Independent Tests of
Anti-Virus Software

Mobile Security Review 2023

TEST PERIOD: MAY 2023

LAST REVISION: 22ND JUNE 2023

WWW.AV-COMPARATIVES.ORG

Content

Introduction

In this report, we aim to aid readers in evaluating both the built-in security measures of Android and the advanced features provided by third-party security apps. Our report covers results from malware protection and battery consumption tests, along with reviews that assess the functionality, app design, and overall usability of each security solution. At the end of each product report, readers can find a table that offers an overview of any anti-theft functions included in that particular product. While some of the apps we've tested might have additional features like app managers, network monitors, and system optimizers, we primarily focus on security, including anti-malware, anti-theft, safe browsing, and privacy in our reviews and only briefly mention any further functionality. To facilitate easier product comparisons, we maintain a consistent structure for each product report.

In 2021, we also evaluated how well some security apps protect against stalkerware on Android[1]. This type of software operates covertly, enabling unauthorized individuals to spy on device owners without their knowledge or consent. While stalkerware and legitimate software (such as parental controls) have blurred lines between them, Google Play has implemented stricter policies in recent years to combat this issue. Consequently, stalkerware is typically installed through side-loading[2] since it is not available on the Play Store.

Mobile security products are designed primarily to safeguard mobile users and their devices from threats such as malicious apps, phishing URLs, fraudulent emails, and other harmful links. Recent versions of Android come equipped with fundamental security features. For example, *Play Protect*, Google's built-in malware scanner, scans apps during installation from Google Play or third-party sources and performs regular device checks for threats. *Safe Browsing* API helps protect against malware and phishing links when browsing the web using Google Chrome. Anti-theft functions, such as lock, locate, alarm, and wipe, are available through Google's *Find My Device*, enabling users to find lost or stolen phones and prevent access to personal data stored on them. The latest Android versions also provide several app auditing features that enable users to review and modify privacy settings (such as dangerous/special permissions and notifications) and usage (such as mobile data, battery consumption, and storage space) of individual apps.

In the following pages, we explore the privacy and security features and limitations of *Google Android*. It is important to note that not all of Google's security features are available to all users due to restrictions on certain Android versions, Android-based operating systems, and geographical locations. We also discuss the current risks that smartphone users face and provide recommendations for enhancing protection. Additionally, we provide a brief overview of common security features in Android security apps. The primary section of this report contains the participating security products, along with the results of malware protection tests, battery drain tests, and in-depth product reviews.

For each product's anti-theft component, we briefly comment on each function and use symbols in the table to indicate its performance 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

Android 6.0 (Marshmallow) introduced run-time permissions, giving users more control over the information and private data installed apps have access to. This approach is very different from the one adopted by earlier Android versions, where apps requested all necessary permissions before 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. Apps targeting Android 9 (Pie) and above are forced to use encrypted connections, such as TLS or HTTPS. Cleartext support (e.g., using HTTP instead of HTTPS) and establishing trust in third-party root CA certificates are only possible if explicitly defined in the app’s network configuration. These make network attacks such as ARP spoofing or MITM become less of a concern.

Android 10 and 11 brought some significant improvements regarding security and privacy which are refined in later versions. These include, for example, the concept of scoped storage (along with the “All files access” permission), restrictions when accessing some resources (e.g., background location, microphone, camera, list of installed apps), and preventing third-party apps from querying specific device information (e.g., IMEI, IMSI, MEID, SIM, build serial number). An auto-reset feature automatically resets all run-time permissions for unused apps.

In Android 12, users have the option to allow apps to access only approximate location information. Indicators for active camera/microphone usage and a system-wide camera/microphone toggle to easily block access to these were added. Apps can also hide non-system-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, and the app cache is cleared.

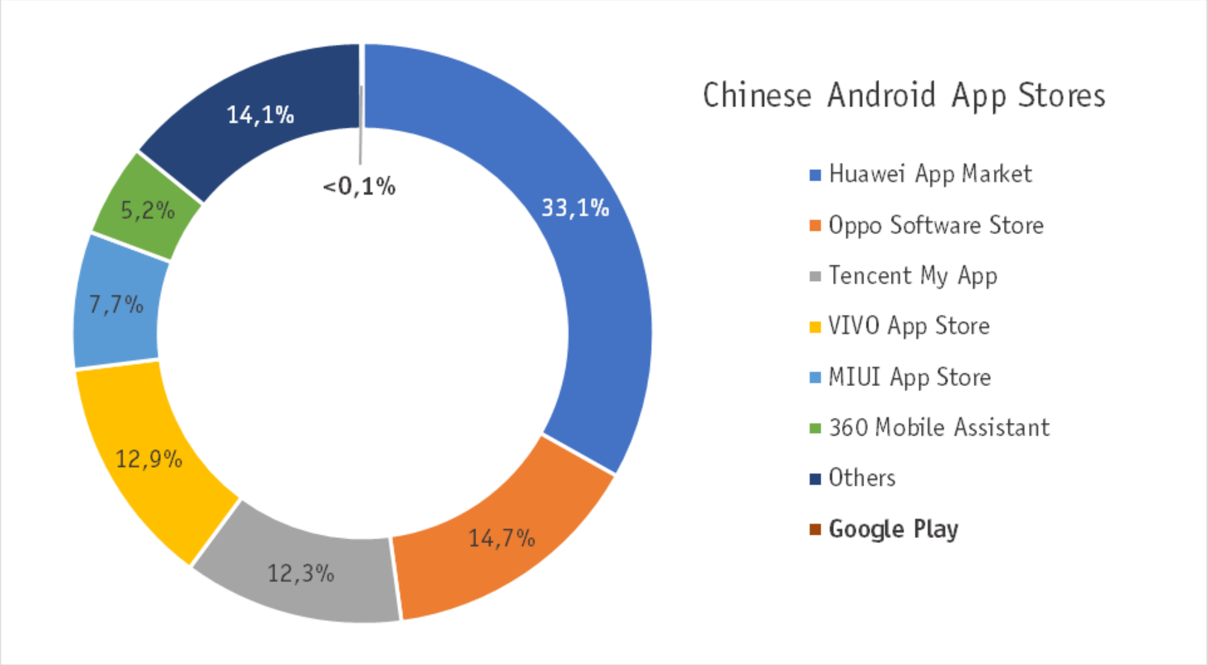
The release of Android 13[3] in August 2022 introduced many changes to Android permissions. In various use cases where apps could access the desired information without user consent, they are now required to declare the necessary permission in the Android manifest file, or both declare and explicitly request it during runtime. These scenarios include using the Google Play services advertising ID for monetization and personalised ads, posting app notifications, discovering nearby Wi-Fi devices without the need of the device's location, reading body sensor information while running in the background, and accessing different types of media individually (e.g., image, video, audio). To adhere to best practices for permissions and build user trust, an app can proactively revoke its access to unused runtime permissions. Furthermore, users can stop the foreground service of an app from the new “Task Manager” feature in the Android notification area and dismiss associated notifications. Apps that allow users to copy sensitive content (e.g., passwords, credit card information) to the clipboard can hide the content from appearing in the clipboard preview.

The resulting restrictions imposed on apps targeting the latest Android version have 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.

[3] https://developer.android.com/about/versions/13

Because of all these changes, 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).

Malware protection by Google Play Protect is getting better each year, but 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 1.69 billion[4] active mobile devices in China, and about 65%[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. A US Executive Order[7] signed in November 2020 prohibits US companies (such as Google) from doing business with blacklisted Chinese companies. Consequently, Google apps and services, including Play Protect, will no longer be available on future device models from certain Chinese manufacturers.

[4] https://datareportal.com/reports/digital-2023-china
[5] https://gs.statcounter.com/os-market-share/mobile/china
[6] https://www.appinchina.co/market/app-stores
[7] https://ofac.treasury.gov/media/49616/download

Protection against Android Malware

Smartphones are now commonly used as popular PC substitutes for a variety of daily tasks such as online shopping, banking, instant messaging, video conferencing, and emailing. However, with the increasing sophistication of cyber-attacks, mobile devices are becoming a prime target, particularly through fraudulent apps that aim to steal user data or money. These malicious apps often disguise themselves as fake versions of popular apps that have been downloaded by millions of users from Google Play[8]. To minimize the risk of falling victim to these threats, we recommend following the guidance provided in this report.

To protect yourself from malicious apps, it is best to download apps exclusively from official app stores such as Google Play or reputable app makers, while avoiding third-party stores and side-loading. Before installing any app, check its reviews in the app store and avoid those with predominantly negative or suspicious feedback. When granting app permissions, be cautious and question any request that seems unnecessary or unrelated to the app’s purpose. Watch out for apps that request excessive access rights, for example, a calculator app that asks for permission to your contacts.

While not every app with suspicious behaviour is necessarily malicious, it is important to assess its legitimacy and usefulness. Google Play regularly updates its policies to ensure a certain level of security, requiring app developers to verify their identity, digitally sign their apps, and meet API level requirements[9]. Apps also undergo multiple review processes and require Google's approval regarding privacy to remain available on Google Play. Moreover, developers must provide information about data collection, sharing, and deletion in the "Data Safety" section of their apps.

Rooting your smartphone can significantly increase the risk of malicious apps taking control over your device and may void the warranty. Public Wi-Fi networks, often found in places like coffee shops and airports, are popular targets for data theft. Avoid entering or sharing sensitive information such as user credentials or credit card information on a public Wi-Fi unless you use a VPN to encrypt your network traffic and prevent hackers from intercepting it. Additionally, disable any unused settings (e.g., Bluetooth, NFC, Wi-Fi calls) or device sharing functions that could be potential attack vectors.

Stay cautious and vigilant when receiving suspicious links via text messages, emails, instant messenger chats, or social media. If the sender is unknown, mark the message as spam or delete it immediately. It is also crucial to keep your mobile device updated with the latest security patches and Android version to address device and API vulnerabilities.

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

The risk of malware on Android phones depends on multiple factors and cannot be answered simply. However, sticking to official app stores like Google Play lowers the infection risk. In Asian countries with many rooted devices and third-party app stores, the likelihood of harmful downloads is higher. Nevertheless, it is important to note that "low risk" does not mean "no risk," as the threat landscape can change quickly[10]. To be prepared, installing appropriate security software on your smartphone is recommended. Currently, in western countries, protecting against data loss from theft or loss is more critical than malware protection.

[8] https://www.av-comparatives.org/tests/android-test-2019-250-apps/
[9] https://developer.android.com/google/play/requirements/target-sdk
[10] https://www.bleepingcomputer.com/news/security/android-apps-with-spyware-installed-421-million-times-from-google-play/

Security Features

In this section, we provide a concise overview of key security components commonly found in Android security products. The primary component is the *malware scanner* which safeguards users from unintentionally installing malicious apps on their device. Similar to antivirus programs for Windows, Android mobile security apps incorporate various protection features. The *real-time protection* actively scans new and existing apps for any malicious behaviour. The *on-demand scanner* examines the device, including internal storage and/or external SD card, for malicious apps that are already installed or downloaded APK files that have not yet been run.

Keeping malware definitions up to date is a critical factor in effective protection, especially for apps that primarily rely on them for detecting malware. Certain tested products offer a cloud-assisted malware scanner to ensure access to the very latest definitions. Definition updates are either retrieved automatically by the app at specified time intervals or triggered manually by the user.

The *anti-theft* component is designed to remotely control a lost or stolen device. Android already includes core anti-theft features such as device lock, locate, wipe, and alarm. The tested security products extend this functionality with features such as location tracking, taking pictures of the thief using the device's cameras, or triggering actions in response to suspicious device activities (e.g., locking the device when the SIM card is changed or trying to uninstall the security app, capturing pictures after multiple failed unlock attempts). Typically, the anti-theft component is managed via a web interface or, in rare cases, using a second phone that has the same security app installed. Some vendors (such as Avast, AVG, Avira) have decided to remove the anti-theft feature from their latest app versions as it did not provide sufficient value compared to Android's built-in features[11].

Many security products include *web protection* which prevents users from unintentionally downloading malicious apps or accessing phishing websites while browsing the Internet. The majority of the tested products offer safe web browsing for at least Google Chrome, the most popular browser on Android. Additionally, some apps support various third-party browsers to accommodate the user's choice for their preferred mobile browser.

App lock is another useful security feature, enabling users to safeguard selected apps from unauthorized access. Users can set up a locking mechanism, such as PIN, password, pattern, or biometrics (e.g., fingerprint or face recognition on supported devices), which is required to launch a protected app. Furthermore, they might be able to customize the app locking behaviour, such as unlocking when connected to a trusted Wi-Fi or locking based on location or 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. This analysis examines app permissions that are uncommon, unnecessary, or inappropriate, as they may pose a risk to the user's privacy. Based on this result, some security apps advise uninstalling "risky" apps.

[11] https://support.avast.com/en-eu/article/Use-Android-Anti-Theft , https://support.avg.com/SupportArticleView?l=en&urlName=use-android-avg-anti-theft&q=Anti+theft&supportType=home

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 2023). 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. The versions listed below apply to the updated product reviews.

Vendor	Product Name	Version	Features
Avast	Mobile Security Free	23.3	● ○ ● ○ ●
AVG	AntiVirus Free for Android	23.3	● ○ ● ○ ●
Avira	Prime for Android	7.20	● ○ ● ● ●
Bitdefender	Mobile Security	3.3	● ● ● ● ○
ESET	Mobile Security Premium	8.1	● ● ● ● ●
Google	Play Protect & OS Features	35.7	● ● ● ○ ●
Kaspersky	Plus for Android	11.100	● ● ● ● ●
Securion	OnAV	1.0	● ○ ○ ○ ○
Trend Micro	Mobile Security	15.5	● ● ● ● ○

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 13 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

For this report, we used Android 13 which is currently the most recent Android version. We used the unmodified version of Android 13 in order to avoid potential problems with hardware manufacturers' or mobile carriers' modifications.

[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.

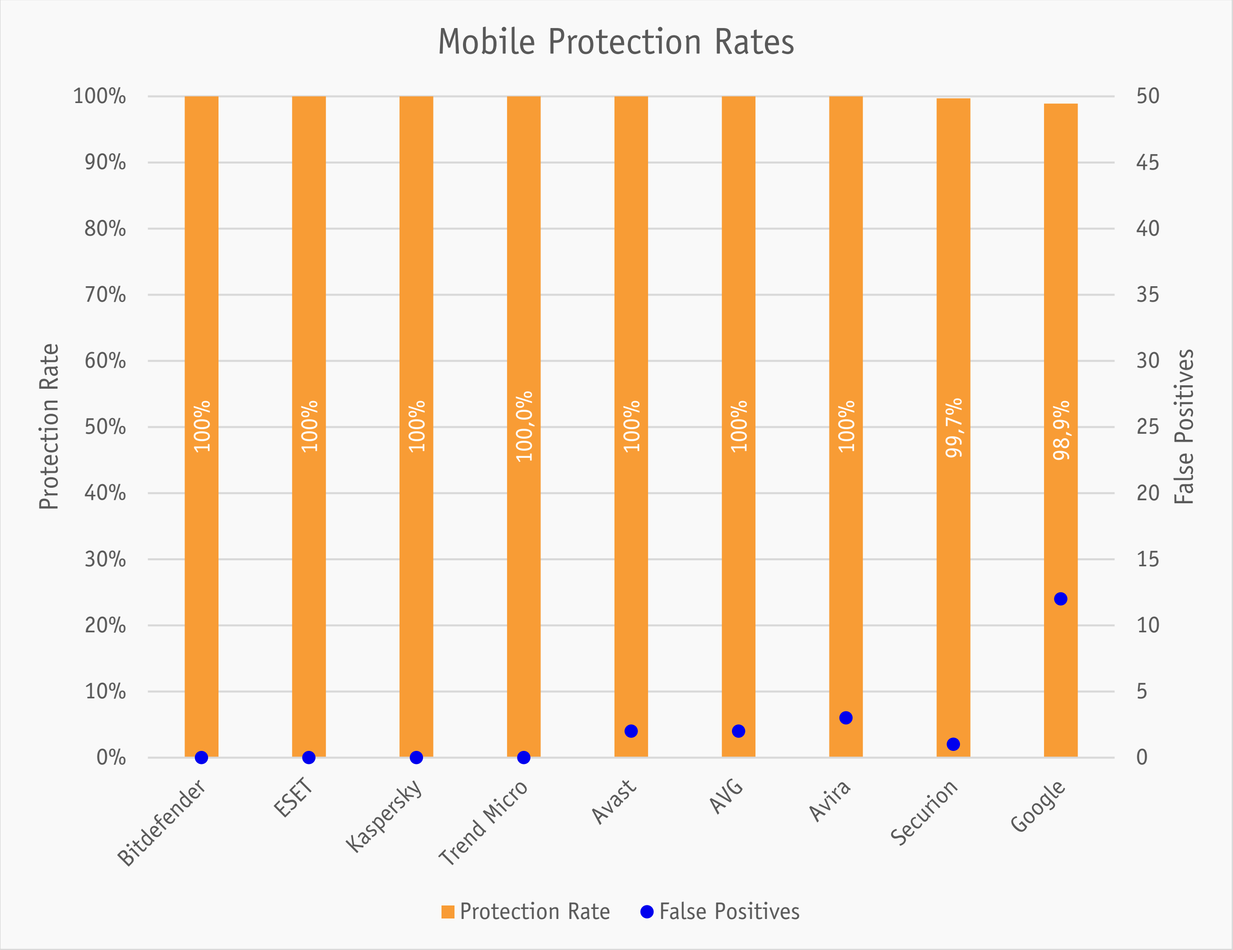
AV comparatives APPROVED Mobile Product 2023

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.

AV comparatives APPROVED Mobile Product 2023	**Avast** Mobile Security Free offers a wide range of features, covering various aspects of device security, privacy monitoring, and performance optimization.
AV comparatives APPROVED Mobile Product 2023	**AVG** AntiVirus Free is a meticulously designed mobile security solution that provides a diverse set of customizable features related to security and privacy.
AV comparatives APPROVED Mobile Product 2023	**Avira** Prime for Android is a feature-rich mobile security app that enhances device security and safeguards user privacy.
AV comparatives APPROVED Mobile Product 2023	**Bitdefender** Mobile Security is a user-friendly mobile security product which combines elaborated device protection and privacy-oriented features in a clean user interface.
AV comparatives APPROVED Mobile Product 2023	**ESET** Mobile Security Premium is a robust security app for Android which includes comprehensive security and privacy measures against vulnerabilities and theft.
X	**Google** Android comes equipped with built-in malware protection, device loss/theft prevention, safe-browsing functionality, and other privacy-related features. Unfortunately, it barely did not reach the required protection level for certification.
AV comparatives APPROVED Mobile Product 2023	**Kaspersky** Plus for Android encapsulates extensive and thoroughly explained security and privacy features in an attractive app design.
AV comparatives APPROVED Mobile Product 2023	**Securion** OnAV is a straightforward and free-to-use mobile security solution for Android, providing malware protection capabilities exclusively.
AV comparatives APPROVED Mobile Product 2023	**Trend Micro** Mobile Security is a well-developed and comprehensive app which integrates malware and theft protection, parental controls, privacy tools, 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 **2,730** 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 15th May 2023. 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, ESET, Kaspersky, Trend Micro	100%	0
Avast, AVG	100%	2
Avira	100%	3
Securion	99.7%	1
Google	98.9%	12[13]

[13] Mostly 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 mobile security apps high marks regarding power usage.

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

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

Review Format

Here we have outlined the structure of the following product reviews for each of the mobile security apps in this test. As the tested products include different feature sets, not every section regarding app features (except for Anti-Malware) might be applicable to them.

Introduction: We provide a concise overview of the product, stating its price model (free or paid) and highlighting its key features. We limit the number of features to the five basic security and privacy features (as denoted by the symbols in the top-right corner of the product review) and up to five additional features that we deem noteworthy. For easy comparison and better readability, we use standardized terms from our feature list which is found at the end of this report.

Usage: We briefly describe the first app start, initial app setup, and how to access the app features from the main app screen.

Anti-Malware: We explain what the malware scan does, if any suggestions for user actions are shown after the initial scan, what scan options (e.g., quick, full, scheduled scan) and settings for the detection behaviour are available, and mention interesting findings if malware is detected.

Anti-Theft: If applicable, we describe how to setup the feature, configure the available commands, and how to trigger them remotely. We also note additional settings and any faulty commands or misbehaviour upon execution. A table at the end of the product review shows a summary of the available anti-theft commands.

Web / Wi-Fi Protection: If applicable, we describe different protection capabilities against web threats and/or vulnerabilities on Wi-Fi networks. These include, for example, anti-phishing, VPN, and Wi-Fi scanner.

App Lock / Audit: If applicable, we describe the locking feature with its settings, which allows protecting selected apps from unauthorized access, and/or the feature to review key aspects of installed apps such as permissions, data usage, and storage space.

Parental Control: If applicable, we consider capabilities for regulating and monitoring children's device activities and safeguarding them from inappropriate content. These include, for example, app locking, web filtering, and daily usage limits.

Privacy Protection: If applicable, we list several other features which can help further improving the user's privacy, e.g., call filter, data leak checker, social network privacy scanner, protection against scam or malicious links in notifications and text messages.

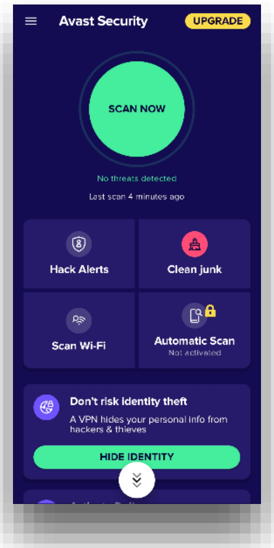
Additional Features: We list additional app features which do not belong to one of the previous categories and we think are worth mentioning. These might include system optimizing tools to stop background apps or remove junk files and a task manager to uninstall/deactivate installed apps.

Conclusion: We give a short conclusion of the product, our experience with it, and leave a statement if any reviewed function did not work properly and was not fixed before this publication.

Avast
Mobile Security Free
23.3.2

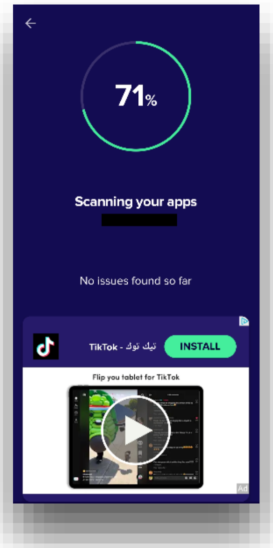
Introduction

Avast Mobile Security Free is an ad-supported product which includes a variety of security-and privacy-oriented features such as anti-malware, safe browsing, app audit, Wi-Fi security, data leak checker, and photo vault. Other app components, such as Clean Junk 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.



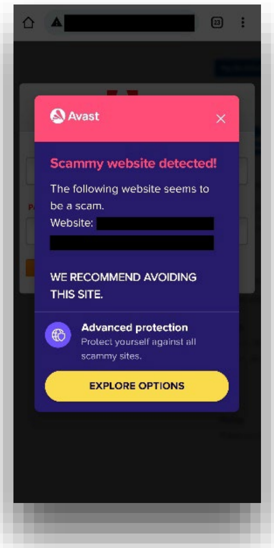
No threats detected
Last scan 4 minutes ago

Don't risk identity theft
A VPN hides your personal info from hackers & thieves



Scanning your apps
[redacted]

No issues found so far



[redacted]

Scammy website detected!

The following website seems to be a scam.
Website: [redacted]

WE RECOMMEND AVOIDING THIS SITE.

Advanced protection
Protect yourself against all scammy sites.

Usage

Upon starting the app, the user must accept Avast's Agreement and Privacy Policy. After viewing a brief overview of basic 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 of apps or all files, which requires the "All files access" permission. All the features can be accessed from the menu in the top left-hand corner.

Anti-Malware

After the first device scan, the app suggests turning on the web protection, setting up a screen lock, and disabling battery optimization. The user can choose between a file scan and, deep scan, or select individual files/folders to scan the File Shield. The external storage (e.g., SD card) is not included when scanning the device storage. The app provides further scan settings, such as the detection of PUP or apps with low reputations, which are enabled by default, and the option to scan apps during installation and upon launch. It is not possible to run a subsequent scan before resolving malware detections or other issues.

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 Network Inspector scans the currently connected Wi-Fi network for security threats which requires access to the device location. Automatic scanning of new networks is also possible.

App Audit

App Insights monitors installed apps regarding privacy and app permissions and provides the user with detailed app info and usage statistics (e.g., daily/weekly/monthly data usage, screen time). 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 securely store up to ten photos, which can only be accessed after entering the user-defined Avast PIN. Hack Alerts allows the user to check whether their email or any related accounts have been involved in a data breach.

The Wi-Fi Speed Test checks the Wi-Fi connection speed and Clean Junk helps to free up storage space by removing temporary or cached files. My Statistics shows a summary of security-related actions taken by Avast on the device, e.g., number of threats prevented.

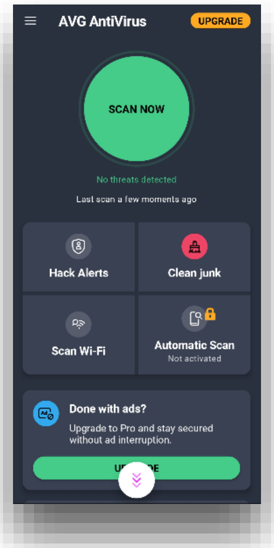
Conclusion

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. The app provides a step-by-step guide to setup each feature.

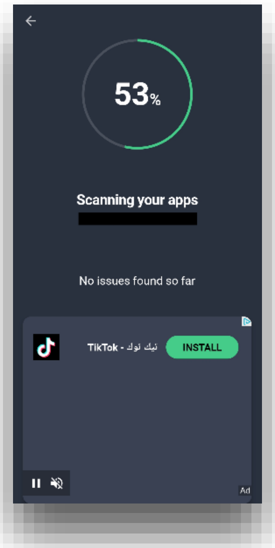
AVG
AntiVirus Free for Android
23.3.2

Introduction

AVG AntiVirus Free for Android is an ad-supported product which includes a variety of security-and privacy-oriented features such as anti-malware, safe browsing, app audit, Wi-Fi security, data leak checker, and photo vault. Other app components, such as Clean Junk and Wi-Fi Speed, help the user monitor different aspects of the 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.

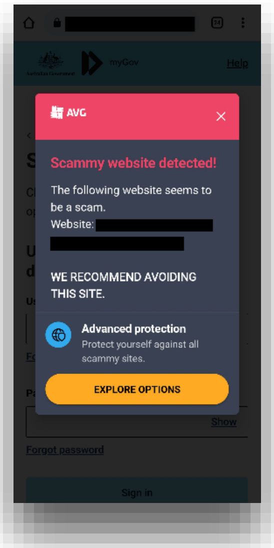


Done with ads?
Upgrade to Pro and stay secured without ad interruption.



Scanning your apps
[redacted]

No issues found so far


[redacted]

Scammy website detected!

The following website seems to be a scam.
Website: [redacted]

WE RECOMMEND AVOIDING THIS SITE.

Advanced protection
Protect yourself against all scammy sites.

Usage

Upon starting the app, the user must accept AVG's Agreement and Privacy Policy. After viewing a brief overview of basic 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 of apps or all files, which requires the "All files access" permission. All the features can be accessed from the menu in the top left-hand corner.

Anti-Malware

After the first device scan, the app suggests turning on the web protection, setting up a screen lock, and disabling battery optimization. The user can choose between a file scan and, deep scan, or select individual files/folders to scan the File Shield.

The external storage (e.g., SD card) is not included when scanning the device storage. The app provides further scan settings, such as the detection of PUP or apps with low reputations, which are enabled by default, and the option to scan apps during installation and upon launch. It is not possible to run a subsequent scan before resolving malware detections or other issues.

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 Network Inspector scans the currently connected Wi-Fi network for security threats which requires access to the device location. Automatic scanning of new networks is also possible.

App Audit

App Insights monitors installed apps regarding privacy and app permissions and provides the user with detailed app info and usage statistics (e.g., daily/weekly/monthly data usage, screen time). 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 securely store up to ten photos, which can only be accessed after entering the user-defined AVG PIN. Hack Alerts allows the user to check whether their email or any related accounts have been involved in a data breach.

The Wi-Fi Speed Test checks the Wi-Fi connection speed and Clean Junk helps to free up storage space by removing temporary or cached files. My Statistics shows a summary of security-related actions taken by AVG on the device, e.g., number of threats prevented.

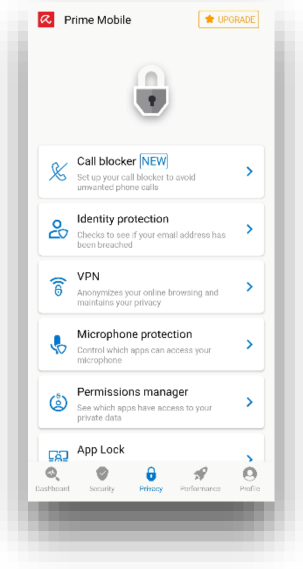
Conclusion

AVG AntiVirus Free for Android 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. The app provides a step-by-step guide to setup each feature.

Avira
Prime for Android
7.20.0

Introduction

Avira Prime for Android is a paid-for security product. Besides malware protection, safe browsing, app lock, and app audit, it provides a data leak checker, unlimited VPN, and call blocking feature.


Prime Mobile UPGRADE

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

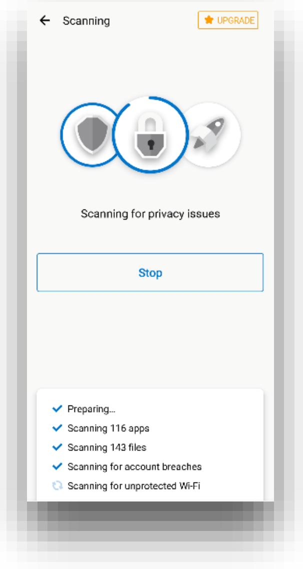
Identity protection
Checks to see if your email address has been breached

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

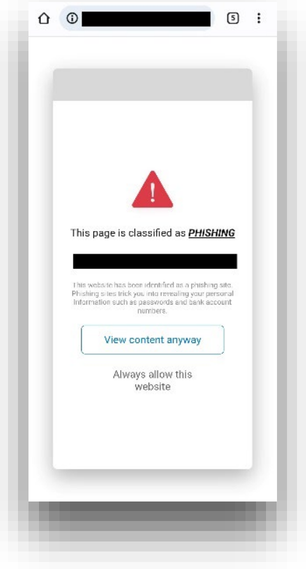
App Lock


Scanning UPGRADE

Scanning for privacy issues

Stop

- Preparing...
- Scanning 116 apps
- Scanning 143 files
- Scanning for account breaches
- Scanning for unprotected Wi-Fi


[redacted]

This page is classified as ***PHISHING***

[redacted]

This website has been identified as a phishing site. Phishing sites trick you into revealing your personal information such as passwords and bank account numbers.

View content anyway

Always allow this website

Usage

After installation, the user must agree to the EULA and Terms and Conditions, and the app asks for the consent to collect and process data for app and marketing improvements. 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. All the features are grouped by the navigation bar at the bottom. Upon performing certain actions (e.g., smart scan) or changing screens, the app title suddenly changed to "Avira Security" which is confusing to users as it refers to the free version of the app.

Anti-Malware

Before the first scan, the user must grant the app the "All files access" permission to scan for malware 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 as no scan was started in these scenarios. As part of the scan results, the user is prompted to check their email address for data breaches.

In our testing, no clear detection alerts were shown. Only the Avira app icon silently appeared in the Android notifications area at the top which will get unnoticed by the user.

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 app includes an unlimited VPN.

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 lists all installed apps by the permissions they request. Additionally, it 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.

Conclusion

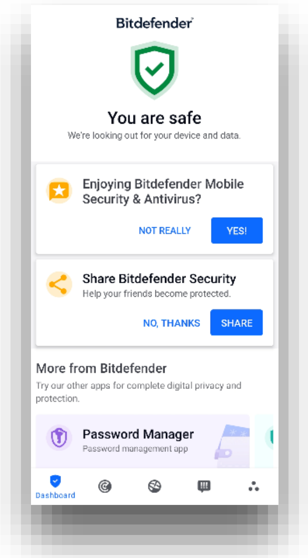
Avira Prime for Android offers a large set of tools to enhance device security and protect the user against privacy leaks. Detection alerts are not clearly displayed and therefore, users might not get informed about a potential infection.

Bitdefender

Mobile Security
3.3.203

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, safe browsing, app lock, data leak checker, data-limited VPN, Wi-Fi security, and scam protection (including SMS, instant messages) 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?

Share Bitdefender Security

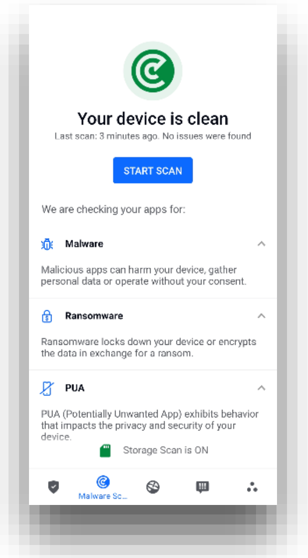
Help your friends become protected.

More from Bitdefender

Try our other apps for complete digital privacy and protection.

Password Manager

Password management app



Your device is clean

Last scan: 3 minutes ago. No issues were found

We are checking your apps for:

Malware

Malicious apps can harm your device, gather personal data or operate without your consent.

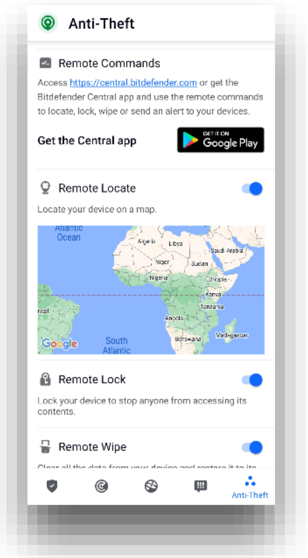
Ransomware

Ransomware locks down your device or encrypts the data in exchange for a ransom.

PUA

PUA (Potentially Unwanted App) exhibits behavior that impacts the privacy and security of your device.

Storage Scan is ON



Anti-Theft

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 to stop anyone from accessing its contents.

Remote Wipe

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 starts the first device scan. The user can navigate through all the features using the menu bar at the bottom of the screen.

Anti-Malware

When granting the "All files access" permission, real-time protection with in-the-cloud detection of malicious apps and files on the internal and external storage is enabled. App Anomaly Detection and Download Scan can be activated as additional scan settings.

Besides the scan result, a list of several malware types with a brief description is displayed. Malware scan is only available with an active Internet connection.

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 to protect the app settings. 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*. A lock screen needs to be configured during the setup of the anti-theft feature in order to use the Lock command.

After granting access to the device camera, the Snap Photo feature silently takes a photo with the front camera, stores it on the device, and uploads it to the remote command interface when the wrong PIN has been entered three times in a row.

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.

Web & Wi-Fi Protection

The Web Protection feature blocks malicious URLs and phishing websites in various browser apps. Bitdefender also includes 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 or using biometrics (e.g., fingerprint, face recognition). In the settings, the user can decide how often protected apps should require the code and if protected apps remain unlocked while connected to a Wi-Fi network marked as trusted.

The Random Keyboard feature randomizes the number position on the keyboard each time the lock screen is displayed. 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. If Chat Protection is turned on, this accounts for chat messages received via certain social media apps as well.

Conclusion

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

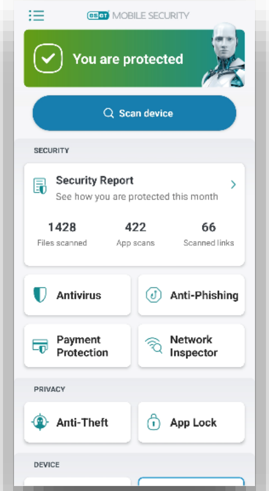
Anti-Theft Details		
Commands App & Web		
Locate Device	✓	Displays the location on *Google Maps*.
Play Sound	✓	Sounds an alarm on the device and/or shows a custom message.
Lock Device	✓	Locks the device only if a pre-defined Android lock screen is configured.
Erase Device	✓	Triggers a factory reset and wipes the external storage.
Additional Features		
Snap Photo	✓	Takes a picture with the device's front camera after 3 failed unlock attempts.

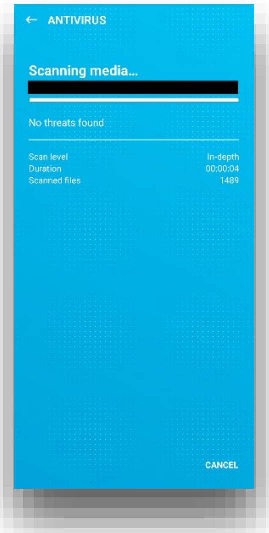
ESET

Mobile Security Premium
8.1.17

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, safe browsing (including messages and notification protection), and Wi-Fi security, it offers privacy-related features such as app audit, app lock, call filter, and payment protection.



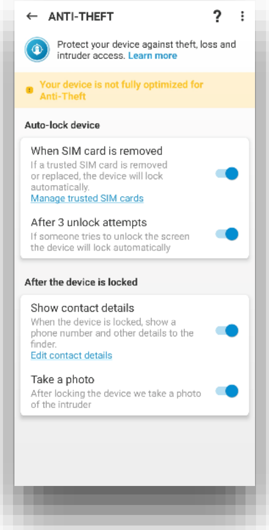


Scanning media...

[redacted]

No threats found

Scan level	In-depth
Duration	00:00:04
Scanned files	1489



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

Your device is not 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 for diagnostics and marketing purposes. 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 "All files access" permission, the user can start the first device scan. All the features can be accessed from the main screen or the menu.

Anti-Malware

Users can choose between two scan levels: Smart (installed apps, DEX/SO files, and archives) 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 and scheduled 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. The detection of potentially unwanted/unsafe applications is disabled by default. 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 configure a PIN to protect the app 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 activities (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 photos taken by the front and back camera, the 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. It is possible to wipe all data from the device and 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 apps against phishing attacks. If the respective options are enabled, it also detects and warns about dangerous links received in social media apps, SMS messages, and app notifications. The Network Inspector scans for vulnerable devices on the currently connected Wi-Fi network and gives device information 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, intruder alert) can be configured in the settings. With Security Audit, the user can review important device settings and permissions of installed apps (including system apps).

Privacy Protection

With the Call Filter feature, the ESET app can be set as the default "caller ID & spam" app in order to block or allow calls from specific phone numbers or contacts based on custom rules. The Safe Launcher feature (Payment Protection) is installed along with the ESET app and prevents malicious apps from reading or replacing on-screen information of protected apps.

Conclusion

ESET Mobile Security Premium offers the full range of protection and security features against vulnerabilities and theft. It stands out for its particularly careful and brief descriptions of each setup step and advanced settings. All anti-theft features worked flawlessly.

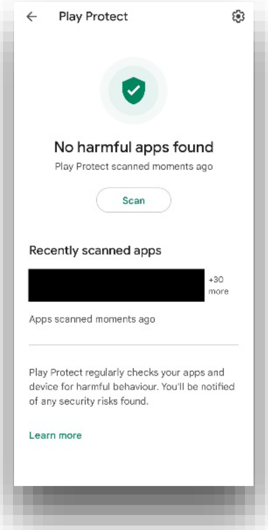
Anti-Theft Details		
	Commands Web	
Device is missing	✓	Marks the device as lost and regularly triggers subsequent actions.
Track	✓	Automatically tracks the location and displays it on *Google Maps* when the device is marked as lost.
Play siren	✓	Sounds an alarm on the device when marked as lost.
Lock	✓	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.

Google

Play Protect & OS Features
35.7.20

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 provide better user experience to mobile end-users. Play Protect 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, safe browsing, and app auditing.



No harmful apps found

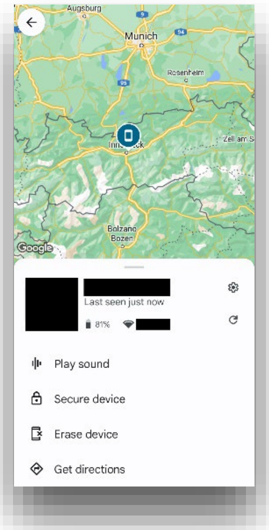
Play Protect scanned moments ago

Recently scanned apps

[redacted] +30 more

Apps scanned moments ago

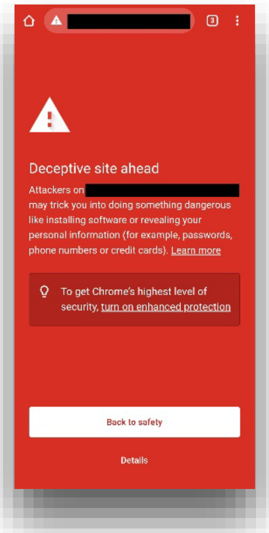
Play Protect regularly checks your apps and device for harmful behaviour. You'll be notified of any security risks found.



[redacted] [redacted]

Last seen just now

81% [redacted]


[redacted]

Deceptive site ahead

Attackers on [redacted] 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

Usage

Play Protect is preinstalled on supported Android devices and can be found either via the Play Store app or Android system settings.

Anti-Malware

Play Protect periodically scans the internal storage and notifies the user of malicious or potentially harmful apps downloaded from Google Play Store and other app sources. These include apps that hide or misrepresent important information and/or 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 permissions of apps, that have not been used for a few months, can be reviewed. Malware protection is only available with an active Internet connection.

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 the standalone app on a second device. Logging into a Google account is mandatory, and the location must be turned on for the target device. The command interfaces show 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 set locking mechanism or by creating 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 internal and external device storage.

Web Protection

The Google Chrome browser app for Android includes a safe browsing feature with "Standard protection" enabled by default. Users are alerted about dangerous websites and downloads. When switching to "Enhanced protection", URLs are submitted to the cloud for deeper analysis and users are warned if their passwords are exposed in a data breach. Options for "Do not Track" and "Always use secure connections" are disabled by default.

App Audit

In the Android system settings, all installed apps are listed, along with detailed information about their notifications and default-app settings, permissions, and device usage (e.g., mobile data, battery, storage). Users can also disable/uninstall an app, force an app stop, and adjust the requested permissions. 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, contacts) and permissions with special access (e.g., device admin rights, all files access, appear on top, install unknown apps).

Conclusion

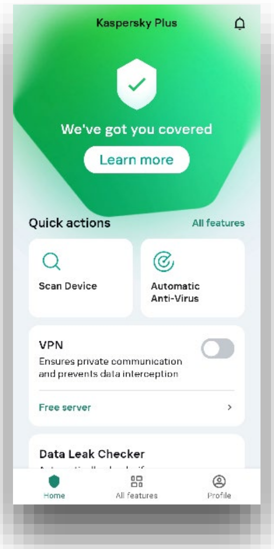
Google Play Protect is preinstalled on certified Android devices, while older devices might receive updates for Play Services and GMS. All the security-related features, such as malware protection, anti-theft, and web protection, can be used for free with a Google account. Depending on the device model, 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. A message and/or phone number 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.

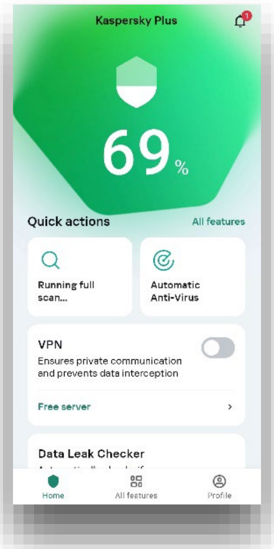
Kaspersky
Plus for Android
11.100.4

Introduction

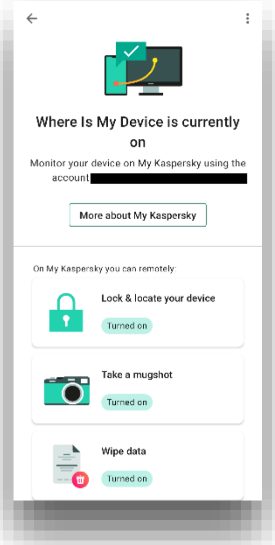
Kaspersky Plus for Android is a well-rounded, paid-for mobile security solution for up to ten devices. It offers a comprehensive set of tools to protect against malware, phishing, theft, and privacy violations. The app functionality is extended by additional features such as app lock, app audit, Wi-Fi security, unlimited VPN, data leak checker, notification protection, and a system settings checker.



VPN
Ensures private communication and prevents data interception



VPN
Ensures private communication and prevents data interception


Where Is My Device is currently on

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

On My Kaspersky you can remotely:

Usage

Upon first opening the app, the user must agree to Kaspersky's EULA, Privacy Policy, and optionally, to the vendor's statements about improving protection and data processing for marketing purposes. After granting the "All files access" permission, the user can either buy a subscription, activate an existing subscription, or start a free trial week. On the app's main screen, a database update as well as a quick scan can be started. The app prompts the user to enable and configure various security-related components, such as anti-theft and safe browsing, run a full device scan, and turn off password visibility in the device settings. The user can access all the features from the menu bar at the bottom of the screen.

Anti-Malware

When starting a scan, the user is asked whether to perform a quick scan (app-only), 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. The default settings include the detection of adware and auto-dialers, and scanning of installed apps and APK files. The user can switch to the extended real-time protection, letting them monitor all file and installed app activities, and change what action should be taken on detection.

Anti-Theft

Anti-theft commands are listed in the table below. The setup requires the user to grant the app the necessary permissions as well as device admin rights, and to configure a secret code/pattern/fingerprint. The SIM card and uninstallation protection can be enabled as well. 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 the device location and images taken 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 web interface also contains a device-specific recovery code used to unlock a device that has been locked remotely.

Web & Wi-Fi Protection

The Safe Browsing component protects the user from visiting phishing websites in supported browser apps. If enabled, any in-app link will be opened in Chrome. Before using the unlimited VPN service, the user must accept Kaspersky's VPN statement. After that, it auto-selects the server closest to the device's current location but you can also manually select from multiple other locations. The Smart Home Monitor notifies the user when a new device joins the Wi-Fi network.

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. In our test, we were able to bypass the lock screen and access the protected app. After reporting the issue to Kaspersky, a fix was promptly released.

The My Apps component shows apps grouped by permissions, and provides details about apps, including their permissions, data usage and how much storage space they take. Furthermore, installed apps can be removed from within this feature.

Privacy Protection

Safe Messaging checks links received in text and instant messages and notifies the user about potential risks. Call Filter automatically declines incoming calls from blacklisted contacts. The Data Leak Checker checks specified email addresses for data breaches. The Weak Settings Scan monitors the system settings for any vulnerabilities.

Conclusion

Kaspersky Plus for Android comprises a great set of security and privacy features, which are thoroughly explained during setup. Features can be extensively customised. All the anti-theft commands worked flawlessly in our test.

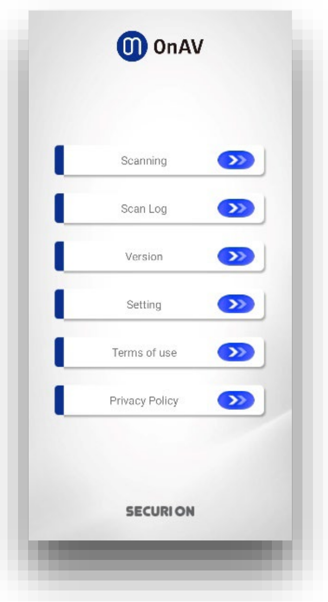
Anti-Theft Details		
Commands Web		
Lock & Locate	✓	Locks the device, displays the location on *Google Maps*, and sends the location in an email.
Mugshot	✓	Locks the device and takes several pictures using the front camera.
Alarm	✓	Locks the device and rings an alarm.
Data Wipe	✓	Triggers a factory reset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

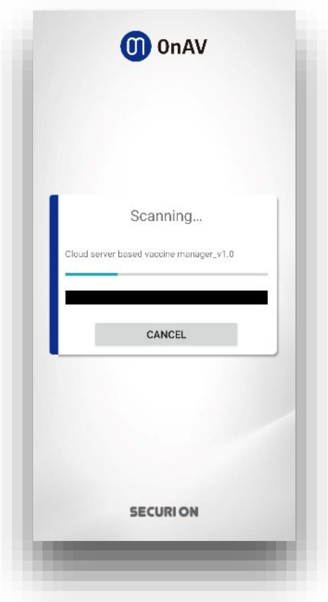
Securion

OnAV
1.0.36

Introduction

Securion OnAV is a slim and free-to-use security product that only provides malware protection. 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.

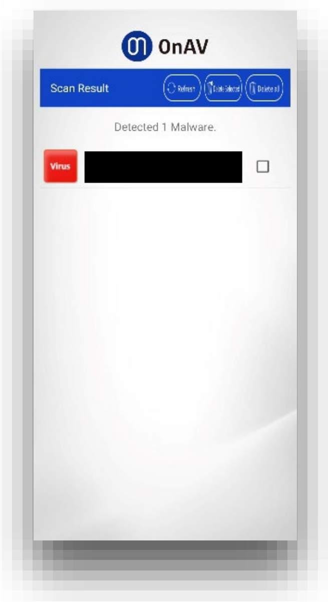




Scanning...

Cloud server based vaccine manager_v1.0

[redacted]



Detected 1 Malware.

[redacted] □

Usage

First, the user must accept the EULA, Terms and Conditions, and the Privacy Policy. In order for its real-time protection to work properly, the app asks for permission to appear on top of other apps and to access all files on the device. 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 version of the detection engine can be viewed from the main menu and the real-time protection can be turned on and off in the app settings.

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.

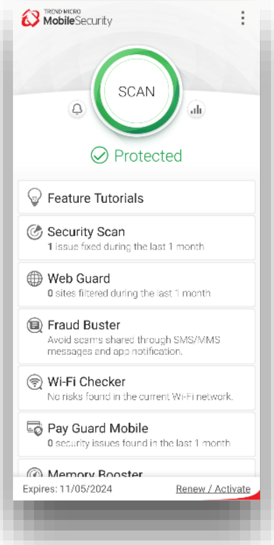
Trend Micro

Mobile Security

15.5.0

Introduction

Trend Micro Mobile Security is a comprehensive, paid-for security product. Besides security features such as a malware scanner, anti-theft, web/Wi-Fi protection, and notification protection it provides parental controls with app lock and age-based web filters, social-network privacy, payment protection, and an additional system tuning tool.



TREND MICRO MobileSecurity

SCAN

Protected

Feature Tutorials

Security Scan
1 issue fixed during the last 1 month

Web Guard
0 sites filtered during the last 1 month

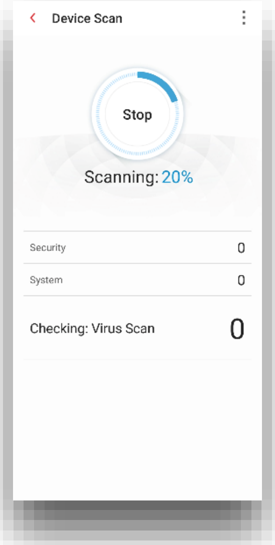
Fraud Buster
Avoid scams shared through SMS/MMS messages and app notification.

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

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

Memory Booster

Expires: 11/05/2024 Renew / Activate

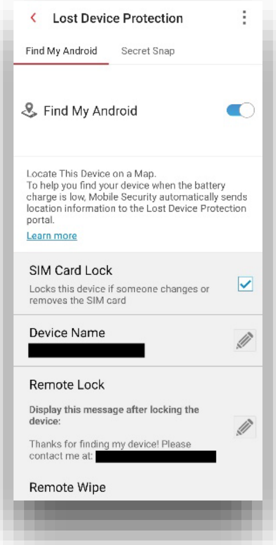


Device Scan

Stop

Scanning: 20%

Security	0
System	0
Checking: Virus Scan	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 or start a two-week trial. After a quick introduction of some security aspects, the user can grant the app all the necessary permissions or skip this step and grant them for each feature individually later. After that, an initial scan is started in the background. In addition to showing the scan results, the app recommends setting up various other features. All the app features are directly accessible from the main screen.

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, and toggle the real-time scan, pre-installation scan, and scan of the memory card. For the latter, you can additionally choose between scanning apps only or all files. Malware signature updates can be triggered manually and run on schedule (daily, weekly, monthly).

Anti-Theft

Anti-theft commands are listed in the table below. The Lost Device Protection feature requires an unlock PIN/pattern to be set in advance and asks for device admin rights. It allows the user to issue remote commands such as Locate, Lock, or Wipe via the web interface *mobilesecurity.trendmicro.com*. The app shows a link to the help page which explains how to access the Lost Device Protection portal. An option to lock the phone whenever the SIM card is changed or removed is also included. The Uninstall Protection prevents the Trend Micro app from being removed without a password.

The Secret Snap feature can take a picture with the front camera after 3, 5 or 7 failed unlock attempts which will be saved in-app. However, no email was sent to the pre-defined email address. Trend Micro told us that they had a temporary issue in their backend which has now been fixed.

Web & Wi-Fi Protection

Web Guard blocks links to malicious websites for directly supported apps. For apps that are not directly supported, the additional VPN-based protection needs to be turned on. 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 any security risks on the current Wi-Fi network.

Parental Controls

The parental controls feature is split into App Lock and Website Filter. With the first, selected apps can be protected with a PIN/pattern. The Website Filter can be set to three pre-defined levels (Child, Pre-teen, 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 of the Web Guard.

Privacy Protection

Fraud Buster scans incoming SMS/MMS messages and app notifications 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 connected Facebook or Twitter account. The Pay Guard Mobile feature monitors financial transactions made with selected apps.

Additional Features

The Memory Booster can free up memory space by stopping background apps. The App Manager allows the user to view all installed apps, uninstall or disable apps at once, and remove unneeded setup files. With Security Report, activities can be viewed in charts.

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 *OpenStreetMap*.
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.
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 2023)									
Product Name	*Android OS*	Avast Mobile Security Free	AVG AntiVirus Free	Avira Prime for Android	Bitdefender Mobile Security for Android	ESET Mobile Security Premium	Kaspersky Plus for Android	Securion OnAV	Trend Micro Mobile Security for Android
Version Number	*13*	23.3	23.3	7.20	3.3	8.1	11.100	1.0	15.5
Supported Android versions	*built-in*	6.0 and higher	6.0 and higher	6.0 and higher	5.0 and higher	6.0 and higher	6.0 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, Arabic, Bulgarian, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Italian, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thai, Turkish, Vietnamese	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	●			●	●	●	●	●	
Customizable automatic (scheduled) scan		●	●	●		●	●		●
Can detect malware sitting on external SD card				●	●	●	●		●
Manual local database update possible (beside automatic updates)		●	●			●	●		●
Scan requires online cloud connection	●				●				
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●		●
User account needed to use product					●	●			●
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					●	●	●		●
App settings protected with password					●	●	●		●
Uninstallation Protection (password required for uninstallation)						●	●		●
Lock on SIM Change						●	●		●
Additional Features (selected by AV-Comparatives)									
Hack Alerts / Data Leak Checker	●	●	●	●	●		●		
System Settings Checker	●	●	●			●	●		●
Wi-Fi Security		●	●		●	●	●		●
Privacy Advisor (audit app permissions)	●	●	●	●		●	●		
App Lock				●	●	●	●		●
Notification/Scam/Link Protection	●				●	●			●
System Optimizer	●	●	●	●					●
Call Blocker/Filter	●			●		●	●		
VPN				●	●		●		●
Task Manager (manage installed apps)	●						●		●
Photo Vault	●	●	●						
Network Monitor (track data usage)	●	●	●						
Payment Protection						●			●
Social Network Privacy Scan							●		●
Parental Control (web content filtering)									●
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, Chinese, Czech, Dutch, French, German, Hungarian, Italian, Japanese, Portuguese, Romanian, Russian, Spanish, Turkish, Vietnamese		English
In-App List Price (without discounts; prices may vary)									
Price 1 Device / 1 Year (USD/EUR)	FREE	FREE	FREE	USD 23 / 25 EUR	USD 15 / 10 EUR	USD 13 / 10 EUR	USD 58 / 47 EUR	FREE	USD 30 / 20 EUR

Copyright and Disclaimer

This publication is Copyright © 2023 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. 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 2023)