Independent Tests of
Anti-Virus Software

Mobile Security Review 2022

TEST PERIOD: MAY 2022

LAST REVISION: 15TH JUNE 2022

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 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.

In 2021, 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 basic security features: Google's built-in malware scanner *Play Protect* scans apps during installation from Google Play 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 latest Android versions, Google has also implemented various app auditing features where users can review and adjust settings for privacy (e.g. dangerous/special permissions, notifications) and usage (e.g. mobile data, battery consumption, storage space) of individual apps.

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, and a short summary of common security features of 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 and safe browsing for Google Chrome, were integrated as regular components as well.

Android 10 brought some significant improvements for security and privacy which are refined in later versions, 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 on background apps. Apps (except for privileged/system apps) are also prevented from accessing specific device information, e.g. non-resettable device identifiers like IMEI, IMSI, MEID, SIM, and build serial number.

In Android 11, users can 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 automatically resets all run-time permissions for unused apps. The scoped storage has been enforced to prevent access to the legacy external storage. However, Android adds the special permission “All files access” for apps that require broad access of files on the internal and external device storage (e.g. anti-virus, file manager, backup apps). Apps are also restricted when querying a full list of installed apps and all their details.

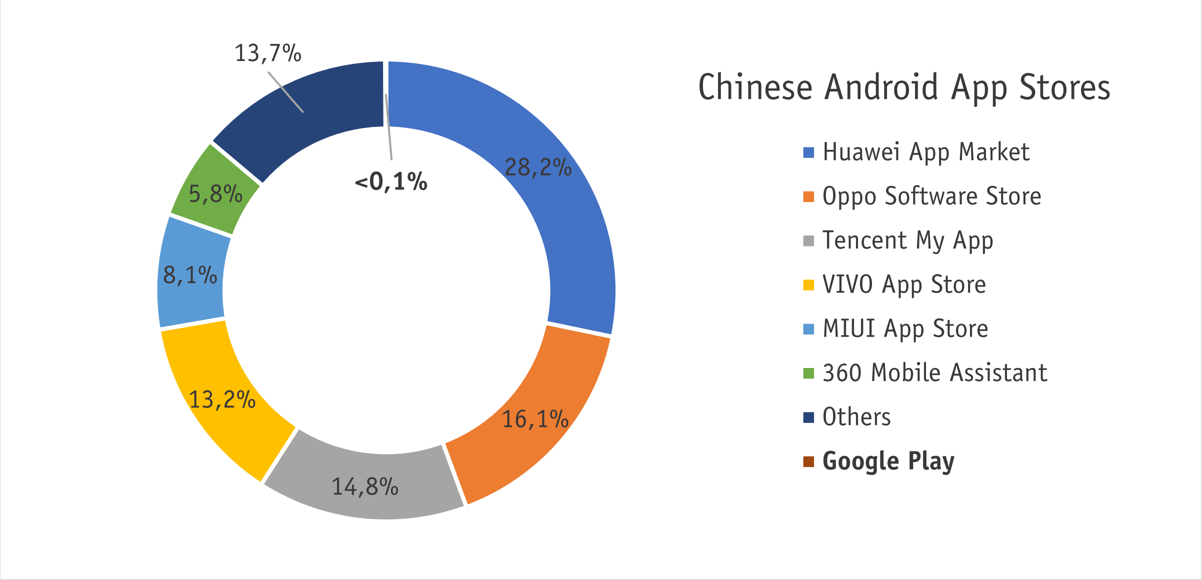
The release of Android 12 in October 2021 introduced a wealth of new features, focusing on further increasing the user’s security and privacy[3]. Users now can allow apps to access only approximate location information. Indicators for camera and microphone access, as well as a system-wide camera and microphone toggle, were added to see when an app is using the camera or microphone, and to easily block access to these for all apps. A privacy dashboard shows a timeline for camera, location, and microphone access. Apps can hide overlay windows of other apps. In addition to auto-resetting all granted permissions, unused apps will be placed in a “hibernation state”, where all background actions are suppressed/prohibited, and the app cache is cleared.

The resulting restrictions imposed on apps targeting Android 10 or later has affected mobile security vendors, among others. Their apps require all available device permissions, including device admin rights, if they are to fully monitor and control the device, and protect sensitive user data against security threats. Because of all the changes made on Android permissions, mobile security apps might provide clearer explanations to users when requesting access to sensitive device areas and setting up in-app security features (e.g. anti-theft).

[3] https://developer.android.com/about/versions/12

For this review, we decided to use the most recent Android version, which is currently Android 12. We used the unmodified version of Android 12 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. Furthermore, devices based on modified Android OS versions (e.g. HarmonyOS, FireOS, LineageOS) do not run Google apps or services by default; hence, there is no built-in malware protection. 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.



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 1.63 billion[4] active mobile devices in China, and about 76%[5] of them run Android as the operating system. The most used Android app stores are shown in the doughnut chart[6] above. Google Play is used by almost no one (<0.1%) because Google Play and most of Google's services are inaccessible in mainland China.

In November 2020, a US Executive Order[7] 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.

[4] https://datareportal.com/reports/digital-2022-china
[5] https://gs.statcounter.com/os-market-share/mobile/china
[6] https://www.appinchina.co/market/app-stores
[7] https://home.treasury.gov/system/files/126/13959.pdf

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[8] versions of popular apps, the genuine versions of which have been downloaded by millions of users[9] (including from Google Play). 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[10]. 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 compromise 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[11] 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.

[8] https://www.av-comparatives.org/tests/android-test-2019-250-apps/

[9] https://www.cleafy.com/cleafy-labs/teabot-is-now-spreading-across-the-globe

[10] https://developer.android.com/distribute/best-practices/develop/target-sdk.html

[11] https://thehackernews.com/2022/05/another-set-of-joker-trojan-laced.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 cameras, 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. 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[12] were taken from Google Play at the time of the test (May 2022). 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	6.48	●●●○●
AVG	AntiVirus Free	6.48	●●●○●
Avira	Antivirus Security Pro for Android	7.13	●●●●●
Bitdefender	Mobile Security for Android	3.3	●●●●○
ESET	Mobile Security Premium	7.3	●●●●●
G DATA	Mobile Security Android	27.4	●●●●●
Google	Play Protect & OS Features	30.4	●●●○●
Kaspersky	Kaspersky Standard for Android	11.84	●●●●●
Malwarebytes	Malwarebytes for Android	3.10	●○●○●
Securion	OnAV	1.0	●○○○○
Trend Micro	Mobile Security for Android	12.15	●●●●○

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 12 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

[12] 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 be 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.

Ten 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 a comprehensive set of security and non-security tools aimed at protecting the user's security and monitoring different privacy and performance aspects of Android devices.

AVG AntiVirus Free is a well-designed mobile security solution including a variety of security- and privacy-related features which can be extensively customized.

Avira Antivirus Security Pro for Android offers features to enhance device security, protect the user's privacy, and remotely control the device via in-app commands.

Bitdefender Mobile Security for Android is an easy-to-use mobile security product with a clean user interface, elaborate device protection, and privacy-oriented features.

ESET Mobile Security Premium is a mobile security app for Android, which includes different and extensively customizable protection and security features against vulnerabilities and theft.

G DATA Mobile Security Android incorporates essential security and privacy functions in a modern and neat user interface to protect a user's device.

X **Google** Android provides built-in malware protection as well as a device loss/theft, safe-browsing, and extensive app audit feature. Unfortunately, it did not reach the required protection level for certification.

Kaspersky Standard for Android is a mobile security app offering a wide range of thoroughly explained security and privacy features within a user-friendly interface.

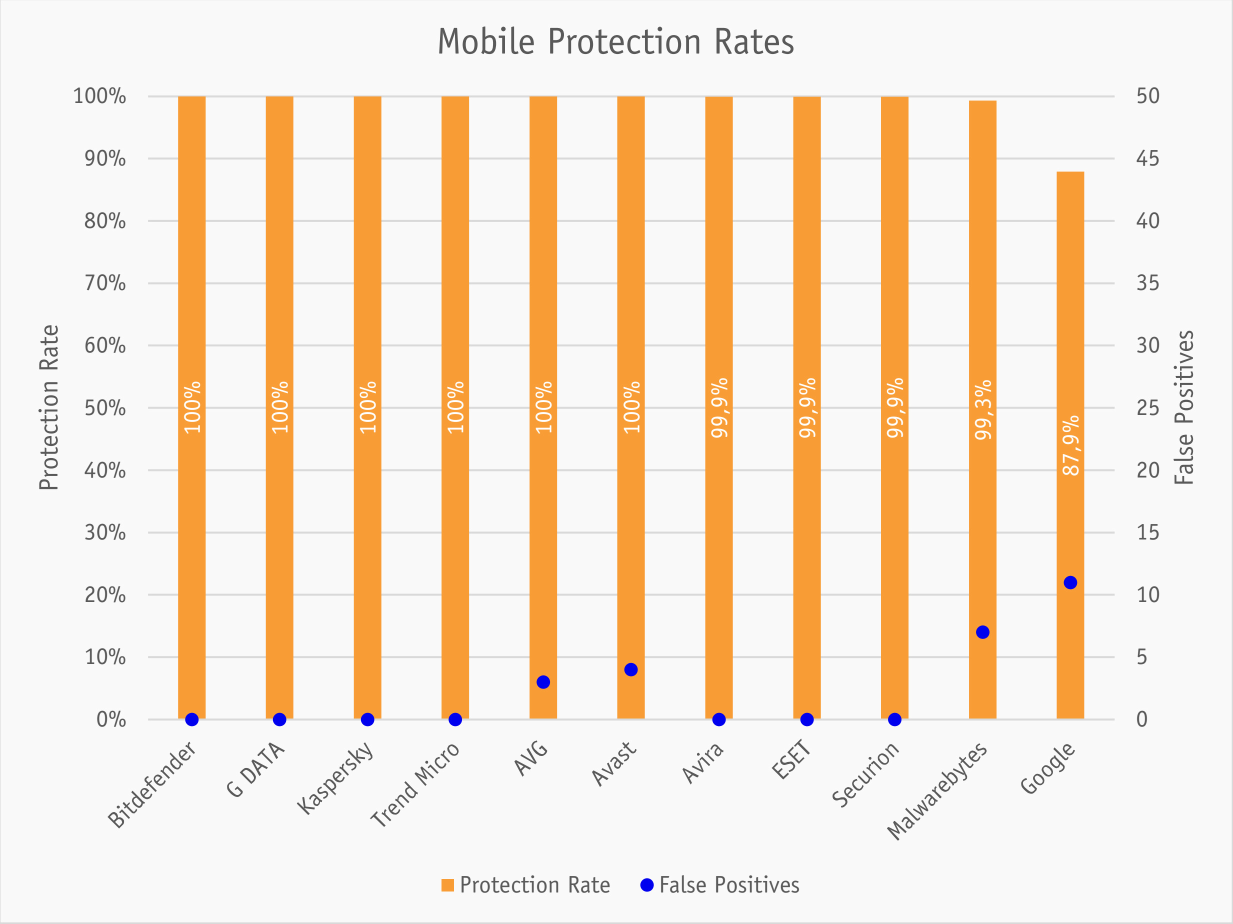
Malwarebytes for Android is a solid mobile security solution that combines real-time malware and ransomware protection, basic web protection, and app auditing.

Securion OnAV is a simple and free-to-use mobile security solution for Android comprising of solely malware protection capabilities.

Trend Micro Mobile Security for Android is a well-developed, comprehensive app, which integrates malware and theft protection, parental controls, and system-tuning features.

Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **3,127** 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. The security products were updated and tested on the 19th May 2022. 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 clean 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**
Bitdefender, G DATA, Kaspersky, Trend Micro	100%	0
AVG	100%	3
Avast	100%	4
Avira, ESET, Securion	99.9%	0
Malwarebytes	99.3%	7
Google	87.9%	11[13]

[13] Detected as privacy risk.

Battery Drain Test Results

As in our previous investigations, we measured the additional power consumption caused by each of the mobile security products. 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 all the tested mobile security products had only a minor influence on battery life, as outlined in the table below. In general, we were able to give the tested security suites high marks regarding power usage.

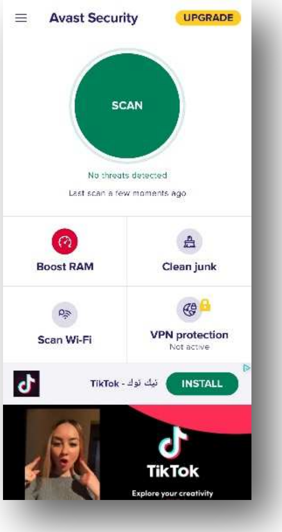
Battery Drain Results	
Avast	🟩
AVG	🟩
Avira	🟩
Bitdefender	🟩
ESET	🟩
G DATA	🟩
Google	🟩
Kaspersky	🟩
Malwarebytes	🟩
Securion	🟩
Trend Micro	🟩

🟩	up to 3%
🟩	3 to 8%
🟨	8 to 15%
🟨	15 to 25%
🟥	more than 25%

Avast
Mobile Security Free
6.48.1

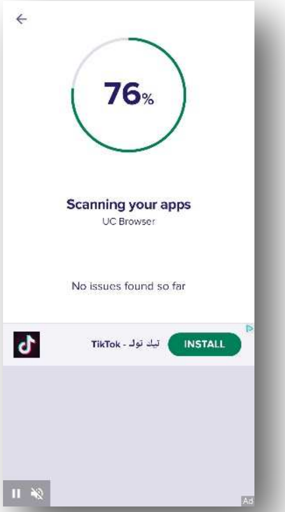
Introduction

Avast Mobile Security Free is an 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.



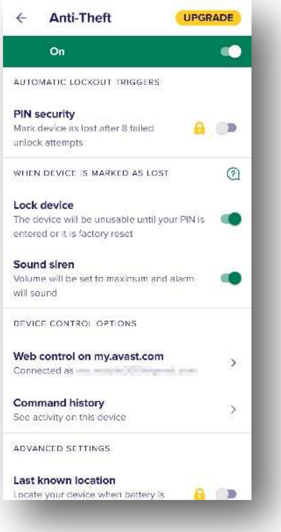
Avast Security UPGRADE

No threats detected
Last scan a few moments ago



Scanning your apps
UC Browser

No issues found so far



Anti-Theft UPGRADE

On

AUTOMATIC LOCKOUT TRIGGERS

PIN security
Mark device as lost after 8 failed unlock attempts

WHEN DEVICE IS MARKED AS LOST

Lock device
The device will be unusable until your PIN is entered or it is factory reset

Sound siren
Volume will be set to maximum and alarm will sound

DEVICE CONTROL OPTIONS

Web control on my.avast.com
Connected as [redacted]

Command history
See activity on this device

ADVANCED SETTINGS

Last known location
Locate your device when battery is

Usage

Upon starting the app, the user must accept Avast's Agreement and Privacy Policy. After viewing a brief overview of the features, the user can continue with the free and ad-supported app version by accepting the Consent Policy for custom ads. The user is then prompted to perform a first scan which requires the "All files access" permission.

Anti-Malware

After the first device scan, the app suggests turning on the web protection, and also prompts the user to set up screen locking to protect private information. The user can start a deep scan, which includes apps and files on the internal storage; otherwise an app-only scan is performed.

The app provides further scan settings, such as 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 file scanner can be used to scan individual files, folders, or the entire internal storage. The external storage (e.g. SD card) is not included when scanning the device storage.

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 must be granted various permissions, among which are device admin rights and appearing on top of other apps, in order to remotely control the device from the web interface. The user can execute the remote commands Locate, Lock, Mark as Lost, Siren, and Wipe. Basic information about the device, such as battery status and the time since the last communication, are also available. The Avast PIN and protection mechanisms can be modified via the web interface.

Upon receiving the location when executing the Locate command, we would welcome it if the web interface were automatically updated to display the new location. In our testing, we had to refresh the page manually.

Web & Wi-Fi Protection

The protection against malicious URLs and phishing websites offered by Web Shield requires the Accessibility permission, and works for different browser apps. 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.

App Audit

App Insights monitors installed apps and provides the user with detailed usage statistics for individual apps (e.g. screen time, 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 labelled with the risk categories “low”, “average”, and “high”, depending on the app’s permissions.

Additional Features

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

Conclusion

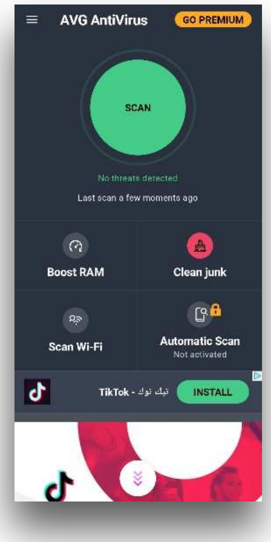
Avast Mobile Security Free is a well-designed anti-malware application that gives the user access to many, but partially restricted, security features. Optimization and privacy-enhancing tools are also available. All the tested anti-theft commands sent to the device worked as expected.

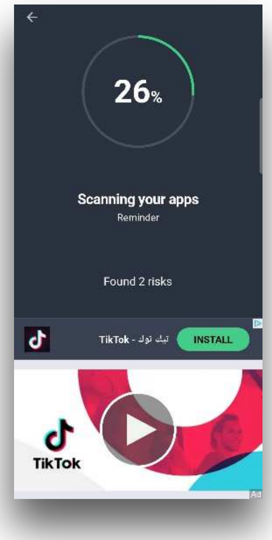
Anti-Theft Details		
Commands Web		
Locate	✓	Displays the location on *Google Maps*. Tracking the device can be enabled.
Mark as Lost	✓	Triggers configured actions like tracking, lock, and siren.
Siren	✓	Activates/deactivates the phone siren.
Lock	✓	Locks/unlocks the phone.
Wipe	✓	Triggers a factory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

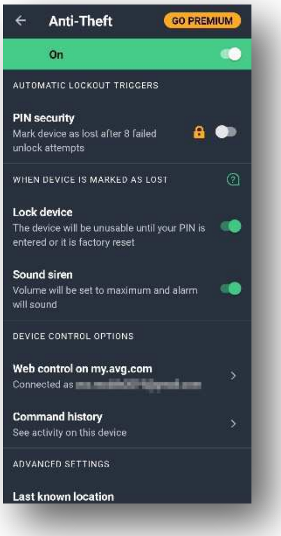
AVG
AntiVirus Free
6.48.2

Introduction

AVG AntiVirus Free is an ad-supported 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.







AUTOMATIC LOCKOUT TRIGGERS

PIN security
Mark device as lost after 8 failed unlock attempts

WHEN DEVICE IS MARKED AS LOST

Lock device
The device will be unusable until your PIN is entered or it is factory reset

Sound siren
Volume will be set to maximum and alarm will sound

DEVICE CONTROL OPTIONS

Web control on my.avg.com
Connected as [redacted]

Command history
See activity on this device

ADVANCED SETTINGS

Last known location

Usage

After installation, the user must agree to the vendor's Privacy Policy and Agreement. The app then shows a short overview of the included features. To continue with the free and ad-supported version, the user must also accept the Consent Policy for personalized advertising. After that, the user is prompted to start a first scan of the device.

Anti-Malware

Prior to starting the first device scan, the app asks for access to all files and folders on the device. Additionally, the user can select a more thorough and deeper scan of apps and files on the internal storage. The external storage (e.g. SD card) is excluded from any scans.

The app also checks the device's security settings, and warns of any disabled protection shields. The settings to treat PUA as malware, and to warn about apps with a poor reputation, are adjustable but already enabled by default.

Anti-Theft

Anti-theft commands are listed in the table below. During the setup of the anti-theft feature, the user must set 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 and appearing on top of other apps. Remote commands such as Locate, Lock, Mark as Lost, 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 view basic device information, such as the battery status.

In our testing, we found it a bit confusing that after successfully receiving the device location using the Locate command, the map was not automatically updated with the new location. We had to manually refresh the page in order to see the changes.

Web & Wi-Fi Protection

Once the app has been granted the Accessibility permission, the Web Shield component 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 and gives information about how much time the user spends on each app, available storage space, which permissions the apps have been granted, and data consumption over a day, week, or month. The feature shows the risk level "high", "average", and "low" for each installed app, according to the permissions it accesses. To limit mobile data usage, a custom data plan can be set up.

Additional Features

Hack Alerts notifies users whenever sensitive information tied to their 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 to remove them. My Statistics summarizes 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.

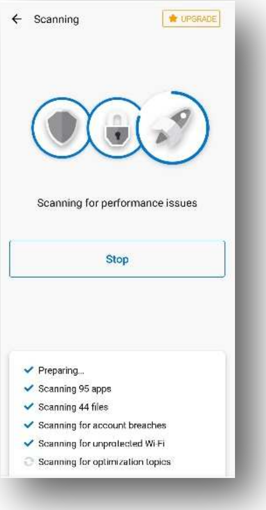
Anti-Theft Details		
	Commands Web	
Locate	✓	Displays the location on *Google Maps*. Tracking the device can be enabled.
Mark as Lost	✓	Triggers configured actions like tracking, lock, and siren.
Siren	✓	Activates/deactivates the phone siren.
Lock	✓	Locks/unlocks the phone.
Wipe	✓	Triggers a factory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

Avira

Antivirus Security Pro for Android
7.13.1

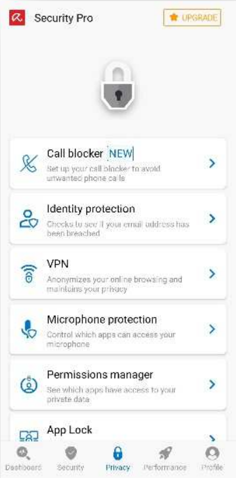
Introduction

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



Scanning for performance issues

- ✓ Preparing...
- ✓ Scanning 95 apps
- ✓ Scanning 44 files
- ✓ Scanning for account breaches
- ✓ Scanning for unprotected Wi-Fi
- Scanning for optimization topics



Call blocker NEW
Set up your call blocker to avoid unwanted phone calls

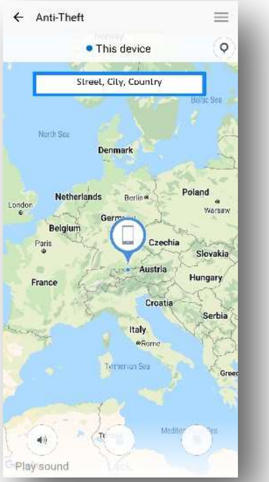
Identity protection
Checks to see if your email address has been breached

VPN
Anonymizes your online browsing and maintains your privacy

Microphone protection
Control which apps can access your microphone

Permissions manager
See which apps have access to your private data

App Lock



Usage

After installation, the user must agree to the EULA and Terms and Conditions, and also configure the data collection preferences of the app. Next, the app offers a dark mode to save battery. After that, the main screen shows up; from here, the user can start the first Smart Scan to check the device's security and performance.

Anti-Malware

Before the first scan, the user must grant the app permission to access all files and folders on the internal and external device storage. If the permission is denied, only installed apps will be scanned. Besides malware, the scan looks for adware and PUAs by default. Riskware detection can be configured, and scans for a set time and day can be scheduled in the Smart Scan options. There is also an option to start an automatic scan when a storage device is connected, or a USB cable is unplugged. However, this feature did not work in our testing; no scan was started in these scenarios.

As part of the scan results, the user is prompted to optimize device memory by stopping background apps and removing large temporary files from the storage.

Anti-Theft

Anti-theft commands are listed in the table below. When activating anti-theft components, the app requests the necessary permissions and device admin rights to get full control over the device. In addition, the app advises the user to turn off the option ”Remove permissions if app is unused” in the system settings. The anti-theft screen displays the device's current position on a map, and registered devices in the menu in the top right-hand corner. Of the three commands Locate, Lock, and Wipe, the last two can only be executed remotely by a second device that has the Avira app installed and is linked to the same user account.

During our testing, we noticed some usability issues which we would like to describe in more detail here. From a usability perspective, it is not clear how to properly set up the anti-theft feature. The user is prompted to grant access to the location without being informed why and which options to select (e.g. "allow while using", "all the time"). We suggest providing at least a brief explanation before showing the permission prompt.

The app advises the user to set up an Android lock screen in advance, as this is absolutely necessary to remotely lock the device. However, when selecting the respective option in the anti-theft settings, the user gets redirected to the wrong Android system settings page ("Biometrics and security"). In that case, the user has to manually navigate to *Android Settings* > *Lock screen*.

Moreover, as the lock screen is already set up with a custom PIN, password, pattern, etc., it is unclear to us why an additional PIN needs to be entered and sent with the Lock command.

When sending the Lock command without any additional information (e.g. message or phone number), it will fail with the error message "Something went wrong". From this, the user is not able to figure out *what* went wrong. We recommend giving more explanation and specifying why sending the command failed. In addition, sending any additional information has no effect, as it will not be shown anywhere on the target device screen.

Web & Wi-Fi Protection

The Web Protection feature detects phishing and other malicious websites while browsing the web with supported browsers. In addition, the user can black- or whitelist websites. The VPN service is limited to 100MB per day.

App Lock & Audit

App Lock restricts access to selected, sensitive apps by locking them using a PIN, pattern, or fingerprint. The user can choose between different locking behaviours (lock immediately, lock after predefined time intervals, lock when screen turns off). 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. The Permissions Manager shows all installed apps grouped by the permissions they request. Additionally, this feature shows which permissions the user has allowed or denied for certain apps.

Privacy Protection

Call Blocker can be used to block phone calls from specified contacts, if the Avira app is set as the default "caller ID & spam app". The Identity Protection checks a specific email address for data breaches.

The Microphone Protection feature is supposed to give only selected apps access to the device microphone when turned on. However, there is no option to select apps for that but instead, a list of apps which need access to the microphone is shown. Moreover, the Google Play entry says that this feature (along with Camera Protection) is only available on Android 10 and lower, although it was visible on our test devices.

Conclusion

Avira Antivirus Security Pro for Android 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. However, the app shows some flaws, especially during the setup of the anti-theft feature and when trying to remotely lock the device using the applicable command.

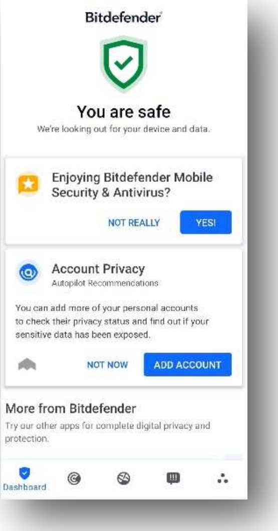
Anti-Theft Details		
Commands App		
Locate	✓	Displays the location on *Google Maps*.
Lock	–	Locks the device with a 4-digit PIN (executable remotely).
Wipe	✓	Triggers a factory reset and wipes the external storage (executable remotely).

Bitdefender

Mobile Security for Android
3.3.167

Introduction

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



Bitdefender

You are safe

We're looking out for your device and data.

Enjoying Bitdefender Mobile Security & Antivirus?

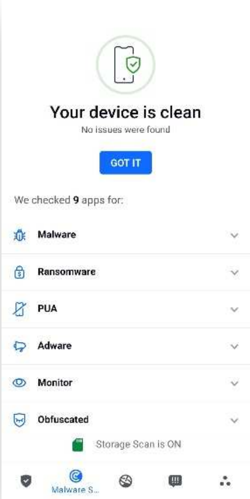
Account Privacy

Autopilot Recommendations

You can add more of your personal accounts to check their privacy status and find out if your sensitive data has been exposed.

More from Bitdefender

Try our other apps for complete digital privacy and protection.



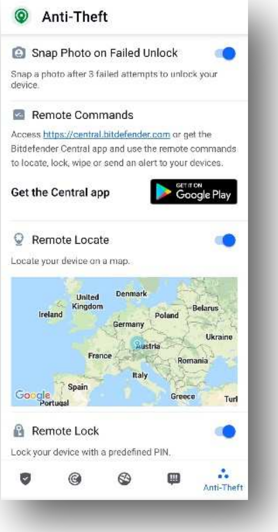
Your device is clean

No issues were found

We checked **9** apps for:

- Malware
- Ransomware
- PUA
- Adware
- Monitor
- Obfuscated

Storage Scan is ON



Anti-Theft

Snap Photo on Failed Unlock

Snap a photo after 3 failed attempts to unlock your device.

Remote Commands

Access https://central.bitdefender.com or get the Bitdefender Central app and use the remote commands to locate, lock, wipe or send an alert to your devices.

Get the Central app

Remote Locate

Locate your device on a map.

Remote Lock

Lock your device with a predefined PIN.

Usage

Upon opening the app for the first time, the user must agree to Bitdefender's subscription agreement, and either log in or create a new account. After that, the app helps the user to configure the necessary features, such as Malware Scanner and Web Protection, and to start the first device scan. On the main screen, the current device status is shown, and the user has access to all the app features.

Anti-Malware

The user can decide whether to run an app-only scan or a more thorough scan of the internal and external device storage by granting the "All files access" permission. Besides the scan result, a list of several malware types with a brief description is displayed. Bitdefender also provides details of detected malware.

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 an app-specific PIN. In order to activate Snap Photo, the app requires permission to access the device camera. The remote commands Locate Device, Lock Device, Play Sound, and Erase Device can be sent from either the Bitdefender Central app or the web interface at *central.bitdefender.com*.

From the command interface, the user can see the device's location and security status (along with a list of threats found on the device), and 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.

In our test, we noticed that after sending the Lock command, a device with no pre-defined Android lock screen does not get locked. After reporting this issue to Bitdefender, they released an updated version. Now, a lock screen needs to be configured during the setup of the anti-theft feature in order to use the Lock command. The web interface informs the user that if an Android lock screen has been properly set up beforehand, this lock type will not be overwritten by the new lock code sent with the Lock command. However, Bitdefender plans to reuse this lock code in a future version of the app.

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.

App Lock

The App Lock component limits 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 position on the keyboard each time the lock screen is displayed. Protected apps remain unlocked while connected to a Wi-Fi network marked as trusted. If Snap Photo is enabled, a photo is taken with the front camera after three failed unlock attempts with the PIN.

Privacy Protection

The Account Privacy feature lets the user check whether an email address has been compromised in a data breach. The email address to be checked needs to be verified with a confirmation code in advance. Scam Alert monitors incoming text messages and notifications for dangerous links and potential scams.

Conclusion

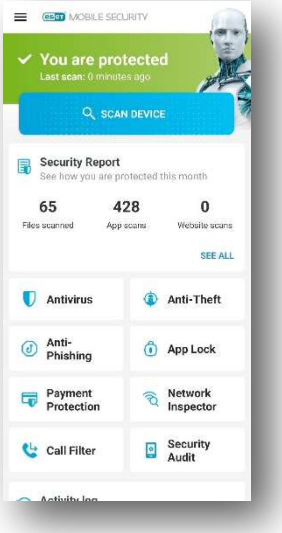
Bitdefender Mobile Security for Android provides a wide range of tools for monitoring the device's security and privacy. All anti-theft features except the Lock command worked as expected in our test.

Anti-Theft Details		
Commands App & Web		
Locate Device	✓	Displays the location on *Google Maps*.
Play Sound	✓	Sounds an alarm on the device and/or shows a custom message (only when the device is unlocked).
Lock Device	✓	Locks the device only if a pre-defined Android lock screen is configured.
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 3 failed unlock attempts.

ESET
Mobile Security Premium
7.3.15

Introduction

ESET Mobile Security Premium is a paid-for and easy-to-use mobile security solution for Android. In addition to malware protection, anti-theft, and anti-phishing, it offers privacy-related features such as app auditing and locking, payment protection, and a call filter.



ESET MOBILE SECURITY

✓ You are protected
Last scan: 0 minutes ago

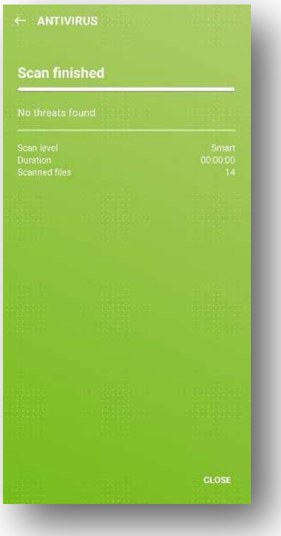
SCAN DEVICE

Security Report
See how you are protected this month

65	428	0
Files scanned	App scans	Website scans

SEE ALL

Antivirus
Anti-Theft
Anti-Phishing
App Lock
Payment Protection
Network Inspector
Call Filter
Security Audit
Activity log



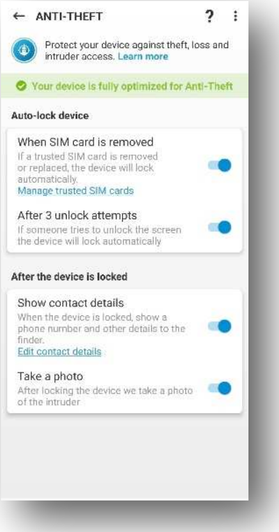
← ANTIVIRUS

Scan finished

No threats found

Scan level	Smart
Duration	00:00:00
Scanned files	14

CLOSE



← ANTI-THEFT

Protect your device against theft, loss and intruder access. Learn more

Your device is fully optimized for Anti-Theft

Auto-lock device

When SIM card is removed
If a trusted SIM card is removed or replaced, the device will lock automatically.
Manage trusted SIM cards

After 3 unlock attempts
If someone tries to unlock the screen the device will lock automatically

After the device is locked

Show contact details
When the device is locked, show a phone number and other details to the finder.
Edit contact details

Take a photo
After locking the device we take a photo of the intruder

Usage

On the first start, the user must agree to the EULA and Privacy Policy, as well as selecting the proper country and language. Next, the app asks for the user's consent to collect anonymous data. The user is then prompted to create an account, or log in to an existing one, prior to activating the product license. After granting the app the permission to access all files and folders, the first device scan starts immediately. All the features can be viewed and accessed on the main screen.

Anti-Malware

Users can choose between two scan levels: Smart (installed apps) and In-Depth (all files). In both cases, the internal and external device storage is scanned. Detection modules can be updated manually, and it is possible to toggle on-charge scans and to schedule scans.

Further settings allow the user to disable real-time protection for download folders, toggle the ESET LiveGrid reputation/feedback system, and to configure actions when removable media is connected. Additionally, the detection of potentially unwanted and unsafe applications can be controlled here. The Adware Detector can help with identifying installed apps that overlay the device screen with unwanted ads.

Anti-Theft

Anti-theft components are listed in the table below. During setup, the user needs to grant the app several permissions and device admin rights, and to configure a PIN to protect the anti-theft settings. The SIM card protection and other locking behaviours (e.g. number of unlock attempts, photo of the intruder) can be configured as well.

Once the device recognizes suspicious behaviour (e.g. removing device admin rights from the app), it will enter the "suspicious mode". In this state, the app locks the device and regularly sends data (photos taken by the front and back camera, device's location, and information about connected Wi-Fi networks) to the web interface at *home.eset.com*. The user can also trigger this mode from the web interface with one click. Device monitoring ends after 14 days but the user will receive a reminder via email 5 days before that time to extend the monitoring period. It is also possible to wipe all data from the device and to automatically save the last known location when the device battery will reach a critical level. A locked device can be unlocked either with the ESET account password or a custom unlock code obtained from the web interface.

Web & Wi-Fi Protection

The anti-phishing component protects a wide range of browser and social network apps against phishing attacks. The Network Inspector scans for vulnerable devices on the currently connected Wi-Fi network, and outputs relevant information about each device such as name, model, IP/MAC address, and OS.

App Lock & Audit

App Lock allows the user to protect selected apps from unauthorised access using a PIN or pattern. The locking type and behaviour (e.g. lock new apps after installation, lock after screen turns off) can be adjusted in the settings. With Security Audit, the user can review important device settings and permissions of installed apps (including system apps) in a clean overview.

Privacy Protection

With the Call Filter feature, the ESET app can be set as the default "caller ID & spam" app in order to block unknown/hidden numbers or contacts defined by custom rules. The Safe Launcher app (ESET Payment Protection) is installed along with the ESET app, and prevents malicious apps from reading and replacing on-screen information while using a protected banking or payment app.

Conclusion

ESET Mobile Security Premium offers comprehensive protection and security features against vulnerabilities and theft. It stands out for its particularly careful and brief descriptions of each setup step and various options. All anti-theft features worked flawlessly.

Anti-Theft Details		
Commands Web		
Device is missing	✓	Marks the device as lost and regularly triggers subsequent actions.
Track	✓	Automatically tracks the location and displays it on *Google Maps* when the device is marked as lost.
Play siren	✓	Sounds an alarm on the device when marked as lost.
Lock	✓	Automatically locks the device when marked as lost.
Wipe	✓	Triggers a factory reset and wipes the external storage when marked as lost.
Message	✓	Sends a message which is shown on the lock screen when device is marked as lost.
I recovered my device	✓	Stops the automatic device monitoring and unlocks the device.
Download activity	✓	All the pictures taken, and locations noted, can be downloaded as an archive.
Additional Features		
Take Photo	✓	Automatically takes pictures with the device's front and back camera when the device is marked as lost.
SIM Card Protection	✓	Locks the device when a (trusted) SIM card is removed.
Uninstall Protection	✓	Marks the device as lost when device admin rights are removed from the app.

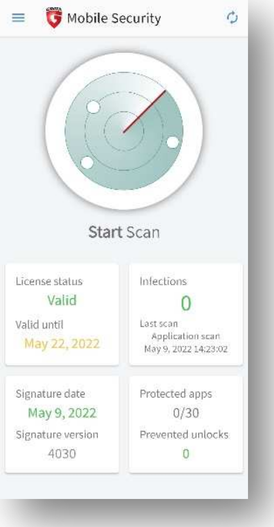
G DATA

Mobile Security Android

27.4.6

Introduction

G DATA Mobile Security Android is a paid-for security solution that 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.



Mobile Security

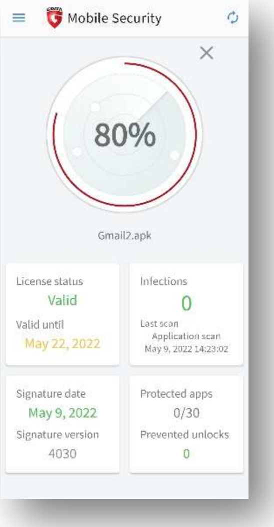
Start Scan

License status: Valid
Valid until: May 22, 2022

Infections: 0
Last scan: Application scan May 9, 2022 14:23:02

Signature date: May 9, 2022
Signature version: 4030

Protected apps: 0/30
Prevented unlocks: 0



Mobile Security

80%

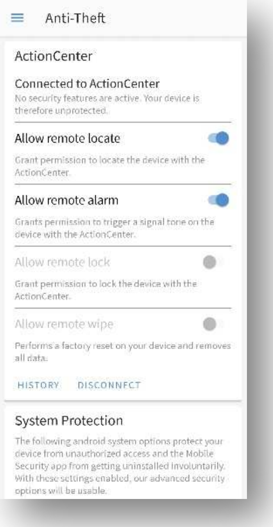
Gmail2.apk

License status: Valid
Valid until: May 22, 2022

Infections: 0
Last scan: Application scan May 9, 2022 14:23:02

Signature date: May 9, 2022
Signature version: 4030

Protected apps: 0/30
Prevented unlocks: 0



Anti-Theft

ActionCenter

Connected to ActionCenter
No security features are active. Your device is therefore unprotected.

Allow remote locate ●
Grant permission to locate the device with the ActionCenter.

Allow remote alarm ●
Grants permission to trigger a signal tone on the device with the ActionCenter.

Allow remote lock ○
Grant permission to lock the device with the ActionCenter.

Allow remote wipe ○
Performs a factory reset on your device and removes all data.

HISTORY DISCONNECT

System Protection
The following android system options protect your device from unauthorized access and the Mobile Security app from getting uninstalled involuntarily. With these settings enabled, our advanced security options will be usable.

Usage

First, the user must 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 all files and folders, the user is redirected to the main screen, where the phone and app status is shown, a system scan can be started, and the protected apps can be managed. The other app components are available from the menu in the upper left-hand corner.

Anti-Malware

From the settings, the user can choose the scan type, whereby App scan is selected by default. A system scan allows the user to perform a full scan of the internal and external storage.

Signatures are configured to update automatically but can be downloaded manually as well. The options to check apps after installation, and to perform periodic scans, are enabled by default.

Anti-Theft

Anti-theft commands are listed in the table below. Various permissions, among which are device admin rights, need to be granted to the app to activate anti-theft. The device must also be added in the G DATA ActionCenter at *ac.gdata.de* – or alternatively the G DATA Mobile Security Center at *msec.gdata.de* – by either scanning a QR code or entering the activation code. The anti-theft settings further 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.

After successfully connecting the device to the web interface, the user can send the remote commands Locate Device, Trigger Signal Tone, Lock Screen, and Delete Personal Data. From the web interface, the user is able to modify in-app settings (including battery-friendly scan options), start scans, and access general device information, along with a list of actions taken by the AV app.

G DATA sends a notification to a pre-defined email address each time an anti-theft feature has been activated. The user can invite other people to the web interface via email, and regulate their access to a subset of anti-theft features.

In our test, we noticed that after sending the Lock command, a device with no pre-defined Android lock screen does not get locked. Instead, the web interface shows a status message, and an email is sent to the user's inbox stating that executing the command failed. After we asked G DATA about this behaviour, they confirmed to improve the user experience in this regard.

Web Protection

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

App Lock & Audit

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

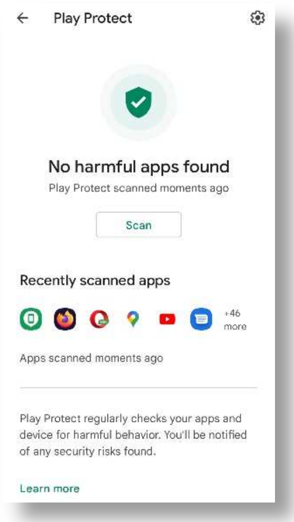
G DATA Mobile Security Android offers a sleek and easy-to-use graphical user interface, including essential security and privacy functions. Except for a minor issue in the Lock command, all anti-theft features worked as expected in our test.

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 can only be deactivated by opening the G DATA app.
Lock screen	▬	Locks the device only if a pre-defined Android lock screen is configured.
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
30.4.17

Introduction

With Google Play Services and Google Mobile Services (GMS), Google-certified Android devices are equipped with several APIs (e.g. for security, privacy, location, accounts, backups) and preinstalled apps (e.g. Chrome, Gmail, Maps, Drive, YouTube) to help developers build more-advanced apps and to provide better user experience to mobile end-users. Play Protect, as part of this collection, is Google's built-in malware protection, which monitors the device for malicious apps and APK files. Device security and privacy is further enhanced with anti-theft, browser protection, and app audit components.



Play Protect

No harmful apps found

Play Protect scanned moments ago

Scan

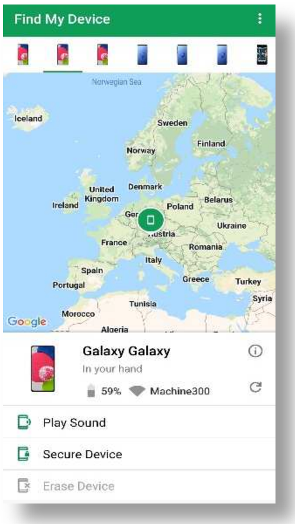
Recently scanned apps

+46 more

Apps scanned moments ago

Play Protect regularly checks your apps and device for harmful behavior. You'll be notified of any security risks found.

Learn more



Find My Device

Galaxy Galaxy

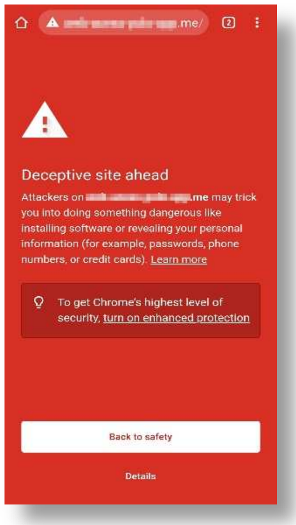
In your hand

59% Machine300

Play Sound

Secure Device

Erase Device



[redacted].me/

Deceptive site ahead

Attackers on [redacted].me may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

To get Chrome's highest level of security, turn on enhanced protection

Back to safety

Details

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 settings "Scan apps with Play Protect" and "Improve harmful app detection" can be turned off and a list of permissions for unused apps can be reviewed.

Anti-Theft

Anti-theft commands are listed in the table below. The anti-theft feature Find My Device can be operated remotely from the web interface at *google.com/android/find* or using the standalone app from Google Play. 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. The user can lock the device with the existing locking mechanism or by setting a new lock PIN/password, and optionally display a message on the device screen. The option to erase the target device deletes all data from the device by forcing a factory reset.

Web Protection

The Google Chrome browser app for Android devices includes a safe browsing feature with “Standard protection”, which alerts users to dangerous sites and downloads. Users can switch to “Enhanced protection” for a deeper analysis and to get warnings about password breaches. Options for “Do not Track” and “Always use secure connections” are disabled by default.

App Audit

In the Android device *Settings* > *Apps*, all installed apps are listed, along with detailed information about their notifications and default-app settings, permissions (including special permissions), and device usage (e.g. mobile data, battery consumption, storage space). From here, users can also disable/uninstall the app, force an app stop, and adjust the permissions the app has requested. To give users even more insight into how apps affect their privacy, all apps can be sorted and viewed by dangerous permissions (e.g. location, camera, microphone) and permissions with special access (e.g. device admin rights, all files access, install unknown apps).

Conclusion

Google Play Protect is preinstalled on approved new Android devices, while older devices will receive updates for Play Services and GMS. All the security-related features, such as malware protection, anti-theft, and web protection, can be used for free with a Google account. Depending on the device model, manufacturers may provide their own device-related security features, which might overlap with pre-existing GMS apps such as Google Chrome and Find My Device. All anti-theft commands worked as expected.

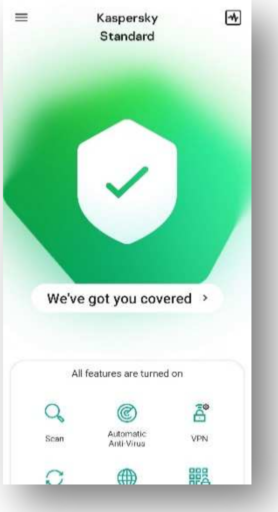
Anti-Theft Details		
Commands App & Web		
Locate	✓	Displays the current or last-known location on *Google Maps*.
Secure Device	✓	Locks the device with a given PIN/password or the pre-defined locking mechanism. Optionally, a message and/or phone number to contact can be displayed on the locked device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

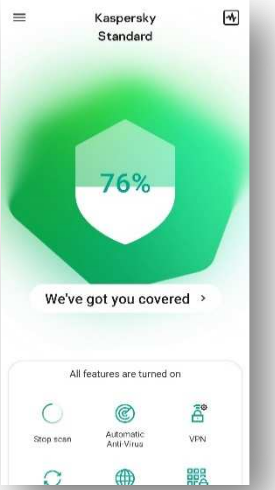
Kaspersky

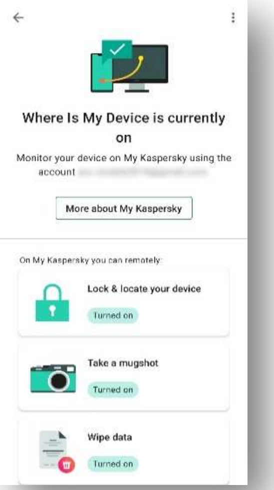
Kaspersky Standard for Android
11.84.4

Introduction

Kaspersky Standard for Android 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. The app also includes a free but data-limited VPN. The app functionality can be extended by installing additional Kaspersky apps from within the app, such as battery optimizer or a QR scanner.






Where Is My Device is currently on

Monitor your device on My Kaspersky using the account [redacted]

Usage

Upon first opening the app, the user must agree to Kaspersky's EULA and Privacy Policy, and grant storage permission to the app. Next, the user must either activate an existing license or start a free trial week. On the app's main screen, a database update as well as a quick scan are started automatically. The app prompts the user to configure and enable various security-related components, such as anti-theft and safe browsing, and suggests running a full device scan.

Anti-Malware

When starting a scan, the user is asked whether to start a quick (app-only) scan, a full scan including all files on the internal and external storage, or a selective scan of specific folders or files.

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 of installed apps and APK files 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.

Anti-Theft

Anti-theft commands are listed in the table below. The setup of the Where Is My Device feature requires the user to grant the app the necessary permissions as well as device admin rights, and to configure a secret code/pattern/fingerprint. Remote commands such as Lock & Locate, Mugshot, Alarm, and Data Wipe can be sent from the web interface at *my.kaspersky.com*.

Here, basic information, such as battery level and activated security features, as well as images taken by the Mugshot command, and the device location, are shown. All commands except for Data Wipe can include a custom message that is displayed on the lock screen. An email is sent after the commands Lock & Locate or Mugshot are successfully executed, and the results are automatically deleted from the web interface after 30 days.

The features SIM Watch and Uninstallation Protection lock the device when they detect a SIM card change or an attempt to uninstall the Kaspersky app, respectively.

Web Protection

The Safe Browsing component protects the user from phishing websites while browsing the web. The supported browsers are displayed in the settings.

Before using the free VPN component, the user must accept Kaspersky's VPN policy. After that, the VPN auto-selects the server closest to the user's current location and offers a daily traffic limit of 300 MB.

App Lock & Audit

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 shows apps grouped by dangerous and special permissions, and provides details about apps, including their permissions and data usage. Furthermore, installed apps can be removed from within this feature.

Privacy Protection

Call Filter automatically declines incoming calls from blacklisted contacts. The Data Leak Checker checks the email address connected to the Kaspersky account for data breaches. The Weak Settings Scan monitors the system settings for any vulnerabilities.

Conclusion

Kaspersky Standard for Android comprises a great set of security and privacy features, which are thoroughly explained by the help links in the upper right-hand corner. Features can be extensively customised, and additional apps can be incorporated. All the anti-theft commands worked flawlessly in our test.

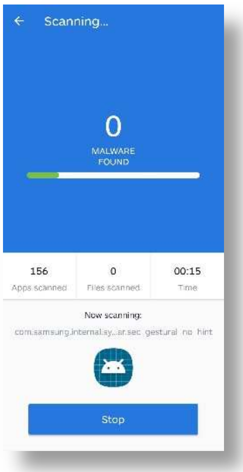
Anti-Theft Details		
Commands Web		
Lock & Locate	✓	Locks the device, displays the location on *Google Maps*, and sends the location in an email.
Mugshot	✓	Locks the device and takes several pictures using the front camera.
Alarm	✓	Locks the device and rings an alarm.
Data Wipe	✓	Triggers a factory reset 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
3.10.1

Introduction

Malwarebytes for Android is a paid-for mobile security product that provides a malware scanner, along with real-time and ransomware protection, a safe browsing feature, and app auditing.

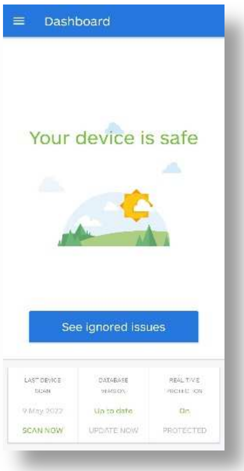


Scanning...

0
MALWARE FOUND

156	0	00:15
Apps scanned	Files scanned	Time

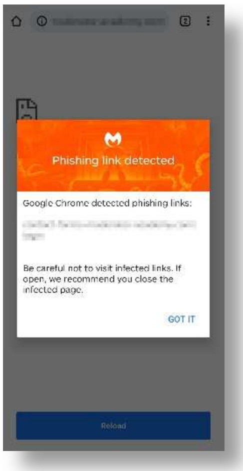
Now scanning:
com.samsung.internal.sy...ar.sec_gestural_no_hint



Dashboard

Your device is safe

LAST DEVICE SCAN	DATABASE VERSION	REAL-TIME PROTECTION
9 May 2022	Up to date	On
SCAN NOW	UPDATE NOW	PROTECTED



Phishing link detected

Google Chrome detected phishing links:

Be careful not to visit infected links. If open, we recommend you close the infected page.

Usage

Upon first launch, the app asks the user to give permission to access all files and folders on the device. After that, a database update is run in the background, and a full system scan can be started manually. The app advises the user to further enhance device security by giving it more privileges, excluding it from the battery optimization, and checking for unsecure system settings in the security audit.

Anti-Malware

The app scans the internal and external device storage, and shows detailed information about the apps and files being scanned, as well as malware found. When enabled, deeper system scans with additional rules are performed. Automatic updates are enabled by default and can be triggered manually. The user can schedule scans for different times and days, after a device boot, or a database update. Scans can be disabled if battery is low, or run only while charging. Giving the app device-admin rights enables full device control for its anti-ransomware remediation feature, and protects itself from being uninstalled easily.

Web Protection

If enabled, the Safe Browsing Scanner will warn the user of phishing and other malicious links. However, the feature does not attempt to block the malicious content.

App Audit

Your Apps shows the list of all system and other installed apps and provides further app details when granting the Usage-Access permission. The Privacy Checker scans and groups the apps according to the permissions they have acquired.

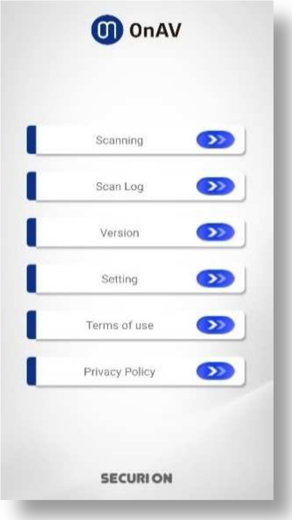
Conclusion

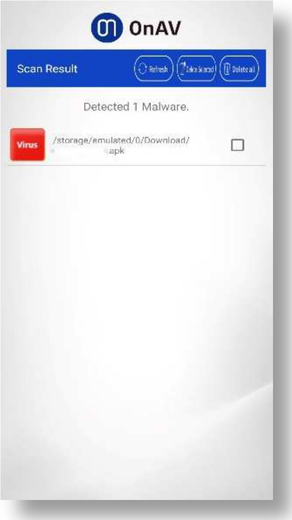
Malwarebytes for Android is a solid mobile security solution, which includes anti-malware, web protection and a detailed audit feature for installed apps. The steps for the initial setup and app settings are clearly explained and leave no questions unanswered. Although phishing websites are not actually blocked, the user does at least get a warning to close the page immediately.

Securion
OnAV
1.0.34

Introduction

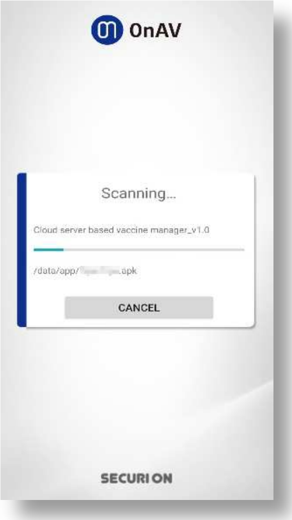
Securion OnAV is an ultra-light and free-to-use AV product that only provides cloud-based malware detection. Without any user registration, it assigns a unique ID to each device to prevent double sign-ups. This review covers the English version of the app only, which differs from its original Korean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





Detected 1 Malware.

/storage/emulated/0/Download/ .apk □



Scanning...

Cloud server based vaccine manager_v1.0

/data/app/ .apk

Usage

First, the user must accept the EULA, Terms and Conditions, and the Privacy Policy. After that, the app asks for permission to appear on top of other apps and to access all files and folders, in order for its real-time protection to work properly. On the main screen, a simple menu listing the main functions is shown.

Anti-Malware

The app only scans the internal storage for malicious apps and files. Detected malware can be deleted selectively or all 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.

We informed Securion about an issue in the malware scanner. The vendor quickly fixed it and released an updated version.

Conclusion

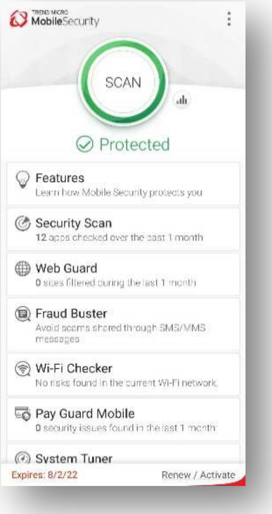
Securion OnAV is a free, user-friendly app that provides just malware protection capabilities. Detected malware is listed in the scan results, where it can be viewed and deleted directly.

Trend Micro

Mobile Security for Android
12.15.0

Introduction

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



TREND MICRO MobileSecurity

SCAN

Protected

Features
Learn how Mobile Security protects you

Security Scan
12 apps checked over the past 1 month

Web Guard
0 sites filtered during the last 1 month

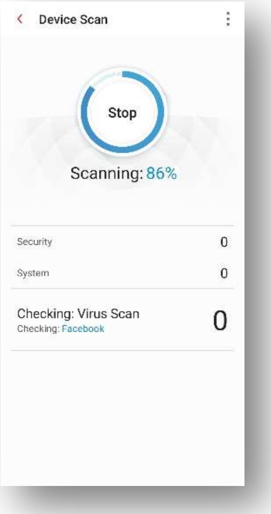
Fraud Buster
Avoid scams shared through SMS/MMS messages

Wi-Fi Checker
No risks found in the current Wi-Fi network.

Pay Guard Mobile
0 security issues found in the last 1 month

System Tuner

Expires: 8/2/22 Renew / Activate



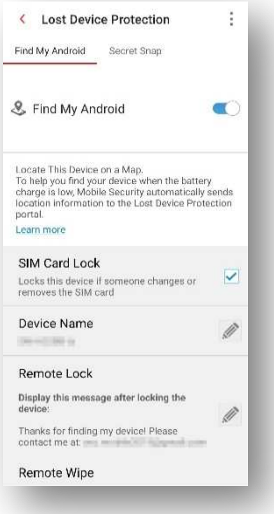
Device Scan

Stop

Scanning: 86%

Security	0
System	0

Checking: Virus Scan
Checking: Facebook 0



Lost Device Protection

Find My Android | Secret Snap

Find My Android

Locate This Device on a Map.
To help you find your device when the battery charge is low, Mobile Security automatically sends location information to the Lost Device Protection portal.
Learn more

SIM Card Lock ☑
Locks this device if someone changes or removes the SIM card

Device Name
[redacted]

Remote Lock
Display this message after locking the device:
Thanks for finding my device! Please contact me at: [redacted]

Remote Wipe

Usage

Upon the first app start, the user is prompted to accept Trend Micro's License Agreement, Privacy, and Data Collection Notice. Next, the user must either activate a license, start a two-week trial, or continue with a limited free version. After that, an initial scan is started in the background. In addition to showing the scan result, the app recommends configuring various other features, including granting the necessary permissions. All the app features are directly accessible from the main screen, with the device status displayed at the top.

Anti-Malware

In the security scan settings, the user can set the protection level, which determines at which threat level the user should be notified. Other options are toggling real-time scanning, enabling a pre-install scan, including the external storage in scans, and if an app-only scan or a scan of the entire device storage should be performed.

Malware signature updates are run periodically (daily, weekly, or monthly) but can also be triggered manually.

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*. An option to lock the phone whenever the SIM card is changed or removed is also included which did not work properly in our first testing. After we told Trend Micro about the issue, they quickly released a bugfix. 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 take a picture with the front camera after 3, 5 or 7 failed unlock attempts, which will be saved on the device and sent to a pre-defined email address.

Web & Wi-Fi Protection

Web Guard blocks links to malicious websites for directly supported apps. For apps that are not directly supported, the VPN protection needs to be activated to browse securely while using these apps. The blocking of phishing sites worked in all the supported browsers. 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 split into App Lock and Website Filter. With the first, selected apps can be protected 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, custom filters, as well as white- or blacklists of individual websites, can be built. The website filter also works in combination with the VPN content filter for apps not directly supported by the Trend Micro app. As with Web Guard, blocking of websites worked with all supported browsers.

Additional Features

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

Conclusion

Trend Micro Mobile Security for Android 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. All anti-theft features worked properly.

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 sent to the account email address 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 Card Lock	✓	Locks the device if the SIM card is changed or 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 2022)											
Product Name	*Android OS*	Avast Mobile Security Free	AVG AntiVirus Free	Avira Antivirus Security Pro for Android	Bitdefender Mobile Security for Android	ESET Mobile Security Premium	G DATA Mobile Security Android	Kaspersky Standard for Android	Malwarebytes for Android	Securion OnAV	Trend Micro Mobile Security for Android
Version Number	*12*	6.48	6.48	7.13	3.3	7.3	27.4	11.84	3.10	1.0	12.15
Supported Android versions	*built-in*	6.0 and higher	6.0 and higher	6.0 and higher	5.0 and higher	5.0 and higher	5.0 and higher	5.0 and higher	7.0 and higher	7.0 and higher	5.0 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, Arabic, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Kazakh, Korean, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovene, Spanish, Swedish, Thai, Turkish, Ukranian, Vietnamese	English, Dutch, French, German, Italian, Japanese, Polish	English, Arabic, Bulgarian, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Italian, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thai, Turkish, Vietnamese	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	●	●	●	●	●	●	●	●	●	●	●
Automatic (scheduled) scan		●	●	●		●	●	●	●		●
Can detect malware sitting on external SD card				●	●	●	●	●	●		●
On-Access scan of apps	●			●		●		●	●	●	
Scan requires online cloud connection	●				●						
Manual local database update possible (beside automatic updates)		●	●			●	●	●	●		●
User account needed to use product					●	●	●				●
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●	●	●		●
Privacy Advisor (audit app permissions)	●	●	●	●		●	●	●	●		
Supported browsers (Safe Browsing), at most five selected by AV-Comparatives	Google Chrome	Google Chrome, Firefox, Opera, Samsung Internet, UC Browser	Google Chrome, Firefox, Opera, Samsung Internet, UC Browser	Google Chrome, Opera, Opera Mini, Samsung Internet	Google Chrome, Firefox, Opera, Opera Mini, Samsung Internet	Google Chrome, Firefox, Opera, Opera mini, Samsung Internet	Google Chrome, Firefox, Opera	Google Chrome, Huawei Browser, Samsung Internet	Google Chrome, Opera, Opera Mini, Samsung Internet		Google Chrome, Samsung Internet
Anti-Theft											
Web Interface for controlling Anti-Theft commands	●	●	●		●	●	●	●			●
Remote Locate, Lock & Wipe (Factory Reset)	●	●	●	●	●	●	●	●			●
Anti-Theft Alarm (cannot be muted by thief)		●	●		●	●	●	●			
Locate-Phone Alarm only (can be muted)	●			●							●
Thief Cam					●	●		●			●
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)											●
Additional Features (selected by AV-Comparatives)											
Task Manager (manage installed apps)	●	●	●				●	●	●		●
Hack Alerts / Data Leak Checker		●	●	●	●			●			
VPN				●	●			●			●
Wi-Fi Security		●	●			●					●
System Optimizer		●	●	●							●
Call Blocker/Filter	●			●		●		●			
Network Monitor (track data usage)	●	●	●								
Payment Protection						●					●
Photo Vault		●	●								
Support											
Online Help & FAQ	●	●	●	●	●	●	●	●	●		●
User Forum	●	●	●	●	●	●		●	●		●
Email Support				●	●	●	●	●	●		●
User Manual (PDF)	●			●	●	●	●	●	●		
Phone Support				●	●	●	●	●			●
Online Chat					●			●	●		●
Supported languages of support	All	English, Czech, French, German, Japanese, Portuguese, Russian, Spanish	English, Czech	English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish	English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish	English, Chinese, Dutch, Estonian, French, German, Hungarian, Italian, Korean, Polish, Portuguese, Russian, Slovenian, Spanish, Turkish	English, Dutch, French, German, Italian, Japanese, Polish	English, Chinese, Czech, Dutch, French, German, Hungarian, Italian, Japanese, Portuguese, Romanian, Russian, Spanish, Turkish, Vietnamese	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 15 / 15 EUR	USD 10 / 10 EUR	USD 15 / 11 EUR	USD 40 /40 EUR	FREE	USD 36 / 20 EUR

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

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

AV-Comparatives
(June 2022)