ManageEngine
Mobile Device Manager Plus

Résolvez ces **10 problèmes de sécurité des périphériques mobiles** avec le MDM

Introduction

La pandémie a profondément modifié les pratiques d'entreprise traditionnelles, entraînant la création généralisée de forces de travail hybrides qui opèrent à la fois sur site et à distance. Il est indéniable que les périphériques mobiles tels que les ordinateurs portables, les smartphones et les tablettes sont devenus les outils privilégiés de ces équipes pour accomplir leurs tâches. Cependant, ces périphériques peuvent être vulnérables à plusieurs menaces de sécurité, ce qui pose un problème urgent lorsqu'ils sont utilisés pour accéder et stocker des données sensibles de l'entreprise.

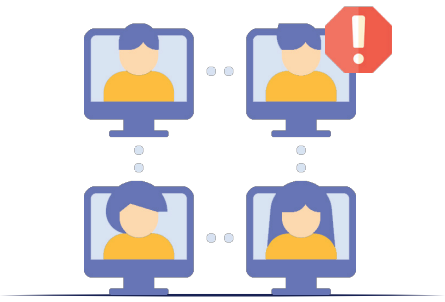
Un paysage de menaces en constante évolution

L'adoption de la culture du travail hybride dans divers secteurs a poussé les organisations de toutes tailles à se tourner vers la transformation numérique. Cela, associé à l'utilisation accrue des périphériques mobiles par les employés, a élargi la surface d'attaque des entreprises, les exposant davantage aux cybercriminels. Selon le rapport sur la sécurité mobile de Check Point de 2021, 97% des entreprises ont été confrontées à des menaces mobiles l'année dernière.

Les administrateurs informatiques ont maintenant la lourde tâche de garantir que tous ces points d'accès sont suffisamment sécurisés pour gérer les données de l'entreprise. Cependant, ce n'est pas une tâche facile. Voici quelques-uns des problèmes courants de sécurité des périphériques mobiles auxquels les administrateurs doivent faire face :

01

Les complexités du télétravail

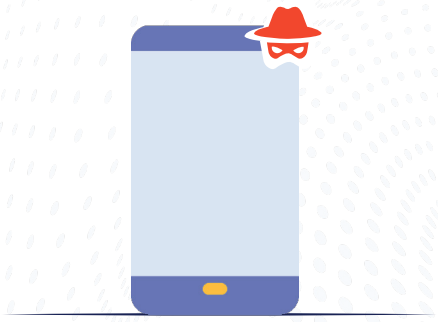


Les travailleurs à distance se connectent souvent aux réseaux Wi-Fi publics pour travailler, simplement parce que c'est plus pratique. Cependant, comme ces réseaux sont partagés et généralement peu sûrs, s'y connecter peut servir d'invitation ouverte aux pirates pour exploiter le périphérique et les données transmises.

En fait, l'année dernière, l'Agence nationale de sécurité a conseillé aux employés d'éviter de se connecter à ces types de réseaux en raison des menaces qu'ils représentent. Ces menaces peuvent inclure un pirate écoutant passivement et collectant des données sensibles, manipulant activement les informations transmises, ou volant les identifiants professionnels de l'employé connecté au réseau. Tout cela peut entraîner une violation de données.

02

Exploitation des fonctionnalités des périphériques intelligents



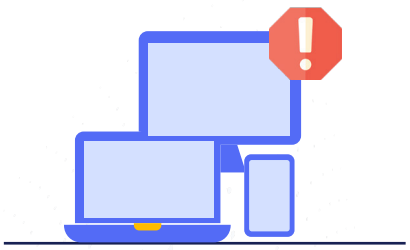
Les périphériques mobiles possèdent plusieurs fonctionnalités intégrées, et les fabricants de smartphones ont conçu des mesures pour s'assurer que ces fonctions ne sont activées que si nécessaire.

Cependant, si un appareil de travail est compromis, ces fonctionnalités peuvent être activées discrètement et utilisées par des personnes malveillantes pour consulter des fichiers sensibles ou écouter des discussions confidentielles.

De plus, les applications installées sur les périphériques intelligents nécessitent souvent des autorisations pour accéder à ces fonctionnalités. Un employé peut choisir d'accorder toutes les autorisations lors de l'installation, permettant ainsi aux applications d'accéder à ces fonctionnalités à tout moment. Dans ce cas, des risques de sécurité peuvent survenir si le développeur de l'application choisit de collecter des données sensibles ou si des personnes malintentionnées exploitent les vulnérabilités de l'application pour faire de même.

03

Confidentialité et sécurité du BYOD



Avec les premiers confinements qui ont obligé les employés du monde entier à travailler de chez eux du jour au lendemain, beaucoup ont choisi d'utiliser leurs propres périphériques pour accomplir leurs tâches professionnelles.

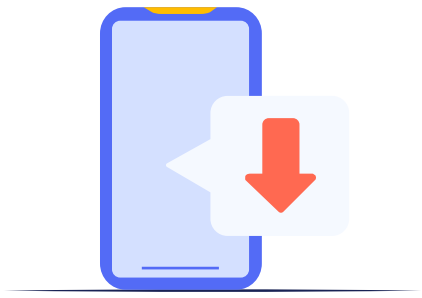
Une étude de Gartner a révélé que 55 % des employés ont utilisé leurs périphériques personnels à des fins professionnelles lorsqu'ils travaillaient à domicile.

Il peut être difficile de surveiller les données d'entreprise sur un périphérique personnel tout en respectant l'espace privé de l'employé. Une surveillance complète du périphérique peut violer la vie privée, alors que l'absence de surveillance peut compromettre la sécurité des données de l'entreprise.

Par exemple, si les employés peuvent utiliser leurs périphériques sans restriction, il n'y aurait quasiment aucune distinction entre les données personnelles et professionnelles sur le périphériquel. Cela pourrait entraîner le partage de données sensibles avec des utilisateurs non autorisés et des applications installées par l'employé. De plus, si l'employé quitte l'entreprise, l'administrateur informatique devra effacer les données professionnelles du périphérique, mais l'employé pourrait ne pas accepter, car cela supprimerait également ses fichiers personnels.

04

L'essor de l'informatique parallèle



Gérer plusieurs périphériques mobiles ainsi que les besoins en ressources et en permissions de plusieurs équipes peut être fastidieux pour les équipes informatiques. Si les employés ne reçoivent pas les applications, le contenu et l'accès nécessaires sur tous leurs périphériques de travail à temps, ils pourraient chercher ces services auprès de sources tierces. Un employé sur deux avoue utiliser des applications et services web personnels pour le travail. Télécharger des applications de sources non fiables peut installer des applications cachées et malveillantes sur le périphérique, qui pourraient potentiellement accéder à toutes ses données, y compris les informations professionnelles sensibles. Sans oublier que l'utilisation de services cloud tiers non autorisés pour le travail met ces données sensibles à la disposition de ces prestataires de services.

Permettre à n'importe quel périphérique de se connecter aux serveurs de l'organisation peut sembler une solution simple, mais cela rendrait très difficile le suivi des connexions, la distinction entre les accès autorisés et non autorisés, et l'audit des modifications apportées aux fichiers de l'entreprise.

05

Logiciels malveillants

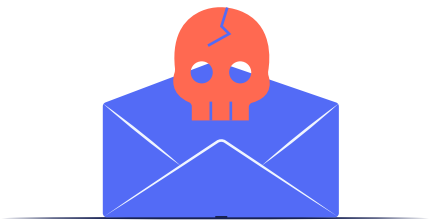
Les logiciels malveillants représentent une grande menace pour la sécurité des données sur les périphériques mobiles. Même si les utilisateurs évitent de télécharger des applications de sources tierces, des applications malveillantes peuvent toujours s'infiltrer dessus.

Un utilisateur pourrait télécharger une application apparemment sûre depuis le magasin d'applications, mais celle-ci pourrait ensuite inciter à installer une mise à jour qui introduirait un malware sur le périphérique. L'application initialement installée, appelée "dropper app", ne serait pas détectée comme malveillante lors d'un scan antivirus.

Par défaut, les périphériques mobiles ne sont pas configurés avec des mesures de sécurité de niveau entreprise, ce qui signifie que les applications et fichiers malveillants ne sont pas automatiquement détectés et peuvent discrètement voler des données d'entreprise. L'installation manuelle des applications de sécurité nécessaires et la configuration des restrictions de sécurité sur chaque périphérique peuvent être fastidieuses.

06

Menaces web cachées



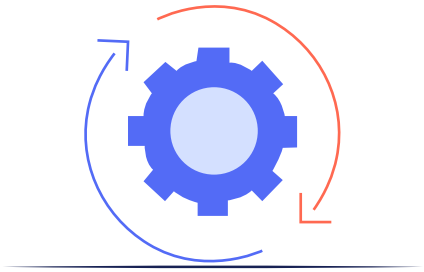
Les emails sont le moyen de communication officiel privilégié au sein des organisations. Les employés devraient pouvoir accéder à leurs boîtes mail professionnelles sur leurs périphériques mobiles afin de permettre un travail hybride complet.

Cependant, les emails sont également une source courante de diverses menaces de sécurité, y compris des pièces jointes malveillantes qui, lorsqu'elles sont ouvertes, peuvent installer discrètement des logiciels malveillants sur le périphérique. Les emails servent également de moyen pour les acteurs malveillants de mener des attaques par social engineering et de phishing pour voler des données telles que l'identité et les identifiants d'un employé, qui pourraient ensuite être utilisés pour accéder, manipuler ou voler et divulguer des données de l'entreprise.

Il existe quelques menaces web supplémentaires qui peuvent être difficiles à contrer sur un périphérique mobile. En plus de l'installation d'applications malveillantes, l'accès à des domaines non sécurisés sur un périphérique professionnel non seulement affecte la productivité de l'employé, mais expose également le périphérique à des menaces de sécurité similaires.

07

Les risques des vulnérabilités non corrigées

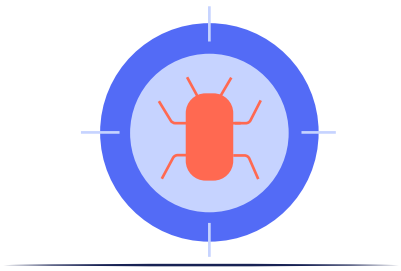


Les hackers adorent exploiter les failles de sécurité qu'ils trouvent dans les systèmes d'exploitation et les applications. Les développeurs publient des correctifs et des mises à jour non seulement pour apporter de nouvelles améliorations mais aussi pour combler ces failles. C'est pourquoi il est crucial d'installer ces mises à jour dès que possible sur les périphériques accédant aux données de l'entreprise. Cependant, les employés oublient souvent ces mises à jour, laissant leurs périphériques professionnels vulnérables aux menaces de sécurité.

En outre, les employés peuvent utiliser des périphériques anciens ou les modifier pour le personnaliser. Cependant, ces périphériques peuvent être vulnérables aux menaces de sécurité, mettant en danger les données de l'entreprise. Il est essentiel que les organisations s'assurent que les mises à jour des applications et du système d'exploitation soient installées à temps et que les périphériques vulnérables n'accèdent pas aux données de l'entreprise.

08

Exploits de type zero-day



Les acteurs malveillants cherchent constamment des vulnérabilités non découvertes dans les logiciels ou applications des périphériques qu'ils peuvent manipuler à leur avantage.

Les attaques zero-day ont augmenté au cours des dernières années et continueront probablement de le faire. Ces attaques permettent aux hackers de cibler des vulnérabilités non détectées et d'accéder à des données sensibles en toute discrétion, sans que l'utilisateur du périphérique ou l'administrateur informatique ne s'en aperçoive, ce qui conduit à des vols massifs de données et des fuites d'informations. Bien que les développeurs de logiciels soient rapides à corriger ces vulnérabilités une fois découvertes, il est souvent déjà trop tard, car les pirates ont déjà volé des données d'entreprise.

09

La prévalence des objets connectés intelligents

Les dispositifs IoT ont conquis les organisations de divers secteurs grâce à leurs fonctionnalités qui augmentent la productivité. Cependant, ces périphériques

comportent également des vulnérabilités de sécurité inhérentes qui offrent une nouvelle porte d'entrée pour les acteurs malveillants. Les hackers peuvent exploiter les faiblesses de l'un de ces périphériques connectés au réseau de l'entreprise et s'en servir pour s'infiltrer plus profondément dans le réseau, ou même lancer un botnet ciblant ces dispositifs non sécurisés pour voler des données de l'entreprise.

10

La question de la conformité

Bien que les menaces de sécurité mentionnées ci-dessus puissent empêcher les organisations de rester conformes aux normes de sécurité et de confidentialité, d'autres facteurs peuvent également compliquer la situation.

Par exemple, respecter les réglementations selon l'emplacement peut sembler impossible, étant donné que les périphériques mobiles peuvent être facilement transportés d'un endroit à l'autre, rendant complexe le respect des règles propres à chaque lieu. Certaines réglementations, comme la RGPD, exigent que les informations sensibles soient protégées par un mot de passe ou un chiffrement en permanence. Répondre à ces exigences lorsque les employés accèdent à ces données via des périphériques mobiles peut être difficile sans l'outil adéquat. Si ces menaces ne sont pas traitées, elles pourraient entraîner une fuite de données et, par conséquent, une violation de conformité, des problèmes juridiques, et des dommages sérieux à la réputation de l'organisation.

Qu'est-ce que le MDM ?

La gestion des périphériques mobiles (MDM) regroupe les outils et pratiques permettant de contrôler les périphériques mobiles utilisés pour le travail au sein de l'entreprise. Grâce au MDM, les administrateurs IT peuvent appliquer des configurations de sécurité, des stratégie et des restrictions sur les périphériques ; gérer les applications et le contenu ; effectuer des actions de gestion proactives et réactives ; et les suivre en permanence. Les outils MDM aident les administrateurs IT à surveiller les périphériques accédant aux données de l'entreprise et à garantir que la confidentialité, l'intégrité et la disponibilité des données sont toujours maintenues.

Comment le MDM peut vous aider
à résoudre ces problèmes de sécurité :

01

Assurez-vous que les employés se connectent uniquement à des réseaux Wi-Fi sécurisés et fiables, ou allez encore plus loin en établissant automatiquement une connexion VPN lorsqu'ils ouvrent une application professionnelle. Distribuez des certificats de sécurité aux périphériques et imposez l'utilisation de protocoles sécurisés pour la communication afin de protéger davantage les données de l'entreprise contre les cybermenaces pendant le transfert.

02

Limitez les fonctionnalités des périphériques qui ne sont pas nécessaires à l'utilisateur et contrôlez les autorisations des applications de manière détaillée pour éviter qu'elles n'accèdent à des permissions non requises. Si le périphérique doit servir un seul but, comme un terminal de point de vente ou une signalisation numérique, il peut être configuré pour exécuter une seule application ou un ensemble spécifique d'applications avec des restrictions strictes, empêchant les utilisateurs finaux de manipuler ces périphériques et d'accéder aux données de l'entreprise.

03

Assurez-vous que les périphériques sont suffisamment sécurisés pour accéder aux données de l'entreprise tout en préservant la confidentialité des employés. Isolez les données et applications de l'entreprise dans un espace de travail virtuel et appliquez les stratégie de sécurité nécessaires uniquement à cet espace, en laissant les fichiers personnels de l'employé intacts. Même si l'employé quitte l'organisation, seul ce conteneur peut être effacé, supprimant ainsi toute donnée professionnelle restante du périphérique.

04

Réduisez les risques liés à l'informatique parallèle en simplifiant la distribution des ressources et la gestion des autorisations. Distribuez et gérez fichiers, applications et permissions en fonction des groupes d'annuaire des utilisateurs de périphérique, garantissant que les équipes aient accès aux ressources nécessaires à temps. Bloquez les applications non sûres ou non fiables pour empêcher les utilisateurs de les installer sur leurs périphériques, et distribuez des applications de confiance afin que les employés puissent consulter les données de l'entreprise en toute sécurité. De plus, vous pouvez autoriser uniquement les périphériques sous gestion à accéder aux serveurs de l'entreprise, empêchant ainsi l'accès aux données depuis des périphériques non autorisés.

05

En plus de bloquer les applications malveillantes ou inutiles, vous pouvez installer automatiquement des applications antivirus ou de détection et réponse sur les périphériques accédant aux données de l'entreprise pour s'assurer que toute application inconnue ou fichier malveillant est mis en quarantaine et supprimé dès qu'il est détecté. Effectuez régulièrement des analyses complètes des périphériques pour détecter tout contenu suspect et le supprimer.

06

Sécurisez l'accès aux boîtes mail de l'entreprise en exigeant l'utilisation de protocoles de sécurité appropriés lors de l'envoi et de la réception d'emails sur un périphérique mobile. Limitez l'utilisation du HTML dans les emails pour vous protéger des menaces cachées et exigez que les pièces jointes de l'entreprise soient ouvertes uniquement avec des applications de confiance. Bloquez les domaines et URL malveillants pour protéger complètement les périphérique mobiles contre les menaces en ligne.

07

Testez les mises à jour des applications et du système d'exploitation, puis planifiez leur distribution au moment opportun. Ainsi, les périphériques accédant aux données de l'entreprise sont toujours à jour, et toutes les vulnérabilités connues sont corrigées. Vous pouvez également détecter automatiquement les périphériques anciens, jailbraké ,ou rootés et les empêcher d'accéder aux serveurs de l'entreprise, garantissant ainsi que les données ne sont pas exposées à des risques de sécurité par ces périphériques.

08

Les mesures de sécurité préventives sont le meilleur moyen de protéger les terminaux contre les attaques de type zero-day. Les outils de gestion des périphériques mobiles peuvent aider à configurer des stratégies de sécurité de haut niveau et des restrictions sur les périphériques, ajoutant ainsi une couche supplémentaire de sécurité sur les données de l'entreprise, et protégeant ainsi les périphériques et leurs données de ces attaques.

09

Intégrez les périphériques IoT utilisés pour le travail dans le système de gestion et configurez-les avec les mesures de sécurité nécessaires pour qu'ils soient aussi sécurisés que n'importe quel autre point d'accès sur le réseau de votre organisation.

10

Surveillez en temps réel les périphériques gérés pour vous assurer qu'ils respectent toujours les normes de l'organisation et du secteur. Les périphériques peuvent avoir des mots de passe obligatoires et un chiffrement des données, maintenant la conformité même lorsque les données sont inactives. Une conformité basée sur la localisation peut être atteinte en suivant l'emplacement des périphériques, et vous pouvez appliquer différentes restrictions de sécurité en fonction de sa position. Les périphériques perdus ou volés peuvent être suivis ou effacés à distance des données de l'entreprise pour éviter que des informations sensibles ne tombent entre de mauvaises mains.

Simplifiez le MDM avec

ManageEngine Mobile Device Manager Plus

En avez-vous assez de gérer les innombrables périphériques mobiles de votre personnel hybride et les problèmes de sécurité qui les accompagnen t? Avec ManageEngine Mobile Device Manager Plus, vous pouvez regrouper sous une même gestion les périphériques d'entreprise et ceux des employés. Cet outil MDM complet vous permet de gérer et sécuriser facilement les périphériques Android, Apple, Windows et Chrome OS depuis une console unique.

Découvrez quelques fonctionnalités de Mobile Device Manager Plus qui simplifieront votre quotidien :

- Profitez d'une inscription simplifiée des périphériques et d'une gestion fluide grâce à une variété d'options qui permettent de les intégrer en masse et à distance.
- Appliquez des mesures de sécurité de niveau entreprise sur les périphériques accédant aux données de l'entreprise, afin de repousser les menaces tout en respectant les normes.
- Distribuez et mettez à jour les applications professionnelles et le contenu sur les périphériques selon les besoins, et planifiez les mises à jour du système d'exploitation au moment opportun pour satisfaire et rendre votre équipe productive.
- Configurez des périphériques à usage unique en les limitant à une seule application ou à un ensemble spécifique d'applications.
- Visualisez et contrôlez à distance les périphériques pour les dépanner, et suivez leur localisation. Effectuez des effacements à distance pour protéger les données de l'entreprise même si le périphérique est égaré.

Essayez Mobile Device Manager Plus dès maintenant et offrez à vos équipes mobiles une gestion centralisée.

DEMANDEZ UNE DÉMO **TÉLÉCHARGEZ**

PG Software EUROPE