Independent Tests of
Anti-Virus Software

Mobile Security Review 2021

TEST PERIOD: JUNE 2021

LAST REVISION: 30TH JUNE 2021

WWW.AV-COMPARATIVES.ORG

Content

Introduction

In this report, we try to assist readers in evaluating both Android's built-in security measures and the additional, more sophisticated features provided by third-party security apps. In addition to the results of comprehensive malware protection and battery consumption tests, the report includes reviews that evaluate the functionality, app design and overall usability of each security solution. A short table at the end of each product report gives an overview of any anti-theft functions included in that product. Many of the reviewed and tested apps have non-security related components, such as app managers, network monitors, and system optimizers. However, we mainly focus on the security features (anti-malware, anti-theft, safe browsing, and privacy) in our reviews, and only mention further functionality briefly. The structure of each product report is kept identical, to allow readers to compare products more easily.

Recently, we also evaluated how well some security apps protect against stalkerware on Android[1]. This type of software does its best to remain undetected, and allows an unauthorized party to spy on the device owner's activities without his or her knowledge or consent. Although there is no clear-cut difference between stalkerware and legitimate software (e.g. parental control), Google Play has been introducing stricter policies to fight this phenomenon in recent years. Most stalkerware can thus be installed only through side-loading[2].

The main purpose of a mobile security product is to protect users and their devices from potential harm inflicted by malicious apps, fraudulent mails, phishing URLs, and other harmful links. Recent Android versions already incorporate some basic security features. Google's built-in malware scanner *Play Protect* scans apps during installation from the Google Play store or a third-party source, and regularly checks the device for any threats. The *Safe Browsing* API protects against malware and phishing links while surfing the Internet using the Google Chrome browser. Anti-theft functions (lock, locate, alarm, and wipe) are provided via Google's *Find My Device* feature, allowing the user to find a lost or stolen phone, and to prevent access to any personal data stored on the device.

In the following pages, we discuss features and restrictions regarding privacy and security in *Google Android*. We note that not all of Google's security features are available to all users, as there are limitations with some Android versions, Android-based operating systems, and geographical locations. After that, we talk about the current risks facing smartphone users, and give recommendations for achieving better protection. At the end of the introduction, we give a short summary of common security features and typical main sub-components of typical Android security apps. In the main section of this report, we present the participating security products, along with the results of the malware protection tests, the battery drain test, and the detailed reviews of the individual products. For a product's anti-theft component, we comment on each function briefly and use the following symbols in the table to indicate how well it worked in our tests.

✔	▬	✖
no issues	minor issue(s)	major issue(s)

[1] https://www.av-comparatives.org/reports/android-stalkerware-report-2021/
[2] https://en.wikipedia.org/wiki/Sideloading

Google Android

With the introduction of run-time permissions in Android 6.0 (Marshmallow), Google gave users more control over the information and private data their apps have access to. This approach is very different from the one adopted by earlier Android versions, where apps asked the user to grant all the necessary permissions prior to installation. Since Android 8.0 (Oreo), the global security setting *Install from unknown sources* has been a run-time permission that needs to be granted for each app once. The built-in malware protection *Play Protect* is preinstalled on devices running Android 8.0 or later, and is also available on older Android devices that support Google Play Services 11 or later. Additional functions for device loss (*Find My Device*) and safe browsing for Google Chrome were integrated as regular components as well.

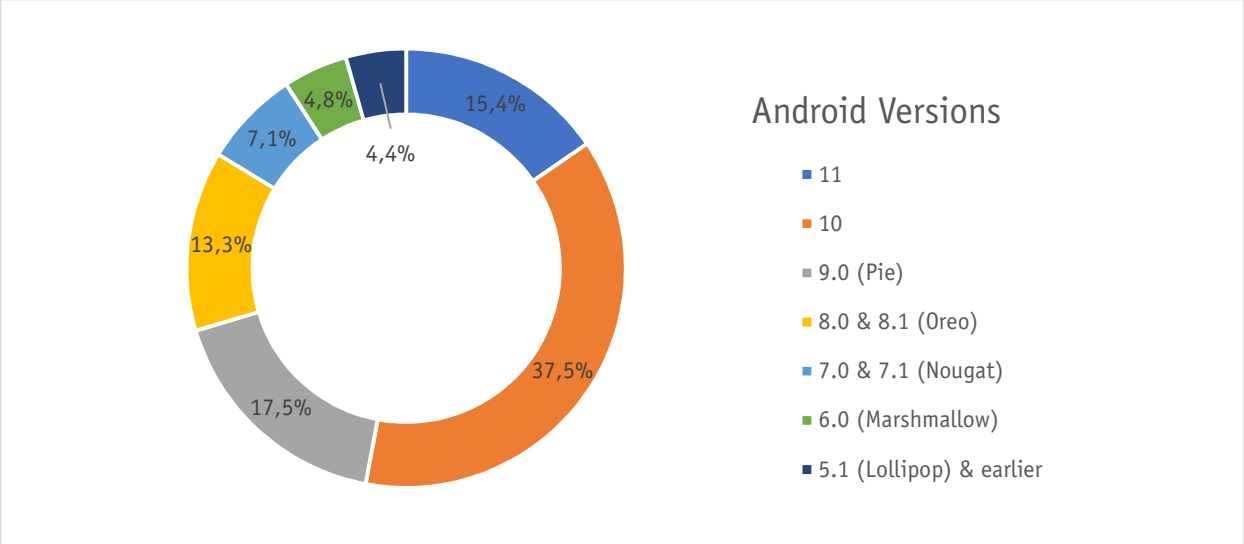
Android 10 brought some significant improvements for user privacy, e.g. the concept of scoped storage, the opportunity to limit the access to some resources (e.g. location) to times when the app is in active use, and certain restrictions to background apps. Apps (except for privileged/system apps) are also prevented from accessing certain device information, e.g. non-resettable device identifiers like IMEI, IMSI, MEID, SIM, and build serial number. The MAC address is randomised by default while connected to networks.

In September 2020, Android 11 became officially available. This builds upon concepts introduced in Android 10, putting special emphasis on transparency and user privacy[3]. One important change is to grant apps one-time permissions concerning location, microphone, and camera. Apps can no longer access location information when running in the background, unless the user explicitly enables the option "Allow all the time" in the system settings. An auto-reset feature was added, which automatically resets all run-time permissions for unused apps. Only privileged apps are allowed to access the device's randomized MAC address. The scoped storage has been enforced to prevent access to the legacy external storage, and apps are also restricted when querying a full list of installed apps and all their details.

For this review, we decided to use the most widely used Android version, which is currently Android 10 (37.5%) as the ring chart below shows[4]. The resulting restrictions imposed on apps for Android 10 or later have affected mobile security vendors, among others. Their apps require all device permissions, including device admin rights, if they are to fully monitor and control the device, and protect sensitive user data against security threats. We used the unmodified version of Android 10, as provided by Google, in order to avoid potential problems with hardware manufacturers' or mobile carriers' modifications.

Although Google Play Protect aims to protect users, there is still room for improvement. Unfortunately, this will not help users in mainland China, due to the service being inaccessible there. For users who are unable to access Android's built-in security features, there is a very strong argument for using a third-party security app. Even for people who do have full access to Google's protection features, a third-party app can still provide very valuable extra protection. We note that third-party security apps for Android supplement, rather than replace, Google's security features.

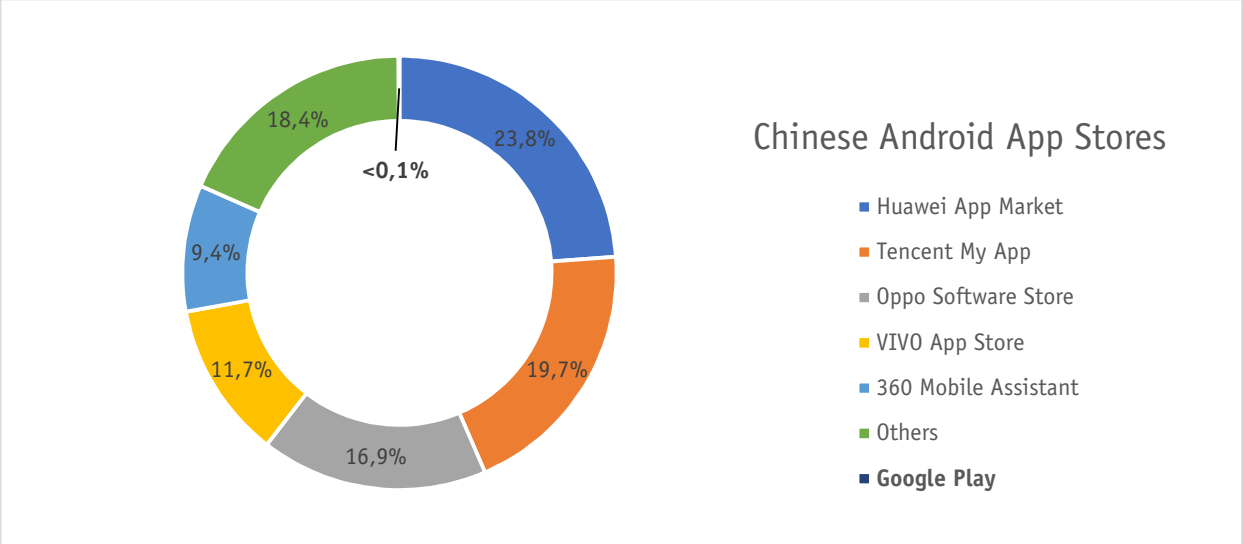
[3] https://developer.android.com/about/versions/11
[4] https://gs.statcounter.com/android-version-market-share/mobile/worldwide/#monthly-202105-202105-bar



Due to Google's built-in malware and protection features, one might think that third-party anti-virus apps are no longer so important for Android devices. However, it should be noted that only Android devices that have installed Google Play and Services, along with Play Protect, benefit from Google's protection. Other devices based on modified Android OS versions (e.g., HarmonyOS, FireOS, LineageOS) do not run Google apps by default; hence, there is no built-in malware protection. In regions such as the United States and Europe, only two official app stores dominate the mobile app market: Google Play and the Apple App Store. The risk of inadvertently downloading and installing malware from Google Play is small, as the app store is regularly checked for fraudulent and dangerous apps.

However, in many Asian countries, especially China, the risk of being infected by malware is much higher. There are many app stores provided by various third-party vendors, and many smartphones are rooted as well. There are about 1.61 billion[5] active mobile devices in China, and about 78.6%[6] of them run Android as the operating system. The most used Android app stores are shown in the ring chart[7] below. With about 23.8% of active users in Q1 2021, Huawei App Market overtook last year's leader, Tencent MyApp, on 19.7%. Google Play is used by almost no one (<0.1%). This is because Google Play and most of Google's services are inaccessible in mainland China.

[5] https://datareportal.com/reports/digital-2021-china
[6] https://gs.statcounter.com/os-market-share/mobile/china
[7] https://www.appinchina.co/market/app-stores



In November 2020, a US executive order[8] was signed, prohibiting US companies (such as Google) from doing business with blacklisted Chinese companies. This also affected Chinese telecommunications and smartphone-manufacturer giants, who produce and sell mobile devices running Android worldwide. Consequently, Google apps and services, including Play Protect, will no longer be available on future device models from certain Chinese developers, but Google[9] assured users that devices sold before May 16th, 2019 would still receive the update to Android 10.

[8] https://home.treasury.gov/system/files/126/13959.pdf
[9] https://support.google.com/android/thread/29434011

Protection against Android Malware

Today, the smartphone is often used as a replacement for the PC, and so is frequently employed for common, daily tasks such as online shopping, online banking, money transfers, instant messaging, video conferencing, and emailing. Cyber-attacks are becoming more and more sophisticated, and increasingly target mobile devices, with fraudulent applications attempting to steal user data or money. These apps often appear as fake[10] versions of popular apps, the genuine versions of which have been downloaded by millions of users[11]. To reduce the risk of becoming a victim, we suggest following the advice given here.

Only download apps from official app stores like Google Play, or stores of reputable app makers; avoid third-party stores and side-loading. A quick look at the reviews in the app store before installing an app might help. Avoid apps with predominantly bad or dubious reviews. Assess requests for irrelevant access rights or permissions by questionable apps critically. Of course, not every app that shows strange behaviour is necessarily malicious, but it is good to consider whether it is genuine and worthy of use. Google Play continuously updates its policy to guarantee a certain degree of security, e.g. requiring app developers to verify their identity, digitally sign their apps, and meet the target API level requirements[12]. In recent years, apps have also had to undergo several review processes and be approved by Google regarding privacy (e.g. access to SMS and background location) to stay in Google Play.

Rooting the smartphone increases the potential that malicious apps will take control of the device. Furthermore, it is not legally clear-cut for some manufacturers whether the warranty is still valid if the phone is rooted. Public Wi-Fi networks (e.g., coffee shop, airport) are popular targets for attackers to steal and comprise sensitive data. Therefore, we advise against entering/sharing sensitive data (user credentials, bank/credit card information, etc.) when connected to a public Wi-Fi, unless you are using a VPN connection; this will encrypt your network traffic and so prevent hackers from reading it. It is also important to keep your mobile device up to date with the latest security patches and Android version, which ensures that previous device vulnerabilities and potentially dangerous APIs are fixed.

How high is the risk of malware infection with an Android mobile phone?

This question cannot be answered in one sentence, as it depends on many different factors. As mentioned in previous sections, when sticking to official stores such as Google Play, the risk of the smartphone becoming infected is relatively low. In Asian countries, where many rooted devices and large number of third-party app stores can be found, the chance of installing a dangerous app is greatly increased. However, we must point out that “low risk” is not the same as “no risk”. The threat situation can change quickly and dramatically. It is better to be ready for this, and to install appropriate security software on the smartphone. Currently, we would say that in western countries, protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

[10] https://www.av-comparatives.org/tests/android-test-2019-250-apps/
[11] https://www.zdnet.com/article/this-android-trojan-malware-is-using-fake-apps-to-infect-smartphones-steal-bank-details/
[12] https://developer.android.com/distribute/best-practices/develop/target-sdk.html

Security Features

In this section, we give a brief overview of common security-related components found in most security products for Google Android. The most obvious component of a mobile security app is the *malware scanner* which protects the user against the inadvertent installation of malicious apps on his or her device. Like anti-virus programs for Microsoft Windows, mobile security apps for Android use a number of different protection features. The *real-time protection* checks new apps during the setup process. This prevents the device being compromised by the installation of a malicious program.

The *on-demand scanner* searches the whole device (internal storage and/or external SD card) for any malicious apps that are already installed, or downloaded APK files that have not yet been run. For apps that rely mainly on malware definitions to detect malware, keeping these definitions up to date is a critical factor in effective protection. Some vendors offer more frequent updates with their paid premium versions than with the corresponding free versions. A number of the tested products offer a cloud-assisted malware scanner to ensure the app has access to the very latest definitions. Updates are either retrieved automatically by the app at specified intervals or triggered manually by the user.

A major component in mobile security apps is the *anti-theft* module. It is designed to remotely control a target device that has been lost or stolen. Android already includes core anti-theft features such as device lock, location, wipe, and alarm. Many of the security products we tested extend this base functionality with additional features such as location tracking, taking pictures of the thief using the device's built-in front camera, or triggering actions on suspicious device activities (e.g., locking device on SIM card change, or taking pictures on multiple failed unlock attempts). Usually, the anti-theft component is controlled via a web interface, or (rarely) using a second phone that has the same security app installed.

Many security products offer *web protection*, which prevents the user from unintentionally downloading malicious apps or accessing phishing websites while surfing the Internet. Almost all products in our test have integrated safe web browsing, at least for Google Chrome, which is the most commonly used Android browser. Some apps support a variety of different third-party browsers in addition, including those made by the respective vendors themselves. This is an important factor, as many users like to use their preferred browser on their smartphones.

Another useful feature some products provide is *app lock*. It allows the user to protect selected apps against unauthorized access. The user can set up a locking mechanism, such as PIN, password, pattern, or fingerprint, which is required to launch a protected app. Some security apps offer options to further customize the app locking behaviour (e.g. unlock when connected to a trusted Wi-Fi, lock by location, or lock by time schedule).

A *privacy advisor* or *app audit* feature is also included in most of the tested products, which typically scans the installed apps for possible privacy violations. In other words, apps are analysed for uncommon, unnecessary, or inappropriate app permissions, which could lead to the user's private sphere being breached. As a result of this scan, some security products advise the user to uninstall "risky" apps.

Products tested

The products included in this year's test and review are listed below. We congratulate the third-party security vendors, who have demonstrated in this test that their solutions are effective and reputable, and helped to raise the standard for all mobile security solutions. The latest products[13] were taken from the Google Play Store at the time of the test (June 2021). After the products were tested, manufacturers had the opportunity to fix any flaws we found. Any problems that have already been solved are noted in the report.

Vendor	Product Name	Version	Features
Avast	Mobile Security (Free)	6.39	
AVG	AntiVirus for Android (Free)	6.39	
Avira	Antivirus Security for Android	7.8	
Bitdefender	Mobile Security	3.3	
G Data	Mobile Security	27.3	
Google	Play Protect & OS Features	25.8	
Kaspersky	Internet Security for Android Premium	11.69	
Malwarebytes	Malwarebytes for Android	3.7	
Securion	OnAV	1.0	
Trend Micro	Mobile Security	12.6	

Symbols

To provide a simple overview of the features of a product, we use the same symbols as those on our website. At the beginning of every report, you will see these symbols; those in orange represent features the product has, while those in grey represent features that are not included. All symbols apply to Android 10 only, which we used in our test.

Anti-Malware	includes a feature to scan against malicious apps
Anti-Theft	includes remote features in case the smartphone gets lost or stolen
Safe Browsing	includes a web filtering feature to block dangerous sites
App Lock	includes a feature to prevent unauthorised access to installed apps
App Audit	includes features to audit installed apps

[13] https://www.av-comparatives.org/list-of-mobile-security-vendors-android/

Overview

The perfect mobile security product for all devices and all users does not exist. As with e.g. Windows products, we recommend drawing up a short list of products that might suitable for you, after reading about the advantages and disadvantages of each product in our review. A free trial version of each candidate product can then be installed and tested for a few days (one at a time); this should make the decision easier. With Android security products in particular, new versions with improvements and new functions are constantly being released.

Eight of this year's products qualify for our "Approved Mobile Product" award. To be certified this year, apps had to have a malware protection rate of at least 99%, not more than 10 FPs, and a battery drain impact of under 8%. Additionally, the core features of each program had to function reliably without any major issues.

Avast Mobile Security (Free) provides well-developed security features for almost any use case, with extensive options to customize each feature.

AVG AntiVirus for Android (Free) offers a wide range of security and non-security features, along with configuration options for many use cases.

Avira Antivirus Security for Android is a comprehensive security app that provides remote device control via in-app commands and privacy-oriented features.

Bitdefender Mobile Security is an easy-to-use mobile security product with elaborate device protection and privacy-enhancing tools.

G Data Mobile Security offers a comprehensive set of security functions for Android devices in a completely redesigned and modern user interface.

X **Google** Android includes built-in malware protection along with a device loss/theft and safe-browsing feature. Unfortunately, the protection rate is still too low, and the false alarm rate too high, for certification.

Kaspersky Internet Security for Android Premium is a mobile security app with a user-friendly interface, which provides an extensive set of features protecting the device and user privacy.

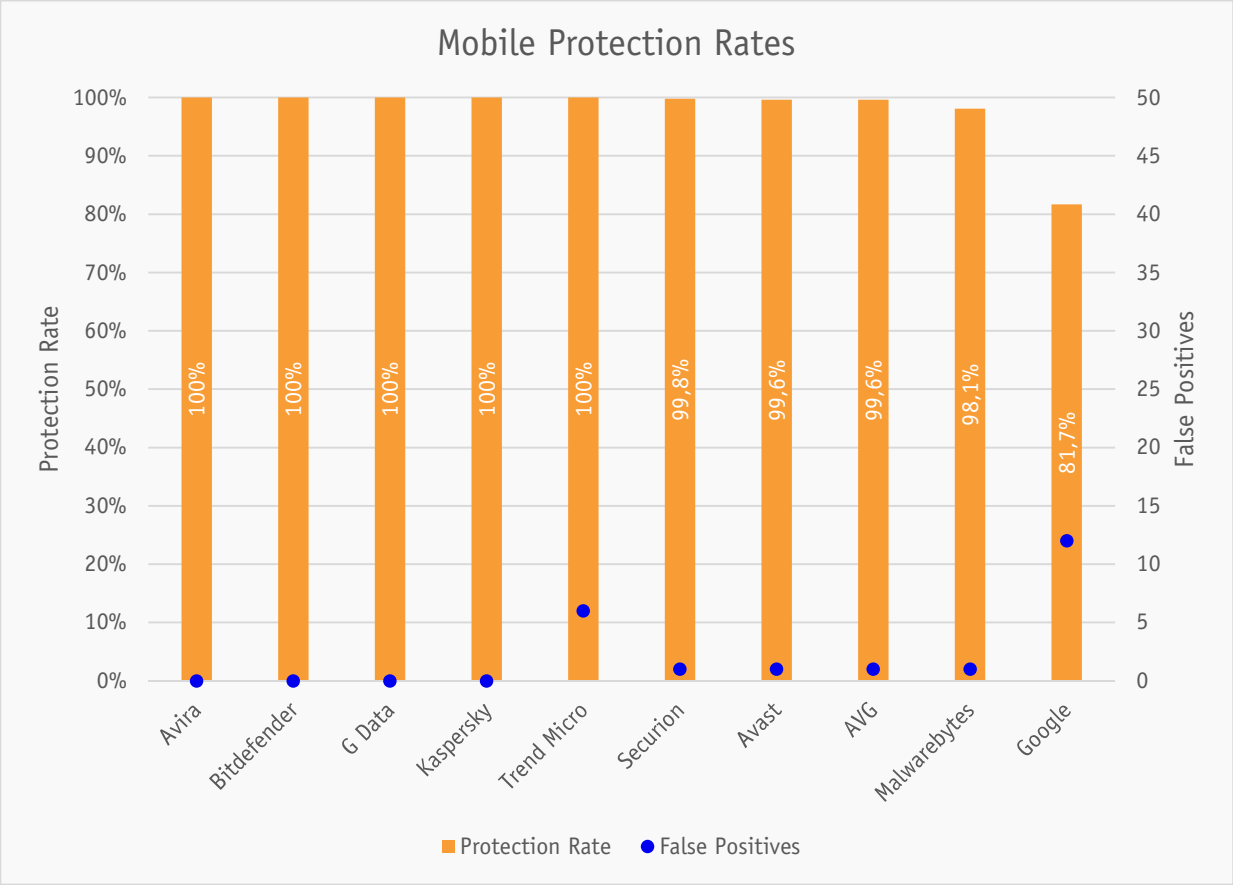
X **Malwarebytes** for Android combines real-time malware and ransomware protection, basic web protection, and app auditing. Unfortunately, it did not reach the required protection level for certification.

Securion OnAV is a slim and basic mobile security solution offering solely malware protection capabilities.

Trend Micro Mobile Security is a well-designed app for Android, which integrates functions for malware, theft, and web protection, as well as further device management tools.

Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **3,568** malicious applications, to create a representative test set. Apps with the same certificates and/or the same internal code were removed, in order to have a test set of genuinely unique samples. So-called "potentially unwanted applications" (PUA) were excluded. The security products were updated and tested on the 8th June 2021. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of APK files. If available, an on-demand scan was conducted first. After this, every undetected app was installed and launched. We did this to allow the products to detect the malware using real-time protection. A false-positives test was also carried out using 500 popular apps. The results can be seen below (sorted by Malware Protection and number of False Alarms; products with identical scores are sorted alphabetically).



Mobile Protection Rates		
	Protection Rate	**False Positives**
Avira, Bitdefender, G Data, Kaspersky	100%	0
Trend Micro	100%	6[14]
Securion	99.8%	1
Avast, AVG	99.6%	1
Malwarebytes	98.1%	1
Google	81.7%	12

[14] Detected as privacy risk.

Battery Drain Test Results

As in our previous reports, we measured the additional power consumption of an installed mobile security product. Testing the battery usage of a device might appear to be very straightforward at first glance. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones, the usage patterns of different users are very varied.

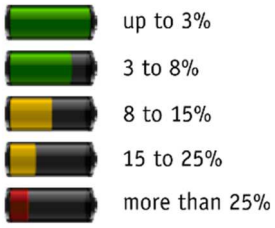
Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users who take advantage of all the possible functions in the device and traditional users who merely make and receive phone calls.

The test determined the effect of the security software on battery use for the average user. The following daily usage scenario was simulated:

- 30 minutes telephony
- 82 minutes looking at photos
- 45 minutes surfing the Internet using the Google Chrome browser
- 17 minutes watching YouTube videos using the YouTube app
- 13 minutes watching videos saved on the phone itself
- 2 minutes sending and receiving mails using the Google Mail client
- 1 minute opening locally saved documents

In our test, we found that the tested mobile security products had only a minor influence on battery life, as outlined in the table below.

Battery Drain Results	
Avast	
AVG	
Avira	
Bitdefender	
G Data	
Google	
Kaspersky	
Malwarebytes	
Securion	
Trend Micro	



In general, we were able to give the tested security suites high marks regarding power usage.

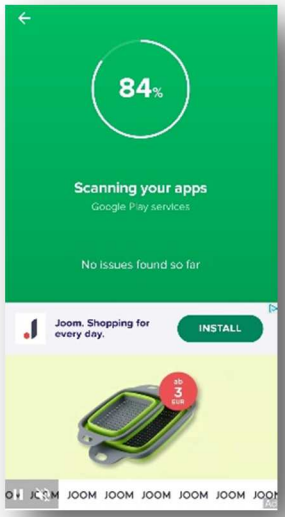
Avast

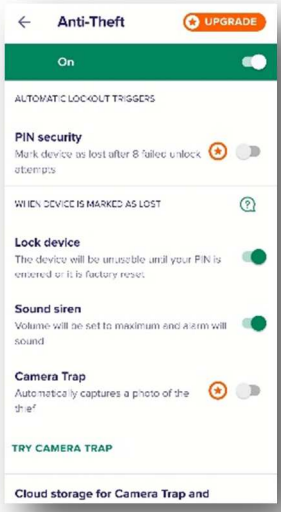
Mobile Security (Free)

6.39.5

Introduction

Avast Mobile Security is a freemium and ad-supported product which includes a variety of security- and privacy-oriented features such as malware scan, web and Wi-Fi security, Hack Alerts, and App Insights. Photo Vault and anti-theft functionality are also included, but with some limitations. Other app components, such as Junk Cleaner and Wi-Fi Speed, help the user monitor different aspects of the device. Avast asked us to test and review the free version of their product. Please note that Avast owns AVG, and the respective Android apps appear to be identical in functionality. There are some minor differences in the user interface, however.





Usage

As soon as the user opens the app for the first time, he/she has to agree to Avast's Agreement and Privacy Policy. Afterwards, the user is prompted to give storage permission in order to start a scan of the device, and to choose between the offered license models. The user must also agree to Avast's Content Policy before being redirected to the main screen.

Anti-Malware

Upon scanning the device for the first time, Avast asks for permissions to access photos, media, and files on the device in order to perform a file-system scan.

If the user decides to deny them, the app performs an app-only scan. The app provides further scan settings, for instance the detection of PUA or apps with low reputations, which are enabled by default, and the option to scan apps during installation and upon launch.

The user is also prompted to activate an additional security measure to scan files for malicious behaviour. The external storage (e.g. SD card) is not included when scanning the device storage. The user is however able to scan custom folders or files, and to schedule a scan for any day and time.

Anti-Theft

Anti-theft commands are listed in the table below. The anti-theft setup requires the user to choose an app-specific PIN – optionally a pattern and/or fingerprint – and an account for resetting the PIN and accessing the web interface at *my.avast.com*. The app has to be granted various permissions, among which are device admin rights, in order to execute remote commands from the web interface. The user can use the remote commands Locate, Lock, Mark as Lost, Wipe and Siren, display a text message upon locking the device, and has access to basic information about the device, such as battery status. The Avast PIN and protection mechanisms can be modified via the web interface. The app allows the user to try out the Camera Trap feature, which activates the front camera of the device.

Web & Wi-Fi Protection

The features Wi-Fi Security and Wi-Fi Speed monitor the network for security threats and test the connection speed, respectively. Automatic scanning of new networks is also possible. Web Shield offers protection against malicious URLs and phishing websites for different browser apps.

App Audit

App Insights allows the user to monitor installed apps, providing him/her with detailed usage statistics for individual apps (e.g. storage, battery impact, mobile data used) over different time periods (daily, weekly, monthly). The user can also set a data usage limit and a corresponding alert. Furthermore, all installed apps are ranked using the risk categories "low", "average", and "high", depending on the private data and permissions they access.

Additional Features

Photo Vault enables the user to store up to ten photos, which are then encrypted and hidden from other users. Hack Alerts allows the user to check whether their email or any related accounts have been involved in a data breach. Junk Cleaner helps free up storage space by removing junk files. Furthermore, My Statistics shows a summary of security-related actions taken by Avast on the device, e.g. number of threats prevented.

Conclusion

Avast Mobile Security is a well-designed anti-malware application that gives the user access to many, but restricted, security features. Optimization and privacy-enhancing tools are also available. All the tested anti-theft commands from and to the device worked as expected.

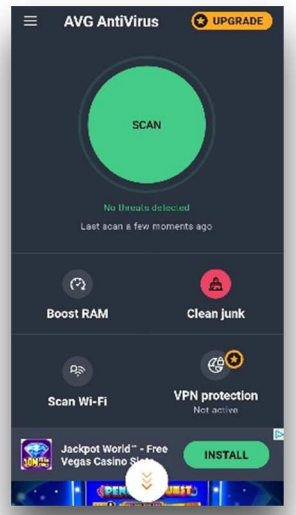
Anti-Theft Details		
Commands Web		
Locate	✔	Displays the location on *Google Maps*. Tracking the device can be enabled.
Mark as Lost	✔	Triggers configured actions like tracking, lock, and siren.
Siren	✔	Activates/deactivates the phone siren.
Lock	✔	Locks/unlocks the phone.
Wipe	✔	Triggers a factory reset and wipes the external storage.

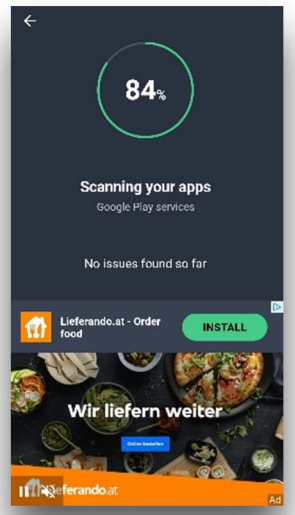
AVG

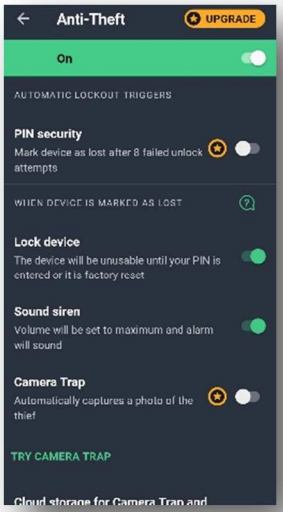
AntiVirus for Android (Free)
6.39.5

Introduction

AVG AntiVirus is a freemium product offering a comprehensive set of tools aimed at protecting the user's security, among which are malware scan, web and Wi-Fi security, and Hack Alerts. The anti-theft and Photo Vault components are included as well, but have some limitations. Further app features allow the user to monitor different privacy and performance aspects of their device. AVG asked us to test and review the free version of their product. Please note that AVG is owned by Avast, and the respective Android apps appear to be identical in functionality. There are some minor differences in the user interface, however.







Usage

After installation, the user has to agree to the vendor's Privacy Policy and Agreement, and is asked for permission to run a file-system scan. The app then lets the user choose to either upgrade to the Pro version or continue with the free and ad-supported version. The user must also accept the Consent Policy on the matter of personalized advertising, and is then redirected to the app's main screen.

Anti-Malware

When a malware scan is started for the first time, the app asks for access to photos, media, and other files on the device. It then starts a scan of the installed apps and, if granted the necessary permissions, of the internal file storage.

The external storage (e.g. SD card) is excluded from this scan. The app checks the device's security settings and warns the user if any of the protection shields, aimed at protecting the device during the download and installation of malicious apps and files, as well as from phishing websites, are currently turned off. The settings to treat PUA as malware, and to warn about apps with a poor reputation, are adjustable but already enabled by default. Furthermore, the user can choose to schedule scans for any day and time.

Anti-Theft

Anti-theft commands are listed in the table below. During the setup of the anti-theft feature, the user has to choose an app-specific PIN, or optionally a pattern and/or fingerprint.

Furthermore, the app needs to be granted various permissions, among which are device admin rights. Remote commands such as Lock, Locate, Siren, and Wipe can be deployed from the web interface at *my.avg.com*, which requires a valid AVG account. From here, the user is also able to modify the AVG PIN, the protection behaviour (lock phone, siren on lock), and the lock screen text, and access basic information about the device, such as its battery status.

Web & Wi-Fi Protection

Upon granting the app the accessibility permission, the user can activate the Web Shield component, which provides protection against phishing websites and malicious URLs for different browser apps. Wi-Fi Security scans the currently connected Wi-Fi network for security threats, while Wi-Fi Speed tests the quality of the connection in terms of download and upload speeds. If the corresponding feature is activated, the app also automatically scans new networks.

App Audit

App Insights lets the user monitor installed apps. Information is given about how much time the user spends on each app, available storage space, which permissions the apps require, and data consumption over a day, week, or month. The feature categorizes the installed apps as high-, average-, and low-permission, according to the private data and permissions they access. Furthermore, a custom data plan can be set up to limit mobile data usage.

Additional Features

Hack Alerts notifies the user whenever sensitive information tied to his/her email or other accounts have been leaked. Photo Vault encrypts and stores up to ten images, which can only be accessed via the AVG PIN. Junk Cleaner analyses the storage for unnecessary files and helps remove them. Additionally, My Statistics lets the user know about all actions taken by AVG to protect the device, e.g. number of threats prevented.

Conclusion

The free and ad-supported version of AVG AntiVirus provides a well-designed and accessible security solution for Android, with an easy-to-use interface and multiple features aimed at protecting and optimizing the device. All tested anti-theft commands behaved as expected.

Anti-Theft Details		
Commands Web		
Locate	✔	Displays the location on *Google Maps*. Tracking the device can be enabled.
Mark as Lost	✔	Triggers configured actions like tracking, lock, and siren.
Siren	✔	Activates/deactivates the phone siren.
Lock	✔	Locks/unlocks the phone.
Wipe	✔	Triggers a factory reset and wipes the external storage.

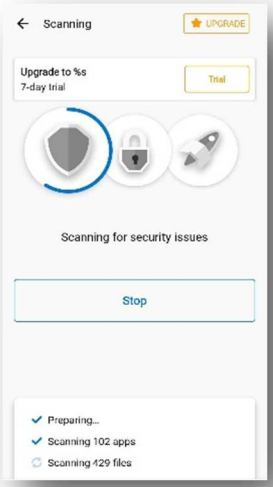
Avira

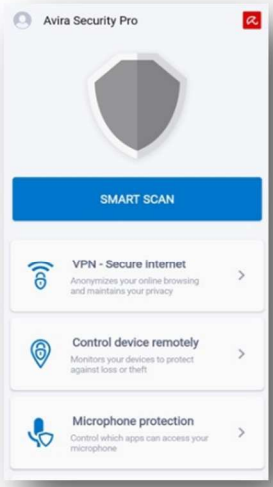
Antivirus Security for Android

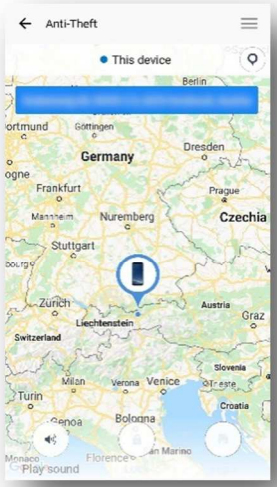
7.8.1

Introduction

Avira Antivirus Security is a paid-for product. In addition to malware protection, anti-theft, app locking, permission monitoring, and performance enhancement tools, it provides microphone- and web-protection features, a data-limited VPN, and Premium Support.







Usage

After installation, the user must agree to the EULA and Terms and Conditions, as well as configuring the data collection policy. The app also suggests trying the dark mode to save battery. After that, the user is redirected to the main screen, from where they can launch a first scan.

Anti-Malware

Before the first scan, the app asks for permission to access the internal data storage, including media, photos, and other files, in order to run a full scan of the internal storage. If the permission is denied, only apps will be scanned. By default, the scan looks for adware and other PUAs. Riskware detection can be configured in the settings, as can automatic scanning when a storage device is connected or a USB cable is disconnected.

There is also an option for scheduling scans to run at a set time and day. As part of the scan results, the user is prompted to enable the VPN connection, check for any data breaches for the provided email account, and run the Optimizer to increase performance.

Anti-Theft

Anti-theft commands are listed in the table below. When activating anti-theft, the app requests the necessary permissions and device admin rights to enable all the features. The anti-theft screen displays a map showing the device's current position and offers three commands: Locate, Lock, and Wipe. The last two of these can only be executed remotely by a second device that has the Avira app installed, and is linked to the same user account. The registered devices can be accessed and controlled from the menu in the top right corner of the anti-theft component.

Web & Wi-Fi Protection

The Web Protection feature blocks phishing and other malicious websites while browsing the web. In our testing, this feature only worked when using the Google Chrome or Samsung Internet browsers. The app provides no information which browser apps are supported. In addition to malicious websites, Web Protection can block user-specified websites defined in the relevant settings.

The Network Scanner informs the user about other devices connected to the same network. The VPN service is limited to 100MB per day.

Privacy Protection

Call Blocker can be used to block phone calls from specified contacts or numbers. Microphone Protection lists apps requiring access to the device's microphone. When enabled, other apps can no longer access the microphone, with the exception of the pre-installed Phone Dialer app. The Identity Protection checks a particular email address for data leaks and lists recently breached companies.

App Audit & Lock

The Permissions Manager shows all installed apps grouped by their requested permissions and can be used to change the permissions or uninstall an app.

App Lock can be used to set up a pattern, PIN, or fingerprint to regulate access to installed apps. The user can choose between different locking behaviours (lock always, lock by location, or lock by schedule). Additionally, there is an option to show a fake crash message when a locked app is accessed. In that case, the user needs to long tap the OK button which opens the prompt to unlock the app.

Conclusion

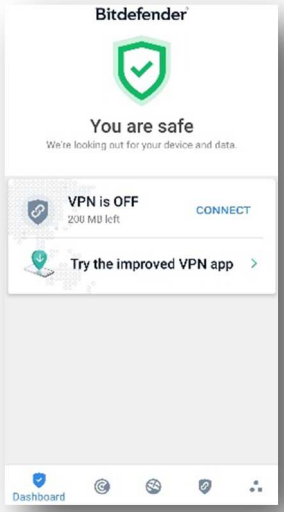
Avira Antivirus Security offers a large set of tools to enhance device security, protect the user against privacy leaks, device loss or theft, and increase the device's performance. All anti-theft commands worked as expected in our test.

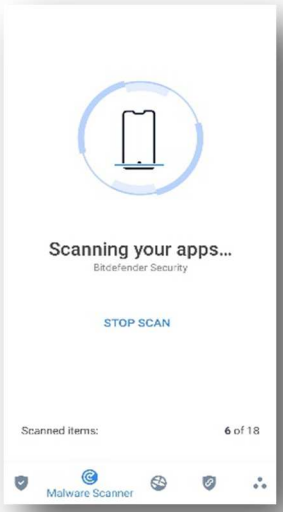
Anti-Theft Details		
Commands App		
Locate	✔	Displays the location on *Google Maps*.
Lock	✔	Locks the device with a 4-digit PIN (executable remotely).
Wipe	✔	Triggers a factory reset and wipes the external storage (executable remotely).

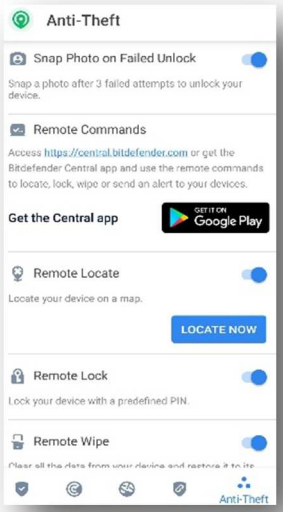
Bitdefender
Mobile Security
3.3.141

Introduction

Bitdefender Mobile Security is a paid-for, security- and privacy-oriented mobile security solution. The Autopilot mode, enabled by default, automatically takes care of security- and privacy-related issues on behalf of the user. Additional app components such as Anti-Theft, Account Privacy, and App Lock ensure that the user is protected against threats.







Usage

Upon opening the app for the first time, the user has to agree to Bitdefender's subscription agreement and either log in or create a new account. After that, the app prompts the user to enable the Web Protection and to start a scan. The user is then redirected to the main screen, where they are provided with a general overview of the device status and potential issues.

Anti-Malware

The user can decide whether to grant the app access to photos, media, and files on the device. If the permission is given, the app scans both the internal and external storage; otherwise an app-only scan is performed. To gain a deeper insight into security, a list of threats the app actively searches for while scanning is provided, along with a brief description.

In-the-cloud detection, which automatically uploads suspicious app information to Bitdefender's servers, is enabled by default.

Anti-Theft

Anti-theft components are listed in the table below. First, the necessary permissions, among which are device admin rights, need to be granted, and the user is asked to choose a PIN. The remote commands Locate device, Lock device, Play sound, and Erase device can be sent either from the Bitdefender Central app or the web interface at *central.bitdefender.com*. When we sent the Locate command in our test, we found that even after waiting 5 minutes, no location was shown on the map, and only the "Loading" indicator was visible.

However, when we looked in Notifications, we saw that the phone's location had been identified. Clicking "View on map" in the notification then displayed the location correctly on Google Maps.

From the web interface, the user is able to see the device's security status, along with a list of threats found on the device in the previous 7 days, and to remotely start a scan. The Snap Photo feature silently takes a photo with the front camera and uploads it to the remote command interface, as well as storing it on the device, after the wrong PIN has been entered three times in a row.

Web & Wi-Fi Protection

The Web Protection feature blocks malicious URLs and phishing websites in various browser apps. Bitdefender also offers a VPN service, providing up to 200 MB of data traffic per day while connected to an automatically chosen server. The option to warn the user each time the device connects to an open Wi-Fi is activated by default.

Account Privacy

The Account Privacy feature lets the user check whether an email address has been compromised in a data breach. Each email needs to be verified with a confirmation code beforehand.

App Lock

The App Lock component restricts access to chosen apps by locking them with a pre-defined PIN. In the settings, the user can decide how often protected apps should require the code. The Random Keyboard feature randomizes the number pattern on the keyboard each time the lock screen is displayed. By marking a specific Wi-Fi network as trusted, protected apps remain unlocked while connected. If Snap Photo is enabled, a photo is taken with the front camera after three failed unlock attempts.

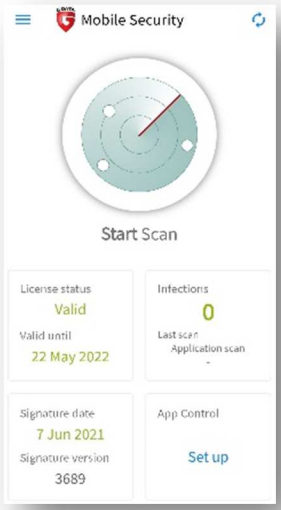
Conclusion

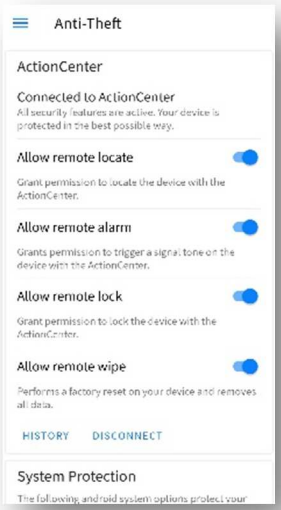
Bitdefender Mobile Security provides a wide range of tools for monitoring the device's security and privacy. All features except the Locate command worked as expected in our test.

Anti-Theft Details		
Commands App & Web		
Locate device	▬	Displays the location on *Google Maps*. In our test, it was only accessible from the notifications.
Play sound	✓	Sounds an alarm on the device and/or shows a custom message.
Lock device	✓	Locks the device with the Android lock screen. The PIN can be set in the command interface.
Erase device	✓	Triggers a factory reset and wipes the external storage.
Additional Features		
Snap Photo	✓	Takes a picture with the device's front camera after multiple failed unlock attempts, and uploads it to the command interface.

G Data
Mobile Security
27.3.2

Introduction
G Data Mobile Security is a paid-for security solution which incorporates various security- and privacy-related features such as malware scan, Anti-Theft, Web Protection, and App Control. No free trial is offered, and the app is only available after purchasing a yearly license.





Usage
First, the user has to accept the EULA and Privacy Policy and decide whether to send anonymous and/or malware-related data. After logging into the account, the user is given a quick tour of the various app components, and then presented with the opportunity to adjust scan-related settings.

After granting the app access to photos, media, and files, the user is redirected to the main screen, where a general overview of the phone and app status is shown, and a system scan can be started. The other app components are available from the menu in the upper left-hand corner.

Anti-Malware
From the settings, the user can decide which type of scan to perform, whereby App scan is selected by default. A system scan allows the user to perform a full scan of the device including the external storage. This scan cannot be performed if the aforementioned permission has not been granted. Signatures are configured to update automatically but can be download manually as well. The options to check apps upon installation, and to perform periodic scans, are enabled by default.

Anti-Theft

Anti-theft commands are listed in the table below. In order to activate Anti-Theft, various permissions need to be granted to the app, among which are device admin rights. The user can access the app's web interface and send remote commands such as Locate device, Trigger signal tone, Delete personal data, and Lock screen, from the G Data ActionCenter at *ac.gdata.de*. The code for the Lock command is set to the device's PIN by default. From the web interface, the user is also able to modify in-app settings, start scans, and access general device information, along with a list of actions taken by the AV app. In addition, battery-friendly scan options (e.g. battery-saving mode, scan only when charging) can be set up. We found the wording in the ActionCenter, "only in charging", rather confusing. We expected that this would trigger a scan immediately when the device is put on charge, but in fact it means "Don't scan unless the device is charging". You have to use the "periodic scan" option to initiate a scan. We notified G Data, who have now improved the description.

The user can invite other people to the web interface via email, and regulate their access to a subset of anti-theft features.

In-app components enable the user to locate the phone when the battery is low, and to trigger an alarm each time the headphones are disconnected, or when a new SIM card is detected. G Data sends a notification to a pre-configured email address each time an anti-theft feature has been activated.

Web Protection

Once enabled, the Web Protection feature blocks phishing websites and malicious URLs for several mobile browser apps. The user can configure this component to be used only when connected to Wi-Fi.

App Audit & Lock

To activate App Control, the user is prompted to set up a PIN, a security question, and a recovery email address. If an app is marked as protected, a lock screen is displayed each time a user launches the app, which will only be removed once the PIN has been entered. App Control shows further app information, such as the permissions granted by the user, and lets the user uninstall apps.

Conclusion

G Data Mobile Security offers an updated and easy-to-use graphical user interface, along with many functions for enhancing security and privacy. All the anti-theft commands worked flawlessly in our test.

Anti-Theft Details		
Commands Web		
Locate device	✔	Displays the current or last-known location on *Google Maps*, and sends an email notification with a link to *Google Maps*.
Trigger signal tone	✔	Rings an alarm on the device, which is switched off when the device is unlocked, and the app is launched.
Lock screen	✔	Locks the device with the Android lock screen.
Delete personal data	✔	Triggers a factory reset and wipes external storage.
Additional Features		
SIM card protection	✔	Locks the device and sends the current location to the registered email address whenever the SIM card is changed.
Headphone protection	✔	Locks the device and rings an alarm when the headset is disconnected.

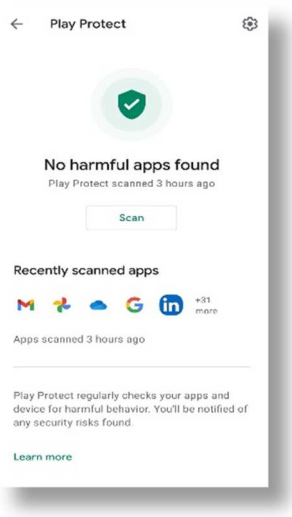
Google

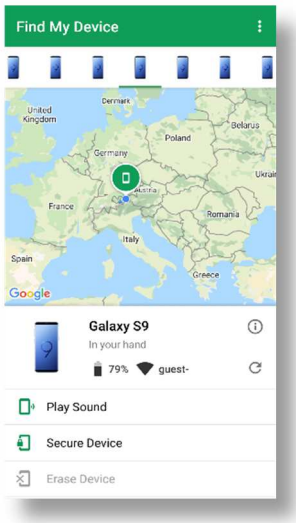
Play Protect & OS Features

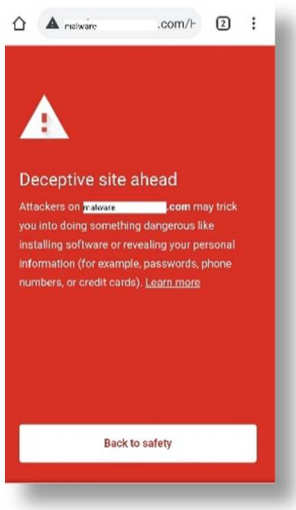
25.8.20

Introduction

Google's Play Protect is built-in malware protection for apps and APK files on certified Android devices that support Google Play Services. These services provide several APIs such as Location, Maps, Drive, Play Protect, Cloud Messaging, and Analytics, to help developers build more-advanced apps. Google Mobile Services (GMS) enhance device privacy and security with e.g. anti-theft and browser protection components.







Usage

Play Protect is preinstalled on supported Android devices and can be found either via Play Store > Profile Icon > Play Protect or in Android Settings > Biometrics and Security > Google Play Protect.

Anti-Malware

Play Protect periodically scans the internal storage and notifies the user of malicious or potentially harmful apps, and apps that misuse permissions to access personal information, thus violating Google's Developer Policy and Unwanted Software Policy. The option "Send unknown apps to Google" and "Improve harmful app detection" can be turned off.

Anti-Theft

Anti-theft commands are listed in the table below. Google's anti-theft feature Find My Device can be operated from the web interface *google.com/android/find* or using a standalone app. Logging in to a Google account is mandatory for both methods. When the device is connected, the interface shows the current or last-known location, battery level, time, and name of the Wi-Fi the device is connected to. Both interfaces offer options to remotely lock the device and delete all data, including the Google account, from the device, by forcing a factory reset. Setting a new PIN or resetting the old screen-lock PIN is also possible.

Web Protection

The Google Chrome browser for Android devices includes a safe browsing feature, which alerts users to dangerous sites or downloads.

App Audit

In the Android Settings > Apps, all installed apps are listed along with information about their permissions, used mobile data, battery consumption, and storage space. The permission manager groups apps by permissions, and allows the user to grant/deny specific permissions for a particular app. The user can disable or uninstall an app, or forcedly stop it.

Conclusion

Google Play Protect is preinstalled on approved new Android devices. Supported devices with older versions of Google Play Services will be updated automatically. All the security-related features, such as malware protection, anti-theft, web protection, app and data backup, can be used for free with a Google account. However, some device manufacturers offer their own security solutions for their specific devices. These utilise the Google Android APIs and may overlap with pre-existing GMS apps such as Google Chrome and Find My Device.

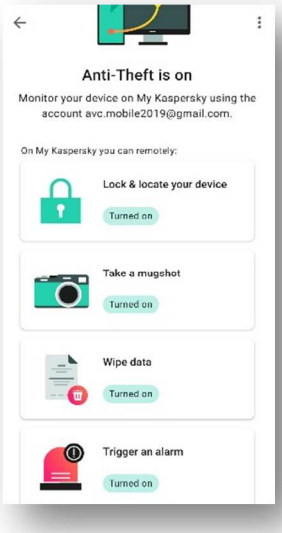
Anti-Theft Details		
Commands Web		
Locate	✔	Displays the current or last-known location on *Google Maps*.
Secure Device	✔	Locks the device with a given PIN/password or the pre-defined security mechanism. Optionally, a message and/or phone number to contact can be displayed on the lock screen.
Erase Device	✔	Triggers a factory reset immediately, or after next device restart, and wipes the external storage.

Kaspersky

Internet Security for Android Premium
11.69.4

Introduction

Kaspersky Internet Security is a well-rounded, paid-for mobile security solution. It offers a comprehensive set of tools to protect against malware, phishing, theft, and privacy violations. Inside the app, the user is able to download additional functionalities, such as parental control, battery optimizer, VPN, or a password manager.



Usage

Upon first opening the app, the user has to agree to Kaspersky's EULA and Privacy Policy, and grant storage access to the app. After activating the license, the user is redirected to the app's main screen, where a local database update as well as a quick scan are started automatically. The app then prompts the user to configure and enable various security-related components, such as anti-theft and Internet protection, and to run a full system scan.

Anti-Malware

The scan settings offer fine-grained control of scan frequency and signature updates in addition to customizable scan behaviour and actions that should be taken when malware is detected.

The default scan settings include the detection of adware and auto-dialers, and scanning installed apps and packages in the Downloads folder. The user can switch to the extended real-time protection, letting the app monitor all file activities and installed apps regularly. Each time the user starts a scan, he/she can decide whether to scan all installed apps, the entire device including external storage, or a specific folder.

Anti-Theft

Anti-theft commands are listed in the table below. The anti-theft setup requires the user to grant the app the necessary permissions, as well as device admin rights.

Remote commands can be sent to the device from the web interface at *my.kaspersky.com* and include Lock & Locate, Mugshot, Alarm, and Data Wipe. In the web interface, the user is not only able to look at the data sent from the device, such as photos of a potential thief taken with the front camera and location coordinates, but also to access general information about the device. Furthermore, after executing the Mugshot or Lock & Locate command, the user receives an email with the location of the device. All commands except for Data Wipe lock the device upon execution and can be sent with a custom lock-screen message. The features SIM Watch and Uninstallation Protection lock the device on detection of a SIM change and an attempt to uninstall the Kaspersky app, respectively. If no other lock screen is set up, the anti-theft PIN is used to lock the device remotely.

Web Protection

The Internet Protection component protects the user from phishing websites in the browser apps Google Chrome, Samsung Internet, and Huawei Browser. The Safe Messaging feature scans incoming messages for phishing and malicious links.

App Audit & Lock

After granting the necessary permissions, the App Lock feature allows the user to select and lock sensitive apps with the same secret code/pattern/fingerprint used for the anti-theft functions. The My Apps component provides details of apps, namely size, date installed, date updated, last use, and permissions requested. Furthermore, installed apps can be removed from within the feature.

Additional features

Call Filter automatically declines incoming calls of blacklisted contacts. The Data Leak Checker monitors the email connected to the Kaspersky account for data breaches.

Conclusion

Kaspersky Internet Security comprises a great variety of security and privacy tools. Each feature is thoroughly explained by the help links in the right upper corner. Features can be extensively customised and additional apps can be incorporated. All the anti-theft commands worked flawlessly in our test.

Anti-Theft Details		
Commands Web		
Lock & Locate	✔	Locks the device, displays the location on *Google Maps*, and sends the location in an email.
Mugshot	✔	Locks the device, and takes several pictures using the front camera.
Alarm	✔	Locks the device and rings an alarm.
Data Wipe	✔	Triggers a factory reset and wipes the external storage.
Additional Features		
SIM Watch	✔	Locks the device if the SIM card is removed or changed.
Uninstallation protection	✔	Locks the device if device admin rights are removed from the app.

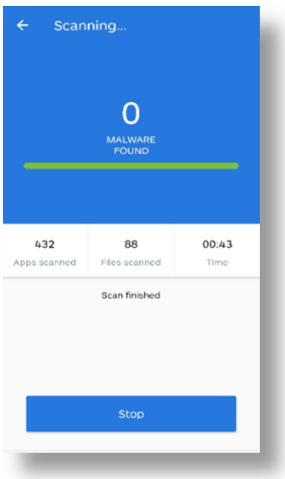
Malwarebytes

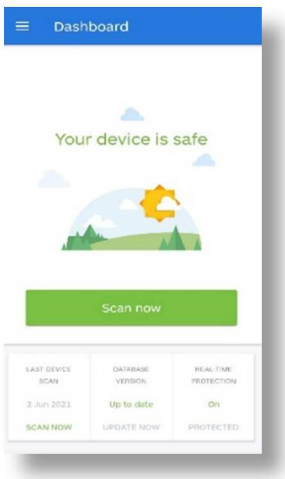
Malwarebytes for Android

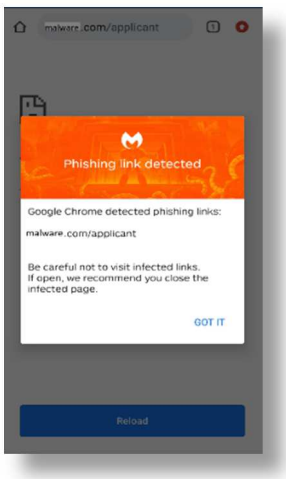
3.7.5

Introduction

Malwarebytes is a paid-for security product for Android, which provides a malware scanner along with real-time and ransomware protection, a safe browsing feature, and privacy audit for installed apps.







Usage

Upon first launch, the app asks the user to give permission to access storage and files, and to agree to the Terms and Conditions. After that, the first scan can be started manually. Warnings at the bottom of the main screen advise the user to further enhance device security by giving the app more privileges and checking the security audit for unsecure device settings.

Anti-Malware

A device scan runs on the internal and external storage and shows detailed information about the apps and files being scanned, as well as malware found. Automatic updates are enabled by default but can be triggered manually. Scans can be scheduled for different times, after a device boot or a database update. To save battery, scans can be performed only while charging, or disabled if battery is low. Deeper system scans with additional rules can also be enabled. The app requires device admin rights for its real-time protection, anti-ransomware remediation, and to protect itself from being uninstalled easily.

Web Protection

After enabling the Safe Browsing Scanner in the app settings, the user will be warned of phishing or other malicious links. However, the feature does not attempt to block the malicious content.

App Audit

Your Apps shows the installed apps (including system apps) in a well-structured view, and provides further detailed app information when granting the Usage-Access permission. Privacy Audit scans and groups the apps according to the permissions they have acquired.

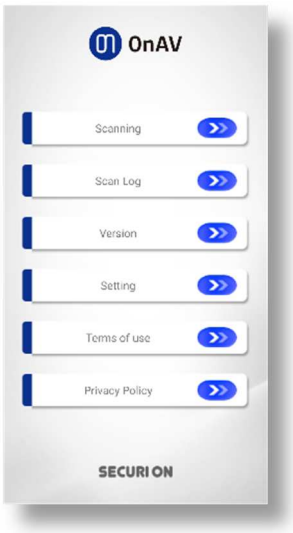
Conclusion

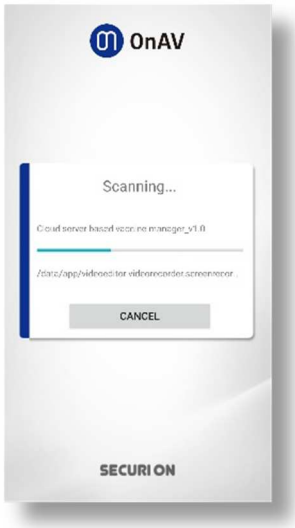
Malwarebytes is a solid security solution for Android, including anti-malware, web protection and a detailed app audit. The initial setup requires the user's attention, but this leaves no questions unanswered. Although phishing websites are not actually blocked, the user does at least get a warning not to trust them.

Securion
OnAV
1.0.30

Introduction

Securion OnAV is an ultra-light and free-to-use AV product that provides cloud-based malware detection. Without any user registration, it assigns a unique ID to each device to prevent double sign-ups. This review covers the English version of the app only, which differs from its original Korean counterpart.





Usage

First, the user must accept the Terms and Conditions allowing anonymous collection of system data and user statistics, and the Privacy Policy. After that, the app asks for permission to access photos, media, and files, as well as to display the app on top of other apps, which is required for real-time notifications.

Anti-Malware

An on-demand scan checks the internal storage and SD card for malicious apps and files. Detected malware can be deleted selectively or in one go. The information about previous scan results can be accessed from the Scan Log menu option in the main screen. The real-time protection can be turned on and off in the app settings.

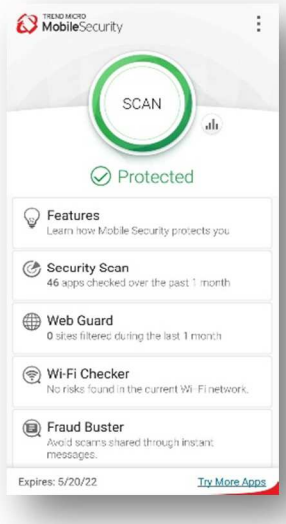
Conclusion

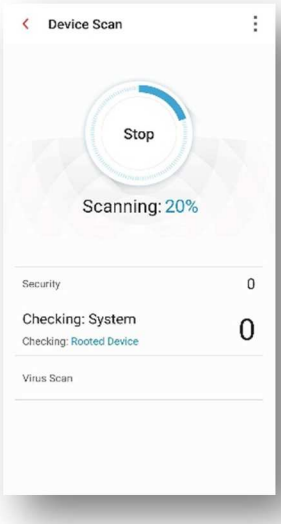
Securion OnAV is a free, user-friendly app that solely provides malware protection capabilities. Detected malware is listed in the scan results where they can be viewed and deleted directly.

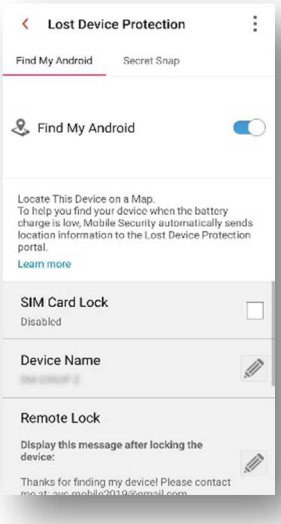
Trend Micro
Mobile Security
12.6.0

Introduction

Trend Micro Mobile Security is a comprehensive, paid-for security product. Besides a malware scanner, Wi-Fi scanner, system tuning, and privacy tools, it provides additional security features such as anti-theft, web protection, and parental controls.







Usage

Upon the first app start, the user is prompted to accept the EULA and Privacy Policy. During a brief tour of the app, an initial scan is started in the background. In addition to the scan result, the app recommends setting up various other features, and granting the necessary permissions. After license activation, all the app features are directly accessible from the main screen, where the device status is displayed at the top.

Anti-Malware

In the security scan settings, the user can adjust the threat level at which they should be notified about potential risks. An app-only scan can be started manually. Other options are toggling the real-time protection, scanning apps prior to the installation, and scanning the external storage. Malware signatures can be updated manually but are updated automatically by default, whereby the update interval can be set to daily, weekly, or monthly.

Anti-Theft

Anti-theft commands are listed in the table below. The Lost Device Protection feature allows the user to issue remote commands such as Locate, Lock, or Wipe via the web interface *mobilesecurity.trendmicro.com*. In addition, you can share the device's location to followers on Facebook. An option to lock the phone whenever the SIM card is removed is also included. If the Uninstall Protection is activated, the Trend Micro App can only be uninstalled with the account password or an unlock code. The Reset command is only supported on devices with Android 7.0 or lower.

The Secret Snap feature can be configured to take a picture with the front camera after 3, 5 or 7 failed unlock attempts, and this will be sent automatically to a pre-configured email address and saved on the device.

Web & Wi-Fi Protection

Web Guard blocks links to malicious websites opened in supported browsers or other apps. For non-supported apps, the VPN can be used to block malicious content. Here, the protection level can be set to low, normal, or high, and the user can define black- and whitelists of websites. The Wi-Fi Checker scans for suspicious interfaces on the current network.

Parental Controls

The parental controls feature is grouped into two categories: App Lock and Website Filter. With the first, the user can select apps to protect with either the Trend Micro account password, a pattern, PIN, or fingerprint. The Website Filter can be set to three predefined levels (Child, Pre-Teen, and Teen), with each of them blocking websites belonging to categories deemed inappropriate for the specific age group.

Moreover, a custom filter as well as white- or blacklists of individual websites can be built. The website filter also works in apps not directly supported by the Trend Micro app, by utilizing the VPN content filter.

Additional Features

The app includes a System Tuner, which can free up memory space and extend battery life. The Social Network Privacy feature can be used to check the privacy settings of a Facebook or Twitter account. The App Manager allows the user to view all installed apps, uninstall or disable apps at once, and to remove unneeded setup files. The Pay Guard Mobile feature monitors financial transactions made with installed banking and shopping apps. Fraud Buster scans incoming messages for phishing links and notifies the user of potential risks.

Conclusion

Trend Micro Mobile Security offers a comprehensive set of security and privacy features, protecting the user against various threats on the device and while browsing the Internet. There are also extensive options to limit access to websites.

Anti-Theft Details		
Commands Web		
Locate	✔	Displays location on *Bing Maps*.
Lock	✔	Locks the device until either the Trend Micro password or a one-time unlock key from the web interface is entered.
Wipe	✔	Triggers a factory reset and wipes external storage.
Share	✔	Posts a *Bing Maps* link with the current location on Facebook.
Additional Features		
SIM Change Protection	✔	Locks the device if the SIM card is removed.
Uninstall Protection	✔	Locks the device if device administrator rights are removed from the app.
Secret Snap	✔	Takes a picture with the front camera.

Feature List Android Mobile Security (as of June 2021)										
Product Name	*Android OS*	Avast Mobile Security (Free)	AVG AntiVirus for Android (Free)	Avira Antivirus Security for Android	Bitdefender Mobile Security	G Data Mobile Security	Kaspersky Internet Security for Android Premium	Malwarebytes for Android	Securion OnAV	Trend Micro Mobile Security
Version Number	*10.0*	6.39	6.39	7.8	3.3	27.3	11.69	3.7	1.0	12.6
Supported Android versions	*built-in*	5.0 and higher	5.0 and higher	5.0 and higher	5.0 and higher	5.0 and higher	4.2 and higher	6.0 and higher	5.0 and higher	4.1 and higher
Supported Program languages	All	English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese	English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese	English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish	English, Czech, Dutch, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Thai, Turkish, Vietnamese	English, Dutch, French, German, Italian, Japanese, Polish	English, Russian, German, French, Italian, Spanish, Portuguese, Turkish, Polish, Czech, Danish, Finnish, Hungarian, Norwegian, Dutch, Swedish, Arabic	English, Dutch, French, German, Indonesian, Italian, Polish, Portuguese, Russian, Spanish, Turkish	English	English, Chinese, Dutch, French, German, Hebrew, Italian, Korean, Portuguese, Spanish, Turkish, Vietnamese
Anti-Malware										
On-Install scan of installed apps	●	●	●	●	●	●	●	●		●
On-Demand scan	●	●	●	●	●	●	●	●	●	●
On-Access scan of apps	●			●			●	●	●	
Can detect malware sitting on external SD card				●	●	●	●	●	●	●
Automatic (scheduled) scan		●	●	●		●	●	●		●
Scan requires online cloud connection	●				●					
Manual local database update possible (beside automatic updates)		●	●			●	●	●		●
User account needed to use product	●				●	●				●
Privacy Advisor (audit app permissions)	●	●	●	●		●	●	●		
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●	●		●
Supported browsers (Safe Browsing)	Google Chrome	Google Chrome, Dolphin, Firefox, Opera	Google Chrome, Dolphin, Firefox, Opera	Google Chrome, Dolphin, Edge, Firefox, Opera, Opera Mini, Samsung Internet	Google Chrome, Brave, Dolphin, Edge, Firefox, Opera, Opera Mini, Samsung Internet	Google Chrome, Edge, Firefox, Opera	Google Chrome, Samsung Internet, Huawei Browser	Google Chrome, Brave, Dolphin, Opera, Opera Mini, Samsung Internet, UC Browser		Google Chrome, Samsung Internet
Anti-Theft										
Web Interface for controlling Anti-Theft commands	●	●	●	●	●	●	●			●
Remote Locate, Lock & Wipe (Factory Reset)	●	●	●	●	●	●	●			●
Thief Cam					●		●			●
Anti-Theft Alarm (cannot be muted by thief)		●	●		●	●	●			
Locate-Phone Alarm only (can be muted)	●			●						●
Lock on SIM Change						●	●			●
Remote Unlock		●	●	●						
App settings protected with password		●	●		●	●	●			●
Uninstallation Protection (password required for uninstallation)							●			●
Parental Control										
App Lock				●	●	●	●			●
Safe Web Browsing (content filtering)										●
Time Limits (device use limits, bedtime intervals)										
Additional Features										
Wi-Fi Security		●	●							●
VPN				●	●					●
Task Manager (manage installed apps)	●	●	●			●	●	●		●
Network Monitor (track data usage)	●	●	●							
System Optimizer		●	●	●						●
Supports landscape mode	●	●					●			●
Other Features	Backup, Battery Monitor, Call Block	Photo Vault, Hack Alerts	Photo Vault, Hack Alerts	Account Privacy	Account Privacy		Call Block, Safe Messaging, Data Leak Checker			Social Network Security, Battery Monitor
Support										
Online Help & FAQ	●	●	●	●	●	●	●	●		●
User Forum	●	●	●	●	●		●	●		●
Email Support				●	●	●	●	●		●
Phone Support				●	●	●	●			●
User Manual (PDF)	●			●	●	●	●	●		
Online Chat					●		●	●		●
Supported languages of support	All	English, Czech, German, French, Japanese, Spanish, Portuguese, Russian	English, Czech	English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish	English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish	English, Dutch, French, German, Italian, Japanese, Polish	English, French, German, Italian, Portuguese, Russian, Spanish	English, Dutch, French, German, Indonesian, Italian, Polish, Portuguese, Russian, Spanish, Turkish		English
In-App List Price (may vary)										
Price 1 Device / 1 Year (USD/EUR)	FREE	FREE	FREE	USD 10 / 8 EUR	USD 15 / 10 EUR	USD 16 / 10 EUR	USD 20 / 11 EUR	USD 12 / 12 EUR	FREE	USD 30 / 20 EUR

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(July 2021)