Les 10 « incontournables » en matière de mobilité d'entreprise sécurisée

Architecture de sécurité et check-list d'évaluation

CITRIX®

www.citrix.fr

Pour une entreprise, la mobilité signifie de nouvelles opportunités. Les employés sont plus satisfaits et plus productifs lorsqu'ils bénéficient d'un accès mobile à leur messagerie, leurs applications et leurs données à partir de tablettes ou de Smartphones. Les entreprises appuyant leur activité sur des solutions de travail mobile s'assurent des avantages concurrentiels et stimulent la croissance de leur chiffre d'affaires.

Dans le cadre d'une étude récente, Aberdeen a révélé que les entreprises qui réussissent le mieux sont trois fois plus susceptibles d'associer leurs flux commerciaux à des périphériques mobiles que les autres.[1] Pourtant, selon la plupart des analystes, les craintes liées à la sécurité sont le principal obstacle freinant l'adoption des programmes BYOD et de mobilité d'entreprise. CSO Magazine a récemment révélé que 17% des entreprises avaient déjà subi une violation de données mobiles.[2]

Les craintes liées à la sécurité mobile

Si l'éventail des craintes liées à la sécurité mobile est large, associé à des réalités aussi diverses que la violation de mot de passe ou l'obligation de chiffrer les périphériques, ce sont incontestablement les violations de données et les pertes de données qui viennent en tête de liste dans l'esprit des personnes en charge des programmes de travail mobile. D'après Jack Gold, expert dans le domaine de la sécurité d'entreprise, ces dernières égareront chaque année trois à quatre fois plus de Smartphones que de notebooks. Gold pose la question suivante : « avec 32 ou 64 Go de mémoire, combien de dossiers contient une tablette ou un Smartphone égaré ? »[3] Le coût estimé d'un dossier égaré étant en moyenne de 250 $,[4] la perte de données peut revenir très cher à l'entreprise. En fait, certaines études estiment le coût d'une violation de données mobiles à plus de 400 000 $ pour une entreprise de taille moyenne et à plus de 100 000 $ pour une PME,[5] la somme pouvant dans certains cas se compter en millions.[6] Cette crainte est donc fondée, un nombre sans cesse croissant de Smartphones et de tablettes se connectant aux réseaux d'entreprise pour accéder à un nombre lui aussi chaque jour plus important d'applications et de données professionnelles.

Au delà de ce problème des données, les directions informatiques craignent également tous les risques associés à l'ouverture de leur réseau interne à un large éventail de périphériques mobiles. Le plus souvent, les Smartphones et les tablettes n'appartiennent pas à l'entreprise et ne sont pas gérés par elle, ce qui signifie qu'ils peuvent être vecteurs de menaces pour le réseau et peuvent impacter négativement la conformité réglementaire de l'entreprise. Trois facteurs principaux contribuent essentiellement à alimenter les craintes de l'entreprise en matière de sécurité.

1. L'essor exponentiel des périphériques et des applications mobiles

D'après une enquête du Center for Telecom Environment Management Standards, 78% des entreprises autorisent l'emploi de périphériques mobiles personnels sur le lieu de travail[7] et les achats de tablettes Apple® iPad® par les directions informatiques d'entreprise ont représenté à eux seuls 16 milliards de $ en 2013.[8] Les périphériques mobiles connaissent un essor phénoménal en volume, et se répandent partout dans l'entreprise : ce ne sont plus uniquement des cadres supérieurs qui les adoptent au travail, mais bien l'ensemble des cadres et des employés, jusqu'aux plus modestes. En outre, peu importe que ces périphériques soient achetés par l'entreprise ou par l'utilisateur, le nombre d'applications qu'ils contiennent connaît une croissance régulière. Asymco, un cabinet d'analyse spécialisé dans la mobilité, a ainsi évalué une moyenne de 60 applications par périphérique iOS®.[9] Comme plus de la moitié des entreprises prennent en charge plus d'un type de périphériques,[10] l'exposition du réseau de l'entreprise aux applications potentiellement malveillantes ou non conformes est énorme. D'après un article du Wall Street Journal intitulé « Vos applications vous regardent », sur 101 applications mobiles étudiées, 56 transmettaient l'identifiant du périphérique, 47 transmettaient des données de localisation géographique et 5 transmettaient des informations personnelles du périphérique vers un serveur tiers.[11] Même si cette étude portait essentiellement sur des applications grand public, elle n'en révèle pas moins la vulnérabilité des périphériques et des réseaux d'entreprise vis-à-vis des applications installées. Même lorsqu'elles ne sont pas considérées comme malveillantes, les applications peuvent accéder aux données sensibles (puis les recueillir et les transmettre) malgré les stratégies mises en place par l'entreprise et en contournant les mécanismes traditionnels de sécurité.

2. La généralisation de l'accès mobile

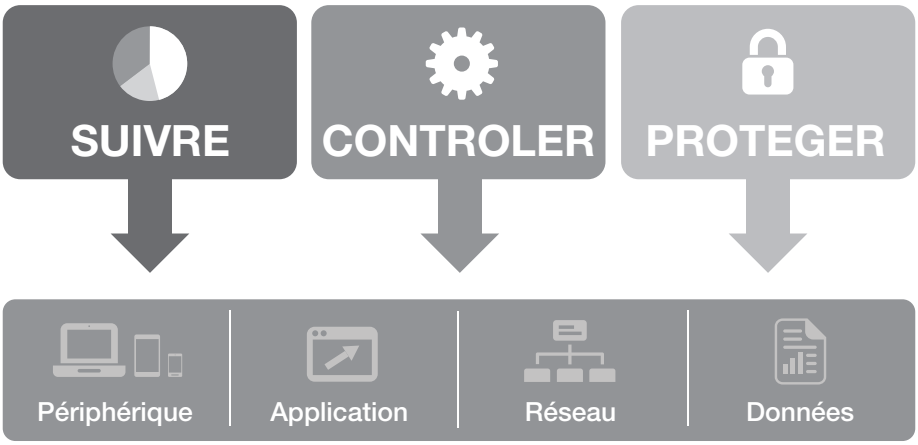
Il existe une forte volonté à tous les niveaux de l'entreprise pour doter la main-d'œuvre de périphériques mobiles et d'un accès mobile aux données et applications professionnelles. La mobilité gagne également sur un plan horizontal, les entreprises la généralisant à l'ensemble de leurs métiers et secteurs d'activité. D'après une enquête Citrix®, plus des trois-quarts des entreprises déploieront des applications mobiles sectorielles en 2013, et plus de la moitié d'entre elles seront stratégiques. De plus, 80% des entreprises développent des applications personnalisées.[12] On trouve ainsi, par exemple, des chaînes de restaurants dotant leur personnel de salle et de cuisine de tablettes iPad, ou bien encore des compagnies aériennes qui remettent à leurs équipages navigants des manuels techniques électroniques, des plans de vol ou des documents de conformité sur des Samsung Galaxy Tabs. Une telle généralisation de l'accès mobile est certes porteuse de promesses, mais elle signifie également que l'accès mobile aux réseaux et aux données de l'entreprise sera offert à un nombre sans cesse plus important d'utilisateurs, via un nombre toujours plus important de périphériques, ce qui multipliera inévitablement les risques.

3. La prolifération des outils de partage de fichiers grand public

Les solutions de sécurisation de la mobilité d'entreprise dont on entend le plus souvent parler se focalisent en général sur le verrouillage ou la suppression à distance des périphériques volés ou égarés. Pourtant, la menace la plus sérieuse vient d'ailleurs : de l'absence totale de contrôle sur le partage de données. Avec plusieurs millions d'utilisateurs partageant chaque jour leurs données sur une infinité de points de connexion connectés via le cloud, le risque de perte de données est largement supérieur à celui représenté par les pertes ou vols potentiels de périphériques. Les outils de partage de fichiers grand public posent un problème particulièrement sérieux du fait de leur effet multiplicateur : les données sauvegardées à l'extérieur du réseau de l'entreprise ne sont pas partagées avec un seul périphérique, mais avec tous les périphériques connectés de façon virale via l'outil de partage. D'après l'étude « Citrix Mobile Device Management Cloud Report », certaines des applications les plus souvent déployées, comme Dropbox ou Evernote, sont également celles le plus souvent placées en liste noire par les entreprises, ce qui souligne à la fois leur utilité et leur dangerosité.[13]

Une architecture de sécurité mobile de bout en bout

Les professionnels de la sécurité informatique se tournent majoritairement pour répondre à ces craintes vers les solutions de gestion des périphériques mobiles (ou solutions MDM) ou de gestion de la mobilité d'entreprise (ou solutions EMM). Cependant, la grande variété des menaces mobiles énumérée précédemment exige la mise en place d'une nouvelle infrastructure de sécurité plus complète, capable d'aller bien au-delà des simples fonctionnalités de verrouillage et suppression des données des solutions MDM. Les entreprises ont désormais besoin d'une solution qui leur offre des outils capables de suivre, contrôler et protéger de façon proactive leur infrastructure de bout en bout (périphériques, applications, données et réseau).



Les 10 « incontournables » en matière de mobilité d'entreprise sécurisée

Le tableau ci-dessous énumère les 10 questions que les entreprises se doivent de poser à leur fournisseur de solution de mobilité d'entreprise.

	Question	Justification
1	Puis-je gérer n'importe quel périphérique d'entreprise ou BYO ?	De nombreuses entreprises ont besoin de fonctionnalités de base pour la gestion de leurs périphériques. Elles doivent configurer de façon centralisée des éléments de sécurité comme les mots de passe ou le chiffrement, et doivent détecter et bloquer les périphériques non conformes (par exemple les périphériques débridés ou hébergeant des applications placées en liste noire). Elles doivent pouvoir supprimer à distance les périphériques volés, égarés ou appartenant à des employés quittant l'entreprise. Un nombre croissant d'entreprises comptant à la fois des périphériques d'entreprise et BYO dans leur environnement, la solution doit permettre aux directions informatiques de désigner facilement le propriétaire et d'appliquer en conséquence les stratégies appropriées.
2	Puis-je sécuriser et gérer toute application Web ou mobile ?	Les applications sont très diverses et ne partagent souvent pas une architecture de sécurité commune. Les directions informatiques doivent pouvoir sécuriser de façon centralisée toute application Web, mobile ou intranet en leur appliquant des stratégies d'accès, des mécanismes de sécurisation des connexions et de contrôle des données si possible dès leur processus de développement.
3	Puis-je offrir à mes utilisateurs des alternatives sécurisées à leurs meilleures applications de productivité sans sacrifier leur expérience ?	Que faire des meilleures applications de productivité adoptées par les utilisateurs mobiles pour leur travail (messagerie, Web, accès aux données) ? L'habitude des utilisateurs consiste à utiliser par défaut l'application native ou celle à laquelle ils sont habitués. Mais qu'en serait-il si les entreprises pouvaient leur fournir une alternative isolée et efficace aux clients de messagerie natifs, navigateurs et outils de partage de fichiers qu'ils affectionnent ?
4	Puis-je offrir une mobilité sécurisée et préserver la vie privée de mes utilisateurs ?	Si beaucoup d'entreprises choisissent de résoudre leurs problèmes de mobilité via une solution complète de gestion de la mobilité d'entreprise, celles sujettes à de strictes obligations en matière de respect de la vie privée optent souvent pour une approche plus légère. Qui peut se traduire par le déploiement limité d'un client de messagerie ou d'une application sécurisée sur le périphérique. La solution doit être suffisamment flexible pour permettre l'un ou l'autre scénario, voire un mélange des deux, par exemple pour une entreprise multinationale souhaitant gérer ses périphériques pour ses employés américains mais uniquement fournir un client de messagerie isolé à son personnel allemand.
5	Puis-je offrir le SSO à mes utilisateurs et délivrer toute application sur tout périphérique ?	Le single sign-on (SSO) est une des rares fonctionnalités de sécurité qui fournit quelque chose à chacun. Les directions informatiques peuvent créer et supprimer les applications plus facilement et s'assurer de la désactivation immédiate de l'accès mobile des employés quittant l'entreprise. Les utilisateurs bénéficient d'un accès simple sans avoir à s'authentifier sur un petit écran. Il s'agit là d'un incontournable pour toute entreprise mobile. Si l'entreprise devient réellement mobile, il y a des chances pour que sa direction informatique ait à provisionner non seulement des applications mobiles, mais aussi des applications Web, SaaS, Windows, et de datacenter. Elle devra alors les rendre disponible à partir d'un point unique : une librairie applicative unifiée.
6	Puis-je fournir un accès réseau basé sur des scénarios ?	Du fait du large éventail de périphériques mobiles accédant au réseau, les directions informatiques doivent définir des stratégies complètes d'accès et de contrôle s'appuyant sur l'analyse des points de connexion et sur la fonction de l'utilisateur pour déterminer quelles applications et données délivrer et quel niveau d'accès aux contenus accorder.

7	Puis-je laisser mes utilisateurs accéder à leur contenu tout en protégeant mes données ?	Les utilisateurs mobiles doivent pouvoir accéder au contenu d'entreprise, mais bien peu d'outils permettent aux directions informatiques de gérer cet accès et ce contrôle de données. Que le contenu réside dans Microsoft® SharePoint® ou au sein d'une application de partage et de synchronisation des données, les directions informatiques devront être capables de définir et d'appliquer des stratégies de données qui préciseront quels utilisateurs peuvent accéder à quels contenus et ce qu'ils peuvent en faire (sauvegarde, transmission par email, copier/coller, etc.).
8	Puis-je être flexible tout en garantissant une sécurité adaptée à la situation ?	De même qu'il est important d'assurer un équilibre entre sécurité et respect de la vie privée, il est primordial d'appliquer la bonne sécurité à chaque situation. Les directions informatiques ont besoin de solutions flexibles capables de fournir une approche de type "bon-mieux-meilleur" en matière de sécurité et d'assurer le juste équilibre entre sécurité et convivialité.
9	Puis-je intégrer mes solutions mobiles aux autres ressources informatiques existantes ?	Les directions informatiques comprennent parfaitement les risques engendrés par les silos technologiques. Les solutions de mobilité d'entreprise doivent donc pouvoir s'intégrer facilement à l'environnement informatique existant. Ce qui implique une intégration directe aux annuaires d'entreprise, aux infrastructures publiques essentielles, aux messageries d'entreprise, aux technologies d'accès telles que le WiFi ou le VPN, et aux applications et postes virtuels. Ce qui implique également l'intégration aux solutions SIEM de gestion des événements et des informations de sécurité et aux systèmes de gestion des journaux, afin que les directions informatiques puissent bénéficier de comptes-rendus pour leur infrastructure mobile comme pour le reste de leur infrastructure.
10	Votre architecture est-elle sécurisée, évolutive et hautement disponible?	Les solutions de gestion de la mobilité d'entreprise doivent être réellement adaptées à l'entreprise. Ce qui signifie que leur architecture aura été spécialement conçue pour conserver les données sensibles à l'abri derrière le pare-feu, et non les laisser exposées sur Internet. Ce qui signifie aussi que les entreprises pourront faire évoluer leur environnement sans en augmenter la complexité. Ce qui signifie enfin que les configurations haute disponibilité conformes aux standards du marché pourront assurer le basculement vers des systèmes de secours en cas de défaillance de la technologie.

Une sécurité mobile de bout en bout

Les structures souhaitant bénéficier d'une réelle mobilité d'entreprise doivent penser au delà de la simple MDM et envisager une sécurité mobile de bout en bout, capable de protéger les périphériques, les applications, le réseau et les données.

La sécurité des périphériques mobiles : problèmes et exigences

Gestion centralisée de la sécurité des périphériques

Je dois configurer des périphériques et appliquer des stratégies. Bon nombre d'entreprises doivent configurer des composants de sécurisation des périphériques (mots de passe, chiffrement) et appliquer des stratégies de façon centralisée. Le travail mobile se généralisant, le nombre toujours plus important de périphériques et d'utilisateurs accédant au réseau via plusieurs périphériques crée un besoin urgent de gestion centralisée des périphériques et stratégies de sécurité basées sur la fonction. Lorsque les périphériques sont volés ou égarés ou qu'un utilisateur quitte l'entreprise, le maintien de la sécurité et de la conformité passe par le verrouillage ou le nettoyage à distance des données d'entreprise résidant sur les périphériques concernés.

Diversité des périphériques mobiles

Au secours ! Il n'existe pas deux périphériques identiques ! Les employés exigent le choix dans ce domaine, et pour de nombreuses entreprises donner suite à cette demande constitue une stratégie intéressante. Elle permet d'attirer et de fidéliser les meilleurs talents et d'économiser sur l'achat des périphériques. Mais contrairement aux PC classiques verrouillés ou aux terminaux de poche BlackBerry® étroitement contrôlés, les périphériques mobiles utilisés aujourd'hui en entreprise sont très divers, présentent tous des degrés de vulnérabilité différents et ne présentent aucune architecture commune (pas même en matière de sécurité de base) qui permette aux directions informatiques de les gérer de façon cohérente. Selon Aberdeen Research, l'entreprise moyenne prend en charge 3,3 plates-formes mobiles,14 parmi lesquelles en général iOS, Android®, Windows® ou BlackBerry. Cette diversité pose des problèmes de sécurité uniques aux directions informatiques : comment, par exemple, surveiller, provisionner, prendre en charge et sécuriser de multiples applications sur différentes plates-formes, ou bien comment s'assurer que les employés ont bien appliqué les mises à jour et les correctifs de systèmes d'exploitation adaptés.

Périphériques BYO ou périphériques d'entreprise ?

Je mets en œuvre un programme BYO et je déploie aujourd'hui un projet d'iPads d'entreprise. Les entreprises gèrent de plus en plus de périphériques BYO à côté de leurs périphériques d'entreprise. Elles doivent donc désigner les propriétaires de ces périphériques d'une façon à la fois précise et conforme, gérer chaque type de périphérique en fonction de ses stratégies et processus propres, et en assurer le suivi dans la durée.

Sécurité des périphériques mobiles : les exigences

Le tableau ci-dessous énumère les différentes exigences essentielles en matière de sécurisation des périphériques mobiles.

Suivi	Contrôle	Protection
• Audit et compte-rendu par type de propriétaire (BYO ou entreprise) • Compte-rendu détaillé (type de périphérique, système d'exploitation, version, intégrité, etc.) • Inventaire des applications installées • Vérification du type d'utilisation du périphérique (itinérance, par exemple) • Visualisation de la localisation du périphérique (et action appropriée si l'utilisateur l'a déplacé en dehors des limites autorisées) • Vérification de l'état de conformité du périphérique (débridé, applications placées en liste noire, etc.)	• Déploiement de stratégies similaires pour les différentes plates-formes et les différents systèmes d'exploitation • Application des stratégies de sécurité et de conformité (mots de passe, etc.) à chaque périphérique • Audit régulier des périphériques pour s'assurer qu'aucune stratégie essentielle n'a été désactivée • Blocage de l'accès réseau pour tout périphérique non conforme • Définition de stratégies de sécurité visant à empêcher l'accès de l'employé aux applications et ressources du périphérique	• Activation du libre-service utilisateur pour les périphériques volés ou égarés • Localisation, verrouillage et nettoyage à distance des périphériques perdus ou volés • Nettoyage total ou sélectif du périphérique au départ d'un employé

La sécurité des applications mobiles : problèmes et exigences

Toute application sur tout périphérique

Je dois assurer le suivi et la gestion de toutes les applications que mes utilisateurs souhaitent mobiles. Les utilisateurs ont toujours des applications de prédilection qu'ils souhaitent utiliser pour leur travail. Les différentes unités de l'entreprise développent des applications métier spécifiques pour leurs employés. Mais les directions informatiques doivent les gérer toutes : elles doivent assurer un provisioning centralisé des applications mobiles, Web, SaaS, Windows et de datacenter et faire en sorte que les utilisateurs puissent y accéder à partir d'un point unique.

Une sécurité applicative cohérente et centralisée

Comment puis-je maintenir une sécurité cohérente dans cette diversité ? Devant les milliers d'applications mobiles à prendre en charge, les directions informatiques éprouvent le plus grand mal à sécuriser leurs applications et leurs intranets d'une façon centralisée et cohérente. Elles doivent composer avec un large éventail d'applications tierces et personnalisées, chacune dotée de sa propre architecture de développement, de ses propres fonctionnalités de sécurité, de sa propre méthodologie d'authentification et d'accès aux données. Et pourtant les directions informatiques doivent absolument appliquer un éventail commun de stratégies à chacune de ces applications !

Sécurité des applications de productivité favorites des utilisateurs

Ce que mes utilisateurs veulent en réalité, c'est leur messagerie, leurs applications Web et leurs documents. La majorité des utilisateurs s'appuie sur quelques applications mobiles « incontournables ». Il s'agit en général d'applications leur permettant d'accéder à leur messagerie, au Web et à leurs données. Les directions informatiques doivent impérativement s'assurer que ces applications sont sécurisées, or, à ce jour, elles ne le sont pas ! Et ces mêmes directions informatiques ne peuvent plus accepter les risques de pertes de données associés à l'accès non sécurisé via messagerie aux intranets d'entreprise ou aux utilisateurs téléchargeant des données sensibles via un outil de partage de fichiers grand public.

De leur côté, les utilisateurs ont pris l'habitude d'une expérience native fantastique et ne peuvent plus accepter de faire un retour en arrière dans ce domaine. Ce qu'il faut désormais, c'est un éventail d'alternatives sécurisées et efficaces à ces applications grand public à succès.

La protection de la vie privée

Il ne s'agit pas uniquement de préserver la sécurité de l'entreprise, mais également de protéger la vie privée de mes utilisateurs. Les solutions complètes de gestion de la mobilité d'entreprise intègrent des fonctionnalités stratégiques comme la géolocalisation des périphériques ou la visualisation des applications installées sur ces périphériques. Mais même si ces fonctionnalités peuvent être désactivées dans de nombreuses solutions, certaines entreprises ne veulent même pas entendre parler de leur existence. Ainsi, par exemple, les entreprises soumises à de fortes contraintes en matière de respect de la vie privée, cherchent souvent un moyen de fournir un accès mobile d'entreprise à leurs utilisateurs sans avoir à gérer l'ensemble de leur périphérique. Par exemple, une entreprise peut souhaiter n'avoir à provisionner qu'un client de messagerie isolé pour ses utilisateurs, afin qu'ils puissent accéder à la messagerie d'entreprise sans que celle-ci n'ait à gérer l'ensemble du périphérique.

Identités fédérées et SSO

Un accès simple pour moi… et pour mes utilisateurs ! Les entreprises mettant en œuvre des initiatives de travail mobile délivrent une multitude d'applications à leurs utilisateurs. Etant donné l'énorme diversité des applications et des types d'applications, il est difficile pour les directions informatiques de parvenir à créer un accès basé sur la fonction de l'utilisateur. Plus grave, il est encore plus difficile pour elles d'assurer le suivi de toutes les applications qu'elles doivent supprimer impérativement lorsqu'un utilisateur quitte l'entreprise. C'est notamment le cas des applications SaaS, qui sont souvent oubliées parce-que les authentifiants de l'utilisateur sont gérés séparément et que ces applications sont moins visibles des directions informatiques.

Du côté de l'utilisateur, l'obligation de se connecter individuellement à chacune de ces applications est fort peu pratique. Avec deux applications, il n'y a pas trop de problèmes. Avec cinq, ça devient pénible. Avec dix ou plus, vous finissez par provoquer une émeute chez vos utilisateurs.

Sécurité des applications mobiles : les exigences

Le tableau ci-dessous énumère les différentes exigences essentielles en matière de sécurisation des applications mobiles.

Suivi	Contrôle	Protection
• Inventaire des applications mobiles installées sur le périphérique) • Suppression totale (et compte-rendu correspondant pour la conformité) des privilèges d'accès de l'utilisateur quittant l'entreprise	• Mise à disposition de toute application (mobile, Web, SaaS, Windows ou de datacenter) sur tout périphérique via une librairie applicative unifiée • Sécurisation centralisée des applications tierces et personnalisées et application de stratégies granulaires durant ou après le développement • Fourniture d'alternatives efficaces mais isolées aux applications de productivité favorites des utilisateurs • Accès des utilisateurs en SSO pour tous les types d'applications	• Connectivité sécurisée des applications et des intranets sans recours au VPN • Protection des données d'entreprise sensibles avec contrôle intégré cohérent des données applicatives • Mécanisme empêchant les utilisateurs d'accéder aux données et aux applications après leur départ de l'entreprise • Protection de la vie privée grâce à l'accès aux applications, intranets et messageries d'entreprise sans avoir à gérer l'intégralité du périphérique

La sécurité des réseaux mobiles : problèmes et exigences

Incapacité à contrôler l'accès

Certains de mes employés utilisent des périphériques conformes, d'autres des périphériques débridés, et d'autres encore utilisent des périphériques inconnus dans des cybercafés. En matière d'accès, il y a autant de besoins que d'utilisateurs ! Du fait du large éventail de périphériques mobiles accédant au réseau, les directions informatiques cherchent un moyen leur permettant de définir des stratégies complètes d'accès et de contrôle s'appuyant sur l'analyse des points de connexion et sur la fonction de l'utilisateur pour déterminer quelles applications et données délivrer et quel niveau d'accès aux contenus accorder.

Incapacité à répondre aux demandes sur le réseau mobile

Je ne suis pas certain que mon réseau mobile puisse traiter toutes les demandes, notamment durant les périodes de pic d'utilisation. Bien que n'étant pas directement liée à la sécurité, une considération essentielle touchant au réseau mobile doit être prise en compte : son évolutivité. De plus en plus d'utilisateurs d'entreprise accédant au réseau via un nombre croissant de périphériques et les entreprises déployant un nombre croissant d'applications mobiles stratégiques, les directions informatiques doivent faire évoluer leur réseau afin qu'il s'adapte au volume toujours plus important de trafic mobile et demeure capable de délivrer les applications mobiles avec de hautes performances.

Sécurité des réseaux mobiles : les exigences

Le tableau ci-dessous énumère les différentes exigences essentielles en matière de sécurisation des réseaux mobiles.

Suivi	Contrôle	Protection
• Analyse des points de connexion mobiles pour vérification de la conformité	• Contrôle de l'accès réseau basé sur la configuration du périphérique, son état, la fonction de l'utilisateur et d'autres facteurs comme le réseau utilisé • Capacité à répondre aux demandes notamment via la répartition de charge pour les requêtes mobiles et capacité à garantir une mise à disposition d'applications mobiles hautement performante	• Protection du réseau de l'entreprise contre les menaces mobiles (malwares, etc.)

La sécurité des données mobiles : problèmes et exigences

Le cas Dropbox

J'ai un problème avec Dropbox. Les outils grand public de partage de fichiers sont devenus particulièrement populaires en entreprise parce qu'ils sont très simples à utiliser et résolvent un vrai problème : ils permettent d'accéder aux données les plus récentes à partir de n'importe quel périphérique. Mais si elles sont utiles, ces applications font courir également un énorme risque de perte de données. Les entreprises ne peuvent suivre et protéger les données dans ces applications, et si elles les placent en liste noire, elles ne résolvent pas pour autant le problème d'accès de leurs utilisateurs. Les entreprises ont donc besoin d'une alternative sécurisée à ces outils, capable de résoudre les problèmes des utilisateurs tout en permettant aux directions informatiques de chiffrer les données et de contrôler l'accès et l'utilisation via des stratégies granulaires

Conteneurs créant des silos de données

Mes utilisateurs ont du mal à accéder à leurs contenus avec les applications isolées. Les conteneurs de données ou d'applications (réponse actuelle de l'entreprise face au risque de perte de données) posent de gros problèmes en termes de convivialité. Très souvent, les utilisateurs ne parviennent pas à accéder à leurs documents dans l'application de leur choix et ne peuvent partager leur contenu entre différentes applications. Ce qui rend la revue et l'édition de contenu ou la collaboration très peu pratique, voire impossible.

Suivi	Contrôle	Protection
• Suivi de l'accès mobile aux données (et alerte)	• Fourniture de « données mobiles à emporter » • Possibilité pour les utilisateurs mobiles de synchroniser et partager en toute sécurité leurs données à partir de périphériques mobiles • Définition de stratégies granulaires de contrôle des données • Contrôle du partage des données entre différentes applications	• Protection des données mobiles grâce à leur chiffrement au repos et en transit • Prévention des pertes de données grâce à un conteneur de données chiffré et sécurisé • Protection des données via le nettoyage du conteneur au départ d'un utilisateur ou lorsqu'un périphérique est égaré, ou suite à d'autres événements (périphérique débridé, etc.)

Autres considérations et exigences associées à la sécurité

Une sécurité adaptée à chaque situation

J'ai des employés à temps plein et des sous-traitants. Ils n'ont pas tous besoin du même niveau de sécurité. Comme dans le cas de la protection de la vie privée, les directions informatiques doivent donc pouvoir appliquer les mesures de sécurité appropriées à chaque situation. Les entreprises comptent des utilisateurs très divers. Certains sont des employés de bureau utilisant un périphérique d'entreprise à des fins personnelles et professionnelles. D'autres travaillent par quarts et partagent donc leur périphérique avec d'autres employés. D'autres encore sont des sous-traitants travaillant sur leurs propres périphériques. Il n'existe donc pas de sécurité mobile universelle convenant à tous ces besoins. Dans les exemples cités ci-dessus, les directions informatiques peuvent avoir besoin de flexibilité, en fournissant un accès et une sécurité mobiles d'entreprise très complets aux employés de bureau, tout en gérant l'intégralité des périphériques partagés des travailleurs par quarts en n'y installant qu'une ou deux applications spécifiques et surtout pas de messagerie, et en se contentant de fournir uniquement un client de messagerie aux sous-traitants.

Ces directions informatiques doivent également pouvoir adopter en matière de sécurité une approche de type « bon-mieux-meilleur » basée sur le profil de risque de l'entreprise. Pour reprendre l'exemple de la messagerie, une entreprise évoluant dans un secteur fortement réglementé pourra choisir un client de messagerie totalement isolé et doté de contrôles très stricts. Une entreprise évoluant dans un secteur un peu moins réglementé mais accordant tout de même une grande importance à la sécurité pourra opter pour une expérience de messagerie native, tout en chiffrant les pièces jointes. Une entreprise évoluant dans un secteur très libre pourra elle déployer une messagerie native et se contentera de nettoyer cette messagerie d'entreprise en cas de perte ou de vol du périphérique ou de départ de l'employé.

Une intégration d'entreprise

Pitié, ne me donnez pas encore un silo à gérer ! Les directions informatiques comprennent parfaitement les risques engendrés par les silos technologiques. Les solutions de mobilité d'entreprise qui ne sont pas directement intégrées au reste de l'informatique posent de sérieux problèmes de gestion et de sécurité. Ainsi, par exemple, les solutions de mobilité ne s'intégrant pas directement à LDAP et mettent en cache de façon périodique les données des utilisateurs font courir le risque qu'un employé ayant quitté l'entreprise n'accède aux applications et aux données à partir de son périphérique mobile durant l'intervalle de temps entre son départ et le moment où la solution synchronisera les données d'annuaire. De même, les solutions de mobilité ne s'intégrant pas aux solutions SIEM et aux outils de gestion des journaux ne permettent pas aux directions informatiques de bénéficier d'une image complète de leur sécurité et de leur conformité.

Une architecture d'entreprise

A quoi servent les fonctionnalités de sécurité si les données personnelles de mon directeur général sont exposées sur Internet ? De trop nombreuses solutions de mobilité d'entreprise ont été conçues sans penser dès le départ à la sécurité. Au lieu de conserver les données sensibles à l'abri du pare-feu et de ménager leur accès via un proxy placé dans la DMZ, elles placent temporairement en cache les données de l'utilisateur dans la DMZ, où elles sont exposées à Internet.

En outre, de nombreuses solutions ne sont pas capables d'évoluer suffisamment pour répondre aux demandes d'une population mobile en constante augmentation. Certaines solutions obligent les directions informatiques à gérer de multiples instances de la même solution dans différents silos distincts. De même, la haute disponibilité est une fonctionnalité nécessaire exigée par les professionnels de l'informatique, bien que peu de solutions ne la proposent vraiment. Certaines solutions ne disposent pas d'une redondance intégrée avec fonctionnalité de clustering haut de gamme et de basculement direct vers des systèmes de secours. Le travail mobile se généralisant et les applications devenant chaque jour plus stratégiques, le choix de la bonne solution mobile s'avère crucial pour l'entreprise.

Autres exigences

Le tableau ci-dessous énumère les autres exigences à prendre en compte en matière de sécurisation des solutions de mobilité d'entreprise.

Suivi	Contrôle	Protection
• Intégration des données mobiles aux outils SIEM et de gestion des journaux pour une meilleure visibilité sur la sécurité et la conformité	• Niveau de sécurité adapté à chaque situation (messagerie pour utilisateurs des secteurs fortement réglementés, applications sécurisées sans gestion du périphérique pour les sous-traitants, etc.) • Contrôle d'accès permanent avec intégration directe aux annuaires d'entreprise • Contrôle d'accès et SSO avec intégration PKI • Accès aux messageries avec intégration aux messageries d'entreprise • Contrôle d'accès d'entreprise avec intégration directe aux solutions WiFi et VPN	• Protection de la vie privée grâce au maintien des données utilisateur derrière le pare-feu • Protection contre les défaillances grâce à une haute disponibilité haut de gamme • Mobilité d'entreprise pérenne grâce au déploiement d'une solution évolutive capable de s'adapter à l'augmentation du nombre de périphériques mobiles sans accroître la complexité

Conclusion

Si la mobilité d'entreprise génère des opportunités à la fois pour l'entreprise et pour les utilisateurs, elle implique également des risques significatifs. Les entreprises ont tout intérêt à s'inspirer de ce livre blanc pour définir leur architecture de sécurité mobile et établir une check-list d'évaluation des différents fournisseurs de solutions de mobilité d'entreprise.

A propos de Citrix XenMobile

Citrix XenMobile est une solution de gestion de la mobilité d'entreprise qui garantit une liberté complète et sécurisée aux périphériques, applications et données mobiles. D'un simple clic, les employés bénéficient d'un accès rapide à toutes leurs applications mobiles, Web, Windows ou de datacenter, via une librairie applicative unifiée leur proposant notamment des applications de productivité efficaces et conviviales, s'intégrant de façon transparente et garantissant une expérience de grande qualité. La solution permet un provisioning et un contrôle basés sur l'identité pour tous les périphériques, toutes les données et toutes les applications, ainsi qu'un contrôle basé sur des stratégies (restriction d'accès aux applications pour les utilisateurs autorisés, suppression automatique de compte pour employés quittant l'entreprise, suppression sélective des applications et données stockées sur les périphériques volés, égarés ou non conformes). Grâce à XenMobile, les directions informatiques peuvent laisser leurs utilisateurs choisir leur périphérique tout en prévenant toute perte de données et en protégeant efficacement leur réseau interne contre les menaces mobiles.

1. "Mobility in ERP 2011" (La mobilité dans les solutions ERP en 2011), Kevin Prouty, Aberdeen, mai 2011

2. "Global State of Information Security Survey" (Enquête sur l'état général de la sécurité des informations), CSO Magazine, 2012

3. "MDM is No Longer Enough" (La MDM ne suffit plus), Citrix webinar with enterprise security expert, Jack Gold, octobre 2011

4. "U.S. Cost of a Data Breach" (Le coût des violations de données aux Etats-Unis), Ponemon Institute, mars 2011

5. State of Mobility Survey (Enquête sur l'état de la mobilité), Symantec, Février 2012

6. In 2010 the average cost of a data breach was $7.2 million (En 2010, le coût moyen d'une violation de données s'élevait à 7,2 millions de $). Doug Drinkwater, 10 février 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"(Perspectives mondiales du marché de la technologie en 2012 et 2013), Andrew Bartels, Forrester, 06 janvier 2012

9. "More Than 60 Apps Have Been Downloaded for Every iOS Device" (Plus de 60 applications ont été téléchargées en moyenne sur chaque périphérique iOS), Asymco, 16 janvier 2011

10. "Market Overview: On-Premises Mobile Device Management Solutions" (Présentation du marché : les solutions de gestion des périphériques mobiles sur site), Forrester, 03 janvier 2012

11. "Your Apps are Watching You" (Vos applications vous regardent), The Wall Street Journal, section, 17 décembre 2010

12. 'Mobile Gets a Promotion' (La mobilité a été promue !) infographic, Citrix, octobre 2012

13. Citrix Mobile Device Management Cloud Report (Etude Citrix sur la gestion des périphériques mobiles), 3ème trimestre 2012

14. "The Need for Mobility Management" (Le besoin en gestion mobile), Aberdeen blog, février 2010

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

À propos de Citrix
Citrix (NASDAQ :CTXS) est l'entreprise cloud qui favorise le travail mobile en permettant aux individus de travailler et de collaborer facilement et en toute sécurité depuis n'importe où. Grâce à ses solutions inégalées de mobilité, de virtualisation de postes, de mise en réseau cloud, de plates-formes cloud, de collaboration et de partage des données, Citrix aide les entreprises à bénéficier de la rapidité et de la réactivité nécessaires au succès dans un monde mobile et dynamique. Les produits Citrix sont utilisés dans le monde entier par plus de 260 000 entreprises et plus de 100 millions d'utilisateurs. Le chiffre d'affaires annuel de l'entreprise a atteint 2,59 milliards de dollars en 2012. Pour en savoir plus : www.citrix.com.

0513/PDF

www.citrix.fr