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

Guide technique mis à jour pour Android 4.4, iOS 7.1, Windows Phone et Surface 8.1.

CITRIX®

citrix.fr/byod **@CitrixBYOD** **citrix.fr/secure** **@CitrixSecurity**

Les périphériques mobiles Android, iOS et Windows (notamment les smartphones, les tablettes et tout ce qui se situe entre les deux) ont radicalement bouleversé l'informatique d'entreprise en offrant aux utilisateurs et aux directions informatiques de nouveaux degrés de mobilité et de flexibilité. Dans le même temps, ils rendent bien plus complexe le maintien d'une sécurité efficace et d'une stricte confidentialité des données.

La mobilité d'entreprise exige une nouvelle approche de la sécurité, une approche pensée pour un monde au sein duquel les périphériques mobiles, les périphériques BYOD, les périphériques d'entreprise contenant des données personnelles, les applications cloud et les réseaux publics utilisés pour le stockage et la consultation des données d'entreprise ont rendu les périmètres verrouillés traditionnels totalement obsolètes.

Au lieu de chercher à protéger toutes les données de l'entreprise, y compris les données publiques non sensibles, les direction informatiques devraient se concentrer sur la protection de ce qui compte vraiment, c'est-à-dire les informations d'entreprise sensibles comme la propriété intellectuelle et les secrets commerciaux, les informations à caractère personnel fortement régulées, les données médicales protégées ou les informations relatives aux transactions financières par carte de paiement. Cette approche implique la mise en adéquation des mesures de sécurité avec la fonction des différents utilisateurs de l'entreprise et l'utilisation sélective d'un large éventail de méthodes d'accès sécurisé, de contrôle de l'utilisation, de prévention de l'exfiltration de données et de lutte contre la manipulation de périphérique, le tout sans interférer avec la disponibilité des données. La gestion de la mobilité d'entreprise joue un rôle central dans cette stratégie, grâce à des fonctionnalités centrées sur les périphériques, les systèmes d'exploitation, les réseaux, les applications, les données et les stratégies. Mais il est également indispensable de bien comprendre le rôle du système d'exploitation mobile lui-même.

A chacune des trois principales plateformes de système d'exploitation mobile (iOS, Android et Windows) sont associés des fonctionnalités et des problèmes de sécurité distincts. Tandis qu'Android offre des fonctionnalités et des avantages destinés tout aussi bien aux entreprises qu'au grand public, sa fragmentation en différentes versions et le manque en fonctionnalités de mise à jour sur les périphériques contrôlés par des opérateurs posent de sérieux problèmes de sécurité. Le système d'exploitation propriétaire iOS d'Apple permet un contrôle étroit depuis le matériel jusqu'aux applications et permet une approche de type jardin clos qui limite les vulnérabilités mais restreint également les options de sécurité traditionnelles accessibles à l'entreprise. Les périphériques basés sur Microsoft Windows 8 comme Windows Phone ou Surface intègrent des fonctionnalités de sécurité avancées et bénéficient de la familiarité des directions informatiques avec les anciennes technologies de sécurité Windows. Cependant, leurs fonctionnalités de sécurité et de gestion diffèrent significativement selon les variantes de système d'exploitation.

Leader sur le marché des solutions d'espace de travail mobile, Citrix a développé des technologies et des meilleures pratiques spécialement conçues pour libérer la pleine potentialité des tout derniers périphériques mobiles au profit de l'informatique personnelle et d'entreprise. Dans ce livre blanc, nous examinons en détail les principales plateformes de système d'exploitation mobile, les fonctionnalités et problèmes de sécurité spécifiques qui leurs sont liés et les mesures que les directions informatiques doivent prendre pour préserver leur contrôle tout en encourageant la productivité et la mobilité. Nous examinons également les fonctionnalités de sécurité fournies par les solutions de mobilité d'entreprise Citrix, notamment Citrix XenMobile, Citrix ShareFile, Citrix XenDesktop, Citrix XenApp et Citrix NetScaler.

Associées, ces solutions garantissent à l'entreprise un contrôle depuis le datacenter sur l'ensemble des données, sur tout périphérique, et répondent aux inquiétudes des directions informatiques en matière de sécurité, peu importe que les stratégies adoptées autorisent ou non la mobilisation des données d'entreprise sur le périphérique.

En quoi la sécurité des périphériques mobiles diffère-t-elle de celle des anciens PC ?

La sécurité mobile ne consiste pas simplement à appliquer à des plateformes mobiles les mesures de sécurisation des PC existantes et familières. Ainsi, par exemple, les antivirus, les pare-feu personnels et le chiffrement complet du disque sont possibles sur Android, Windows Phone et Surface, mais leur utilisation aurait pour conséquence de refuser l'accès des périphériques iOS au réseau, iOS ne prenant pas en charge à ce jour ces anciens mécanismes de contrôle. Toutefois, la vérification d'applications effectuée par Apple rend quasiment inutile, au moins pour l'instant l'utilisation d'applications de sécurité sur le périphérique lui-même. Un architecte chargé d'autoriser de façon sécurisée l'accès des périphériques iOS en entreprise devra donc plutôt aborder le problème sous l'angle de la protection des données.

L'architecture de sécurité d'Android est très similaire à celle d'un PC Linux. S'appuyant sur Linux, Android bénéficie de tous les avantages et souffre de quelques-uns des inconvénients de des distributions Linux (ou distro), ainsi que de problèmes inhérents à tout système d'exploitation mobile. Cependant, les périphériques iOS diffèrent significativement des PC, à la fois en termes d'utilisation et de sécurité. L'architecture iOS semble même disposer dans ce dernier domaine de réels avantages qui pourraient bien résoudre un certain nombre de problèmes de sécurité des PC. Comparez ci-dessous le modèle de sécurité et de réduction des risques des PC avec ceux propres à Android et à iOS, et vous comprendrez que les mécanismes de contrôle exigés par les PC ne sont pas nécessairement nécessaires au modèle iOS. De plus, Windows Phone et Surface améliorent de nombreuses façons le modèle de PC traditionnel.

Comparaison des mesures de sécurité associées aux anciens PC et aux tablettes et smartphones Android, iOS et Windows

Mesure de sécurité	PC	Android	iOS	Windows
Contrôle du périphérique	Optionnel	Optionnel	Optionnel	Optionnel
Antimalware local	Optionnel	Optionnel	Indirect	Natif
Chiffrement des données	Optionnel	Configuration	Natif	Configuration
Séparation/isolation des données	Optionnelle	Native	Native	Native
Environnement d'exploitation géré	Non	Non	Oui	Oui
Correction d'application	Gérée par l'utilisateur	Gérée par l'utilisateur	Native	Native
Accès pour modifier les fichiers système	Administrateur requis	Rooting requis	Débridage requis	Administrateur requis

L'architecture Android peut être configurée pour garantir une sécurité poussée, comme cela a été le cas pour une version d'Android adoptée pour être utilisée par le Ministère de la défense américain. En outre, la NSA prend en charge un modèle Android à sécurité renforcée (ou SE), ce qui permet d'intégrer un système d'exploitation Linux SE au noyau Android.

Présentation de l'architecture de sécurité Android

L'architecture Android fournit une plateforme permettant la personnalisation de la sécurité, depuis un niveau basique jusqu'à un niveau avancé. Les mesures de sécurité doivent être spécifiquement activées et appliquées, la plateforme Android fournissant les fonctionnalités suivantes :

Quelques fonctionnalités de sécurité aidant les développeurs à concevoir des applications sécurisées :

- Android Application Sandbox, qui isole les données et l'exécution du code application par application, renforcé par l'application de SELinux et l'intégrité de démarrage
- Architecture applicative Android avec mise en œuvre de fonctionnalités de sécurité courantes comme le chiffrement, les permissions et l'IPC sécurisé
- Système de fichiers chiffré pouvant être activé pour protéger les données sur les périphériques volés ou égarés

Il est toutefois important que les développeurs soient familiarisés avec les meilleures pratiques de sécurité Android, afin d'être certain qu'ils tireront profit de ces fonctionnalités et de limiter la probabilité de l'introduction involontaire d'autres problèmes de sécurité susceptibles d'affecter leurs applications.

Comment utiliser mon téléphone ou ma tablette Android de façon sécurisée ?

L'architecture de sécurité Android a été conçue pour que vous puissiez utiliser en toute sécurité votre téléphone ou votre tablette sans avoir à apporter une quelconque modification au périphérique ou à installer un quelconque logiciel spécial. Les applications Android s'exécutent au sein du bac à sable applicatif (Application Sandbox), qui limite l'accès aux informations et données sensibles sans autorisation préalable de l'utilisateur. Pour bénéficier pleinement de la protection Android, il est important que les utilisateurs ne téléchargent et n'installent que des logiciels provenant de sources connues et sécurisées, ne visitent que des sites Web sécurisés et évitent de recharger leurs périphériques sur des stations d'accueil non sécurisées.

Plateforme ouverte, l'architecture Android permet aux utilisateurs de visiter tout site Web et de charger tout logiciel proposé par tout éditeur sur leur périphérique. Comme pour un ordinateur personnel, l'utilisateur doit savoir qui fournit le logiciel qu'il télécharge et doit décider s'il accorde à l'application les fonctionnalités qu'elle demande. Cette décision peut s'appuyer sur la connaissance personnelle qu'a l'utilisateur de l'éditeur du logiciel et en déterminant d'où vient ce logiciel. La fonctionnalité d'analyse des rebonds et des applications tierces aide à détecter les applications contenant un malware.

Les problèmes de sécurité associés à Android

La plateforme ouverte Android est ouverte au rooting et au déverrouillage. Le rooting est le processus qui consiste à devenir la racine, le super-utilisateur avec tous les droits sur le système d'exploitation. Le déverrouillage donne droit à modifier le bootloader, ce qui autorise l'installation d'autres versions du système d'exploitation et des applications. Android dispose également d'un modèle de permission plus ouvert avec lequel tout fichier se trouvant sur un périphérique Android est soit lisible par une application donnée, soit lisible par tout le monde. Ceci implique que si un quelconque fichier doit être partagé entre différentes applications, la seule façon de l'autoriser est d'accorder la lecture par tout le monde.

Les mises à jour vers la dernière version d'Android ne sont pas toujours disponibles et sont parfois contrôlées par l'opérateur. Ce manque de mise à jour peut engendrer la persistance de problèmes de sécurité. Vérifiez régulièrement les menus successifs « Settings/More/About device/Software update » (Paramètres/Plus/A propos du périphérique/Mise à jour logicielle) afin d'établir si la plateforme peut être mise à jour.

La prise en charge de contenu actif (notamment Flash, Java, JavaScript et HTML5) permet le passage des malwares et des attaques par le biais de ces vecteurs. Assurez-vous que les solutions de sécurité peuvent détecter et contrer les attaques utilisant le contenu actif.

Le système d'exploitation Android est une cible de prédilection pour les malwares mobiles, notamment pour les chevaux de Troie par SMS, qui envoient du texte à des numéros surtaxés et à des applications malveillantes pour abonner les utilisateurs à leur insu, détourner des informations personnelles et même prendre sans autorisation le contrôle à distance du périphérique. C'est tout particulièrement vrai pour les applications provenant de librairies applicatives malveillantes dont la sécurité n'a pas été vérifiée et validée. Si KitKat ajoute bel et bien « des douzaines d'amélioration de sécurité au profit des utilisateurs, » il est tout de même plus prudent de renforcer les périphériques Android via une solution antimalware afin de garantir une posture de sécurité plus robuste.

Les dernières fonctionnalités Android et ce qu'elles impliquent pour les directions informatiques

Le tableau suivant résume les avantages pour l'utilisateur et les impacts sur la sécurité informatique des dernières fonctionnalités des tablettes et smartphones Android 4.4.

Les nouveautés dignes d'intérêt dans Android 4.4		
Android 4.4 (Kit Kat) étend les capacités de SELinux afin de protéger le système d'exploitation Android, en s'exécutant par défaut en mode Application des règles et en intégrant de nouvelles fonctionnalités destinées à contrôler la sécurité. La mise en œuvre de ces fonctionnalités peut varier d'un constructeur ou d'un périphérique à un autre. Les fonctionnalités notables suivantes et leur impact sont examinées dans ce livre blanc.		
Fonctionnalité Android	**Avantage pour l'utilisateur du périphérique**	**Impact informatique**
Traitement des certificats et améliorations apportées à KeyStore	L'établissement de listes blanches et le marquage de certificats permettent de s'assurer que seuls des certificats valides sont utilisés, les algorithmes à courbe elliptique rationalisent un chiffrement renforcé et les avertissements émis par les certificats CertificateAuthority (CA) facilitent l'interception des attaques de type « man-in-the-middle ».	Améliorations et automatisation bienvenues dans le sous-système de chiffrement Android. L'introduction d'une API à clé publique et d'autres fonctionnalités de gestion de KeyStore simplifiera et étendra les capacités des directions informatiques.
En permanence à l'écoute	Prononcer « OK Google» sans toucher à quoi que ce soit active le périphérique. Cette fonctionnalité n'est disponible pour l'instant que sur Nexus 5, mais son extension est d'ores et déjà prévue.	Les périphériques peuvent enregistrer au vol des conversations imprévues et peuvent dynamiquement activer ou désactiver des fonctionnalités en fonction de ce qui est dit.

Ajout automatique de contenu manquant	L'ajout automatique d'un contact manquant, de ressources proches, de cartes et d'adresses comble les lacunes détectées.	Les utilisateurs travaillant sur des sites sécurisés ou pour le compte de clients fortement sensibilisés à la sécurité ne doivent pas fournir d'informations géographiques détaillées et doivent donc désactiver cette fonctionnalité.
Intégration cloud	L'intégration du stockage local et cloud signifie que l'information peut être automatiquement stockée et synchronisée sur les différents périphériques, les différentes applications et dans le cloud.	L'utilisation de Google Drive et de services tiers de partage de fichiers personnels sera native pour les applications et activée via des API. Les directions informatiques doivent s'assurer qu'une solution d'entreprise est bien disponible et activée.
SMS, Google Hangouts pour SMS	Il est possible d'utiliser et de configurer ses SMS à des fins personnelles.	Si Google Hangouts est formidable pour une utilisation personnelle, il est nécessaire de configurer et d'appliquer un système de SMS uniquement dédié aux communications professionnelles.

En plus des fonctionnalités fournies dans le cadre du système d'exploitation Android, les fabricants de périphériques, les opérateurs et les partenaires enrichissent constamment Android de nouvelles fonctionnalités.

Samsung SAFE et KNOX

Samsung SAFE est un programme de sécurité développé par Samsung et destiné à fournir des périphériques d'entreprise offrant des contrôles de sécurité supérieurs à ce qui est proposé sur la plupart des périphériques Android courants. Samsung SAFE comprend des mécanismes de gestion des applications et des périphériques mobiles tels que le chiffrement AES-256 sur périphérique, la connectivité VPN et la prise en charge de Microsoft ActiveSync Exchange pour les applications natives PIM, d'agenda et de messagerie d'entreprise.

Samsung KNOX fournit un degré supplémentaire de protection prolongeant l'action de SAFE, en garantissant une sécurité complète pour les données d'entreprise et l'intégrité de la plateforme mobile. Les fonctionnalités de KNOX comprennent un conteneur à double compartiment pour isoler les espaces professionnel et personnel, un VPN par application, la mesure de l'intégrité du noyau et un démarrage sécurisé personnalisable garantissant que seuls les logiciels vérifiés et autorisés peuvent s'exécuter sur le périphérique.

Citrix adopte une approche intégrée en prenant en charge les API SAFE et KNOX. Citrix XenMobile s'appuie sur KNOX grâce à des mécanismes MDM et MAM renforcés, gérés eu sein du portail d'administration. Nous examinerons ces fonctionnalités de manière plus détaillée un peu plus loin dans ce livre blanc.

Présentation de l'architecture de sécurité iOS

Le système d'exploitation propriétaire iOS est soigneusement contrôlé. Les mises à jour s'effectuent à partir d'une source unique et les applications Apple de l'AppStore sont vérifiées, y compris à l'aide de tests de sécurité de base. L'architecture de sécurité iOS a intégré un cadre basé sur les bacs à sable (sandboxing), de même que la mise en œuvre de mesures de sécurité spécifiques à une configuration et une chaîne de contrôle poussé s'étendant depuis le matériel jusqu'aux applications.

D'après Apple, la sécurité d'iOS s'appuie sur :

Une approche par couches de la sécurité La plateforme iOS fournit des technologies et des fonctionnalités de sécurité très poussées sans compromettre l'expérience de l'utilisateur. Les périphériques iOS sont conçus pour rendre la sécurité aussi transparente que possible. De nombreuses fonctionnalités de sécurité sont activées par défaut, ce qui fait que les utilisateurs n'ont pas besoin d'être des experts de la sécurité pour assurer la protection de leurs données.

Chaîne de démarrage sécurisée Chaque étape du processus de démarrage (depuis la mise en œuvre des bootloaders jusqu'aux noyaux en passant par le firmware de bande de base), est signé par Apple afin de garantir l'intégrité. C'est uniquement lorsqu'une étape a été totalement vérifiée que le périphérique passe à la suivante.

Les bacs à sable applicatifs Toutes les applications tierces sont isolées, ce qui fait que leur accès aux fichiers stockés par d'autres applications est restreint, de même que les modifications qu'elles peuvent apporter au périphérique. Ceci empêche les applications de recueillir ou de modifier des informations comme un virus ou un malware le ferait.

Avec le lancement d'iOS 7, Apple a introduit TouchID pour rationaliser l'authentification du périphérique, la protection cryptographique FIPS 140-2 pour les données sensibles, Activation Lock pour renforcer encore la protection des périphériques volés ou égarés et de nombreuses autres améliorations de sécurité d'arrière-plan.

Les problèmes de sécurité associés au modèle iOS

Apple a adopté une approche de type « jardin clos » pour l'architecture iOS, ce qui empêche les propriétaires des périphériques d'accéder au système d'exploitation ou de le modifier. Pour apporter une quelconque modification, le périphérique doit être débridé. Le débridage est le processus qui consiste à supprimer des protections et à autoriser un accès racine au périphérique. Une fois cet accès racine obtenu, les modifications et les personnalisations sont possibles. Apple a en outre adopté des mécanismes matériels supplémentaires afin de dissuader toute tentative de débridage.

Les dernières fonctionnalités iOS et ce qu'elles impliquent pour les directions informatiques

Le tableau suivant résume les avantages pour l'utilisateur et les impacts sur la sécurité informatique des dernières fonctionnalités des tablettes et smartphones Apple iOS 7.1.

Les nouveautés dignes d'intérêt dans iOS 7.1		
En plus des améliorations bienvenues apportées aux fonctionnalités de sécurité, Apple a publié un document détaillant la sécurité iOS depuis iDevice vers iCloud. Les fonctionnalités notables suivantes et leur impact sont examinées dans ce livre blanc.		
Fonctionnalité iOS	**Avantage pour l'utilisateur du périphérique**	**Impact informatique**
Activation Lock	Une fois configurée, cette fonctionnalité rend inutile tout téléphone volé ou égaré, ce qui devrait dissuader significativement les voleurs.	A des implications sur la propriété et la gestion du périphérique. Complémentaire à la gestion de la mobilité d'entreprise
Touch ID	Touch ID est le vérificateur d'identité par empreintes digitales d'Apple. Il n'est disponible actuellement que sur les iPhone 5s. Il permet l'accès transparent au périphérique.	TouchID fonctionne mieux sous 7.1 et Apple a transféré les paramètres TouchID et de mot de passe à un niveau supérieur, les rendant de fait plus simples à configurer.
Enregistrement automatique	Les utilisateurs reçoivent des périphériques préconfigurés et prêts à l'emploi.	Les périphériques achetés chez Apple dans le cadre du programme d'enregistrement des périphériques (Device Enrollment Program) sont très faciles à enregistrer via la MDM.
FIPS 140-2	Un chiffrement robuste et vérifié protège toutes les données sur le périphérique.	Les entreprises tenues d'utiliser FIPS 140-2 au niveau de leurs périphériques peuvent désormais utiliser des iPhone et des iPad.

Comparaison des mécanismes de sécurité iOS7.x et Android

Lorsque l'on compare iOS et Android, il est important de noter que les contrôles Android varient significativement d'un périphérique, d'une version de système d'exploitation et même d'un opérateur à un autre. Dans certains cas, par exemple, les versions les plus anciennes d'Android ne permettent pas le chiffrement au niveau du périphérique.

	iOS7.x	**Android**
Chiffrement du périphérique	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Chiffrement OTA	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Mot de passe pour le périphérique	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Verrouillage/suppression à distance	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Vérification des applications	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur

Mot de passe pour l'application	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Chiffrement des applications	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Conteneur d'applications	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Accès réseau sécurisé aux applications	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur
Contrôle d'ouverture	Oui	Varie selon le périphérique, le système d'exploitation, l'opérateur

Présentation de l'architecture de sécurité Windows Phone et Surface

Microsoft a encore développé les familières architectures et technologies Windows dans les derniers systèmes d'exploitation de ses smartphones et tablettes. Des fonctionnalités de sécurité intégrées comme BitLocker, Defender, SmartScreen, le pare-feu personnel ou le contrôle de compte utilisateur s'appuient sur une robuste architecture de sécurité mobile.

D'après Microsoft, la sécurité des plateformes Windows Phone et Surface est basée sur les composants suivants :

Sécurité de la plateforme applicative Microsoft adopte une approche à plusieurs volets afin de faciliter la protection des tablettes et de smartphones Windows contre les malwares. L'un des éléments de cette approche est le processus de démarrage sécurisé (ou Trusted Boot), qui contribue à prévenir l'installation de rootkits.

Chambres et capacités Le concept de chambre est basé sur le principe du moindre privilège et s'appuie sur l'isolation pour sa mise en œuvre. Chaque chambre fournit une enceinte sécurisée et, grâce à un processus de configuration, une enceinte isolée au sein de laquelle un processus peut s'exécuter de façon sûre. Chaque chambre est définie et mise en œuvre via un système de stratégies. Pour chaque chambre, la stratégie de sécurité définit les capacités du système d'exploitation que les processus de cette chambre sont autorisés à appeler.

Une capacité est une ressource pour laquelle des contraintes commerciales, de confidentialité, de sécurité ou de coût ont été définies pour toute utilisation sur Windows Phone. Quelques exemples de capacités : données de localisation géographique, caméra, microphone, réseau, capteur, etc.

Les problèmes de sécurité liés à Windows

Les systèmes d'exploitation des anciens PC Windows sont très connus et fortement ciblés par les pirates, ce qui signifie que tout partage de code ou de service entre les plateformes PC et mobiles est susceptible de générer des vulnérabilités étendues. L'architecture de sécurité renforcée des plateformes Windows mobiles (tout particulièrement avec la version Windows 8), a largement fait progresser le degré de sécurisation de Windows.

L'utilisateur par défaut bénéficie des droits de l'administrateur, ce qui lui octroie un accès bien trop important pour le simple travail quotidien. Il est donc recommandé de créer un utilisateur distinct pour l'utilisation quotidienne et de réserver les privilèges d'administrateur aux cas exigeant la mise en œuvre de tâches administratives. Cette capacité de l'utilisateur à devenir administrateur sur le périphérique a bien évidemment les mêmes conséquences que s'il devenait l'utilisateur racine : il bénéficie d'un niveau d'accès bien trop élevé pour son niveau de privilège, ce qui peut impacter négativement la sécurité.

Autre problème important : le modèle de sécurité Windows et ses mécanismes de contrôle sont tellement connus que le périphérique est bien souvent géré de façon excessive par la direction informatique. Ce qui aboutit en fin de compte à une approche de type « ça ou rien » en matière de sécurité et d'utilisation et pousse souvent les utilisateurs, en réaction à cette gestion excessive, à adopter un autre périphérique.

Les dernières fonctionnalités Windows et ce qu'elles impliquent pour les directions informatiques

Le tableau suivant résume les avantages pour l'utilisateur et les impacts sur la sécurité informatique des dernières fonctionnalités des tablettes et smartphones Windows Phone et Surface 8.1.

Les nouveautés dignes d'intérêt dans Windows Phone et Surface		
Microsoft a renforcé les plateformes Windows mobiles en intégrant directement des fonctionnalités de sécurité d'entreprise. Les fonctionnalités notables suivantes et leur impact sont examinées dans ce livre blanc.		
Fonctionnalité Windows	**Avantage pour l'utilisateur du périphérique**	**Impact informatique**
BitLocker	Dans Windows Phone 8, le chiffrement du périphérique s'appuie sur la technologie BitLocker pour chiffrer toutes les données de stockage internes sur le téléphone via AES 128.	Un chiffrement géré par l'utilisateur n'est pas approprié pour les données d'entreprise sensibles. Les directions informatiques doivent appliquer une gestion d'entreprise du chiffrement.
Windows Defender	Cette fonctionnalité contribue à protéger votre PC en temps réel contre les virus, spywares et autres logiciels malveillants.	Les antivirus et antimalwares natifs constituent un complément utile aux plateformes mobiles.
SmartScreen	Le filtre SmartScreen dans Internet Explorer aide à protéger les utilisateurs contre le hameçonnage et les attaques de malware en les alertant lorsqu'un site Web ou un site de téléchargement a été signalé comme peu sûr.	Les stratégies informatiques doivent s'assurer que les utilisateurs tiennent compte des alertes SmartScreen.
Prévention des pertes de données	Information Rights Management (IRM) permet aux créateurs de contenu d'attribuer des droits relatifs aux documents qu'ils envoient à d'autres utilisateurs. Les données des documents protégés par des droits sont chiffrées et ne peuvent être visualisées que pas les utilisateurs autorisés.	Exige Windows Rights Management Services (RMS) et Windows Phone.
Pare-feu	Un pare-feu personnel protège les connexions réseau et applicatives entrantes et sortantes.	La configuration du pare-feu doit être définie et contrôlée par la direction informatique.

Comment les périphériques mobiles modernes protègent les données sensibles

Les modèles de mobilité bouleversent les responsabilités traditionnelles des directions informatiques : les normes organisationnelles strictement définies laissent progressivement la place à une multitude de normes impliquant une myriade de périphériques, de systèmes d'exploitation et de stratégies. Il n'existe pas d'approche uniforme en matière de mobilité et chacun des composants spécifiques de la chaîne (propriété du périphérique, capacités du périphérique, localisation des données, applications) doit être pris en considération dans le schéma de sécurité.

Toutefois, les mesures de contrôle les plus courantes, comme par exemple la protection par un antivirus d'entreprise, ne peuvent pas être installées et maintenues sur tous les périphériques mobiles. Les entreprises doivent donc s'intéresser à l'efficacité de certaines mesures de sécurité mobile en fonction du contexte et de leurs besoins spécifiques, et suivre les recommandations internes des architectes de la sécurité de l'entreprise. Pour en savoir plus sur la façon dont la gestion de la mobilité d'entreprise, la virtualisation de postes et d'applications Windows et un service d'entreprise de partage et de synchronisation de données procèdent pour contrer les menaces mobiles potentielles, consultez le tableau ci-dessous.

Menaces et mesures de sécurité mobile correspondantes (appliquées via la gestion de mobilité d'entreprise, la virtualisation de postes et d'applications Windows, un service d'entreprise de partage et de synchronisation de données et la mise en réseau)

Menace	Vecteur de la menace	Mesure de sécurité mobile
Exfiltration de donnée	Données quittant l'enceinte de l'entreprise Impression d'écran Saisie d'écran Caméra Copie sur un support amovible Perte de sauvegarde Email	Les données demeurent au sein du datacenter ou son chiffrées et gérées sur le périphérique Contrôle des applications/ périphériques Restriction d'utilisation des supports amovibles Sauvegardes chiffrées Email non mis en cache dans les applications natives Restriction des saisies d'écran
Falsification de données	Modification par une autre application Tentatives de falsification non détectées Périphérique débridé	Isolation d'applications/de données Tenue de journaux Détection de périphériques débridés Authentification mutuelle Micro VPN applicatif
Perte de données	Perte de périphérique Accès ou périphérique non approuvé Erreurs et mauvaises configurations Vulnérabilités applicatives	Données gérées sur le périphérique Chiffrement du périphérique Chiffrement des données Mises à jour et correctifs

Malware	Modification de système d'exploitation	Environnement d'exploitation géré
	Modification d'application	Environnement applicatif géré
	Virus	Architecture*
	Rootkit	

*Si les architectures de systèmes d'exploitation mobiles peuvent être renforcées contre les malwares, des virus résidant de façon latente sur les PC peuvent tout de même passer par le biais de documents infectés. Il est donc recommandé que des fonctionnalités antimalware soient activées pour tous les environnements hôtes auxquels le périphérique mobile se connecte (tout particulièrement pour les messageries).

Du fait de la présence de périphériques personnels dans l'entreprise, il est prudent de conserver les informations d'entreprise les plus sensibles loin du périphérique afin de limiter leur vulnérabilité. Par défaut, les données d'entreprise sensibles doivent être accessibles à distance, sans quitter le datacenter, et ne doivent jamais être copiées sur un périphérique mobile. Les données qui doivent être mobilisées doivent être sécurisées par le biais de mesures comme le chiffrement ou la suppression des données à distance sur les périphériques mobiles. Les applications qui doivent être mobilisées et contrôlées peuvent être placées dans des conteneurs afin de prévenir toute interaction avec des applications non professionnelles.

Tout ce qui vous manque

Les applications mobiles n'affichent pas toujours le contenu de la même façon que les applications natives sur un PC. Voici quelques problèmes courants :

- Les vidéos qui ne sont pas dans des formats mobiles natifs ne pourront être lues (WMV ou Flash, par exemple)
- Les applications de messagerie ont souvent des problèmes pour afficher les graphiques correctement , ne sont pas correctement configurés pour la prise en charge des certificats de sécurité, ne chiffrent pas les données et ne gèrent pas les notifications de rappel et autres fonctionnalités spéciales
- L'agenda ne peut pas afficher l'état libre/occupé et rencontre des problèmes avec les événements régulièrement mis à jour ou qui ne sont pas actuels
- Les applications de présentation ne conservent pas la police, les illustrations et la présentation générale de PowerPoint
- Les applications de traitement de texte ne montrent pas quand le suivi des modifications est activé et n'affichent pas les commentaires et les notes. Certaines informations ne sont donc pas affichées et des mises à jour essentielles peuvent manquer.

Sécuriser les informations d'entreprise accessibles depuis les tablettes et les smartphones grâce à Citrix

Citrix fournit une librairie applicative unifiée sur le périphérique mobile, permettant l'accès aux applications de productivité et aux applications commerciales, notamment aux données gérées via ShareFile. ShareFile permet l'accès à des données hors ligne depuis des périphériques mobiles. ShareFile et XenMobile aident les directions informatiques à protéger les données sensibles stockées sur les périphériques mobiles grâce à la création de conteneurs, au chiffrement et à des stratégies de contrôle complet des données permettant de prévenir toute fuite imputable aux utilisateurs. Les données placées dans des conteneurs sur le périphérique peuvent être supprimées à distance par la direction informatique à tout moment. Cette suppression peut également être déclenchée automatiquement par des événements spécifiés, comme par exemple le débridage d'un périphérique. La librairie applicative unifiée Citrix délivre tout aussi bien des applications mobiles que des applications et des postes de travail Windows hébergés via XenApp et XenDesktop. En fournissant un accès mobile distant à des ressources hébergées de façon centralisée, les directions informatiques peuvent maintenir les données au sein du datacenter, où elles peuvent être parfaitement sécurisées. Que l'entreprise choisisse

de conserver ses données et ses applications sensibles au sein du datacenter, de les héberger sur des périphériques ou de leur permettre de devenir mobiles, la direction informatique peut appliquer les stratégies définies grâce à XenMobile et à ShareFile.

Les applications mobiles sécurisées par Citrix s'appuient sur les capacités d'authentification renforcée et de chiffrement du trafic réseau de Citrix NetScaler Gateway. La passerelle SSL/VPN NetScaler Gateway fournit des micro VPN applicatifs pour permettre l'accès en arrière-plan aux applications d'entreprise, mobiles et Web, en agissant comme un point d'application des stratégies réseau afin de garantir une sécurité réseau adaptée à chaque application. Les micro VPN applicatifs n'exécutent que des données d'entreprise bien définies, dans le cadre d'une utilisation professionnelle, contribuant ainsi à mieux gérer le trafic tout en sécurisant la confidentialité des données de l'utilisateur. XenMobile permet la gestion et le contrôle unifiés de tous les types d'applications (notamment mobiles, Web, SaaS et Windows), de données, de périphériques et d'utilisateurs.

Le chiffrement Citrix protège les données de configuration, les bitmaps d'écran et l'espace de travail de l'utilisateur. Citrix utilise la fonctionnalité de la plateforme mobile native pour chiffrer les données au repos et en mouvement via des interfaces réseau WiFi et 3G/4G.

Comment XenMobile contribue à protéger les applications et les périphériques

XenMobile garantit une liberté totale aux périphériques, applications et données mobiles. XenMobile 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 volés ou égarés. Son conteneur sécurisé permet non seulement de chiffrer les données applicatives, mais également de séparer les données personnelles des données professionnelles. Ainsi, les directions informatiques peuvent laisser les utilisateurs choisir leur périphérique, tout en ayant la capacité d'éviter les fuites et de protéger le réseau interne contre les menaces mobiles.

Protection au niveau du système d'exploitation XenMobile Device Manager s'assure que tout ce qu'il faut est bien en place pour mettre en œuvre et gérer les fonctionnalités au niveau du système d'exploitation :

- Protectionpar mot de passe au niveau des applications
- Chiffrement
- WiFi
- Inventaire des périphériques
- Inventaire des applications
- suppression complète/sélective
- API spécifiques à certains fabricants de périphériques (Samsung, HTC, etc.)
- Configuration automatique du WiFi
- Restriction de l'accès aux ressources du périphérique, notamment librairies applicatives, caméra et navigateur
- Prise en charge des contrôles de sécurité de Samsung SAFE et KNOX

Chiffrement et sécurité XenMobile permet aux directions informatiques d'interdire les copier/coller ou de ne les autoriser que pour des applications autorisées. Par l'intermédiaire de Worx Mobile Apps, des fonctionnalités comme le chiffrement AES-256 ou la validation FIPS 140-2 protègent les données d'entreprise stratégiques au repos. Des contrôles d'ouverture vous permettent de spécifier que certains documents ne peuvent être ouverts que dans des applications bien déterminées. Même les liens vers les sites Web peuvent être obligés de s'ouvrir dans un navigateur sécurisé.

En transit, les données sont protégées via une fonctionnalité de micro VPN applicatif, qui permet l'accès sécurisé aux ressources de l'entreprise (applications, intranet, messagerie). Les tunnels micro VPN applicatifs sont spécifiques à chaque application et chiffrés afin d'être protégés des communications associées aux autres périphériques ou aux autres tunnels micro VPN applicatifs.

Détection du débridage XenMobile détecte le débridage et l'état racine grâce à des méthodes propriétaires comme l'inspection binaire ou la disponibilité d'API.

Stratégies de géolocalisation Les services de localisation permettent aux directions informatiques d'établir un périmètre géographique de contrôle au sein duquel les périphériques ou certaines applications peuvent être utilisés. si le périphérique quitte ce périmètre, son contenu peut être totalement ou sélectivement supprimé.

Gestion des applications mobiles (ou MAM) La MAM contrôle l'utilisation, les mises à jour, l'infrastructure réseau et la sécurité des données au profit des applications. Chaque application présente sur le périphérique peut bénéficier de son propre tunnel chiffré en SSL, uniquement utilisable par cette application. Lorsqu'un employé quitte l'entreprise, la direction informatique peut supprimer à distance et de façon sélective les données d'entreprise à partir des conteneurs d'applications gérés, sans toucher à une quelconque donnée ou application personnelle sur le périphérique. XenMobile offre également une librairie applicative unique et sécurisée permettant aux périphériques mobiles d'accéder à la fois aux applications publiques et privées.

Applications de productivité sécurisées Les applications de productivité Citrix intégrées comprennent un navigateur Web sécurisé, un conteneur de messagerie/agenda/contacts et ShareFile, un service sécurisé de synchronisation et de partage de fichiers. Elles permettent aux utilisateurs de naviguer de façon transparente sur les sites intranet sans qu'il ne soit nécessaire de recourir aux coûteuses solutions VPN qui ouvrent le réseau de l'entreprise à toutes les applications du périphérique. Grâce à Worx Mobile Apps, tout développeur ou administrateur peut ajouter des fonctionnalités d'entreprise : chiffrement des données, authentification par mot de passe ou micro VPN applicatif.

Worx Mobile Apps comprend :

WorxMail: WorxMail est une application iOS et Android native complète de messagerie, d'agenda et de gestion des contacts qui fonctionne et gère les données exclusivement au sein d'un conteneur sécurisé présent sur le périphérique mobile. WorxMail prend en charge les API Exchange ActiveSync et offre des fonctionnalités de sécurité, telles que le chiffrement des courriers électroniques, des pièces jointes et des contacts.

WorxWeb : WorxWeb est un navigateur mobile pour les périphériques iOS et Android, qui permet un accès sécurisé aux applications Web internes d'entreprise, externes SaaS et HTML5, tout en préservant l'expérience du navigateur natif du périphérique. Grâce à un micro VPN applicatif, les utilisateurs accèdent à tous leurs sites Web, y compris à ceux contenant des informations sensibles. WorxWeb offre une expérience utilisateur transparente grâce à son intégration à WorxMail, permettant aux utilisateurs de cliquer sur des liens et d'ouvrir leurs applications natives à l'intérieur du conteneur sécurisé sur leur périphérique mobile.

Worx Home : Worx Home est le point de contrôle central de toutes les applications XenMobile et de tout le contenu stocké sur le périphérique. Worx Home gère le point d'origine de l'expérience utilisateur (authentification, applications, gestion des stratégies et stockage des variables de chiffrement).

Associées, ces fonctionnalités de XenMobile (et d'autres) offrent aux directions informatiques la capacité à :

Unifier le contrôle sur l'accès distant aux applications et aux données. La librairie applicative d'entreprise unifiée Citrix regroupe de façon sécurisée les applications et les postes de travail Windows virtualisés, les applications Web, SaaS, mobiles natives ainsi que les données en un point unique permettant de gérer et de contrôler les stratégies et les comptes s'appliquant aux services de l'utilisateur.

Isoler et sécuriser les messageries d'entreprise. L'un des plus gros avantages de WorxMail est qu'il permet de maintenir la messagerie d'entreprise au sein d'un bac à sable ou d'un conteneur et de la dissocier du reste du périphérique. Imaginez la différence avec l'utilisation d'ActiveSync et de l'application de messagerie mobile native. Dans ce cas, un administrateur doit obligatoirement prendre un certain niveau de contrôle sur le périphérique et l'utilisateur doit accepter l'éventualité d'une suppression du contenu du périphérique en cas de problème. Les données d'accès, de chiffrement et de profil sont toutes associées au périphérique. En outre, l'approche par bac à sable permet le chiffrement à la fois du corps du mail et de toute pièce jointe.

Eviter toute interférence avec le contenu personnel présent sur les périphériques mobiles. Grâce à WorxMail, l'utilisateur consent uniquement à la suppression éventuelle en cas de problème des données d'entreprise stockées dans son conteneur WorxMail, et non de l'intégralité des données de son périphérique. La messagerie d'entreprise et les contacts professionnels sont isolés, protégés et contrôlés par le conteneur, et non par le périphérique. Les messageries personnelle et professionnelle sont également séparées grâce à l'approche d'isolation par bac à sable, qui contribue à maintenir la stricte séparation des emails et des contacts.

XenMobile et Samsung SAFE et KNOX XenMobile prend en charge les contrôles de sécurité de Samsung SAFE et KNOX, y compris la gestion du conteneur the KNOX. L'intégration étroite entre Worx Mobile Apps et le conteneur KNOX sécurisé garantit que les données d'entreprise sensibles (notamment les emails soumis à des réglementations de conservation) ne seront jamais exposés aux malwares qui pourraient résider sur le système d'exploitation ou à des applications non gérées du portefeuille applicatif personnel de l'utilisateur. En outre, la solution permet également la prise en charge des pistes d'audit pour vérifier l'intégrité des données à des fins de conformité. XenMobile permet également l'utilisation de contrôles et de fonctionnalités de sécurité supplémentaires pour KNOX, notamment la communication inter-applicative sécurisée, le contrôle de la surveillance géographique, le contrôle intelligent du trafic réseau et la gestion sécurisée du contenu. (Attention : des licences Samsung Knox supplémentaires peuvent être nécessaires.)

XenMobile et iOS 7.x XenMobile prend en charge et prolonge les contrôles iOS natifs par le biais de fonctionnalités de sécurité supplémentaires. Pour iOS 7 comme pour KNOX, XenMobile offre les améliorations suivantes :

Fonctionnalité XenMobile	Détails
Librairie applicative d'entreprise	Accès unifié avec possibilité de provisionner les applications mobiles, SaaS, Web et Windows directement sur le point d'origine du périphérique
SSO amélioré	Accès d'un seul clic aux applications mobiles, SaaS, Web et Windows

Ecosystème d'applications d'entreprise	Ecosystème d'applications le plus large grâce à Worx App Gallery
Contrôle du réseau	contrôle de l'utilisation des applications basé sur les réseaux WiFi
Contrôle SSID autorisé	Contrôle granulaire des réseaux internes associés aux applications
Contrôle de la surveillance géographique	Sécurité renforcée pour verrouiller, supprimer ou notifier en fonction de la localisation du périphérique
Accès en ligne/hors ligne	Limitation des applications à un accès en ligne ou restriction de la durée d'utilisation hors ligne
Communication inter-applicative	Contrôle des communications entre les différentes applications gérées
Provisioning et déprovisioning très simples	Activation/désactivation de l'accès
Messagerie sécurisée	Messagerie isolée avec agenda et contacts d'entreprise, avec visibilité sur la disponibilité des contacts
Navigateur sécurisé	Navigateur HTML5 totalement fonctionnel pour contenus et sites intranet d'entreprise sécurisés
Gestion sécurisée du contenu	Accès, annotation, édition et synchronisation de fichier depuis tout périphérique
Suite complète d'applications EMM	Applications répondant à tout scénario d'utilisation EMM et fonctionnalités stratégiques comprenant notamment ShareFile, GoToMeeting, GoToAssist et Podio

Comment ShareFile contribue à la protection des fichiers et des données

ShareFile offre de robustes fonctionnalités gérées de partage et de synchronisation des données, totalement intégrées à XenMobile. Cette solution permet également aux directions informatiques de stocker les données sur site ou dans le cloud et contribue à mobiliser les investissements existants comme SharePoint ou les réseaux de partage de fichiers. Un riche contenu intégré reprenant toutes les fonctionnalités de ShareFile permet aux utilisateurs de répondre à tous leurs besoins de mobilité, de productivité et de collaboration à partir d'une seule application très intuitive. Grâce à ShareFile, les directions informatiques peuvent :

Sécuriser les données par le biais de stratégies complètes de sécurisation de périphériques. ShareFile offre des fonctionnalités étendues permettant de garantir la sécurité des données sur les périphériques mobiles. ShareFile offre des fonctionnalités de suppression à distance et de pilule empoisonnée qui désactivent l'accès aux données sensibles en cas de violation de sécurité. Les directions informatiques peuvent également restreindre l'accès des périphériques mobiles modifiés et activer le verrouillage par mot de passe afin de tirer profit des capacités de chiffrement du périphérique mobile.

Stimuler la productivité des utilisateurs avec un éditeur de contenu riche en fonctionnalités sur les appareils mobiles. Les utilisateurs peuvent créer, réviser et modifier des documents Microsoft Office dans l'application ShareFile, puis les éditer avec les outils similaires proposés dans leurs applications de bureau Microsoft Office.

Restreindre l'utilisation des applications tierces et renforcer la sécurité des données sur les périphériques mobiles. Les directions informatiques peuvent restreindre la capacité des applications tierces non autorisées à ouvrir et modifier des données ShareFile. Un éditeur intégré permet aux directions informatiques de restreindre l'utilisation des éditeurs tiers parfois employés par les utilisateurs, empêchant ainsi le stockage de copies de données sensibles dans ces applications.

Conserver la structure des dossiers et des sous-dossiers sur les périphériques mobiles. Vous pouvez marquer des dossiers complets comme des fichiers individuels afin de permettre leur accès hors ligne depuis des périphériques mobiles.

Renforcer la disponibilité. Associée à la prise en charge de l'édition de documents, l'accès hors ligne à des dossiers complets aide les utilisateurs à être totalement productif en tout lieu.

Bénéficier d'un suivi, de journaux et de comptes-rendus relatifs à l'accès aux fichiers et aux activités de synchronisation et de partage. Les directions informatiques jouissent d'un suivi complet de chaque événement déclenché par l'utilisateur (date, type, localisation et adresse réseau). Plusieurs versions successives d'un même fichier peuvent être stockées dans le but de créer des pistes d'audit permettant de suivre les activités de modification. Si une suppression à distance est initiée, la direction informatique peut suivre l'activité des fichiers sur le périphérique entre le moment ou la suppression a été initialisée et celui où elle a été achevée avec succès, et recevoir une notification lui confirmant le succès de cette suppression.

Rationaliser l'administration et la sécurité. Grâce à l'intégration de ShareFile avec XenMobile, la direction informatique peut en toute simplicité s'appuyer sur le provisioning et de déprovisioning basés sur la fonction, l'authentification à deux facteurs, les contrôles basés sur des stratégies et le suivi applicatif en temps réel.

ShareFile vous permet de choisir où stocker vos données. Grâce à la fonctionnalité StorageZones de ShareFile, les entreprises peuvent gérer leurs données sur site au sein d'environnements de stockage StorageZones gérés par le client, ou bien choisir des environnements StorageZones gérés par Citrix (environnements cloud sécurisés proposés sur de nombreux sites répartis dans le monde) ou bien encore privilégier une association des deux. Grâce à StorageZones avec gestion client, les directions informatiques peuvent placer les données au sein du datacenter de l'entreprise afin de répondre au mieux à ses besoins spécifiques de conformité et de souveraineté des données.

Afin d'assurer une sécurité maximale à ceux qui choisissent de stocker leurs données dans le cloud, les datacenters hébergeant les bases de données et l'application Web ShareFile sont conformes à la norme SSAE 16, et les datacenters hébergeant l'application de stockage des fichiers sont conformes aux normes SSAE 16 et ISO 27001. Afin de protéger les données relatives à ses clients, Citrix met en œuvre et maintient des contrôles physiques, techniques et organisationnels supplémentaires, appropriés et commercialement raisonnables.

ShareFile est conforme à la norme PCI-DSS et fera bientôt l'objet d'un accord d'association HIPAA. Citrix propose également ShareFile Cloud for Healthcare, une enclave sécurisée hébergée au sein d'un cloud privé, permettant aux directions informatiques de télécharger, de stocker et de partager les informations médicales et d'assurer une stricte conformité aux obligations réglementaires régissant le secteur médical. ShareFile Cloud for Healthcare permet notamment la conformité à la norme HIPAA.

Comment XenDesktop et XenApp contribuent à la protection des applications et des données

XenDesktop et XenApp fournissent un accès distant sécurisé à des applications et à des postes de travail Windows hébergés de façon centralisés, ainsi qu'aux données qui leur sont associés, en maintenant ces différentes ressources bien protégées à l'abri du datacenter. Bien que les périphériques (et les personnes qui les utilisent) soient mobiles, les données elles-mêmes demeurent sécurisées et protégées au sein du datacenter. XenApp et XenDesktop constituent un moyen simple, efficace et sécurisé de délivrer des applications Windows tierces ou développées en interne à une main-d'œuvre mobile.

Comment NetScaler contribue à la protection des fichiers et des données

NetScaler garantit une connectivité sécurisée pour la mobilité, permettant la mise en œuvre du single sign-on (SSO), d'une robuste authentification multifacteur, du chiffrement et d'une fonctionnalité de micro VPN applicatif. L'utilisation de NetScaler automatise la sécurité réseau en évitant au propriétaire du périphérique d'avoir à activer et à désactiver des VPN ou à mémoriser la façon de se connecter en toute sécurité aux applications cloud et Web. NetScaler aide les directions en charge de la sécurité et de la conformité en garantissant que toutes les mesures nécessaires d'authentification, de chiffrement, de tenue de journaux et de protection du réseau sont bien appliquées.

Meilleures pratiques pour une sécurité mobile

Afin d'assurer une sécurité et un contrôle efficaces, les entreprises doivent compléter les fonctionnalités de sécurité inhérentes aux technologies Citrix et aux périphériques mobiles par des meilleures pratiques destinées à la fois aux utilisateurs et aux directions informatiques. Chaque membre de l'entreprise doit assumer la responsabilité de suivre ces mesures, essentielles à la garantie d'une mobilité d'entreprise et d'un BYOD sécurisés et contrôlés. Citrix recommande aux utilisateurs et aux administrateurs d'appliquer les directives suivantes lorsqu'ils utilisent Citrix avec des tablettes ou des smartphones Android, iOS ou Windows.

Actions recommandées aux utilisateurs

Les utilisateurs ont la responsabilité de protéger les informations d'entreprise sensibles de leur employeur. Ils peuvent contrôler l'installation et la configuration de leur périphérique, adopter de bonnes pratiques d'utilisation quotidienne, s'appuyer sur XenMobile, ShareFile, XenDesktop et XenApp pour contribuer à assurer la sécurité et effectuer plusieurs autres actions recommandées. Les administrateurs peuvent s'assurer que les utilisateurs respectent ces meilleures pratiques en les appliquant automatiquement sous forme de stratégies dans XenMobile. Les meilleures pratiques destinées aux utilisateurs sont décrites ci-dessous.

Installation et configuration du périphérique	
Plateforme	Ne débridez ou ne figez pas votre périphérique si celui-ci est utilisé en environnement d'entreprise, et rejetez toute demande d'installation de certificats tiers **Android :** Si vous devez partager l'utilisation de votre périphérique, utilisez différents comptes utilisateur pour vos enfants et les autres invités **iOS :** Aucune configuration nécessaire **Windows :** Créez un compte distinct pour l'administrateur et employez un compte utilisateur sans privilège pour le travail quotidien

Authentification	Utilisez un verrouillage par mot de passe pour protéger l'accès au périphérique mobile (utilisez un mot de passe complexe à huit caractères) **Android :** Configurez l'écran de verrouillage en définissant le mot de passe ou le code PIN, activez le verrouillage automatique après un délai d'expiration et activez le verrouillage instantané couplé à la touche Marche/Arrêt **iOS :** Paramétrez Demande de mot de passe sur Immédiatement et évitez la découverte du mot de passe en activant l'option Effacez les données. Activez le verrouillage automatique et paramétrez-le sur une minute. Utilisez TouchID s'il est disponible sur votre périphérique **Windows :** Définissez un mot de passe de compte et exigez la saisie d'un mot de passe après une mise en veille de l'affichage depuis x minutes
Chiffrement	Chiffrez le périphérique et les sauvegardes et contrôlez la localisation des sauvegardes **Android :** Chiffrez le périphérique **iOS :** Définissez un mot de passe ou une phrase de sécurité pour chiffrer le périphérique et les sauvegardes dans iTunes et iCloud **Windows :** Configurez BitLocker
Services cloud	Configurez les services afin que les données d'entreprise sensibles ne soient pas sauvegardées sur un cloud grand public. Ceci doit comprendre les documents, les informations de compte, les mots de passe sans fil, les paramètres et les messages **Android :** Désactivez la sauvegarde personnelle sur le compte Google **iOS :** Désactivez l'iCloud personnel **Windows :** Désactiver le OneDrive personnel
Bluetooth et partage	Désactivez le transfert des données pour les connexions non sécurisées. Par exemple, désactivez le transfert de vos contacts et de votre annuaire lorsque vous utilisez le Bluetooth pour vos appels téléphoniques ou pour écouter de la musique dans une voiture de location **iOS :** Désactivez la synchronisation des contacts **Windows :** Désactivez le partage
Réseau et sans fil	Utilisez uniquement des réseaux sécurisés, assurez-vous du chiffrement du réseau et utilisez un VPN ou un micro VPN applicatif pour fournir le chiffrement, peu importe les fonctionnalités réseau sous-jacentes. La fonctionnalité WorxWeb de XenMobile permet la connectivité avec micro VPN applicatif **Android :** Configurer le sans fil pour bénéficier des notifications réseau **iOS :** Configurez le sans fil pour demander à rejoindre des réseaux **Windows :** Dans les paramètres de partage avancé, dans le menu panneau de contrôle, désactivez la détection de réseau pour les réseaux invités et publics et activez le partage protégé par mot de passe

Email	La messagerie étant fréquemment utilisée pour le partage (et la perte) de données sensibles, utilisez ShareFile pour conserver les pièces jointes sensibles éloignées des emails et utilisez WorxMail avec XenMobile lorsqu'un conteneur de messagerie gérée est souhaité **Android:** Configurez l'accès à la messagerie afin de toujours utiliser une connexion sécurisée **iOS :** Assurez-vous que l'option utiliser SSL est bien activée pour tous les comptes pris en charge et utilisez S/MIME, s'il est configuré **Windows :** Configurez les comptes pour la prise en charge SSL
Mises à jour du périphérique / Perte du périphérique	Sachez comment sauvegarder toutes vos données pour pouvoir les transférer sur un nouveau périphérique et comment tout effacer de façon sécurisée sur un ancien périphérique. Assurez-vous de connaître la procédure à suivre pour signaler à votre direction informatique la perte ou le vol de votre périphérique **Android :** Utilisez la fonctionnalité native Sauvegarder mes données et mes paramètres ou une solution tierce de sauvegarde, et utilisez la fonctionnalité Réinitialiser aux données d'usine pour effacer vos données personnelles **iOS :** Demandez à votre direction informatique si elle met en œuvre une solution de gestion des périphériques mobiles (MDM) lui permettant de localiser et de nettoyer à distance votre périphérique en cas de perte ou de vol. Si ce n'est pas le cas, configurez Trouver mon iPhone et utilisez cette fonctionnalité pour nettoyer votre périphérique volé ou égaré* **Windows :** Utilisez l'Historique des dossiers ou une solution tierce de sauvegarde et supprimez tout pour réinstaller Windows afin d'effacer vos données personnelles
Confidentialité	Empêchez l'affichage et le partage involontaires des données personnelles et sensibles **Android :** Désactivez le recueil des Diagnostics et Données d'utilisation dans le menu Paramètres/Général/A propos de **iOS :** Activez Limiter le suivi des publicités dans le menu Général/A propos de/Publicité et configurez Notifications afin d'afficher uniquement les informations dans le Centre de notification à partir d'applications qui ne mettront pas en péril la confidentialité **Windows :** Configurez Notifications pour n'Afficher les notifications applicatives sur l'écran de verrouillage que pour les applications sécurisées? Désactivez Laisser Windows sauvegarder mes recherches pour les suggestions de recherches futures. Activez Ne conservez-pas l'historique dans Internet Explorer. Supprimez l'historique de recherche dans Windows. Désactivez Laisser les applications utiliser mon nom et mon image de compte. Et désactivez Aider Windows Store en envoyant des URL pour le contenu Web utilisé par les applications

* L'application Trouver mon iPhone, téléchargeable gratuitement sur App Store, permet aux utilisateurs de localiser facilement un périphérique manquant sur une carte et de lui faire afficher un message ou émettre un son. Les utilisateurs peuvent même verrouiller le périphérique égaré à distance ou supprimer les données qu'il contient afin de préserver la confidentialité.

Diagnostics et fonctionnalités de développeurs	Désactivez les fonctionnalités utilisées par les développeurs et susceptibles d'affaiblir la sécurité et la confidentialité **Android :** Désactivez Options de développeurs et Dépannage USB **iOS :** Désactivez l'envoi de diagnostics et de données d'utilisation dans le menu Paramètres/Général/A propos de/Diagnostics et Utilisation **Windows :** Travaillez en tant qu'utilisateur sans privilège et non en tant qu'administrateur, afin de désactiver l'accès aux diagnostics système et administratifs
Applications	N'installez que des applications provenant de sources favorablement connues (librairies applicatives d'entreprise et librairies applicatives de plateformes officielles) **Android :** N'acceptez pas d'applications exigeant des permissions excessives et assurez-vous que l'option Administration du périphérique/Sources inconnues n'est pas sélectionnée **iOS :** Utilisez des applications provenant d'Apple App Store **Windows :** Utilisez des applications provenant de Microsoft Store
Mises à jour	Appliquez les mises à jour logicielles lorsque de nouvelles versions sont disponibles **Android :** Allez sur A propos du périphérique/Mise à jour logicielle pour les mises à jour de système d'exploitation et sur l'application Play Store pour les mises à jour d'applications **iOS :** Allez sur Général/Mise à jour logicielle pour vérifier la présence éventuelle de mises à jour iOS et sur l'application App Store pour celle de mises à jour d'applications **Windows :** Utilisez Windows Update pour les mises à jour de système d'exploitation et Store pour les mises à jour d'applications
Logiciel de sécurité	Configurez les fonctionnalités et logiciels de sécurité intégrés, y compris le pare-feu et utilisez au besoin une solution antimalware **Android :** Recherchez dans Play Store les applications de sécurité qui répondent à vos besoins de sécurité personnels et professionnels **iOS :** Aucune configuration particulière nécessaire **Windows :** Configurez le pare-feu Windows. L'antivirus Windows Defender est préinstallé

Utilisation quotidienne

- Appuyez sur le bouton Marche/Arrêt pour verrouiller le périphérique dès qu'il n'est pas utilisé.
- Vérifiez la localisation des imprimantes avant toute impression de documents sensibles.
- Signalez un périphérique volé ou égaré à votre direction informatique afin qu'elle puisse désactiver les certificats et les autres méthodes d'accès associées à ce périphérique.
- Utilisez un portail en libre-service pour verrouiller et localiser les périphériques égarés.
- Réfléchissez aux implications en matière de confidentialité avant d'autoriser des services de géolocalisation, et limitez leur utilisation aux applications sécurisées.
- Gérez soigneusement l'accès aux comptes iTunes AppleID, Google et OneDrive, qui sont associés à des données sensibles.

Autres considérations et meilleures pratiques

- Conservez les données sensibles non gérées à distance des périphériques mobiles partagés. Lorsque des informations d'entreprise sont stockées localement sur un périphérique, il est recommandé que ce périphérique ne soit pas partagé sans restrictions. Demandez à votre direction informatique comment utiliser les technologies Citrix afin de conserver les données au sein du datacenter et de maintenir la confidentialité des périphériques personnels.
- Si vous devez disposer de données sensibles sur un périphérique mobile, utilisez ShareFile et XenMobile pour placer vos données sensibles dans un conteneur et contrôler les endroits où les données d'entreprise transitent et sont stockées.
- Utilisez les fonctionnalités supplémentaires d'authentification et de chiffrement de ShareFile et de XenMobile afin de limiter les risques de contournement de l'écran de verrouillage.
- Configurez les services de localisation afin de désactiver le suivi de la localisation pour les applications auxquelles vous ne souhaitez pas transmettre ces informations.
- Configurez les notifications afin de désactiver l'affichage des notifications lorsque le périphérique est verrouillé pour les applications susceptibles d'afficher des données sensibles.
- Configurez AutoFill (remplissage automatique des noms et mots de passe) afin de limiter la divulgation de mots de passe par lecture par dessus l'épaule ou surveillance (si souhaité et autorisé par les stratégies d'entreprise).

Autres responsabilités incombant aux propriétaires de périphériques mobiles accédant aux messageries d'entreprise

Les tablettes et smartphones Android, iOS et Windows prennent en charge de façon native Microsoft Exchange et d'autres environnements de messagerie. XenMobile peut servir à configurer des stratégies de messagerie sur le périphérique, ou à en bloquer l'accès si celui-ci devient non conforme.

Pour les environnements hautement sécurisés, WorxMail, un client de messagerie isolé et convivial, peut être utilisé pour contrôler les emails et leurs pièces jointes grâce à des stratégies de contrôle des données très détaillées.

Actions recommandées aux administrateurs

Les administrateurs sont responsables de la mise en œuvre et de l'application des stratégies définies par les responsables de la sécurité, la direction informatique et les responsables commerciaux. Les principales actions recommandées sont énumérées ci-dessous.

- Publiez une politique d'entreprise qui précise l'utilisation acceptable des périphériques grand public et personnels dans l'entreprise. Assurez-vous que cette politique soit connue des utilisateurs.
- Publiez une politique d'entreprise pour les services cloud, et tout particulièrement pour les outils de partage de fichiers.
- Activez les mesures de sécurité telles que les antivirus afin de protéger les données au sein du datacenter.
- Appliquez une politique qui précise les niveaux d'accès aux applications et aux données autorisés et non autorisés sur les périphériques grand public.
- Définissez via NetScaler Gateway un délai d'expiration de session qui soit cohérent avec la politique d'entreprise.
- Précisez si le mot de passe de domaine peut être mis en cache sur le périphérique ou si les utilisateurs doivent le saisir à chaque fois qu'ils demandent l'accès.
- Activez le SSO pour les applications mobiles les plus couramment utilisées, à la fois pour des raisons de sécurité et de convivialité.
- Déterminez et configurez les méthodes d'authentification NetScaler Gateway autorisées.

Conclusion

La mobilité d'entreprise et le BYOD obligent les entreprises à s'adapter à de nouveaux défis en matière de sécurité. Citrix permet une approche centralisée de la sécurité qui protège les informations d'entreprise sensibles sans pénaliser la productivité, offrant ainsi aux entreprises un moyen efficace de répondre aux besoins d'une main-d'œuvre toujours plus mobile. Avec Citrix, l'entreprise peut adopter une approche plus moderne et plus efficace de sécurisation des données.

Ce document ne prétend pas être un guide exhaustif de présentation de la sécurité mobile d'entreprise sur périphériques Android, iOS et Windows. Citrix recommande une évaluation stratégique globale intégrant XenMobile, ShareFile, XenDesktop, XenApp et NetScaler.

Validité des versions : Ce document s'applique à Android 4.4, Apple iOS 7.1 et Windows 8.1, à compter d'avril 2014.

Pour en savoir plus sur les solutions BYOD Citrix et les technologies Citrix sécurisées par nature, consultez http://www.citrix.fr/byod et http://www.citrix.fr/secure ou suivez-nous sur Twitter @CitrixBYOD et @CitrixSecurity.

Ressources supplémentaires

- 10 éléments essentiels pour une stratégie de mobilité d'entreprise sécurisée
- Les meilleures pratiques pour rendre le BYOD simple et sécurisé
- Gestion de la mobilité d'entreprise : Adopter le BYOD via la mise à disposition sécurisée des applications et données
- Les 10 incontournables pour une mobilité d'entreprise sécurisée

Pour obtenir une information plus spécifique aux différents matériels en matière de sécurisation des périphériques iOS, Android, Windows Phone et Surface en entreprise, consultez :

Apple iOS

- L'iPad en entreprise – Centre informatique : Sécurité
- L'iPhone en entreprise – Centre informatique : Sécurité

Android

- KitKat, les fonctionnalités Android 4.4

Windows Phone et Surface

- Windows Phone 8 : sécurité et chiffrement

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, Etats-Unis

Centre de développement Royaume-Uni
Chalfont, Royaume-Uni

À propos de Citrix
Citrix (NASDAQ:CTXS) est l'entreprise de référence dans le domaine de la virtualisation, des réseaux et des infrastructures cloud permettant aux individus de travailler et de collaborer différemment. Les solutions cloud de Citrix aident les directions informatiques et les fournisseurs de services à bâtir, gérer et sécuriser des espaces de travail virtuels offrant des applications, postes de travail, données et services de qualité, accessibles à tous, quel que soit l'appareil, le réseau ou la plate-forme cloud. Cette année, Citrix célèbre 25 ans d'innovation qui rend aujourd'hui l'informatique plus accessible et les employés plus productifs grâce à de nouvelles méthodes de travail. Le chiffre d'affaires annuel de l'entreprise a atteint 2,9 milliards de dollars en 2013. 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.

0414/PDF

citrix.fr/byod **citrix.fr/secure**