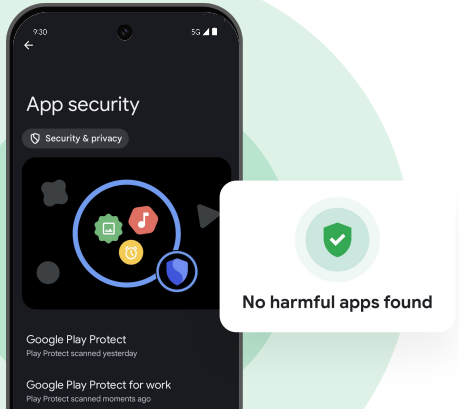
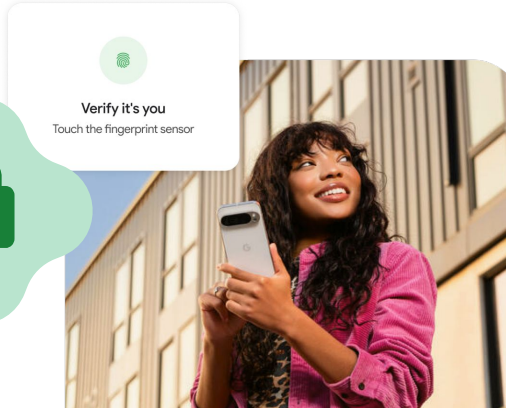
Android

Guidebook sur la sécurité mobile pour les PME





Présentation

Mettre en place une sécurité des données robuste est particulièrement important pour les petites entreprises. Selon Hiscox[1], 25 % des petites entreprises font faillite après une brèche de sécurité, dont le coût moyen s'élève à 200 000 $.

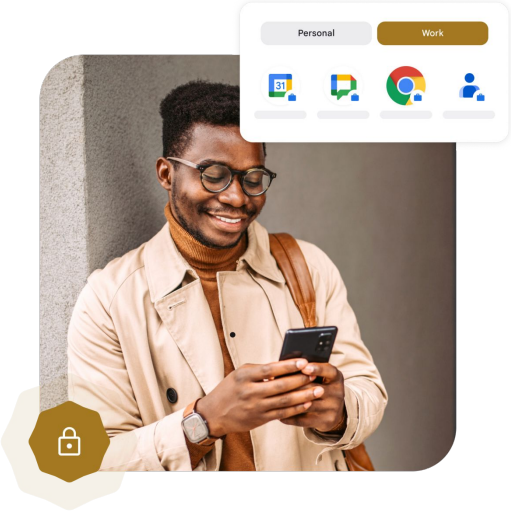
Dans le monde hyperconnecté actuel, vos smartphones et tablettes sont des outils puissants, mais ils représentent aussi un risque de sécurité potentiel s'ils ne sont pas gérés correctement.

L'une des plus grandes menaces qui pèsent sur les utilisateurs d'appareils mobiles est l'hameçonnage. En effet, 83 % des sites d'hameçonnage[2] ciblent spécifiquement ce type d'appareils. Les pirates informatiques utilisent désormais l'IA pour mettre au point des attaques sophistiquées capables de tromper les utilisateurs, même les plus expérimentés.

Gérer le cycle de vie complet des appareils professionnels, puis assurer la sécurité ainsi que la confidentialité des données des employés et de l'entreprise peut sembler complexe. Pourtant, cette tâche peut s'avérer simple, à condition de disposer des bons outils.

Android offre des solutions de protection simples et discrètes pour sécuriser les appareils ainsi que les données de l'entreprise ou encore pour empêcher les attaques par hameçonnage. C'est particulièrement important pour les entreprises qui ne disposent pas d'une équipe informatique dédiée, chargée de gérer et de sécuriser les appareils.

Dans ce guide, nous présentons les bonnes pratiques pour protéger les données de votre entreprise et nous expliquons en quoi Android est une plate-forme si robuste et sécurisée.



[1] Hiscox Cyber Readiness Report
[2] 2024 Global Mobile Threat Report de Zimperium

Comprendre les modèles d'enregistrement d'un appareil Android

Il existe trois approches (ou modèles) spécifiques que les entreprises peuvent adopter pour sécuriser leurs appareils et leurs données. Chaque modèle offre aux équipes informatiques un contrôle plus poussé sur l'appareil.

01

Le premier modèle, qui n'inclut ni solution de gestion de la mobilité en entreprise (EMM), ni fonctions de gestion, est dit "initié par l'utilisateur". Dans ce modèle, l'équipe informatique de l'entreprise informe les utilisateurs et les guide sur les bonnes pratiques à adopter pour configurer des paramètres de sécurité et de confidentialité spécifiques sur leur appareil.

02

Pour le second modèle, Device Trust from Android Enterprise offre un modèle basé sur l'approche zero trust pour une sécurité renforcée. Cette approche permet aux fournisseurs de solutions de confiance d'inspecter l'état de sécurité d'un appareil, que celui-ci soit géré par un EMM ou non. Cela inclut un large éventail de solutions, y compris des fournisseurs d'identité (IdP), des solutions de défense contre les menaces mobiles (MTD), des solutions de détection et de réponse pour les entreprises (EDR) et des fournisseurs de réseaux privés virtuels (VPN). Étant intégrées à Android Enterprise, ces solutions partenaires peuvent vérifier que les appareils remplissent des critères spécifiques avant de leur accorder l'accès aux ressources de l'entreprise.

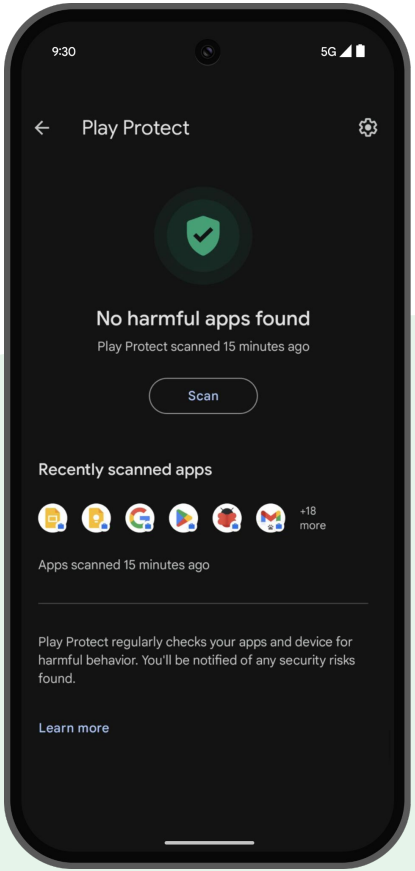
03

Le troisième modèle repose sur des contrôles d'EMM, qui permettent aux entreprises d'exercer un contrôle plus strict sur les appareils des utilisateurs, qu'ils appartiennent à l'entreprise ou qu'ils fassent partie d'un programme Bring Your Own Device (BYOD). Sur les appareils personnels, l'entreprise enregistre un profil professionnel, ce qui permet au service informatique de contrôler toutes les facettes de ce profil, tout en préservant la confidentialité de l'utilisateur dans son espace personnel.

Android Enterprise propose plusieurs modèles d'enregistrement des appareils pour répondre aux besoins des PME

Tous les modèles s'intègrent entre eux pour offrir de la flexibilité aux PME, et tous peuvent être utilisés ensemble selon les besoins de l'entreprise. En exploitant les fonctionnalités de sécurité robustes d'Android et en appliquant les bonnes pratiques énoncées un peu plus loin, votre entreprise pourra œuvrer en toute confiance dans l'environnement mobile.

L'engagement d'Android pour le progrès dans le domaine de la sécurité, ainsi que sa flexibilité ou encore son rapport coût-efficacité en font le choix privilégié des petites et moyennes entreprises.



Règles et paramètres de sécurité recommandés pour chaque modèle d'enregistrement

Des conseils spécifiques pour chaque modèle : initié par l'utilisateur, Device Trust from Android Enterprise et solution EMM.

Chacun de ces modèles offre aux utilisateurs un certain niveau de confidentialité, et à l'entreprise un certain niveau de contrôle, en fonction de vos exigences.

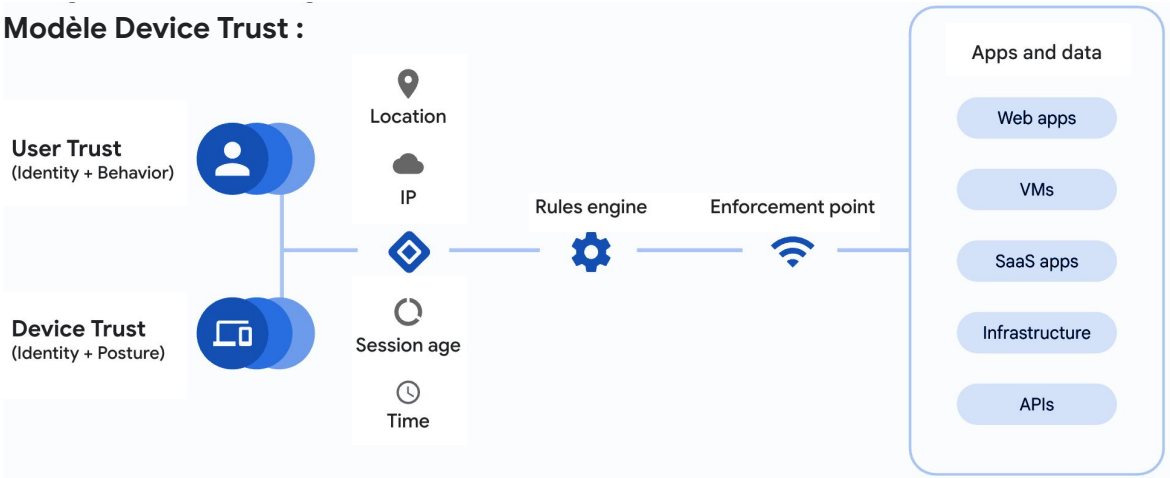
01 Paramètres de sécurité initiés par l'utilisateur

L'équipe informatique expliquera aux utilisateurs comment configurer manuellement les paramètres suivants sur leurs appareils Android et pourquoi le faire, afin de contribuer à protéger les données des utilisateurs ainsi que celles de l'entreprise.

- Activer le verrouillage en cas de détection de vol
- Activer le verrouillage à distance
- Activer le verrouillage de l'appareil hors connexion
- Activer la vérification de l'identité
- Activer l'espace privé
- Définir un code ou un mot de passe d'au moins 6 caractères, sans répétitions.
- S'assurer que Google Play Protect est activé
- Installer uniquement des applications provenant de Google Play Store

02 Modèle zero trust

En plus des restrictions et des contrôles offerts par Device Trust from Android Enterprise, les équipes informatiques doivent également demander aux utilisateurs de configurer et de mettre à profit l'ensemble des fonctionnalités de sécurité initiées par l'utilisateur qui sont décrites dans la section 1.



Choisissez dans la liste suivante les contrôles que vous souhaitez implémenter avant d'autoriser l'accès aux ressources de l'entreprise. Le choix des paramètres dépend des partenaires Device Trust. Veuillez consulter leur documentation.

02 Device Trust from Android Enterprise

Choisissez dans la liste suivante les contrôles que vous souhaitez implémenter avant d'autoriser l'accès aux ressources de l'entreprise. Le choix des paramètres dépend des partenaires Device Trust. Veuillez consulter leur documentation.

Signal	Description
Modèle ou marque de l'appareil	Indique le modèle et la marque de l'appareil.
État de gestion	Indique la gestion et l'application de gestion.
État du réseau	Indique des informations sur tous les réseaux actifs de l'appareil.
Niveau du correctif de sécurité de l'appareil	Indique le niveau du correctif de sécurité actuel de l'appareil (y compris le niveau de correctif de la mise à jour du système Play).
Niveau du correctif de sécurité publié	Indique le niveau du correctif de sécurité publié par Google pour le composant à jour correspondant sur l'appareil*.
État du chiffrement du disque	Indique si l'espace de stockage de l'appareil est chiffré.
Version d'OS et OTA en attente	Indique la version de l'OS de l'appareil et indique si une mise à jour de l'OS est en attente.
Verrouillage de l'écran et contrôle qualité	Indique la complexité du verrouillage d'écran actuel de l'utilisateur.
État Play Protect	Indique si le service Google Play Protect est activé.

03 Activé par les règles EMM

Les administrateurs informatiques peuvent consulter la documentation de leur solution EMM pour savoir comment configurer ces ensembles de règles minimales afin de protéger les utilisateurs. Les solutions EMM permettent aux administrateurs informatiques de configurer les appareils de trois manières : profil professionnel uniquement, appareil détenu par l'entreprise, mais activé personnellement (COPE) ou entièrement géré. Les appareils COPE et ceux dotés d'un profil professionnel permettent tous deux à l'entreprise de contrôler un profil professionnel, mais seuls les appareils COPE offrent un contrôle plus poussé sur l'ensemble de l'appareil. Voici quelques exemples de contrôles de sécurité à prendre en compte :

- Créer des mots de passe d'au moins 6 caractères
- Autoriser au maximum 10 tentatives de déverrouillage de l'appareil
- Activer Google Play Integrity
- Désactiver les captures d'écran
- Interdire l'ajout de comptes dans le profil professionnel
- Désactiver les options pour les développeurs
- Interdire les installations provenant de sources inconnues
- Désactiver le copier-coller entre profils
- Désactiver Android Debug Bridge (ADB)
- Utiliser Google Play d'entreprise avec des listes d'autorisation
- Empêcher la désactivation de la navigation sécurisée dans Chrome

Bonnes pratiques lors du déploiement d'appareils Android dans votre entreprise

01 Informer les employés et leur demander d'activer les fonctionnalités de sécurité intégrées

Bonne pratique

Protégez vos données contre les voleurs et les accès non autorisés grâce à de nouvelles fonctionnalités intégrées, conçues pour sécuriser les informations confidentielles de votre entreprise. Voici comment procéder :

A

Activez le verrouillage en cas de détection de vol, qui utilise l'IA, les capteurs de mouvement de votre appareil, le Wi-Fi ainsi que le Bluetooth pour détecter un mouvement associé au vol et verrouiller automatiquement l'appareil.

B

Activez et utilisez le verrouillage à distance. En cas de perte ou de vol de votre appareil, vous pouvez utiliser le verrouillage à distance avec un numéro de téléphone validé pour verrouiller rapidement l'écran de votre appareil.

C

Activez le verrouillage de l'appareil hors connexion. Le verrouillage de l'appareil hors connexion verrouille automatiquement l'écran de votre appareil après sa déconnexion pour vous aider à protéger vos données. Par exemple, si quelqu'un vole votre téléphone et désactive la connexion Internet pour vous empêcher de le localiser avec l'application Localiser mon appareil, le téléphone se verrouille après avoir été utilisé hors connexion pendant une courte période.

01 Informer les employés et leur demander d'activer les fonctionnalités de sécurité intégrées

Bonne pratique

Protégez vos données contre les voleurs et les accès non autorisés grâce à de nouvelles fonctionnalités intégrées, conçues pour sécuriser les informations confidentielles de votre entreprise. Voici comment procéder :

D

Activez la vérification de l'identité. Pour valider votre identité, la vérification de l'identité nécessite des données biométriques et d'autres mesures de protection. Votre identité est validée lorsque vous effectuez des actions sensibles sur votre appareil ou que vous modifiez votre compte Google en dehors de vos lieux vérifiés.

E

Masquez les applications sensibles avec l'espace privé. Pour protéger vos applications privées contre les accès non autorisés, Android propose un espace privé. Cela crée un espace distinct et masqué sur votre appareil dans lequel vous pouvez organiser vos applications personnelles. Même si votre téléphone déverrouillé tombe entre de mauvaises mains, vos applications sensibles qui figurent dans l'espace privé resteront protégées.

F

Google a également intégré des fonctionnalités antihameçonnage directement dans Google Messages afin de protéger les utilisateurs contre les techniques d'hameçonnage avancées. De plus, de nouvelles fonctionnalités comme la protection antispam et l'affichage du numéro de l'appelant sur Android renforcent la protection des utilisateurs.

02 Utiliser le répertoire des solutions Android Enterprise Recommended

Bonne pratique

Créez une liste d'appareils approuvés pour une utilisation professionnelle à partir du répertoire des solutions Android Enterprise Recommended.

Les appareils qui figurent dans notre répertoire des solutions font l'objet de tests de sécurité rigoureux et reçoivent des mises à jour régulières.

La validation Android Enterprise Recommended garantit que votre entreprise dispose d'appareils dont la sécurité est renforcée et dont les fonctionnalités sont optimisées pour les besoins de l'entreprise.

03 Déployer une solution de gestion des appareils pour un contrôle centralisé

Bonne pratique

Utilisez une solution EMM pour appliquer les règles de sécurité, effacer et/ou verrouiller les appareils à distance et gérer l'installation d'applications. Pour trouver une liste de partenaires EMM validés et approuvés, vous pouvez consulter le répertoire des solutions EMM Android Enterprise Recommended.

L'intégration étroite d'Android avec les solutions EMM permet un contrôle précis et une gestion efficace de la sécurité pour les entreprises de toutes tailles.

04 Des mises à jour de sécurité régulières

Bonne pratique

Utilisez les règles d'Android Enterprise concernant les appareils à travers une solution EMM afin de vous assurer que tous les appareils sont à jour et disposent des derniers correctifs de sécurité Android. Android Enterprise offre aux administrateurs la possibilité d'appliquer des règles concernant la mise à jour de l'OS et des applications qui répondent aux besoins de l'entreprise.

Android s'engage à publier des mises à jour de sécurité régulières tous les 30 jours, afin que l'ensemble des fabricants d'appareils et des opérateurs puisse les proposer rapidement. De plus, si vous choisissez des appareils figurant dans le répertoire des solutions, ceux-ci doivent proposer des mises à jour tous les 90 jours au moins. Certains fabricants d'appareils, comme Pixel et Samsung, proposent désormais sept ans de mises à jour de sécurité et de l'OS. Cela permet de corriger rapidement les éventuelles failles.

05 Mettre en œuvre une authentification forte

Bonne pratique

Les contrôles Android Enterprise permettent de définir des exigences quant aux méthodes de déverrouillage des appareils. Il peut s'agir de codes, de schémas ou de mots de passe, qui peuvent être associés au déverrouillage par empreinte digitale et par reconnaissance faciale. Les administrateurs peuvent demander aux utilisateurs de définir des exigences spécifiques qui répondent aux besoins de l'entreprise. Veillez à exiger au moins six chiffres sans répétitions, conformément aux dernières exigences du NIST SP 800-53.

La prise en charge des données biométriques par Android, associée au stockage sécurisé des clés, offre aux utilisateurs une expérience fluide et contribue à protéger votre appareil grâce à une authentification sécurisée, intégrée à un matériel robuste.

06 Déployer et gérer des applications de façon sécurisée

Bonne pratique

Autorisez les utilisateurs à installer des applications uniquement depuis le Google Play Store et exigez que Google Play Protect soit activé en permanence. Avec Google Play d'entreprise, les administrateurs peuvent compiler une liste d'applications approuvées et définir des autorisations.

Google Play d'entreprise empêche le téléchargement indépendant d'applications non approuvées. Google Play Protect, de son côté, analyse activement toutes les applications installées pour détecter les logiciels malveillants.

07 Protéger les données en transit

Bonne pratique

Utilisez des VPN pour établir des connexions sécurisées aux services professionnels lorsque vous êtes en déplacement, assurez-vous que tous les services utilisent le protocole HTTPS et que les connexions Wi-Fi à votre réseau d'entreprise sont correctement configurées.

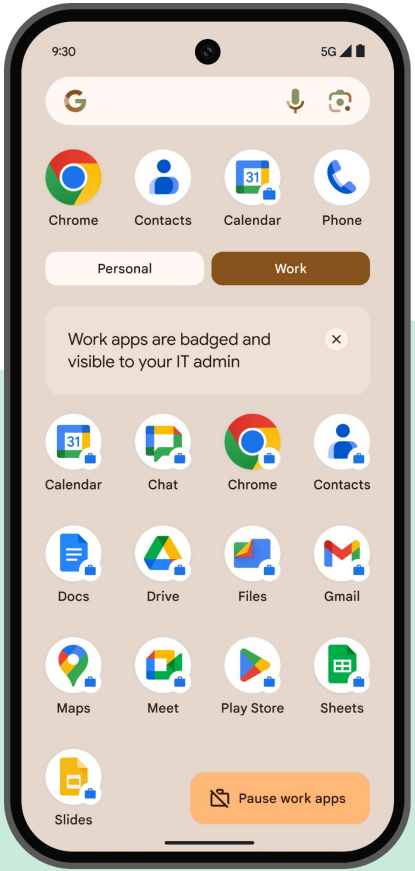
Le chiffrement intégré d'Android ainsi que la prise en charge des VPN contribuent à protéger vos données, qu'elles soient stockées sur l'appareil ou transmises sur le réseau.

08 Utiliser le profil professionnel Android

Bonne pratique

Si les employés utilisent des appareils personnels (BYOD), les administrateurs doivent mettre en place un profil professionnel pour séparer les données professionnelles et personnelles sur un même appareil.

Le profil professionnel Android est une fonctionnalité disponible uniquement sur Android qui crée un environnement sécurisé et isolé pour protéger les données d'entreprise et préserver la confidentialité des données personnelles.



Points clés à retenir

Pour limiter les appels au service informatique ou au centre d'assistance, il est essentiel de former les utilisateurs et de leur fournir des instructions claires sur la configuration de chacun des trois modèles.

Consultez le répertoire des solutions AE pour découvrir une sélection d'appareils et de partenaires approuvés. Cette ressource peut vous aider à choisir les produits les plus adaptés à vos besoins spécifiques.

Mettez en place une solution de sécurité en priorité, même si c'est au travers d'une approche basique. La sécurisation des appareils professionnels entraîne des coûts différents pour chaque modèle. Choisissez un modèle offrant un équilibre entre le niveau de sécurité requis et les coûts de mise en œuvre et de maintenance.

Android

Pour plus d'informations :

www.android.com/enterprise/security