Examen de la sécurité mobile 2023

- Produits testés
- Résultats des tests
- Avis sur les produits
- Prix

Introduction

Dans ce rapport, nous visons à aider les lecteurs à évaluer à la fois les mesures de sécurité intégrées d'Android et les fonctionnalités avancées fournies par les applications de sécurité tierces.
Notre rapport couvre les résultats des tests de protection contre les logiciels malveillants et de consommation de la batterie, ainsi que des examens qui évaluent la fonctionnalité, la conception des applications et la convivialité globale de chaque solution de sécurité.
À la fin de chaque rapport de produit, les lecteurs peuvent trouver un tableau qui offre un aperçu des fonctions antivol incluses dans ce produit particulier.
Bien que certaines des applications que nous avons testées puissent avoir des fonctionnalités supplémentaires telles que des gestionnaires d'applications, des moniteurs réseau et des optimiseurs de système, nous nous concentrons principalement sur la sécurité, y compris l'anti-malware, l'antivol, la navigation sécurisée et la confidentialité dans nos critiques et ne mentionnons que brièvement toute fonctionnalité supplémentaire. Pour faciliter les comparaisons de produits, nous maintenons une structure cohérente pour chaque rapport de produit.

Détails

En 2021, nous avons également évalué dans quelle mesure certaines applications de sécurité protègent contre les stalkerwares sur Android.
Ce type de logiciel fonctionne secrètement, permettant à des personnes non autorisées d'espionner les propriétaires d'appareils à leur insu ou sans leur consentement.
Alors que les stalkerwares et les logiciels légitimes (tels que le contrôle parental) ont brouillé les lignes entre eux, Google Play a mis en place des politiques plus strictes ces dernières années pour lutter contre ce problème.
Par conséquent, le stalkerware est généralement installé via le chargement latéral car il n'est pas disponible sur le Play Store.

Les produits de sécurité mobile sont principalement conçus pour protéger les utilisateurs mobiles et leurs appareils contre les menaces telles que les applications malveillantes, les URL de phishing, les courriels frauduleux et autres liens nuisibles.
Les versions récentes d'Android sont équipées de fonctionnalités de sécurité fondamentales.
Par exemple, Play Protect, le scanner de logiciels malveillants intégré de Google, analyse les applications pendant l'installation à partir de Google *Play* ou de sources tierces et effectue des vérifications régulières des

appareils pour détecter les menaces.
Navigation sécurisée L’API aide à protéger contre les logiciels malveillants et les liens de phishing lorsque vous naviguez sur le Web à l’aide de Google Chrome.
Des fonctions antivol, telles que le verrouillage, la localisation, l’alarme et l’effacement, sont disponibles via *Localiser mon appareil* de Google, permettant aux utilisateurs de retrouver des téléphones perdus ou volés et d’empêcher l’accès aux données personnelles qui y sont stockées.
Les dernières versions d’Android fournissent également plusieurs fonctionnalités d’audit d’applications qui permettent aux utilisateurs de consulter et de modifier les paramètres de confidentialité (tels que les autorisations et notifications dangereuses / spéciales) et l’utilisation (telles que les données mobiles, la consommation de la batterie et l’espace de stockage) des applications individuelles.

Dans les pages suivantes, nous explorons les fonctionnalités de confidentialité et de sécurité et les limites de *Google Android*.
Il est important de noter que toutes les fonctionnalités de sécurité de Google ne sont pas disponibles pour tous les utilisateurs en raison de restrictions sur certaines versions d’Android, les systèmes d’exploitation basés sur Android et les emplacements géographiques.
Nous discutons également des risques actuels auxquels sont confrontés les utilisateurs de smartphones et fournissons des recommandations pour améliorer la protection.
En outre, nous fournissons un bref aperçu des fonctionnalités de sécurité courantes dans les applications de sécurité Android.
La section principale de ce rapport contient les produits de sécurité participants, ainsi que les résultats des tests de protection contre les logiciels malveillants, des tests de décharge de la batterie et des examens approfondis des produits.

Pour le composant antivol de chaque produit, nous commentons brièvement chaque fonction et utilisons des symboles dans le tableau pour indiquer ses performances dans nos tests.

Aucun problème

Problème(s) mineur(s)

Problème(s) majeur(s)

Google Android

Android 6.0 (Marshmallow) a introduit des autorisations d'exécution, donnant aux utilisateurs plus de contrôle sur les informations et les données privées auxquelles les applications installées ont accès.
Cette approche est très différente de celle adoptée par les versions antérieures d'Android, où les applications demandaient toutes les autorisations nécessaires avant l'installation. Depuis Android 8.0 (Oreo), le paramètre de sécurité global *Installer à partir de sources inconnues* est une autorisation d'exécution qui doit être accordée pour chaque application une fois.
La protection intégrée contre les logiciels malveillants Play Protect est préinstallée sur les appareils fonctionnant sous Android 8.0 ou version ultérieure et est également disponible sur les appareils Android plus anciens qui prennent en charge Google *Play* Services 11 ou version ultérieure.
Des fonctions supplémentaires, pour la perte d'appareil et la navigation sécurisée pour Google Chrome, ont également été intégrées en tant que composants réguliers.
Les applications ciblant Android 9 (Pie) et versions ultérieures sont obligées d'utiliser des connexions chiffrées, telles que TLS ou HTTPS.
La prise en charge du texte clair (par exemple, l'utilisation de HTTP au lieu de HTTPS) et l'établissement de la confiance dans les certificats d'autorité de certification racine tiers ne sont possibles que s'ils sont explicitement définis dans la configuration réseau de l'application.
Cela rend les attaques réseau telles que l'usurpation ARP ou MITM moins préoccupantes.

Android 10 et 11 ont apporté des améliorations significatives en matière de sécurité et de confidentialité qui sont affinées dans les versions ultérieures.
Il s'agit, par exemple, du concept de stockage limité (ainsi que de l'autorisation « Accès à tous les fichiers »), des restrictions lors de l'accès à certaines ressources (par exemple, emplacement en arrière-plan, microphone, caméra, liste des applications installées) et d'empêcher les applications tierces d'interroger des informations spécifiques sur l'appareil (par exemple, IMEI, IMSI, MEID, SIM, numéro de série de build).
Une fonctionnalité de réinitialisation automatique réinitialise automatiquement toutes les autorisations d'exécution pour les applications inutilisées.

Dans Android 12, les utilisateurs ont la possibilité d'autoriser les applications à accéder uniquement aux informations de localisation approximatives.
Des indicateurs d'utilisation active de la caméra/microphone et une bascule caméra/microphone à l'échelle du système pour bloquer facilement l'accès à ceux-ci ont été ajoutés.
Les applications peuvent également masquer les fenêtres non superposées au système d'autres applications.
En plus de la réinitialisation automatique de toutes les autorisations accordées, les applications inutilisées seront placées dans un « état de mise en veille prolongée », où toutes les actions en arrière-plan sont supprimées et le cache de l'application est effacé.

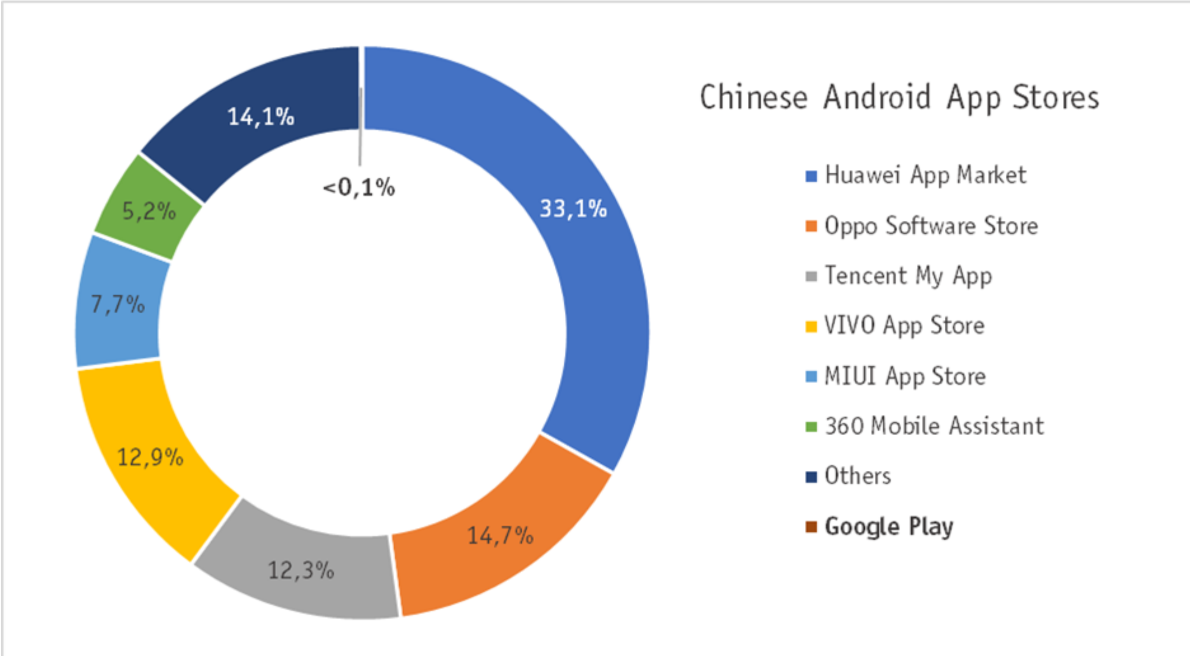
La sortie d'Android 13 en août 2022 a introduit de nombreux changements dans les autorisations Android.
Dans divers cas d'utilisation où les applications peuvent accéder aux informations souhaitées sans le consentement de l'utilisateur, elles doivent désormais déclarer l'autorisation nécessaire dans le fichier manifeste Android, ou à la fois la déclarer et la demander explicitement pendant l'exécution.
Ces scénarios incluent l'utilisation de l'identifiant publicitaire des services Google Play pour la monétisation et les annonces personnalisées, la publication de notifications d'application, la découverte d'appareils Wi-Fi à proximité sans avoir besoin de l'emplacement de l'appareil, la lecture des informations du capteur corporel tout en cours d'exécution en arrière-plan et l'accès individuel à différents types de médias (par exemple, image,

vidéo, audio).
Pour respecter les meilleures pratiques en matière d’autorisations et renforcer la confiance des utilisateurs, une application peut révoquer de manière proactive son accès aux autorisations d’exécution inutilisées.
En outre, les utilisateurs peuvent arrêter le service de premier plan d’une application à partir de la nouvelle fonctionnalité « Gestionnaire des tâches » dans la zone de notification Android et ignorer les notifications associées.
Les applications qui permettent aux utilisateurs de copier du contenu sensible (par exemple, des mots de passe, des informations de carte de crédit) dans le presse-papiers peuvent empêcher le contenu d’apparaître dans l’aperçu du presse-papiers.

Les restrictions qui en résultent imposées aux applications ciblant la dernière version d’Android ont affecté les fournisseurs de sécurité mobile, entre autres.
Leurs applications nécessitent toutes les autorisations d’appareil disponibles, y compris les droits d’administrateur de l’appareil, si elles doivent surveiller et contrôler entièrement l’appareil, et protéger les données utilisateur sensibles contre les menaces de sécurité.

En raison de tous ces changements, les applications de sécurité mobile peuvent fournir des explications plus claires aux utilisateurs lorsqu’ils demandent l’accès à des zones sensibles de l’appareil et configurent des fonctionnalités de sécurité intégrées à l’application (par exemple, un antivol).

La protection contre les logiciels malveillants par Google Play Protect s’améliore chaque année, mais il y a encore place à l’amélioration.
Malheureusement, cela n’aidera pas les utilisateurs en Chine continentale, car le service y est inaccessible.
En outre, les appareils basés sur des versions modifiées du système d’exploitation Android (par exemple, HarmonyOS, FireOS, LineageOS) n’exécutent pas d’applications ou de services Google par défaut.
Par conséquent, il n’y a pas de protection intégrée contre les logiciels malveillants.
Pour les utilisateurs qui ne peuvent pas accéder aux fonctionnalités de sécurité intégrées d’Android, il existe un argument très fort en faveur de l’utilisation d’une application de sécurité tierce.
Même pour les personnes qui ont un accès complet aux fonctionnalités de protection de Google, une application tierce peut toujours fournir une protection supplémentaire très précieuse.
Nous notons que les applications de sécurité tierces pour Android complètent, plutôt que de remplacer, les fonctionnalités de sécurité de Google.



Soure: https://www.appinchina.co/market/app-stores

Dans des régions comme les États-Unis et l'Europe, seuls deux magasins d'applications officiels dominent le marché des applications mobiles : Google Play et l'App Store d'Apple.
Le risque de télécharger et d'installer par inadvertance des logiciels malveillants à partir de Google Play est faible, car l'App Store est régulièrement vérifié pour détecter les applications frauduleuses et dangereuses.
Cependant, dans de nombreux pays asiatiques, en particulier en Chine, le risque d'être infecté par des logiciels malveillants est beaucoup plus élevé.
Il existe de nombreux magasins d'applications fournis par divers fournisseurs tiers, et de nombreux smartphones sont également enracinés.
Il y a environ 1,69 milliard d'appareils mobiles actifs en Chine, et environ 65% d'entre eux exécutent Android comme système d'exploitation.
Les magasins d'applications Android les plus utilisés sont indiqués dans le tableau des beignets ci-dessus.
Google Play n'est utilisé par presque personne (<0,1%) car Google Play et la plupart des services de Google sont inaccessibles en Chine continentale.
Un décret américain signé en novembre 2020 interdit aux entreprises américaines (telles que Google) de faire des affaires avec des entreprises chinoises figurant sur la liste noire. Par conséquent, les applications et services Google, y compris Play Protect, ne seront plus disponibles sur les futurs modèles d'appareils de certains fabricants chinois.

Protection contre les logiciels malveillants Android

Les smartphones sont maintenant couramment utilisés comme substituts PC populaires pour une variété de tâches quotidiennes telles que les achats en ligne, les opérations bancaires, la messagerie instantanée, la vidéoconférence et l'envoi de courriels.
Cependant, avec la sophistication croissante des cyberattaques, les appareils mobiles deviennent une cible de choix, en particulier par le biais d'applications frauduleuses qui visent à voler les données ou l'argent des utilisateurs.
Ces applications malveillantes se déguisent souvent en fausses versions d'applications populaires

téléchargées par des millions d’utilisateurs à partir de Google Play.
Afin de minimiser le risque d’être victime de ces menaces, nous vous recommandons de suivre les conseils fournis dans le présent rapport.

Pour vous protéger contre les applications malveillantes, il est préférable de télécharger des applications exclusivement à partir de magasins d’applications officiels tels que Google Play ou de fabricants d’applications réputés, tout en évitant les magasins tiers et le chargement latéral.
Avant d’installer une application, vérifiez ses avis dans l’App Store et évitez ceux avec des commentaires principalement négatifs ou suspects.
Lorsque vous accordez des autorisations d’application, soyez prudent et remettez en question toute demande qui semble inutile ou sans rapport avec l’objectif de l’application. Méfiez-vous des applications qui demandent des droits d’accès excessifs, par exemple, une application de calculatrice qui demande l’autorisation à vos contacts.

Bien que toutes les applications au comportement suspect ne soient pas nécessairement malveillantes, il est important d’évaluer leur légitimité et leur utilité.
Google Play met régulièrement à jour ses règles pour garantir un certain niveau de sécurité, en obligeant les développeurs d’applications à vérifier leur identité, à signer numériquement leurs applications et à répondre aux exigences au niveau de l’API.
Les applications sont également soumises à plusieurs processus d’examen et nécessitent l’approbation de Google en matière de confidentialité pour rester disponibles sur Google Play.
De plus, les développeurs doivent fournir des informations sur la collecte, le partage et la suppression des données dans la section « Sécurité des données » de leurs applications.

L’enracinement de votre smartphone peut augmenter considérablement le risque que des applications malveillantes prennent le contrôle de votre appareil et peut annuler la garantie.
Les réseaux Wi-Fi publics, souvent trouvés dans des endroits comme les cafés et les aéroports, sont des cibles populaires pour le vol de données.
Évitez de saisir ou de partager des informations sensibles telles que les informations d’identification de l’utilisateur ou les informations de carte de crédit sur un réseau Wi-Fi public, sauf si vous utilisez un VPN pour chiffrer votre trafic réseau et empêcher les pirates de l’intercepter.
De plus, désactivez tous les paramètres inutilisés (par exemple, Bluetooth, NFC, appels Wi-Fi) ou les fonctions de partage d’appareils qui pourraient être des vecteurs d’attaque potentiels.

Restez prudent et vigilant lorsque vous recevez des liens suspects via des messages texte, des courriels, des discussions de messagerie instantanée ou des médias sociaux. Si l’expéditeur est inconnu, marquez le message comme spam ou supprimez-le immédiatement.
Il est également crucial de garder votre appareil mobile à jour avec les derniers correctifs de sécurité et la version Android pour résoudre les vulnérabilités de l’appareil et de l’API.

Quel est le risque d’infection par un logiciel malveillant avec un téléphone mobile Android?

Le risque de logiciels malveillants sur les téléphones Android dépend de plusieurs facteurs et ne peut pas être résolu simplement.

Cependant, s’en tenir aux magasins d’applications officiels comme Google Play réduit le risque d’infection.
Dans les pays asiatiques avec de nombreux appareils enracinés et des magasins d’applications tiers, la probabilité de téléchargements nuisibles est plus élevée. Néanmoins, il est important de noter que « faible risque » ne signifie pas « aucun risque », car le paysage des menaces peut changer rapidement.
Pour être préparé, il est recommandé d’installer un logiciel de sécurité approprié sur votre cellulaire.
Actuellement, dans les pays occidentaux, la protection contre la perte de données due au vol ou à la perte est plus critique que la protection contre les logiciels malveillants.

Caractéristiques de sécurité

Dans cette section, nous fournissons un aperçu concis des principaux composants de sécurité couramment trouvés dans les produits de sécurité Android.
Le composant principal est le *scanner de logiciels malveillants* qui protège les utilisateurs contre l’installation involontaire d’applications malveillantes sur leur appareil.
Semblables aux programmes antivirus pour Windows, les applications de sécurité mobile Android intègrent diverses fonctionnalités de protection.
La *protection en temps réel* analyse activement les applications nouvelles et existantes à la recherche de tout comportement malveillant.
L’analyseur à la demande examine l’appareil, y compris le stockage interne et/ou la carte SD externe, à la recherche d’applications malveillantes qui sont déjà installées ou téléchargées fichiers APK qui n’ont pas encore été exécutés.

La mise à jour des définitions de logiciels malveillants est un facteur essentiel pour une protection efficace, en particulier pour les applications qui s’appuient principalement sur elles pour détecter les logiciels malveillants.
Certains produits testés offrent un scanner de logiciels malveillants assisté par le cloud pour garantir l’accès aux toutes dernières définitions.
Les mises à jour des définitions sont soit récupérées automatiquement par l’application à des intervalles de temps spécifiés, soit déclenchées manuellement par l’utilisateur.

Le composant *antivol* est conçu pour contrôler à distance un appareil perdu ou volé. Android inclut déjà des fonctionnalités antivol de base telles que le verrouillage de l’appareil, la localisation, l’effacement et l’alarme.
Les produits de sécurité testés étendent cette fonctionnalité avec des fonctionnalités telles que le suivi de localisation, la prise de photos du voleur à l’aide des caméras de l’appareil ou le déclenchement d’actions en réponse à des activités suspectes de l’appareil (par exemple, verrouiller l’appareil lorsque la carte SIM est changée ou essayer de désinstaller l’application de sécurité, capturer des photos après plusieurs tentatives de déverrouillage infructueuses).
En règle générale, le composant antivol est géré via une interface Web ou, dans de rares cas, à l’aide d’un deuxième téléphone sur lequel la même application de sécurité est installée.
Certains fournisseurs (tels que Avast, AVG, Avira) ont décidé de supprimer la fonction antivol de leurs dernières versions d’applications car elle ne fournissait pas une valeur suffisante par rapport aux fonctionnalités intégrées d’Android.

De nombreux produits de sécurité incluent *une protection* Web qui empêche les utilisateurs de télécharger involontairement des applications malveillantes ou d’accéder à des sites Web de phishing tout en naviguant sur

Internet.
La majorité des produits testés offrent une navigation Web sécurisée pour au moins Google Chrome, le navigateur le plus populaire sur Android.
En outre, certaines applications prennent en charge divers navigateurs tiers pour s'adapter au choix de l'utilisateur pour son navigateur mobile préféré.

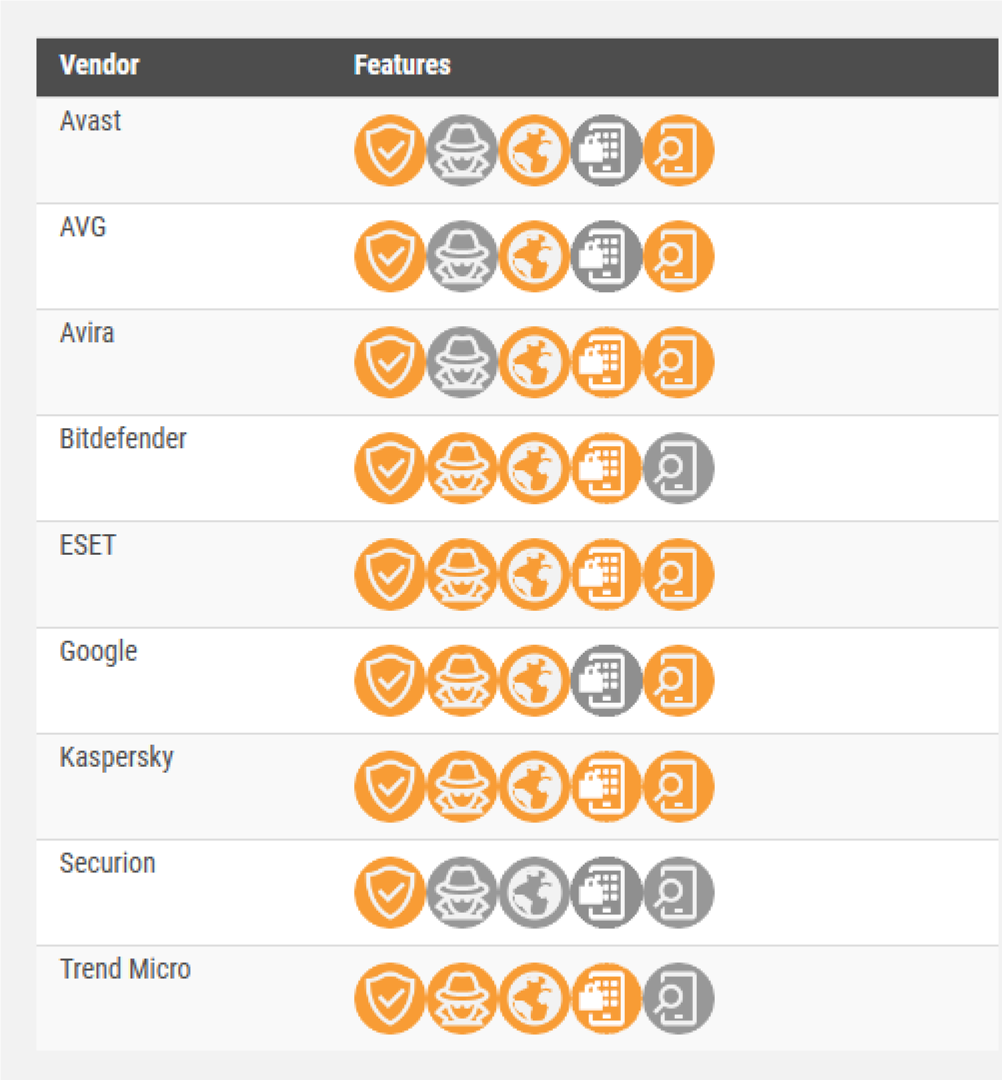
Le verrouillage des applications est une autre fonctionnalité de sécurité utile, permettant aux utilisateurs de protéger les applications sélectionnées contre tout accès non autorisé. Les utilisateurs peuvent configurer un mécanisme de verrouillage, tel qu'un code PIN, un mot de passe, un modèle ou une biométrie (par exemple, une empreinte digitale ou une reconnaissance faciale sur les appareils pris en charge), qui est nécessaire pour lancer une application protégée.
En outre, ils peuvent être en mesure de personnaliser le comportement de verrouillage de l'application, comme le déverrouillage lorsqu'ils sont connectés à un réseau Wi-Fi de confiance ou le verrouillage en fonction de l'emplacement ou du calendrier.

Un *conseiller de confidentialité* ou une fonctionnalité *d'audit d'application* est également inclus dans la plupart des produits testés, qui analyse généralement les applications installées à la recherche d'éventuelles violations de la vie privée.
Cette analyse examine les autorisations d'application qui sont rares, inutiles ou inappropriées, car elles peuvent présenter un risque pour la vie privée de l'utilisateur.
Sur la base de ce résultat, certaines applications de sécurité conseillent de désinstaller les applications « risquées ».

Produits testés

Les produits inclus dans le test et l'examen de cette année sont énumérés ci-dessous. Nous félicitons les fournisseurs de sécurité tiers, qui ont démontré dans ce test que leurs solutions sont efficaces et réputées, et ont contribué à élever la norme pour toutes les solutions de sécurité mobile.
Les derniers produits ont été tirés de Google Play au moment du test (mai 2023).
Après que les produits ont été testés, les fabricants ont eu la possibilité de corriger les défauts que nous avons trouvés.
Tous les problèmes qui ont déjà été résolus sont notés dans le rapport.
Les versions répertoriées ci-dessous s'appliquent aux avis de produits mis à jour.

Avast Mobile Security gratuit 23.3	Fonctionnalités de Google Play Protect & OS 35.7
AVG AntiVirus Gratuit pour Android 23.3	Kaspersky Plus pour Android 11.100
Avira Prime pour Android 7.20	Securion OnAV 1.0
Bitdefender Mobile Security 3.3	Trend Micro Mobile Security 15.5
ESET Mobile Security Premium 8.1	

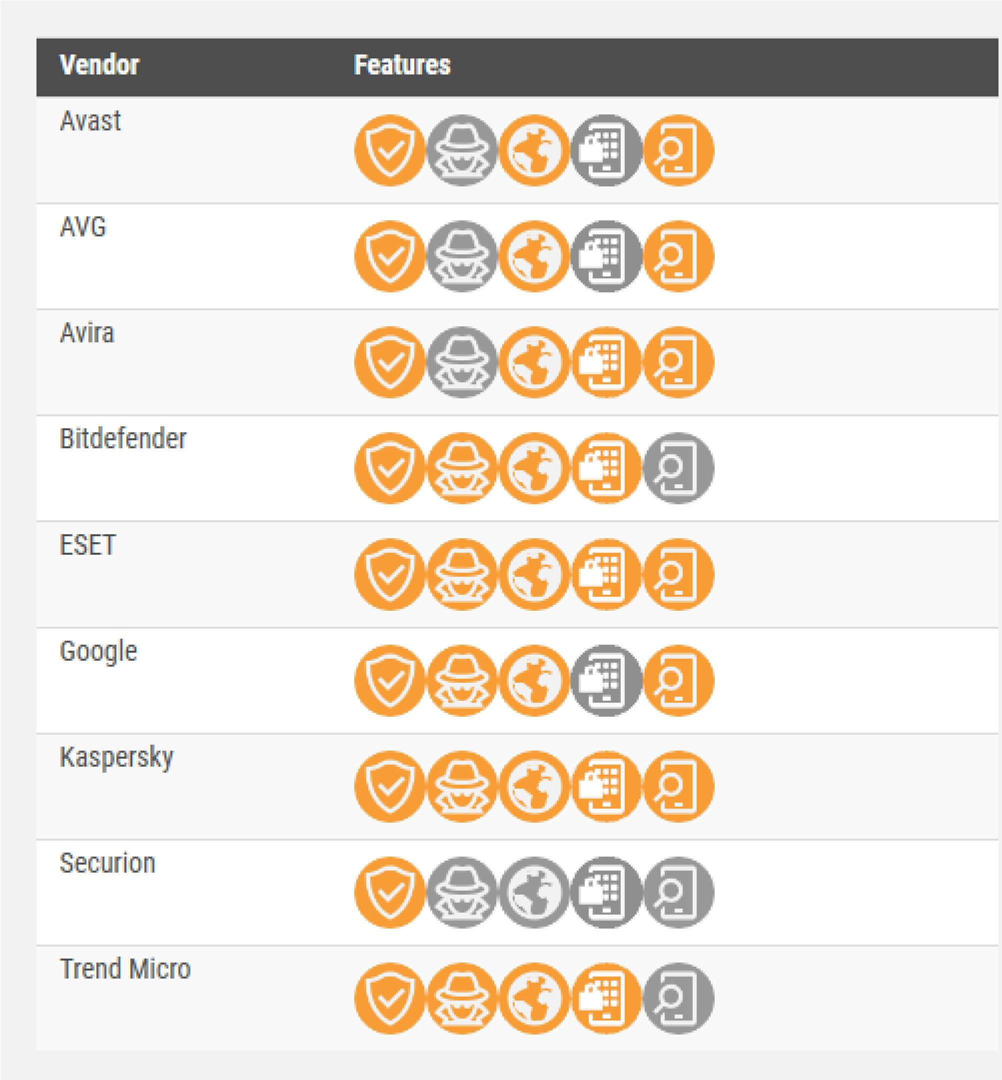


Vendor	Features
Avast	
AVG	
Avira	
Bitdefender	
ESET	
Google	
Kaspersky	
Securion	
Trend Micro	

Symboles

Pour fournir un aperçu simple des caractéristiques d'un produit, nous utilisons les mêmes symboles que ceux de notre site Web.
Au début de chaque rapport, vous verrez ces symboles.
Ceux en orange représentent les caractéristiques du produit, tandis que ceux en gris représentent les caractéristiques qui ne sont pas incluses.
Tous les symboles s'appliquent uniquement à Android 13, que nous avons utilisé dans notre test.

Pour ce rapport, nous avons utilisé Android 13 qui est actuellement la version Android la plus récente.
Nous avons utilisé la version non modifiée d'Android 13 afin d'éviter les problèmes potentiels avec les modifications des fabricants de matériel ou des opérateurs mobiles.

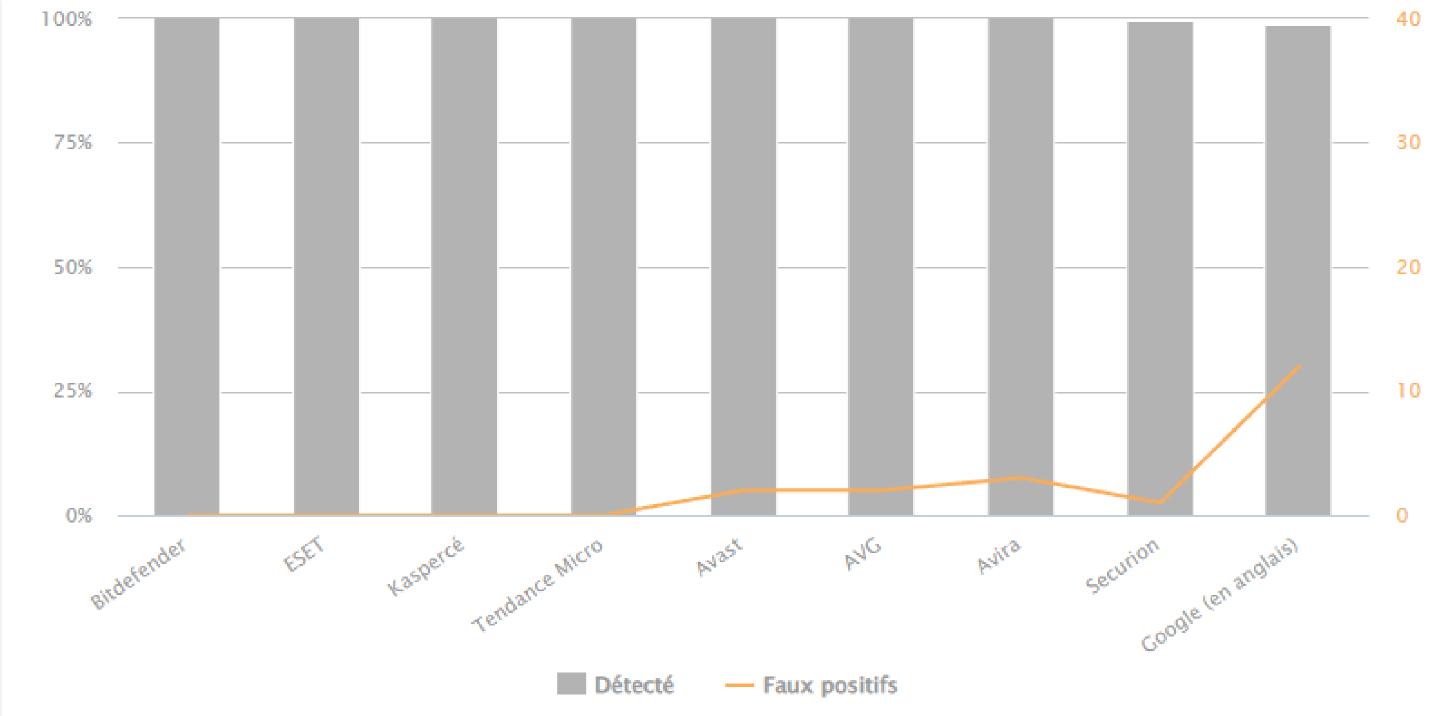


Procédure d’essai

Le logiciel malveillant utilisé dans le test a été collecté par nous dans les quelques semaines précédant le test.
Nous avons utilisé **2 730** applications malveillantes pour créer un ensemble de tests représentatif.
Les applications avec les mêmes certificats et/ou le même code interne ont été supprimées, afin de disposer d’un ensemble de test d’échantillons véritablement uniques. Les produits de sécurité ont été mis à jour et testés le 15 mai 2023.
Le test a été effectué avec une connexion Internet active sur des smartphones Android authentiques (aucun émulateur n’a été utilisé).
L’ensemble de test se composait exclusivement de fichiers APK.
Si disponible, une analyse à la demande a d’abord été effectuée.
Après cela, toutes les applications non détectées ont été installées et lancées.
Nous avons fait cela pour permettre aux produits de détecter le malware à l’aide d’une protection en temps réel.
Un test de faux positifs a également été effectué à l’aide de 500 applications propres.

Résultats des tests

Les résultats peuvent être vus ci-dessous (triés par protection contre les logiciels malveillants et nombre de fausses alarmes; les produits avec des scores identiques sont triés par ordre alphabétique).



Tarifs de protection mobile		
	Taux de protection	Faux positifs
Bitdefender, ESET, Kaspersky, Trend Micro	100%	0
Avast, AVG	100%	2
Avira	100%	3
Securion	99.7%	1
Google (en anglais)	98.9%	12[1]

[1] Principalement détecté comme un risque d'atteinte à la vie privée.

Résultats du test de décharge de la batterie

Comme lors de nos enquêtes précédentes, nous avons mesuré la consommation d'énergie supplémentaire causée par chacun des produits de sécurité mobile.
Tester l'utilisation de la batterie d'un appareil peut sembler très simple à première vue.
Si l'on entre plus dans les détails, les difficultés deviennent évidentes.
En particulier avec les téléphones mobiles, les habitudes d'utilisation des différents utilisateurs sont très variées.

Certains utilisent largement les fonctions multimédia, d’autres visualisent beaucoup de documents, tandis que d’autres n’utilisent que les fonctions téléphoniques.
Nous devons faire la différence entre les utilisateurs expérimentés qui profitent de toutes les fonctions possibles de l’appareil et les utilisateurs traditionnels qui se contentent de passer et de recevoir des appels téléphoniques.

Le test a déterminé l’effet du logiciel de sécurité sur l’utilisation de la batterie pour l’utilisateur moyen.
Le scénario d’utilisation quotidienne suivant a été simulé :

- 30 minutes de téléphonie
- 82 minutes à regarder des photos
- 45 minutes de navigation sur Internet à l’aide du navigateur Google Chrome
- 17 minutes à regarder des vidéos YouTube à l’aide de l’application YouTube
- 13 minutes à regarder des vidéos enregistrées sur le téléphone lui-même
- 2 minutes d’envoi et de réception de courriels à l’aide du client Google Mail
- 1 minute d’ouverture de documents enregistrés localement

Lors de notre test, nous avons constaté que tous les produits de sécurité mobile testés n’avaient qu’une influence mineure sur la durée de vie de la batterie, comme indiqué dans le tableau ci-dessous.
En général, nous avons pu attribuer aux applications de sécurité mobile testées des notes élevées en matière de consommation d’énergie.

Résultats de décharge de la batterie	
Avast	
AVG	
Avira	
Bitdefender	
ESET	
Google (en anglais)	
Kasperсé	
Securion	
Tendance Micro	

jusqu’à 3 % | 3 à 8 % | 8 à 15 % | 15 à 25 % | > 25 %

Avis sur les produits

Format de révision

Ici, nous avons décrit la structure des critiques de produits suivantes pour chacune des applications de sécurité mobile dans ce test.
Étant donné que les produits testés incluent différents ensembles de fonctionnalités, toutes les sections concernant les fonctionnalités de l'application (à l'exception d'Anti-Malware) peuvent ne pas leur être applicables.

Introduction:
Nous fournissons un aperçu concis du produit, indiquant son modèle de prix (gratuit ou payant) et soulignant ses principales caractéristiques.
Nous limitons le nombre de fonctionnalités aux cinq fonctionnalités de sécurité et de confidentialité de base (indiquées par les symboles dans le coin supérieur droit de l'examen du produit) et à cinq fonctionnalités supplémentaires que nous jugeons remarquables.
Pour faciliter la comparaison et améliorer la lisibilité, nous utilisons des termes normalisés de notre liste de fonctionnalités qui se trouve à la fin de ce rapport.

Usage:
Nous décrivons brièvement le premier démarrage de l'application, la configuration initiale de l'application et comment accéder aux fonctionnalités de l'application à partir de l'écran principal de l'application.

Anti-malware:
Nous expliquons ce que fait l'analyse des logiciels malveillants, si des suggestions d'actions de l'utilisateur sont affichées après l'analyse initiale, quelles options d'analyse (par exemple, analyse rapide, complète, planifiée) et les paramètres du comportement de détection sont disponibles, et mentionnons des résultats intéressants si un logiciel malveillant est détecté.

Antivol :
Le cas échéant, nous décrivons comment configurer la fonctionnalité, configurer les commandes disponibles et comment les déclencher à distance.
Nous notons également des paramètres supplémentaires et des commandes erronées ou un mauvais comportement lors de l'exécution.
Un tableau à la fin de l'examen du produit montre un résumé des commandes antivol disponibles.

Protection Web / Wi-Fi:
Le cas échéant, nous décrivons différentes fonctionnalités de protection contre les menaces Web et/ou les vulnérabilités sur les réseaux Wi-Fi.
Il s'agit, par exemple, de l'anti-hameçonnage, du VPN et du scanner Wi-Fi.

Verrouillage / Audit de l'application:
Le cas échéant, nous décrivons la fonction de verrouillage avec ses paramètres, qui permet de protéger les applications sélectionnées contre les accès non autorisés, et/ou la fonctionnalité pour examiner les aspects clés des applications installées tels que les autorisations, l'utilisation des données et l'espace de stockage.

Contrôle parental :
Le cas échéant, nous envisageons des capacités pour réguler et surveiller les activités des appareils des

enfants et les protéger contre les contenus inappropriés.
Il s’agit, par exemple, du verrouillage des applications, du filtrage Web et des limites d’utilisation quotidienne.

Protection de la vie privée :
Le cas échéant, nous énumérons plusieurs autres fonctionnalités qui peuvent aider à améliorer davantage la confidentialité de l’utilisateur, par exemple, le filtre d’appel, le vérificateur de fuite de données, le scanner de confidentialité des réseaux sociaux, la protection contre les liens frauduleux ou malveillants dans les notifications et les messages texte.

Caractéristiques supplémentaires:
Nous énumérons les fonctionnalités supplémentaires de l’application qui n’appartiennent pas à l’une des catégories précédentes et nous pensons qu’elles méritent d’être mentionnées.
Ceux-ci peuvent inclure des outils d’optimisation du système pour arrêter les applications en arrière-plan ou supprimer les fichiers indésirables et un gestionnaire de tâches pour désinstaller / désactiver les applications installées.

Conclusion:
Nous donnons une brève conclusion du produit, notre expérience avec celui-ci, et laissons une déclaration si une fonction révisée n’a pas fonctionné correctement et n’a pas été corrigée avant cette publication.

Niveaux d’attribution atteints dans cet examen de la sécurité mobile

AV comparatives
APPROVED
Mobile Security
2023

Notes

Le produit de sécurité mobile parfait pour tous les appareils et tous les utilisateurs n’existe pas.
Comme pour les produits Windows, par exemple, nous vous recommandons d’établir une courte liste de produits qui pourraient vous convenir, après avoir lu les avantages et les inconvénients de chaque produit dans notre revue.
Une version d’essai gratuite de chaque produit candidat peut ensuite être installée et testée pendant quelques jours (un à la fois).
Cela devrait faciliter la décision.

Avec les produits de sécurité Android en particulier, de nouvelles versions avec des améliorations et de nouvelles fonctions sont constamment publiées.

Huit des produits de cette année sont admissibles à notre prix « Produit mobile approuvé ». Pour être certifiées cette année, les applications devaient avoir un taux de protection contre les logiciels malveillants d'au moins 99%, pas plus de 10 FP et un impact de décharge de la batterie inférieur à 8%.
De plus, les fonctionnalités de base de chaque programme devaient fonctionner de manière fiable sans problèmes majeurs.

Avast	**APPROUVÉ**
AVG	**APPROUVÉ**
Avira	**APPROUVÉ**
Bitdefender	**APPROUVÉ**
ESET	**APPROUVÉ**
Google (en anglais)	NON APPROUVÉ
Kaspercé	**APPROUVÉ**
Securion	**APPROUVÉ**
Tendance Micro	**APPROUVÉ**

Droits d'auteur et avis de non-responsabilité

Pour plus d'informations sur AV-Comparatives et les méthodologies de test, veuillez visiter notre site Web.

AV-Comparatives
(Juin 2023)

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230711
"C'est ensemble qu'on avance"