés sur des stratégies pour surveiller l'utilisation du contenu de l'entreprise, y compris le DLP mobile et la possibilité de verrouiller, de supprimer et de chiffrer à distance les applications et les données.
- **Des opportunités professionnelles mobiles :** Familiarisez-vous avec les objectifs et le calendrier de vos secteurs d'activité. Veillez à ce que l'informatique tienne compte des objectifs de vos secteurs d'activité, à savoir s'ils souhaitent mobiliser leurs applications préférées pour leurs utilisateurs et partenaires, ou s'ils souhaitent développer ou étendre des applications personnalisées pour certains périphériques.

☑ Considérations relatives aux données	• **Quelles sont les règles en matière de données ?** Revoyez la politique d'accès aux données mobiles de votre service informatique afin que votre entreprise puisse définir des stratégies basées sur des rôles, des groupes, des périphériques et des scénarios pour ceux qui seront autorisés à accéder aux applications et aux espaces de stockage contenant de la propriété intellectuelle, des informations d'identification, des données de Business Intelligence, des données financières non publiques, des annonces à venir, etc. Par ailleurs, de nombreux utilisateurs peuvent posséder plus d'un périphérique ; veillez donc à ce que les utilisateurs puissent accéder en toute sécurité aux mêmes données dans leurs applications, sur le Web et dans les datacenters à partir de plusieurs périphériques. • **Evaluez les risques associés aux données :** Déterminez la valeur et le risque associés aux données auxquelles les employés accéderont, et réfléchissez aux conséquences d'une perte ou d'une violation de données. Veillez à ce que votre comité de direction et vous-même considériez le ratio risque-bénéfice comme acceptable. • **Empêcher les fuites de données :** Veillez à ce que votre service informatique soit en mesure de protéger les données sensibles. Assurez-vous que votre service informatique a réfléchi à une façon d'empêcher les fuites de données sensibles via les périphériques mobiles. • **Faciliter la collaboration :** Au-delà de la protection des données, veillez à ce que les utilisateurs ayant besoin d'accéder aux données puissent y accéder et interagir avec elles facilement. La rationalisation de l'accès facilitera l'application de vos stratégies en matière de sécurité, car les utilisateurs seront moins enclins à essayer de contourner les mesures de sécurité mises en place.
☑ Considérations relatives aux politiques	• **Conformité aux normes :** Examinez les politiques réglementaires, de secteur et d'entreprise auxquelles votre organisation est tenue (réglementations de type HIPAA, recommandations du secteur de type PCI, lignes directrices comme celles de la SEC, cadres informatiques de type ITIL, autres politiques d'entreprise) et veillez à ce que votre stratégie mobile soutienne vos contrôles de conformité actuels. • **Considérations de confidentialité et globales :** Vérifiez la législation et la réglementation étrangère des régions dans lesquelles votre entreprise exerce son activité ou fournit des services à ses clients, et veillez à ce que votre stratégie mobile soutienne votre respect à ces politiques. Cela ne concerne pas seulement la sécurité, mais aussi les réglementations portant sur la confidentialité des utilisateurs pouvant vous aider à mettre en œuvre vos solutions de mobilité d'entreprise dans les diverses régions dans lesquelles vous êtes implanté. Revoyez vos politiques d'accès et de périphériques mobiles (élaboration des politiques, supervision et reporting) avec votre comité d'audit, votre comité de direction et votre conseil d'administration. • **Contrat mobile des employés :** Définissez des stratégies claires et établissez des limites en matière de possession des périphériques, de responsabilité, de remplacement, de support et de supervision. Au-delà des stratégies de sécurité et d'accès, réfléchissez au « contrat mobile » entre l'utilisateur et l'entreprise. Qui possède le périphérique et qui finance le service ? Qui est responsable du remplacement des périphériques ? Outre cet ensemble de considérations, définissez une politique claire pour la « mise en retraite » des périphériques après le départ d'un employé. • **Configuration minimum requise :** Définissez votre niveau de flexibilité pour les périphériques n'étant pas associés à une solution de gestion de la mobilité complète. Par exemple, définirez-vous une politique permettant à certains sous-traitants et utilisateurs dans certaines régions de continuer à accéder à leur messagerie et/ou à une application sécurisée indispensable depuis leur périphérique mobile, sans compromettre la confidentialité de l'utilisateur ? • **Remboursements :** Si vous déployez un programme de BYOD, offrirez-vous une compensation ou un remboursement pour le périphérique et/ou le service ? Le cas échéant, comment gérerez-vous cela et qui sera éligible au programme ? Aurez-vous encore la possibilité de profiter de réductions de quantité auprès de fournisseurs de services ?

☑ Considérations relatives à la sécurité	• **Conformité des périphériques, des utilisateurs et des applications :** Comprenez comment votre service informatique gérera la présence de périphériques malveillants, d'utilisateurs non autorisés et d'applications mobiles non conformes sur le réseau. • **Sécurité des données :** Comprenez comment votre service informatique protégera les données d'entreprise d'un éventuel accès non autorisé, d'une perte accidentelle et de menaces internes. • **Supervision des menaces :** Comprenez comment votre service informatique surveillera votre infrastructure de sécurité afin de détecter les menaces, ainsi que les performances du réseau, des applications et des périphériques. Si vous disposez d'une politique de maintenance de journaux à des fins de conformité et juridiques, veillez à ce qu'elle définisse la collecte, la maintenance et la protection de ces journaux. • **Mise hors service :** Comprenez comment votre service informatique supprimera les données sur les périphériques en cas de perte ou de vol, ou après le départ d'un employé. Si vous envisagez d'autoriser les périphériques personnels sur le lieu de travail, réfléchissez à une stratégie pour supprimer les données d'entreprise sans toucher au contenu personnel. Veillez à élaborer un plan pour définir des stratégies et des processus clairs pour tous les employés concernés. • **Intégration SIEM :** Comprenez comment votre service informatique intégrera votre système de gestion des périphériques mobiles à un système de sécurité des informations et de gestion des événements (ou autre système), et veillez à disposer d'un plan pour cela.
☑ Considérations relatives à l'évolutivité et à la haute disponibilité	• **Disponibilité :** Veillez à ce que votre service informatique élabore et prenne en charge un accord de niveau de service en matière de disponibilité, et vérifiez qu'il soit conforme aux exigences de votre entreprise. • **Croissance de l'entreprise :** Veillez à ce que votre stratégie mobile tienne compte de la croissance et permette à votre service informatique de prendre en charge tous les utilisateurs que vous souhaitez mobiliser aujourd'hui et par la suite. • **Coûts d'évolutivité :** Veillez à ce que votre stratégie mobile vous permette de faire évoluer les utilisateurs de façon rentable et tienne compte de tous les coûts associés au matériel, aux logiciels et aux services. • **Tolérance en matière de redondance et de défaillances :** Comprenez le plan de haute disponibilité de votre stratégie mobile. Si votre stratégie inclut une répartition des charges, une redondance de serveur et de données et, dans le cadre d'une solution basée sur le cloud, une redondance globale en cas de reprise après sinistre, veillez à ce que ces investissements y figurent.
☑ Considérations relatives aux serveurs	• **Considérations en matière de qualité de service :** Déterminez si votre stratégie mobile envisage la supervision de la qualité de service des télécommunications. Le cas échéant, veillez à ce que votre service informatique définisse les actions à prendre vis-à-vis des informations de Business Intelligence recueillies. • **Dépenses de télécommunications :** Déterminez si votre stratégie mobile envisage la gestion des dépenses de télécommunications. Veillez à définir vos objectifs en termes d'économies, ainsi que des mécanismes de mesure pour évaluer vos progrès par rapport à vos objectifs. • **Support à distance :** Déterminez si votre stratégie mobile inclut des services de support à distance, de diagnostic et de dépannage, et identifiez les mécanismes en place. • **Libre-service pour les utilisateurs :** Déterminez si votre service informatique envisage d'offrir un portail en libre-service aux utilisateurs, leur permettant de réaliser des actions fondamentales de sécurité et de gestions sur leur périphérique.

A propos de Citrix XenMobile

Citrix XenMobile est une solution de gestion de la mobilité d'entreprise offrant une liberté totale en matière de périphériques mobiles, d'applications et de données, tout en garantissant la sécurité. Les employés ont accès rapidement, en un seul clic, à toutes leurs applications mobiles, Web, Windows et du datacenter à partir d'un magasin d'applications unifié, y compris à des applications de productivité exceptionnelle qui s'intègrent en toute transparence pour une superbe expérience utilisateur. Cette solution offre des options de provisioning et de contrôle des applications, des données et des périphériques basés sur l'identité, des contrôles basés sur des stratégies, tels que la restriction de l'accès aux applications aux utilisateurs autorisés, le déprovisioning de compte automatique pour les employés licenciés et la suppression à distance des données et applications sur les périphériques perdus, volés ou non conformes. Grâce à XenMobile, l'équipe informatique peut satisfaire les utilisateurs en matière de choix de périphérique, tout en évitant les pertes de données et en protégeant le réseau interne contre les menaces mobiles.

1. « Mobility in ERP 2011 », Kevin Prouty, Aberdeen, mai 2011
2. « Global State of Information Security Survey », CSO Magazine, 2012
3. « MDM is No Longer Enough » (Le MDM ne suffit plus), conférence en ligne Citrix avec l'expert en sécurité des entreprises, Jack Gold, octobre 2011
4 « U.S. Cost of a Data Breach », Ponemon Institute, mars 2011
5. State of Mobility Survey, Symantec, février 2012
6. En 2010, le coût moyen d'une violation de données était de 7,2 millions de dollars. Doug Drinkwater, 10 févr. 2012, TABTIMES.COM
7. marketwatch.com/story/ctemsr-research-78-of-enterprises-allow-bring-your-own-device-byod-2012-07-24?siteid=nbkh
8. « Global Tech Market Outlook for 2012 and 2013 », Andrew Bartels, Forrester, 6 janvier 2012
9. « More Than 60 Apps Have Been Downloaded for Every iOS Device », Asymco, 16 janvier 2011
10. « Market Overview: On-Premises Mobile Device Management Solutions », Forrester, 3 janvier 2012
11. Rapport de cloud sur la gestion des périphériques mobiles Citrix, 3e trimestre 2012

CITRIX®

A propos de Citrix

Citrix (NASDAQ : CTXS) est la société de cloud computing qui rend possible la mobilité, en permettant aux utilisateurs de travailler et de collaborer en tout lieu, et ce en toute simplicité et sans aucun risque. Avec ses solutions leaders du marché pour la mobilité, la virtualisation de postes, les réseaux et plateformes de cloud, la collaboration et le partage de données, Citrix aide les organisations à atteindre la vitesse et l'agilité nécessaires pour réussir dans un monde mobile et dynamique. Les produits Citrix sont utilisés dans plus de 260 000 organisations et par plus de 100 millions d'utilisateurs à travers le monde. Citrix a réalisé un chiffre d'affaires de 2,59 milliards de dollars en 2012. En savoir plus sur www.citrix.fr.

0513/PDF **citrix.fr**