Construire une **stratégie de Mobilité d'Entreprise** gagnante

MobileIron

Ce livre blanc a été réalisé grâce au sponsoring de MobileIron.

proximus

Pour **une entreprise mobile moderne**

La dernière décennie a été marquée par une croissance vertigineuse de la mobilité au niveau mondial. Depuis l'arrivée du premier iPhone, en 2007, les appareils mobiles se sont généralisés plus vite que toute autre technologie dans l'histoire. Tout a changé avec l'informatique mobile.

Les applications ne sont plus tributaires de l'ordinateur de bureau et les utilisateurs considèrent comme normal de pouvoir utiliser tour à tour, de manière transparente, ordinateurs de bureau, tablettes et smartphones, partout et en permanence. Aujourd'hui, l'approche multicanal se transforme en expérience omnicanal et devient la nouvelle norme pour tous les consommateurs.

La tendance 'Bring Your Own Device' s'est solidement ancrée dans les organisations. Les entreprises en reconnaissent de plus en plus les avantages, car elle permet aux membres du personnel d'utiliser leurs appareils mobiles personnels à des fins professionnelles. Les entreprises deviennent mobiles, avec ou sans le consentement explicite de leurs organes exécutifs, voire à l'insu de ces derniers. Dans de nombreux cas, la tendance à la mobilité naît au sein même de l'organisation, les départements marketing, la hiérarchie des Business Managers et les utilisateurs-pionniers accélérant le besoin d'une stratégie mobile.

Les préoccupations liées à la mobilité d'entreprise vont toutefois au-delà des collaborateurs de l'entreprise. De plus en plus, les clients, mais aussi les fournisseurs, sous-traitants et autres acteursclés de votre écosystème utilisent des appareils mobiles pour recueillir des informations concernant votre société et vos produits, pour interagir avec le personnel de vente et de gestion et pour acheter ou fournir des produits et services.

Pour fonctionner de manière efficace, une société a besoin d'organisations IT pour gérer les utilisateurs mobiles tout en surveillant et en gérant l'utilisation, afin de préserver la sécurité et la sûreté des exploitations. Les sociétés ont besoin de nouvelles stratégies et technologies pour évoluer en toute confiance dans leur parcours de mobilité.

Comme vous le découvrirez à la lecture de ces pages, le concept d'Enterprise Mobility ne consiste pas simplement à acheter la technologie la plus récente ou à mettre une solution d'e-mail sur le téléphone d'un membre du personnel. La mobilité touche à la transformation de votre activité pour favoriser l'émergence de nouvelles sources de productivité. Proximus peut vous aider à définir une stratégie d'entreprise pertinente et à transformer de manière sûre vos processus d'entreprise critiques, en faisant appel à des solutions et des services professionnels de mobilité d'entreprise éprouvés et à la pointe du secteur.

Une approche globale de la **mobilité d'entreprise**

EMM, le fondement de votre stratégie de mobilité d'entreprise

Si vous prévoyez de gérer quoi que ce soit sur une plateforme mobile, l'Enterprise Mobility Management (EMM) constitue le point de départ de votre démarche. Les solutions EMM connectent les appareils mobiles aux flux de travail de l'entreprise et gèrent l'évolution incessante des numéros et des types d'appareils. Les organisations utilisent des systèmes et services EMM pour assurer les tâches de provisioning, de tracking et d'audit, de support et de protection des données. Les solutions EMM sont le cordon ombilical reliant les appareils mobiles à leur infrastructure d'entreprise.

Trois capacités techniques de base EMM aident les organisations IT à assurer ces services, dont certains se chevauchent. Les organisations peuvent utiliser toutes ces ressources ou seulement certaines d'entre elles, en fonction de leurs exigences.

1 Le Mobile Device Management (MDM)

Est une technologie sous-jacente gérant à distance le cycle de vie des appareils mobiles et leurs plateformes respectives. Les solutions MDM impliquent généralement l'installation de profils uniques sur les appareils mobiles, ce qui permet aux organisations d'effectuer un contrôle et un cryptage à distance sur les smartphones et tablettes et de leur appliquer des règles déterminées. Ils peuvent par exemple s'utiliser pour effacer toutes les applications et données d'un appareil en cas de perte ou de vol de ce dernier[1]. La technologie MDM permet aussi aux sociétés de disposer d'instantanés en temps réel de l'inventaire, du provisioning ou de la configuration du SE d'un appareil et offre aussi une visualisation ainsi que des outils de contrôle à distance en cas de panne.

2 Les outils Mobile Application Management (MAM)

Permettent aux organisations de gérer leurs applications mobiles en lieu et place de solutions matérielles. Les solutions MAM couvrent le déploiement et la mise à jour des applications mobiles, en ce compris le support administratif et la gestion des licences d'application. Elles permettent aussi aux organisations d'appliquer des politiques de sécurité et de contrôle à ces applications, en les retirant de manière individuelle et sélective - avec les données associées - d'un appareil spécifique. Les informations d'entreprise peuvent donc être protégées, sans devoir effacer entièrement le contenu d'un appareil. Les outils MAM peuvent également fournir des fonctions d'analyse pour aider les administrateurs et les propriétaires d'applications à comprendre les modes de consommation.

[1] De 2011 à 2016, la SNCB a rapporté 17.589 GSM qui ont été trouvés dans les trains.

3 La solution Mobile Content Management (MCM)

Permet aux professionnels d'accéder au contenu des appareils mobiles. Selon Gartner[2], elle joue trois grands rôles. L'un d'entre eux consiste à imposer des règles, par exemple l'accès conditionnel aux fichiers joints aux e-mails, la synchronisation de fichiers avec un répertoire de back-end ou encore avec un répertoire dans le cloud. Les outils MCM jouent également un rôle de fourniture de contenu. En d'autres termes, ils appliquent des règles de distribution, de remplacement et de suppression de fichiers commandées par le serveur. L'intégration est un autre rôle dévolu au Mobile Content Management : outre les règles de base relatives à l'accès aux fichiers, les outils MCM ajoutent également une compatibilité mobile pour les systèmes de gestion de droits de tiers ainsi que des solutions de protection contre les pertes de données d'entreprise (Data Loss Protection - DLP) et de gestion de droits digitaux d'entreprise (Enterprise Digital Rights Management - EDRM).

[2] Gartner, Magic Quadrant for Enterprise Mobility Management Suites, 6 juin 2017

L'Enterprise Mobility Management une solution qui se généralise

Les fournisseurs ont différentes manières d'aborder la gestion du cycle de vie mobile. Par ailleurs, les besoins des organisations varient fortement d'un secteur à l'autre. La plupart des clients utilisent des fonctions MDM, MAM et MCM. D'autres, comme les solutions Mobile Identity et Access Management (MIA), Mobile Information Management (MIM), Mobile Expense Management (MEM) et Containment, pour n'en citer que quelques-unes, ne sont utilisées que par une fraction plus restreinte d'entre eux.

Unified Endpoint Management (UEM)

Et pourtant, l'EMM évolue au-delà de son champ d'application initial (les appareils mobiles, les applications et la gestion de contenu). Une fusion s'opère en effet entre l'informatique client et l'informatique mobile pour former des groupes informatiques d'utilisateurs finaux. "La définition de l'EMM évolue. Autrefois utilisée pour désigner essentiellement la gestion des appareils et applications mobiles, la notion d'EMM évoque davantage aujourd'hui les outils au service de la mobilité au sens large – en y englobant les appareils Windows 10 et MacOS", explique David Johnson, analyste principal chez Forrester Research[3].

Ainsi est né le besoin d'une solution unique, permettant de gérer à la fois les appareils traditionnels du client et les appareils mobiles. Microsoft et Apple ont ajouté des API MDM à leurs plateformes pour faciliter cette convergence. Le principal défi inhérent à la mise en œuvre de la solution Unified Endpoint Management est lié aux exigences historiques auxquelles sont généralement confrontées les organisations, comme des applications Win32 et des GPO Windows complexes, que les outils EMM ne permettent pas de gérer à l'heure actuelle. Toutefois, des changements s'esquissent, qui permettront de plus en plus à ces outils EMM de gérer les PC. Tout d'abord, Microsoft continue à améliorer les API MDM sous Windows 10, comblant ce faisant le retard par rapport aux GPO. Ensuite, les fournisseurs de solutions EMM proposent des fonctionnalités propriétaires pour combler ces lacunes dans des domaines tels que les règles de sécurité, la gestion de scripts et le déploiement d'applications Win32.

> "l'EMM s'étend à la gestion unifiée des points terminaux, combinant des fonctions EMM avec des PC et des ordinateurs portables du client, et ce, dans une double perspective : appareils de l'entreprise et BYOD. Les plateformes EMM s'étendent aussi aux points terminaux connectés non traditionnels, tels que les objets connectés portables (wearables), l'affichage numérique, les kiosques et d'autres scénarios liés à l'IoT."[4]
>
> **Phil Hochmuth**, Enterprise Mobility Research Program Director chez IDC

On notera toutefois que tous les objets IoT n'entrent pas dans le champ d'application des outils EMM. Certains appareils seront gérés directement par les constructeurs ou disposeront d'outils de gestion propres. Et beaucoup d'appareils n'auront tout simplement pas besoin d'être gérés. Quoi qu'il en soit, il est clair que la diversité et le nombre d'appareils continueront à croître et les organisations IT doivent s'y préparer.

[3] Matt Kapko, What is EMM? Enterprise Mobility Management explained, Computerworld, 9 octobre 2017
[4] Phil Hochmuth, IDC MarketScape: Worldwide Enterprise Mobility Management Software 2017 Vendor Assessment, août 2017

Protéger votre entreprise **des menaces mobiles**

L'application de règles ne suffira pas indéfiniment pour répondre aux enjeux inhérents à la sécurité mobile. Selon Dionisio Zumerle, Research Director pour la sécurité mobile chez Gartner[5].

Mobile Threat Protection (MTP)

En fonction du secteur, des réglementations en vigueur, de la sensibilité des données, des cas d'utilisation spécifiques et de la culture en matière de risque, les organisations ont intérêt à envisager sérieusement d'adopter des solutions Mobile Threat Protection solutions, progressivement, mais sans attendre. Des organes hautement réglementés, à l'instar des institutions financières, et des organisations sensibles, comme les infrastructures de soins de santé, feraient bien d'adopter plus vite encore les solutions MTP.

En dépit de la croissance, en termes d'adoption, du marché de la protection contre les menaces mobiles, une grande confusion et de nombreux points d'interrogation subsistent chez les utilisateurs finaux quant aux risques traités précisément par les solutions MTP et à l'urgence ou l'utilité éventuelles de ces dernières. Naturellement, la détection des menaces mobiles et la défense à leur opposer n'ont rien d'une sinécure : pour être efficace, la technologie doit couvrir l'utilisateur, l'application, l'appareil (téléphones et tablettes iOS et Android) et les menaces pesant sur le réseau.

Les solutions MTP ne doivent pas seulement être en mesure de détecter les comportements insolites en traçant les modèles de comportement attendus ou acceptables, mais aussi d'inspecter les appareils mobiles pour y identifier les défauts de configuration susceptibles d'ouvrir un accès aux programmes malveillants. Les systèmes MTP doivent permettre de surveiller le trafic sur le réseau, de désactiver les connexions suspectes et de scanner les applications pour identifier celles d'entre elles susceptibles de compromettre la sécurité des données d'entreprise.

Et par-dessus tout, les organisations IT doivent veiller à sélectionner une solution MTP capable d'intégrer de manière optimale leurs outils EMM.

Les programmes malveillants mobiles ont augmenté de plus de

100 %

en glissement continu en 2016, représentant environ

7,5 %

de tous les programmes malveillants

(Source : AV-TEST T Security Report 2015/16)

[5] Gartner, *Market Guide for Mobile Threat Defense Solutions*, 22 août 2017

Proximus Enterprise Mobility Management

Les solutions EMM représentent, chez Proximus, le point d'intégration central des réglementations en matière mobile. Pierre angulaire de la gestion des ressources mobiles au niveau de l'entreprise, **Proximus EMM** est la plateforme privilégiée pour **fédérer les règles relatives aux autres services et outils.**

Grâce à ses solides capacités d'intégration avec des composantes d'infrastructure de tiers, notre solution EMM offre une base commune, interplateformes pour la définition, l'hébergement, la validation, l'application et la mise à jour des **règles relatives aux appareils pour un large éventail d'outils et services** : passerelles, proxies, VPN, contrôles et certificats d'accès réseau, systèmes de gestion des contenus et des droits, gestion d'identité et d'accès, contrôles de versions et back-ups ou encore initialisation et nettoyage de contenu d'appareils.

Interface unique en termes de règles et de responsabilités, Proximus EMM permet d'éviter une inflation du nombre d'agents et une pléthore d'utilitaires ajoutés monopolisant les ressources locales et compliquant du même coup, pour les administrateurs système, la tâche de coordination des règles.

Proximus EMM comprend également une fonctionnalité supplémentaire offrant un accès conditionnel à des référentiels en mode cloud (MI Access). À la différence des approches classiques en matière de sécurité, notre solution corrèle l'identité de l'utilisateur avec des informations uniques telles que le statut de l'appareil et de l'application. Proximus EMM conserve les données d'entreprise dans certaines limites IT pour éviter leur stockage sur des appareils non sécurisés ainsi que toute connexion à des applications non gérées ou tout partage d'informations avec des services de cloud non autorisés.

Notre solution EMM permet aux organisations de profiter d'une approche basée sur des normes et apte à sécuriser n'importe quel service de cloud, Office 365 compris, sans avoir besoin d'intégration propriétaire.

1 La composante MDM

La composante **MDM** de notre solution constitue la pierre angulaire de toute solution EMM. Grâce à elle, **IT permet au personnel de travailler de manière productive sur leurs appareils mobiles et ordinateurs de bureau de prédilection**, de sécuriser et gérer les appareils mobiles et les ordinateurs de bureau sur des systèmes d'exploitation multiples (dont Android, iOS, MacOS et Windows 10), de fournir des e-mails d'entreprise sécurisés, une configuration automatique des appareils et une sécurité basée sur certificat. Notre solution MDM permet aux administrateurs d'effacer de manière sélective les données d'entreprise se trouvant sur des appareils mobiles et des ordinateurs de bureau sans affecter les données personnelles.

2 Les fonctions MAM

Les fonctions **MAM** permettent à IT de **constituer et maintenir un catalogue d'applications d'entreprise**, de sécuriser des applications sur n'importe quel appareil, d'authentifier des utilisateurs finaux sur l'appareil et de séparer applications d'entreprise et applications personnelles sur les appareils mobiles et les ordinateurs de bureau.

3 Le module MCM

Le module **MCM** permet à IT de **sécuriser des données d'entreprise sur des appareils mobiles et des ordinateurs de bureau** sans compromettre l'expérience de l'utilisateur final. Les utilisateurs peuvent ainsi, d'une manière intuitive, accéder à des documents provenant d'un e-mail, de SharePoint ou d'autres systèmes de gestion de contenus d'entreprise de même qu'à des services de cloud d'entreprise ou personnel, les annoter et les partager.

Toutes les parties prenantes au sein de votre entreprise profitent des avantages de Proximus EMM.

Avantages pour l'entreprise : sécurité et compliance

- Aide votre organisation à se conformer au Règlement général sur la protection des données de l'UE (RGPD)
- Évite que toute donnée critique ne se retrouve dans de mauvaises mains en cas de perte ou de vol d'appareil
- Évite tout risque de fuite de données, intentionnelle ou non, vers des tiers
- Vos collaborateurs n'ont accès qu'aux données auxquelles ils ont le droit d'accéder

Avantages pour le personnel IT : contrôle et convivialité

- Gestion simple et sûre du parc d'appareils
- Déploiement efficace d'appareils mobiles préconfigurés
- Propose un aperçu de tous les appareils mobiles dans votre organisation, de l'endroit où ils se trouvent et de leurs utilisateurs
- Permet de rassembler des groupes d'utilisateurs et des appareils mobiles et de leur assigner des règles sans devoir le faire de manière individuelle pour chaque appareil ou chaque utilisateur

Avantages pour le collaborateur : bon équilibre entre sécurité, expérience d'utilisateur et productivité

- Permet à votre personnel de travailler de manière sécurisée de n'importe où

Proximus Unified Endpoint Management

Si les fonctions EMM permettent déjà de résoudre la plupart des cas utilisateur les plus classiques au niveau de la gestion de PC, il restait jusqu'à présent quelques lacunes dans le modèle EMM, qui empêchaient IT de se passer des outils traditionnels de gestion de PC.

Proximus UEM réconcilie les mondes du mobile et de l'ordinateur de bureau. Cette solution, qui enrichit les fonctions EMM, offre aux équipes IT une manière simplifiée de **moderniser la sécurité et la gestion sous Windows 10** sans renoncer aux règles et actions granulaires qu'elles ont mises en place au cours des 20 dernières années.

Notre solution UEM permet aux organisations IT de s'écarter de plus en plus d'un modèle à deux vitesses coûteux et complexe, dans lequel les PC sont gérés par des outils traditionnels tandis que les appareils mobiles sont gérés par des outils modernes. Des scripts utilisant les GPO peuvent à présent coexister avec des profils EMM, sans devoir faire appel à des outils traditionnels de gestion de PC. Toutes les commandes peuvent désormais utiliser le protocole EMM pour envoyer des informations à l'appareil, qu'il s'agisse d'un script ou d'une API EMM. En d'autres termes, les organisations IT peuvent consacrer tous leurs efforts à la hausse de la productivité de l'organisation, avec à la clé une efficience et une agilité accrues et à moindre coût, et ce, sans devoir transiger sur la sécurité des appareils des utilisateurs itinérants que l'on trouve dans l'entreprise moderne.

Avantages

Proximus UEM permet aux équipes IT :

- D'avoir un contrôle complet des PC avec EMM
- De gérer des PC à distance, over-the-air
- De limiter le besoin d'images de desktops
- D'utiliser les commandes basées sur GPO avec des scripts PowerShell déployés par EMM
- De modifier et gérer facilement le registre
- De déployer sans effort des apps Win32 encapsulées non-MSI
- D'avoir une meilleure visibilité du système de fichiers

Proximus UEM déverrouille désormais des possibilités de gestion de PC auparavant impossibles avec EMM. Par exemple :

- Définir un appareil périphérique
- Créer des raccourcis sur le bureau
- Déterminer le matériel raccordé à l'appareil
- Avoir une meilleure visibilité des logiciels sur l'appareil
- Voir quels fichiers se trouvent dans un dossier
- Disposer d'une visibilité accrue dans le registre
- Apporter des modifications au registre
- Supprimer des logiciels inutiles ou indésirables sur l'appareil, même s'il s'agit d'une application système

Proximus Mobile Threat Protection

Les solutions EMM permettent de gérer et d'appliquer des règles, mais ne sont pas conçues pour régler spécifiquement le statut de sécurité d'un appareil mobile. En effet, elles ne fournissent pas d'informations relatives aux menaces, pas plus qu'elles ne détectent les programmes malveillants.

Et pourtant, les menaces mobiles gagnent en importance et le nombre de programmes malveillants dans les App Stores est en hausse. Les enjeux sont plus élevés que jamais :

> Le coût moyen d'une violation de données d'entreprise a été estimé à 18.000 EUR par jour par l'Institut Ponemon[6].

Proximus MTP utilise la détection d'applications malveillantes pour identifier des menaces connues et inconnues en appliquant l'émulation de menace, l'analyse avancée de code statique, la réputation d'application et l'apprentissage automatique. Sa réponse dynamique aux menaces permet d'empêcher les appareils compromis d'accéder au réseau de votre entreprise, tout en permettant à cette dernière de définir un certain nombre de contrôles de règles adaptables.

Proximus MTP permet aux équipes IT et Security :

- D'effectuer une analyse d'application avancée pour détecter les menaces, connues ou non
- De surveiller l'activité sur le réseau pour y détecter les comportements suspects ou malveillants
- D'évaluer les vulnérabilités au niveau de l'appareil (OS) pour réduire la surface d'attaque
- De détecter et de bloquer les attaques lancées sous forme de phishing par SMS et conçues pour voler des clés d'authentification d'entreprise

Proximus MTP n'a jamais d'impact sur les performances des appareils ni sur la durée de vie des batteries. L'essentiel de l'analyse de risque s'effectue en effet dans le cloud. L'application sur l'appareil fonctionne de manière transparente en arrière-plan jusqu'à ce qu'une activité malveillante soit détectée. À ce moment, elle alerte l'utilisateur final et l'invite à réagir.

[6] Ponemon Institute, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, octobre 2016

Intégration avec EMM

L'intégration transparente avec Proximus EMM – et aussi avec la plupart des solutions EMM sur le marché – permet à Proximus MTP de proposer une plateforme complète, ajoutant une couche critique de sécurité aux solutions Enterprise Mobility Management. Notre solution MTP peut s'utiliser pour modifier de manière dynamique les privilèges d'accès afin de refléter les niveaux de risque, en transformant les règles de gestion statique en une protection active des appareils.

Quel que soit le type d'appareils que compte votre parc mobile, l'intégration entre Proximus MTP et votre plateforme EMM s'opère d'une manière aussi rapide qu'aisée. Le déploiement et la gestion peuvent s'effectuer automatiquement via votre outil EMM, ce qui permet d'en accélérer l'adoption et de réduire les coûts opérationnels globaux. Notre solution évolue au rythme de votre outil EMM, protégeant de manière transparente les appareils mobiles ajoutés. De cette manière, vous êtes assuré de disposer des couches de sécurité dont vous avez besoin pour gérer et protéger vos appareils mobiles, même dans un environnement hautement dynamique.

Avantages

- Permet de déployer n'importe quel appareil mobile iOS ou Android dans le réseau de votre organisation en toute confiance
- Protège contre les tentatives d'espionnage les informations sensibles présentes sur les appareils mobiles
- Améliore la visibilité et la protection vis-à-vis des menaces mobiles les plus récentes, avec une sécurité mobile qui s'intègre aisément à vos infrastructures de mobilité et de sécurité existantes (MDM, MAM, NAC, SIEM, etc.)
- Renforce les mesures de sécurité de Microsoft Exchange et des solutions conteneur
- Permet de réagir rapidement aux attaques interplateformes prenant la forme d'une menace persistante avancée ou APT (Advanced Persistent Threat)
- Permet aux sous-traitants d'accéder en toute sécurité à des données d'entreprise à partir d'appareils non gérés
- Préserve l'expérience et la vie privée de l'utilisateur, tout en ajoutant la protection requise via des mandats aux niveaux réglementaire ou de l'organisation

Pourquoi choisir **Proximus** ?

L'adoption des smartphones devrait passer de 1,47 milliard d'appareils en 2016 à plus de 1,7 milliard en 2021[7]. Il est donc impératif pour les organisations de trouver une manière d'intégrer et de sécuriser rapidement le vaste éventail d'appareils avec lesquels le personnel vient travailler en entreprise.

Les atouts combinés des meilleurs fournisseurs de technologies, dont les **technologies MobileIron et CheckPoint**, et l'offre complète de services professionnels proposée par Proximus permettent aux organisations de profiter des avantages de solutions mobiles pouvant résolument revendiquer le label de 'classe business'.

Il n'existe pas d'approche standard en matière de gestion de mobilité d'entreprise, et le chemin menant à cette mobilité est semé d'embûches pour nombre d'entreprises. Proximus peut vous aider à envisager tous les scénarios mobiles possibles, à planifier les défis, à construire une stratégie solide, à utiliser les bonnes technologies, à mettre en place les règles adaptées et à tirer parti des meilleures pratiques pour faire de votre initiative mobile une réussite.

Les besoins peuvent varier fortement en fonction de la taille de l'entreprise et du type d'activité ou encore des conditions réglementaires, et les exigences EMM évoluent au fil de l'évolution des plateformes mobiles. Pour suivre tous ces changements, Proximus engage des experts afin de comprendre le paysage changeant dessiné par les appareils mobiles et les implications pour la gestion de la mobilité.

Proximus propose les solutions Enterprise Mobile Management dont les organisations ont besoin pour mieux servir leurs clients dans le monde digital d'aujourd'hui, ainsi que les services de consultance technique et les services gérés connexes. Proximus a également pour ambition de fournir des services de bout en bout, reposant sur des SLA clairs.

Nos solutions Enterprise Mobile Management vous permettent :
- D'éviter toute perte de données critiques, grâce à des solutions EMM et MTP robustes
- De réduire la complexité et diminuer les coûts
- De simplifier la gestion des données et les activités quotidiennes
- De diminuer votre empreinte IT grâce à une utilisation de ressources hautement efficace
- De comprendre comment réduire les risques et analyser les retours sur investissement pour justifier de futurs investissements
- D'évaluer la situation actuelle de votre entreprise et de développer une feuille de route pour supporter des initiatives futures
- D'améliorer les Service Level Agreements et l'efficacité de votre organisation

Nous menons en permanence des examens et des audits pour améliorer nos systèmes de gestion. Nous surveillons et analysons aussi nos résultats et les commentaires de nos clients, de notre personnel et d'autres parties prenantes pour identifier nos objectifs en matière de qualité, de sécurité et de protection ainsi que d'environnement.

[7] IDC, *Worldwide Quarterly Mobile Phone Tracker*, 29 août 2017

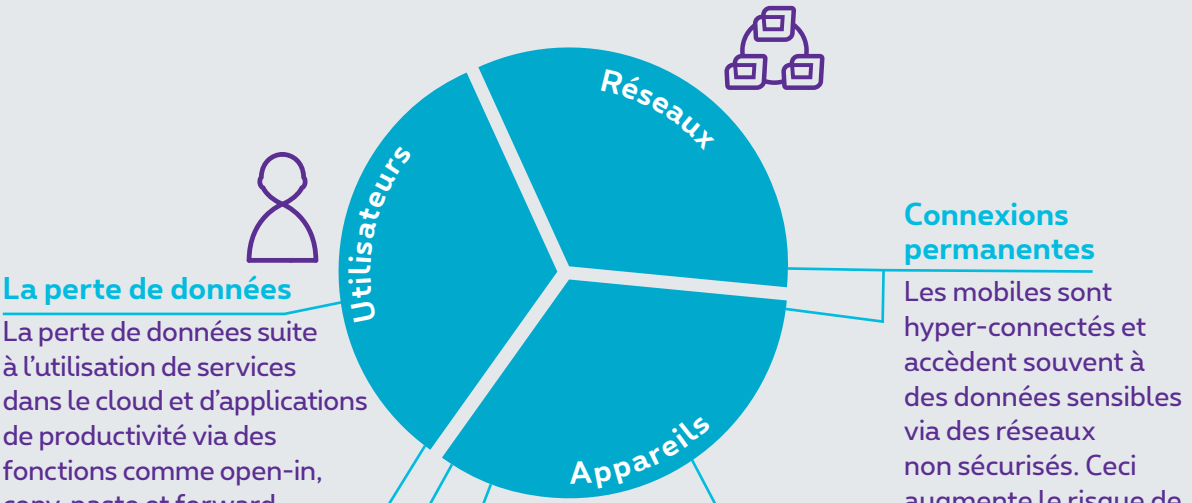
Infographiques et chiffres

Vecteurs de menace mobile

L'un des principaux défis mobiles à relever pour IT consiste à sécuriser les données et les applications – y compris celles de tiers – sur tous les appareils mobiles, sans impact sur l'expérience utilisateur native. Avant l'ère mobile, les principaux risques en matière de sécurité étaient les programmes malveillants et les virus, qui résultaient de la vulnérabilité des systèmes en 'open file' et d'un noyau non protégé. Aujourd'hui, les systèmes d'exploitation mobiles disposent d'un système de fichiers 'sandboxed' et d'un noyau protégé, qui ont rendu moins préoccupantes les menaces traditionnelles liées à la sécurité. Toutefois, les technologies mobiles font face à trois autres types de menaces : celles basées respectivement sur l'utilisateur, sur l'appareil et sur le réseau.

Les vecteurs de menace sur mobiles sont différents de ceux sur PC.

Les systèmes d'exploitation mobile 'sandboxed' sont sécurisés. Les menaces, comme les logiciels malveillants, sont réduites par le design OS. Empêcher la perte de données sur les mobiles requiert un focus sur différents vecteurs de risque.



La perte de données

La perte de données suite à l'utilisation de services dans le cloud et d'applications de productivité via des fonctions comme open-in, copy, paste et forward

Effraction d'appareils

Exploitation de vulnérabilités dans l'OS comme le jailbreak et le root d'appareils, le contournement de la sécurité, et l'installation d'applications malveillantes d'app stores non-authorisés

Applications malveillantes et risquées

Recueillir et partager des données comme les informations personnelles identifiables et localisation de l'appareil avec publicité par des tiers et systèmes d'analyse

Connexions permanentes

Les mobiles sont hyper-connectés et accèdent souvent à des données sensibles via des réseaux non sécurisés. Ceci augmente le risque de perte de données par Wi-Fi sniffing, points d'accès non fiables et les attaques Man-in-the-Middle (MitM)

Facteur de forme

Le facteur de forme portative fait que les appareils mobiles sont susceptibles à la perte ou au vol

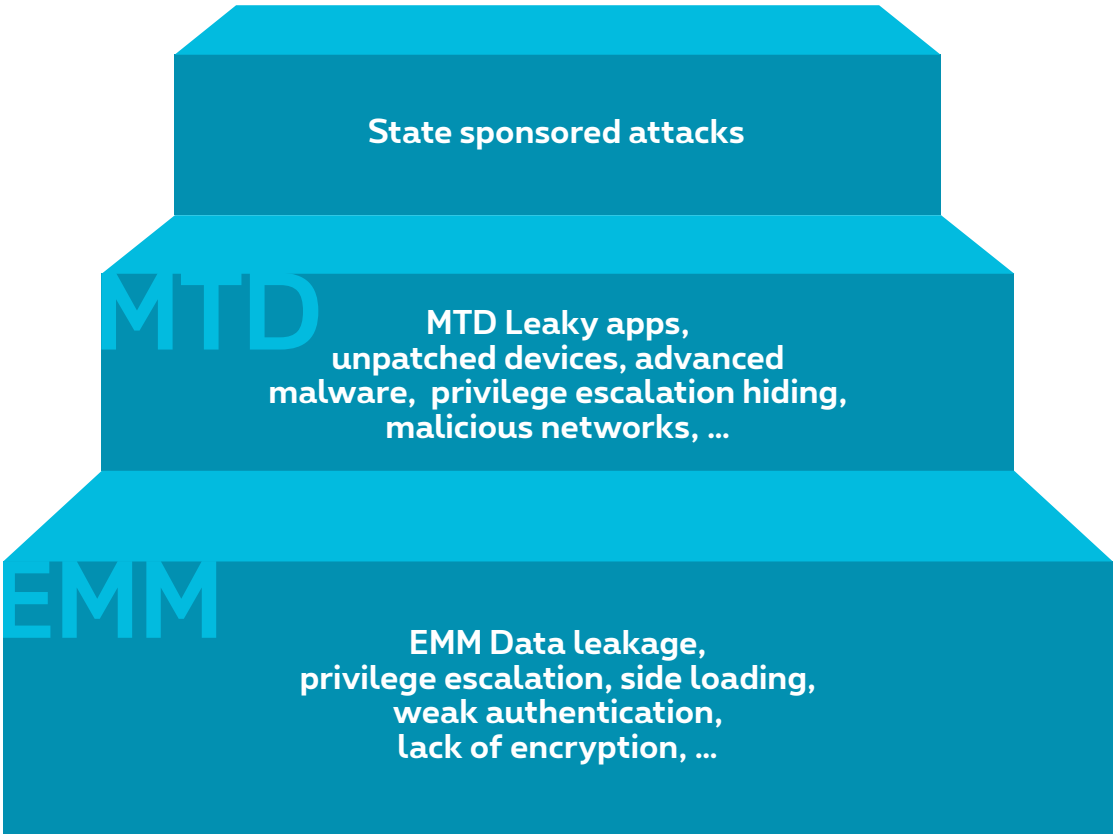
Source : MobileIron

Infographiques et chiffres

En mars 2017, pour la première fois, le nombre de connexions internet simultanées enregistrées sur Android a été supérieur au nombre enregistré sous Windows.

Source : StatCounter, Android overtakes Windows for first time, 3 avril 2017

Menaces liées à la sécurité mobile traitées par les technologies EMM et MTD



Source : Gartner, *Market Guide for mobile threat defense solutions*, 22 août 2017

Plus d'infos

Proximus est votre conseiller de confiance en matière de solutions mobiles pour tout ce qui touche à la sécurité et à la gestion des applications, données et services mobiles.
Rendez-vous sur **www.proximus.be** ou prenez contact avec votre Account Manager.