Cinq étapes pour appliquer une stratégie de protection contre les menaces mobiles

La protection de votre entreprise contre les menaces mobiles se joue contre la montre. Faites-vous tout votre possible pour vous protéger des attaques ?

Arrive-t-il à vos collaborateurs d'utiliser les réseaux Wi-Fi gratuits des aéroports, des hôtels ou des cafés ? Et les ports USB ? Comment pouvez-vous être sûr que les appareils de vos collaborateurs sont protégés des attaques de type « man-in-the-middle » (MITM) ou d'une tentative de vol de leurs identifiants professionnels par un pirate ? Avez-vous mis en place une stratégie pour reconnaître et bloquer ce type d'attaques ?

Ce guide en cinq étapes vous aide à élaborer une stratégie basée sur des bonnes pratiques, qui vous assure des informations exploitables et une protection immédiate contre les menaces mobiles avancées dirigées vers votre personnel itinérant. Découvrez comment une solution embarquée de protection contre les menaces mobiles peut protéger vos appareils, vos applications et vos données des derniers risques de sécurité.

MobileIron

MKT FR-A4 v1.0

L'efficacité d'une stratégie de protection contre les menaces mobiles (Mobile Threat Defense, MTD) se joue contre la montre, car les attaques ciblant les appareils mobiles s'intensifient à vitesse grand V, tout comme leur niveau de gravité. Les organisations derrière ces attaques sont motivées par un but fort lucratif, qui les rend toujours plus tenaces et performantes dans leur domaine. Selon un rapport de sécurité publié en 2017 par le Ponemon Institute, les sociétés auraient 28 % de chances de subir une violation de données récurrente entraînant la perte d'au moins 1 000 dossiers contenant des informations personnelles de clients – informations de la plus haute valeur pour les cybercriminels[1]. Ce type d'attaques peut avoir des conséquences désastreuses : outre la perte ou la compromission de données, une violation de données fortement médiatisée peut nuire à vos relations clients et à la réputation de votre entreprise, générer une perte de revenus, induire des amendes et des frais de justice exorbitants, et aspirer un précieux capital temps et RH pour redresser la situation.

Si vous ne le faites pas déjà, l'heure est venue de faire tout votre possible pour protéger votre entreprise contre ce niveau de risque. Ces cinq bonnes pratiques vous aident à identifier vos lacunes en matière de sécurité et à garantir une protection complète sur tous les appareils mobiles ayant accès aux applications et aux données de l'entreprise, partout où travaillent vos collaborateurs, et quel que soit le réseau utilisé.

Paysage actuel des menaces mobiles

75 % DES ATTAQUES
SONT PERPÉTRÉES PAR DES PIRATES EXTÉRIEURS

81 % DES VIOLATIONS PAR PIRATAGE
EXPLOITENT DES MOTS DE PASSE VOLÉS

73 % DES VIOLATIONS
ONT UNE MOTIVATION FINANCIÈRE [2]

ICT Security Magazine, « 2017 Data Breach Investigations Report, 10th Edition »

1 https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states

2 https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

MobileIron

Étape 1
Activer une protection intégrée et invisible contre les menaces

Avec certaines solutions de sécurité mobile, la sécurisation des appareils mobiles repose entièrement sur les utilisateurs finaux, ce qui constitue une approche MTD peu raisonnable et inefficace. Ces solutions de « sécurité basée sur l'utilisateur » obligent chaque collaborateur mobile à aller dans le magasin d'applications de la société, à télécharger le client et à suivre les nombreuses étapes requises pour installer, activer et maintenir à jour l'application. Pire encore, une fois le client installé, l'équipe informatique n'a que très peu de contrôle sur l'application, puisque les utilisateurs peuvent la supprimer ou la désactiver à leur guise, exposant alors les données d'entreprise à tous les risques. Selon une étude, plus d'un tiers des sociétés ne parviendraient pas à sécuriser convenablement leurs appareils mobiles, ne disposant pas du budget ni des ressources nécessaires pour déployer systématiquement une sécurité avancée à l'échelle de l'organisation[3].

Les services informatiques sont souvent tributaires des utilisateurs pour l'activation des dernières applications de sécurité sur les appareils. Toutefois, si les utilisateurs ne mettent pas à jour leurs appareils, la société devient vulnérable aux attaques, les règles de sécurité n'étant pas respectées par tous les terminaux. Il n'est donc pas surprenant de lire, dans un rapport publié en 2017 par Dimensional Research, que « deux tiers des répondants déclarent avoir des doutes quant à la capacité de leur organisation à se protéger contre une cyberattaque mobile, alors même que la quasi-totalité des spécialistes de la sécurité prédit une explosion du nombre d'attaques mobiles »[4].

Afin de garantir une protection totale et immédiate sur chaque appareil mobile ayant accès aux ressources internes, les organisations doivent arrêter de dépendre des utilisateurs pour l'installation des dernières mises à jour. Pour déployer une sécurité mobile avancée de manière systématique, Gartner recommande aux organisations d'« intégrer la solution MTD avec l'outil de gestion de la mobilité en entreprise (Enterprise Mobility Management, EMM) »[5]. Dans cette approche, les administrateurs informatiques déploient la protection et les mises à jour de sécurité directement sur les appareils via la plateforme EMM. Les utilisateurs n'ont donc rien à faire pour télécharger et activer les dernières mises à jour de sécurité, et les règles de confidentialité sont respectées. Une solution intégrant EMM et MTD permet également à l'équipe informatique de se concentrer sur des priorités plus stratégiques et de réduire les coûts opérationnels en évitant aux administrateurs d'avoir à courir après les utilisateurs pour s'assurer de la conformité de leurs appareils.

« Deux tiers des répondants déclarent avoir des doutes quant à la capacité de leur organisation à se protéger contre une cyberattaque mobile, alors même que la quasi-totalité des spécialistes de la sécurité prédit une explosion du nombre d'attaques mobiles. »

– Dimensional Research,
« The Growing Threat of Mobile Security Breaches:
A Global Survey of Security Professionals »

3 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
4 https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
5 https://www.gartner.com/doc/3789664/market-guide-mobile-threat-defense

Étape 2
Voir tous les types de cyberattaques

Le manque de visibilité sur les menaces mobiles constitue l'un des plus grands défis de sécurité mobile pour les entreprises aujourd'hui. Plus de la moitié (51 %) des sociétés interrogées ont déclaré ne pas savoir si des logiciels malveillants avaient déjà été téléchargés sur les appareils mobiles utilisés par leurs collaborateurs[6]. En réalité, certaines solutions de sécurité mobile contribuent à ce manque de visibilité en se concentrant uniquement sur les menaces applicatives. Pourtant, toutes les cyberattaques ne se ressemblent pas. Il existe plusieurs types de vecteurs d'attaque capables de contourner cette approche étroite par d'autres subterfuges. Les organisations ne peuvent donc pas se concentrer sur un seul niveau, mais doivent assurer une sécurité mobile complète et entièrement intégrée pour se protéger des attaques ciblant les appareils, les réseaux et les applications.

- **Attaques au niveau de l'appareil :** Cette catégorie regroupe certaines des menaces les plus graves, car, en cas de réussite, les pirates peuvent prendre le contrôle total de l'appareil et en extraire du contenu chiffré. Les attaques au niveau de l'appareil se font souvent via le téléchargement d'une application gratuite ou un SMS qui lance un logiciel malveillant dès son ouverture par l'utilisateur.
- **Attaques au niveau du réseau :** Bien qu'utiles et pratiques, les réseaux publics sont également une porte ouverte vers les appareils mobiles pour les attaques. Par exemple, un point d'accès non autorisé provenant d'un réseau Wi-Fi gratuit dans un hôtel ou un café peut lancer une attaque de type MITM et intercepter des communications entre l'appareil et le réseau d'entreprise. Le pirate peut alors rapidement analyser l'appareil à la recherche d'éventuelles failles connues à exploiter pour le compromettre, collecter des noms d'utilisateur, des mots de passe et des données internes confidentielles qu'il pourra utiliser plus tard pour accéder aux ressources de l'entreprise.
- **Attaques au niveau de l'application :** Ces attaques se produisent généralement lorsqu'un utilisateur peu méfiant installe une application depuis un magasin d'applications tiers. L'application contient un logiciel malveillant qui peut accéder aux autorisations, exécuter une attaque sur l'appareil et s'infiltrer sur le réseau interne pour voler des données d'entreprise.

Les solutions qui exploitent des algorithmes d'apprentissage automatique sophistiqués et une détection basée sur le comportement sur l'appareil mobile permettent aux organisations de bloquer ce type d'attaques connues et inconnues (« zero day »). Au lieu de se concentrer sur le seul vecteur de menace de niveau applicatif, les outils à apprentissage automatique reconnaissent et bloquent instantanément toute activité anormale, telle que la configuration non autorisée d'un VPN ou le téléchargement d'une application gratuite.

« Plus de la moitié (51 %) des sociétés interrogées ont déclaré ne pas savoir si des logiciels malveillants avaient déjà été téléchargés sur les appareils mobiles utilisés par leurs collaborateurs. »

– Zimperium,
« Mobile Security 2017 Spotlight Report »

6 http://go.zimperium.com/2017-mobile-security-report

Étape 3
Fournir des informations exploitables sur les menaces

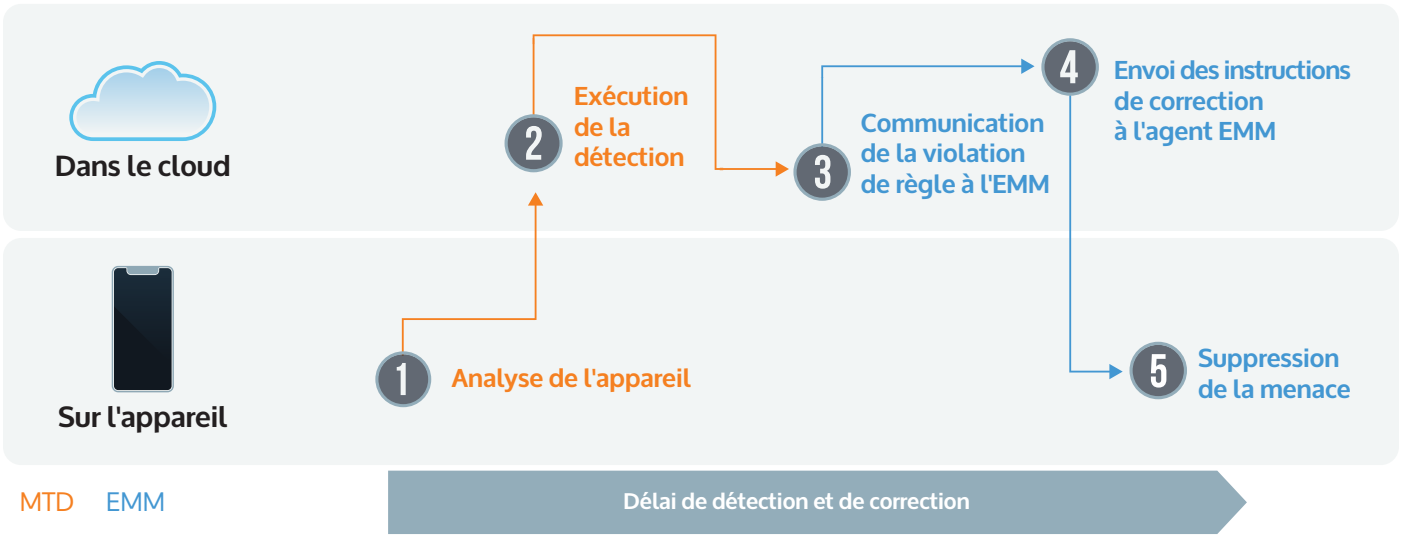
Au même titre que le manque de visibilité, un déferlement d'alertes attribuant la même priorité à toutes les menaces peut créer des zones d'ombre en matière de sécurité. Une telle situation peut générer une « fatigue des alertes » et ralentir le processus décisionnel des administrateurs de la sécurité mobile.

Pour produire des informations exploitables sur les menaces, les solutions MTD doivent intégrer un moteur d'analyse utilisant des algorithmes d'apprentissage automatique pour discerner les comportements normaux des comportements malveillants sur l'appareil même. Via l'analyse des écarts légers au niveau des statistiques d'OS, de la mémoire, du processeur et d'autres paramètres système de l'appareil mobile, l'apprentissage automatique identifie avec précision le type spécifique d'attaque malveillante, tout en fournissant des informations détaillées sur l'auteur, la nature, le lieu, la date et le fonctionnement de l'attaque.

Embarquées sur l'appareil, les solutions à apprentissage automatique détectent les attaques même lorsque l'utilisateur n'est pas connecté au réseau et même s'il s'agit d'un logiciel malveillant inconnu, d'une nouvelle menace ou d'une attaque « zero day ». Par ailleurs, ce type de solution s'avère plus rapide que les solutions basées sur le cloud, le tunneling du trafic via le cloud n'étant pas nécessaire. Les experts de la sécurité mobile peuvent identifier rapidement les menaces imminentes, les classer par priorité et prendre des mesures immédiates pour empêcher qu'une attaque grave ne permette au pirate d'accéder aux ressources de l'entreprise.

Détection et correction

Autres solutions MTD et EMM

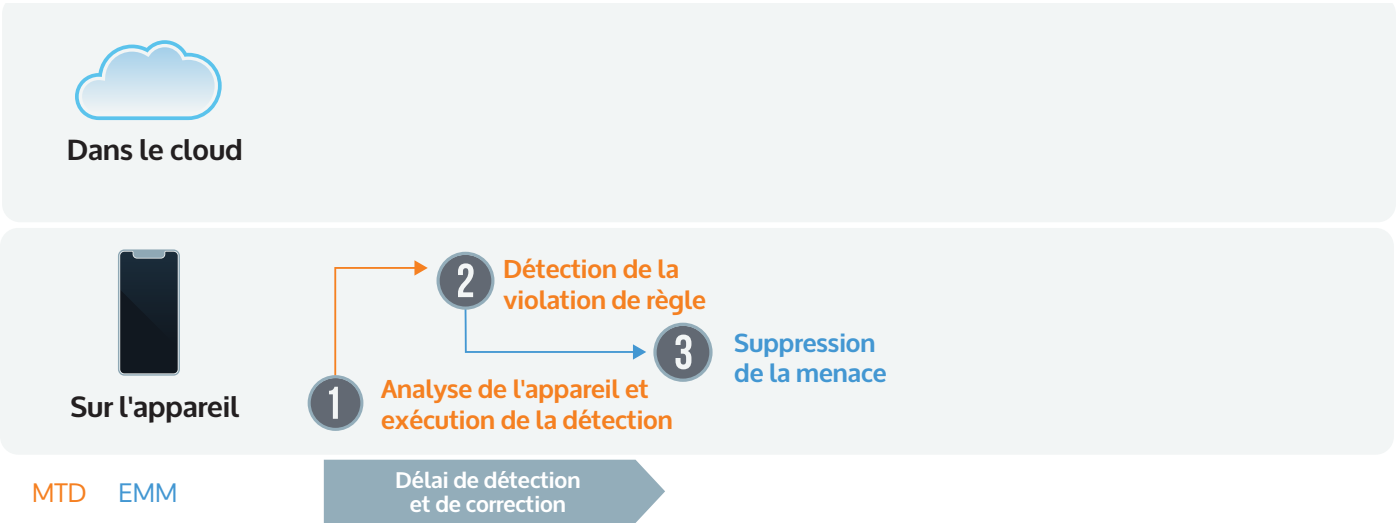


Étape 4
Corriger les menaces à la vitesse de l'appareil

Les attaques se produisent à la vitesse de l'appareil. Il est donc indispensable que la solution de sécurité intégrée réagisse à la même vitesse. Les solutions MTD basées uniquement sur le cloud peuvent retarder la détection et la correction des menaces mobiles sur l'appareil, car elles doivent tout d'abord analyser ce dernier puis envoyer des alertes à partir du cloud afin d'informer la plateforme EMM d'une violation de sécurité. Cela peut entraîner un retard de réaction critique pour contrer une attaque potentiellement dévastatrice, telle qu'une attaque MITM, qui peut frapper un appareil via un accès Wi-Fi gratuit. Dans ce type de situation, le pirate lance une attaque qui compromet l'appareil mobile et lui procure davantage de contrôle sur ce dernier que n'en a l'utilisateur même. Par exemple, le pirate peut télécharger la totalité des contacts de l'utilisateur, voler des messages électroniques et se connecter sous l'identité de l'utilisateur pour envoyer un e-mail d'hameçonnage au PDG, ce qui peut provoquer une faille de sécurité majeure à l'échelle de la société.

Une solution MTD embarquée sur l'appareil réagit aux menaces à la vitesse de l'appareil, car elle ne nécessite aucune étape supplémentaire pour détecter et corriger les éventuelles menaces. Résidant sur l'appareil même, la solution détecte les violations de règle et bloque les menaces, notamment les menaces MITM, instantanément sur l'appareil. Dans cette course contre la montre, ce système vous confère un avantage décisif sur les pirates et vous évite de sérieux problèmes en chaîne.

Détection et correction
Solution MobileIron Threat Defense



Étape 5
Des rapports détaillés pour faciliter la conformité

Afin de respecter les obligations réglementaires applicables, telles que le Règlement général sur la protection des données (RGPD), la norme PCI Data Security Standard (PCI DSS), la loi Health Insurance Portability and Accountability Act (HIPAA) ou le dispositif Notifiable Data Breaches (NDB), pour ne citer que quelques exemples, toute entreprise internationale doit mettre en place des processus d'audit et de reporting clairs.

Pour les entreprises mobiles, cette exigence est d'autant plus difficile à respecter que les utilisateurs ne sont plus attachés à des ordinateurs de bureau contrôlés par le service informatique : ils accèdent aux applications et données de l'entreprise depuis tout un éventail d'appareils mobiles personnels et professionnels, via divers réseaux. Comme le souligne un rapport : « Afin de respecter le RGPD, l'un des défis sera de sécuriser les informations d'identification personnelles (IIP) présentes sur les ordinateurs portables et d'autres appareils mobiles. Non protégées par le pare-feu de la société, ces données sont plus difficiles à surveiller et plus exposées aux attaques. »[7]

Pour respecter les exigences de conformité, il est crucial de pouvoir surveiller et gérer l'ensemble des appareils et des applications, afin d'avoir en permanence une vision claire des menaces et des risques mobiles. Grâce à la génération rapide de rapports d'audit, à la consultation des journaux des menaces et au suivi des historiques détaillés d'accès et d'utilisation, les administrateurs peuvent rapidement identifier les vulnérabilités potentielles et garantir la conformité de la totalité des utilisateurs, appareils et applications. Cette approche permet aux entreprises de garantir le respect des directives de conformité, en s'assurant que tout est mis en œuvre pour protéger l'organisation des risques mobiles.

« Afin de respecter le RGPD, l'un des défis sera de sécuriser les informations d'identification personnelles (IIP) présentes sur les ordinateurs portables et d'autres appareils mobiles. Non protégées par le pare-feu de la société, ces données sont plus difficiles à surveiller et plus exposées aux attaques. »

RGPD : Rapport « GDPR Compliance for Mobile Workers », octobre 2017

7 https://gdpr.report/news/2017/10/13/gdpr-compliance-mobile-workers

MobileIron THREAT DEFENSE

MobileIron Threat Defense : la solution pour une sécurité mobile embarquée, simple et intelligente

Chez MobileIron, nous savons que les cybercriminels inventent sans cesse des techniques toujours plus sophistiquées pour voler vos données par tous les moyens. C'est pourquoi nous nous engageons à innover constamment et à proposer de nouvelles solutions qui permettent à nos clients de gagner la course contre la montre face aux dernières menaces de sécurité mobile. Au cœur de cet engagement, MobileIron Threat Defense vous accompagne au cours des cinq étapes essentielles du déploiement d'une sécurité mobile embarquée avancée. Notre solution se présente sous la forme d'une seule et unique application intégrée, qui offre plusieurs avantages majeurs :

- Une seule et unique application de protection contre les menaces, entièrement intégrée à la plateforme EMM
- Aucune action requise de l'utilisateur pour l'activation ou la mise à jour de la sécurité sur l'appareil
- Blocage des menaces connues et « zero day » sur les appareils iOS et Android, même hors connexion, grâce au dispositif de sécurité mobile avancée
- Détection et correction instantanées de tout type de menaces sur l'appareil grâce aux algorithmes d'apprentissage automatique

Vous disposez ainsi d'une solution de sécurité embarquée, simple et intelligente, qui fournit des informations exploitables et une protection immédiate contre les menaces à tous les niveaux (appareils, réseaux et applications) pour l'ensemble de votre personnel mobile. Vous pouvez alors mettre en œuvre une stratégie de sécurité mobile moderne, qui s'appuie sur la base déjà solide de la plateforme EMM pour fournir ces protections supplémentaires contre les menaces mobiles. À la clé pour vous, plus de temps à consacrer à l'essentiel : veiller à la productivité de vos collaborateurs mobiles et assurer à votre entreprise un avantage concurrentiel, notamment sur le plan de l'innovation.

Pour en savoir plus sur notre solution entièrement intégrée de détection et de correction des menaces, rendez-vous sur www.mobileiron.com/threatdefense.

MobileIron

401 East Middlefield Road
Mountain View, CA 94043, États-Unis
globalsales@mobileiron.com
www.mobileiron.com
Tél. : +1 877 819 3451
Fax : +1 650 919 8006