Independent Tests of
Anti-Virus Software


# Mobile Security Review 2020

TEST PERIOD: JUNE 2020
LANGUAGE: ENGLISH
LAST REVISION: 2ND JULY 2020

WWW.AV-COMPARATIVES.ORG

# Contents

# Introduction

In this report, we try to assist readers in evaluating both Android's built-in security measures and the additional and more sophisticated features provided by third-party security apps. In addition to the results of comprehensive malware protection and battery consumption tests, the report includes reviews that evaluate the functionality, app layout and overall usability of each security solution. A short table at the end of each product report gives an overview of any anti-theft function included in that product. Many of the reviewed and tested apps have non-security related components, such as a task manager, network monitor, system optimizer, and data backup feature. 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 January 2019, we conducted a malware protection test[1] with 250 Android security apps. One purpose of this test was to distinguish genuine and effective apps from dubious/ineffective ones, and it used highly prevalent malware from the previous year. The test described in this report was much more in-depth and demanding, as it used very recent malware samples, and also investigated additional security features and battery drain. Consequently, it allowed the tested apps to demonstrate their effectiveness against current threats, along with their all-round security capabilities and performance. Recently, we also evaluated how well some security apps protect against stalkerware on Android[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, harmful links, and phishing URLs. Recent Android versions already incorporate some basic security features. Google's built-in malware scanner *Play Protect* scans apps during installation from the Google Play store or a third-party source, and regularly checks the device for any threats. The *Safe Browsing* API protects against malware and phishing links while surfing the Internet using the Google Chrome browser. Anti-theft functions (lock, locate, alarm, and wipe) are provided via Google's *Find My Device* feature to find a lost or stolen phone, and to prevent access to any personal data stored on the device.

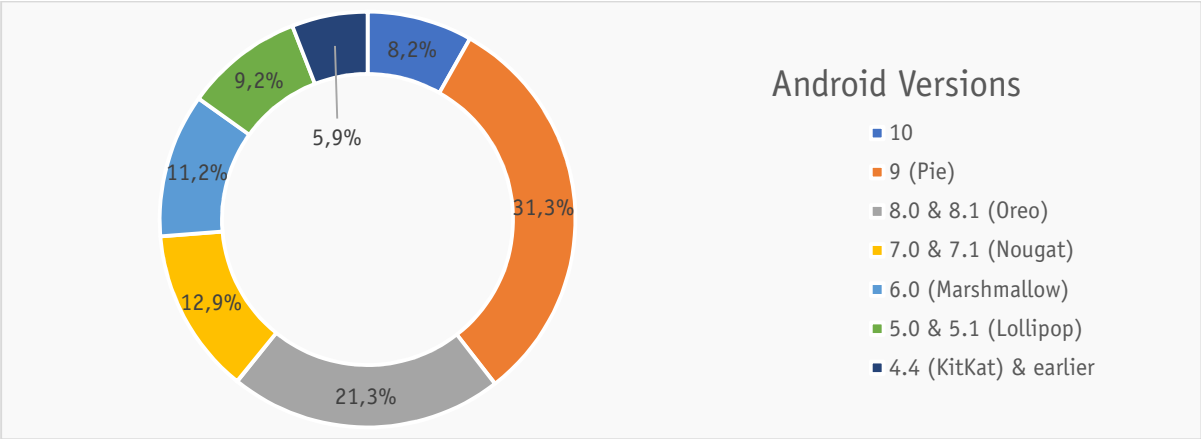
On the following pages, we discuss the new features, changes, and restrictions regarding privacy and security introduced in the latest operating system version *Android 10*, which are crucial for the future development of Android apps. Furthermore, we will argue why it is not advisable to rely only on the built-in malware protection provided by Play Protect, but instead install a third-party anti-virus app. After that, we talk about the current risks facing smartphone users, and give recommendations for achieving better protection. At the end of the introduction, we give a short summary of common security features and main sub-components of typical Android security apps. In the main section of this report, we present the participating security products, along with the results of the malware protection tests, the battery drain test, and the detailed reviews of the individual products. For a product's anti-theft component, we comment on each function briefly and use the following symbols in the table to indicate how well it worked in our tests.

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

[1] https://www.av-comparatives.org/tests/android-test-2019-250-apps/
[2] https://www.av-comparatives.org/reports/stalkerware-report-2020/

# Google Android

Since the introduction of Android 6.0 (Android Marshmallow), users have been able to control app permissions at runtime. Moreover, they can grant and revoke individual permissions for specific apps at any time, which gives them more control over the information and private data their apps have access to. This approach is very different from the one adopted by Android 5.1.1 or lower, where apps ask the user to grant all the necessary permissions prior to installation. Android Marshmallow still runs on about 11% of all Android devices worldwide, as the ring chart of the Android version distribution below shows[3].




Since Android 8.0 (Android Oreo), the global security setting *Install from unknown sources* has been a run-time permission that needs to be granted for each app once. In addition, the built-in malware protection *Play Protect* is preinstalled on devices running Android 8.0 or later, and checks apps and APK files when they are downloaded from Google Play or third-party sources, and constantly monitors all installed apps for any signs of malware. Play Protect is also available on older Android devices that support Google Play Services 11 or later. Functions for device loss (*Find My Device*) and safe browsing (for Google Chrome) are integrated as regular components as well.

In September 2019, Android 10 was officially rolled out, bringing some significant improvements for user privacy and security[4]. The concept of *scoped storage* has been introduced, which allows apps to have access to their own app-specific directory as well as files and media, such as photos, videos, and audio, created by the app on external storage, without requesting any storage-related permission. With scoped storage enabled, apps can no longer access the app-specific directories belonging to other apps. In order to access media files created by other apps, the READ_EXTERNAL_STORAGE permission is required and the app must ask for explicit user consent to access or modify other files created by other apps on the external storage. Android 10 gives the user the opportunity to limit the access to some resources (e.g. location) to times when the app is in active use. For accessing the location while running in the background, the app must ask for the additional ACCESS_BACKGROUND_LOCATION permission. Apps are also prevented from accessing certain device information. For example, non-resettable device identifiers like IMEI, IMSI, MEID, SIM, and build serial number are only accessible by apps signed with the platform key and privileged system apps that have been granted the privileged permission READ_PRIVILEGED_PHONE_STATE.

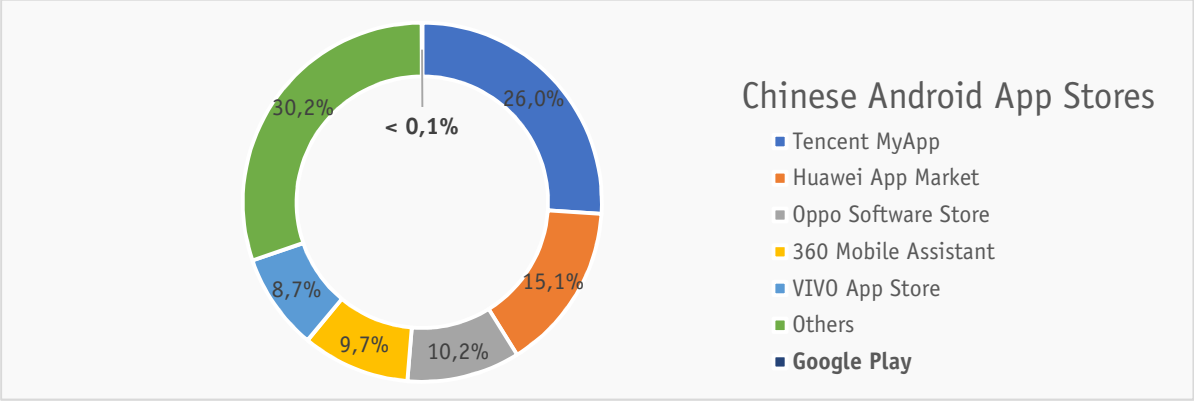
[3] Taken from Android Studio in June 2020
[4] https://developer.android.com/about/versions/10

Lack of this permission might affect some anti-virus apps that rely on this information for certain features, such as the detection of a SIM card change. The MAC address is randomised by default while connected to networks, and apps no longer have access to the file location */proc/net*, which contains information regarding the device's network state. Apps running in the background are limited in starting Activities. They must either fulfill certain conditions or display a notification, encouraging the user to take action. Currently, Android 10 is only installed on about 8% of all Android devices worldwide.

Due to Google's built-in malware and protection features, one might think that third-party anti-virus apps are no longer so important for Android devices. However, this can only be true for Android devices that have installed Google Play and Services along with Play Protect. Other devices based on modified Android OS versions (e.g., FireOS, LineageOS) do not run Google apps by default; hence, there is no built-in malware protection. In regions such as the United States and Europe, only two official app stores dominate the mobile app market: Google Play and 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 1.1 billion active mobile devices in China, and 70% of them run Android as the operating system[5]. The most-used Android app stores are shown in the ring chart below. With a market share of about 26%, Tencent MyApp is by far the most widely used app store, whereas Google Play lags far behind, and is used by almost no one (<0.1%). This is because Google Play and most of Google's services are inaccessible in mainland China.

In May 2019, an USA executive order[6] was signed, prohibiting USA companies (e.g. Google) from doing business with blacklisted foreign firms producing telecommunications components. This also affected Chinese telecommunication 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 devices[7] from certain Chinese developers. Google has assured users that older devices sold before May 16th, 2019 will still receive the update for Android 10.




[5] https://www.appinchina.co/
[6] https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/
[7] https://support.google.com/android/thread/29434011

This year's malware-protection test results show that Google Play Protect continues to improve its effectiveness, as it performed better than last year. Unfortunately, this will not help users in mainland China, due to the service being inaccessible there.

For this review, we decided to use Android 10, even though it is currently only available on a limited number of devices. However, device manufacturers will update older devices gradually. On the one hand, testing with Android 10 enables the apps to make full use of the new and enhanced OS functionalities. On the other hand, significant changes and restrictions were introduced with Android 10 regarding privacy and security which need to be addressed by mobile security vendors. Their apps require all device permissions, including device admin rights, if they are to fully monitor and control the device, and protect sensitive user data against security threats. We used the unmodified version of Android 10, as provided by Google, in order to avoid potential problems with hardware manufacturers' or mobile carriers' modifications.

# Protection against Android Malware

Cyber-attacks on mobile devices are becoming more and more sophisticated, with fraudulent applications attempting to steal users' data or money. To reduce the risk of this happening, 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[8]. 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.

A quick look at the reviews in the app store before installing an app might help. Avoid apps with predominantly bad or dubious reviews (and bear in mind that at least one fake AV program got good reviews before being exposed as useless)[9]. Rooting the smartphone increases the potential that malicious apps will take control of the device. Furthermore, it is not legally clear-cut for some manufacturers whether the warranty is still valid if the phone is rooted. Public Wi-Fi networks (e.g., coffee shop, airport) are popular targets for attackers to steal and comprise sensitive data. Therefore, we advise against entering/sharing sensitive data (user credentials, bank/credit card information, etc.) when connected to a public Wi-Fi, unless you are using a VPN connection. This will encrypt your network traffic and so prevent hackers from reading it.

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

This question cannot be answered in one sentence, as it depends on many different factors. As mentioned in previous sections, when sticking to official stores such as Google Play, the risk of the smartphone becoming infected is relatively low. In Asian countries, where many rooted devices and large number of third-party app stores can be found, the chance of installing a dangerous app is greatly increased. Today, the smartphone is often used as a replacement for the PC, and so is frequently employed for daily tasks such as online shopping, online banking, money transfers, instant messaging, emailing and so on, which are common targets for information thieves.

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.

# AVC UnDroid Analyzer

At this point, we would like to recommend *AVC UnDroid*, our malware analysis tool, which is available free to all users. It is a static analysis system for detecting suspected Android malware and adware and providing statistics about it. Users can upload APK files and see the results in various analysis mechanisms.


We invite readers to try it out: https://www.av-comparatives.org/specials/undroid/

[8] https://en.wikipedia.org/wiki/Sideloading
[9] https://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/

# 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 o*n-demand scanner* searches the whole device (internal storage and/or external SD card) for any malicious applications that are already installed, or downloaded APK files that have not yet been run. For apps that rely mainly on malware definitions to detect malware, keeping these definitions up to date is a critical factor in effective protection.

Some vendors offer more frequent updates with their paid premium versions than with the corresponding free versions. A number of the tested products offer a cloud-assisted malware scanner to ensure the app has access to the very latest definitions. Updates are either retrieved automatically by the app at specified intervals or triggered manually by the user.

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

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

Another useful feature many 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 some 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, such as access to contacts, calendar, files on internal storage, GPS position, or the camera, 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[10] were taken from the Google Play Store at the time of the test (June 2020). 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 | 6.29 | |
| | AVG | AntiVirus | 6.27 | |
| | Avira | Antivirus Security | 6.6 | |
| | Bitdefender | Mobile Security | 3.3 | |
| | G DATA | Mobile Security | 26.6 | |
| | Google | Play Protect & OS Features | 20.1 | |
| | Kaspersky | Internet Security | 11.48 | |
| | Securion | OnAV | 1.0 | |
| | Trend Micro | Mobile Security | 11.5 | |

## 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 10 only, which we used in our test.

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

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

# Overview

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


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

**Avast** Mobile Security provides a wide range of security features and device monitoring tools, with extensive options to customize each feature.

**AVG** AntiVirus offers various security and non-security features, along with configuration options for many use cases.

**Avira** Antivirus Security is a well-developed security app for Android that provides remote device control via in-app commands.

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

**G DATA** Mobile Security offers a comprehensive anti-malware app for Android, including parental control functions and a proprietary safe browser app.

X **Google** Android includes built-in malware protection, as well as a device loss/theft and safe-browsing feature for free. The protection rates are still too low, but steadily improving.

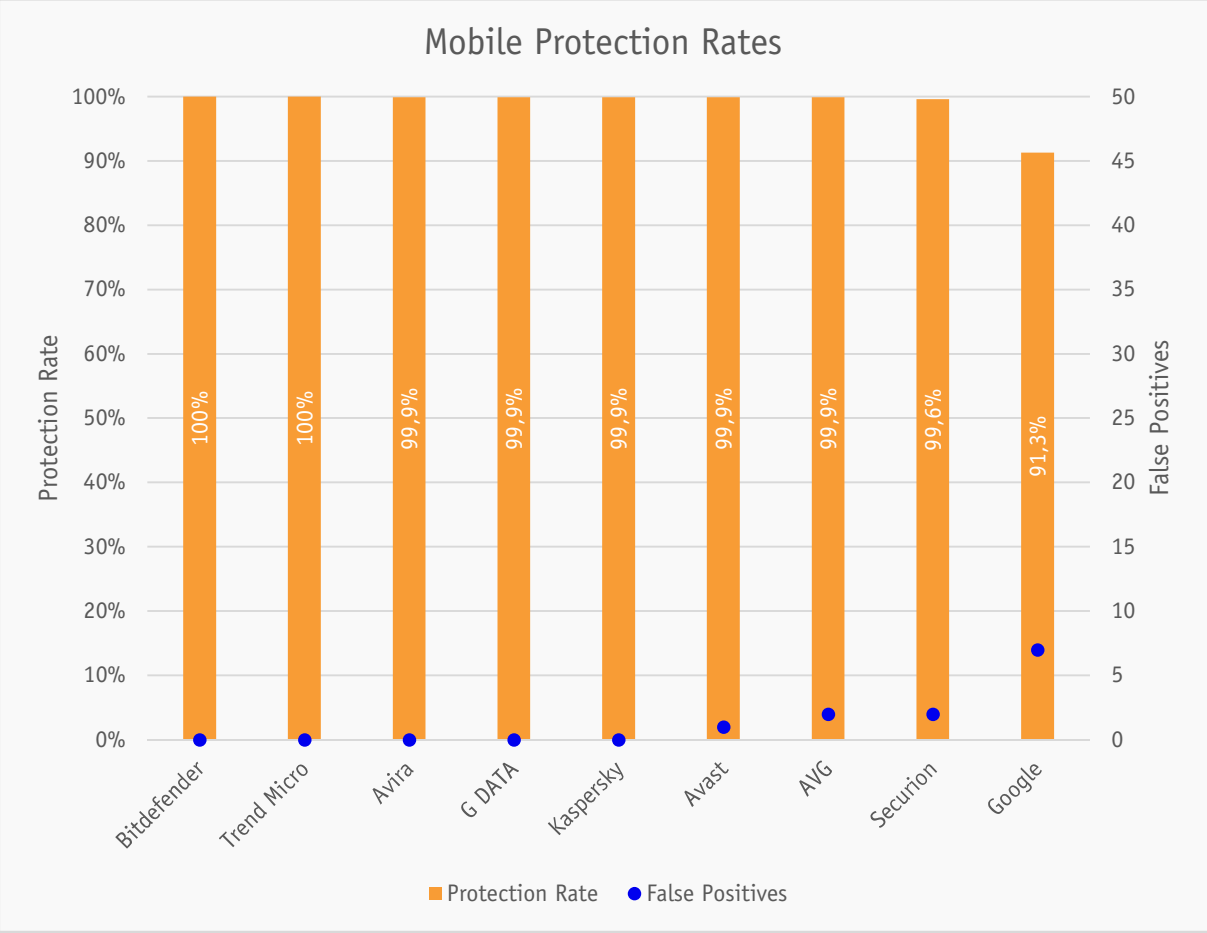
**Kaspersky** Internet Security is a mobile security app with a clean user interface, providing an extensive set of protection features.

**Securion** OnAV is a very simple security solution offering only malware protection.

**Trend Micro** Mobile Security is a well-designed app which provides malware and theft protection, as well as further device management tools.

## Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **3,220** malicious applications, to create a representative test set. Apps with the same certificates and/or the same internal code were removed, in order to have a test set of genuinely unique samples. So-called "potentially unwanted applications" (PUA) were excluded. The security products were updated and tested on the 8th June 2020. 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. 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 by downloading 500 popular apps from various popular app stores. 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, Trend Micro** | 100% | 0 |
| **Avira, G DATA, Kaspersky** | 99.9% | 0 |
| **Avast** | 99.9% | 1 |
| **AVG** | 99.9% | 2 |
| **Securion** | 99.6% | 2 |
| **Google** | 91.3% | 7 |

# Battery Drain Test Results

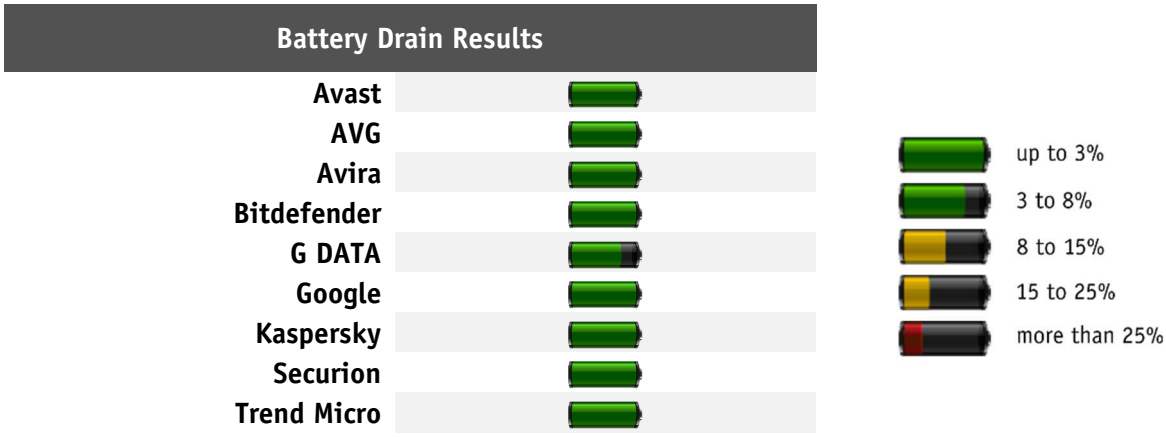
As in our previous reports, we measured the additional power consumption of an installed mobile security product. Testing the battery usage of a device might appear to be very straightforward at first glance. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones,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

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

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

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

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

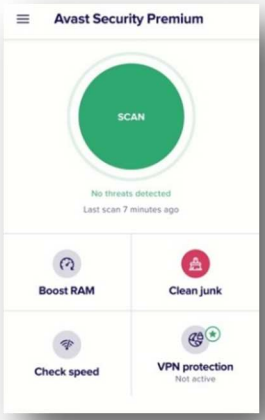


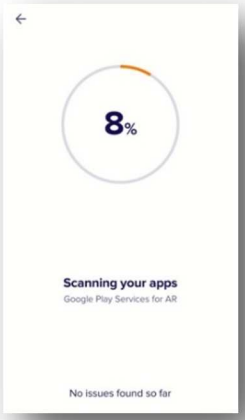

In general, we were able to give the tested security suites high marks regarding power usage. Only one product in this year's test showed a slightly increased battery drain: **G DATA**.

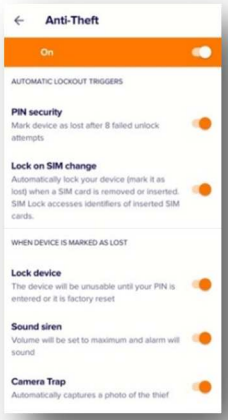
**Avast**
Mobile Security
6.29.1

## Introduction

Avast Mobile Security is a freemium product with three versions: Free, Premium and Ultimate. All include various security-related features, including malware scan, photo vault, app audit, and anti-theft functions. They also provide additional non-security related functionality, such as App Insight and Junk Cleaner, which aim to monitor applications and free up storage space by removing junk files, respectively. The Premium version offers App Locking and additional anti-theft measures. The Ultimate edition includes a VPN on top of the Premium features.




## Usage

After installation, the user has to agree to the EULA and Privacy Policy. He/she then has to choose between the free, ad-supported version, or the Premium or Ultimate versions, both of which require a monthly, six-monthly, or yearly subscription. Afterwards, the user is redirected to the main screen.

## Anti-Malware

When a malware scan is started for the first time, the app requests permissions for photos, media, and files on the device. The installed apps and user data are then checked for any threats. The app provides options such as the detection of PUA or apps with low reputations, which are enabled by default. It also warns the user if either its App Install, File, and Web shield are turned off. The internal device storage can also be scanned, although the external storage is excluded.

The user is able to scan custom folders or files via the File Scanner, and to schedule a scan for any day and time.

## Anti-Theft

Anti-theft commands are listed in the table below. During the setup of the anti-theft feature, the user has to choose an app-specific PIN, or optionally a pattern and/or fingerprint. Next, they have to grant the app various permissions, including device admin rights, in order to execute remote commands, such as Locate, Lock, and Wipe, from the web interface at *my.avast.com*. The user can access theft-protection data, such as recorded audio, and photos of a potential thief from the web interface or a pre-configured Google Drive account. The Avast PIN and protection mechanisms are accessible via the web interface, and the phone's last known location is displayed on the map when the battery charge level is critically low.

The anti-theft component also includes a feature that marks the device as lost if either the SIM card is changed, or the user fails to input the correct PIN for 8 times in a row. At the time of testing, the SIM change protection did not work properly on our test devices, as no action (e.g. lock, locate, alarm) was triggered. Avast tells us that the SIM lock feature is not supported on devices running Android 10 or later, and will be removed in an upcoming version of the app.

## Web & Wi-Fi Protection

Avast provides the features Wi-Fi Security and Wi-Fi Speed, which scan and monitor the network for security threats, and test the speed of the connection, respectively. Web Shield offers protection against phishing websites for different browser apps. In addition, the Ultimate version of the app provides a VPN service.

## App Audit & Lock

App Insights shows an overview of installed apps, as well as detailed usage statistics for individual apps, including battery impact, storage, mobile data, over different time periods (daily, weekly, monthly).

It categorizes the installed apps as high-, average-, and low-permission, according to their respective requirements. The user can also set up a data usage limit.

The App Lock feature limits access to chosen apps by locking them with the Avast PIN. The time until an app is automatically locked again can be configured.

## Additional Features

Photo Vault allows the user to place photos inside the vault, which are then encrypted and hidden from other users. Junk Cleaner analyses the storage for junk files and helps to remove them.

## Conclusion

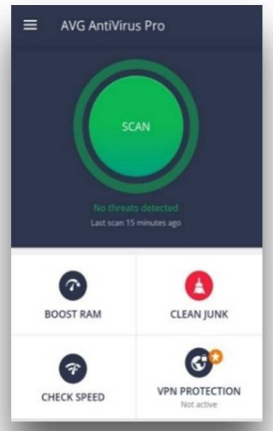
Avast Mobile Security offers many security-related functions and additional features aiming at improving privacy and device performance, which can be extensively customized. All anti-theft commands worked flawlessly.

| Anti-Theft Details | | |
|---|---|---|
| **Commands Web** | | |
| **Locate** | ✔ | Displays location on *Google Maps*. Tracking the device can be enabled. |
| **Mark as Lost** | ✔ | Triggers configured actions like tracking, lock, siren, and camera trap. |
| **Siren** | ✔ | Activates/deactivates the phone siren. |
| **Lock** | ✔ | Locks/unlocks the phone. |
| **Wipe** | ✔ | Triggers a factory reset and wipes external storage. |
| **Record Audio** | ✔ | Records audio for a pre-defined duration of 1-5 minutes. |
| **Take Picture** | ✔ | Takes a picture with the front- or back camera. Optional: The camera is triggered when the screen is turned on the next time. |
| **Message** | ✔ | Shows an on-screen message on the device. |
| **Call** | ✔ | Initiates a hidden phone call from the device to a specified phone number. |
| **Additional Features** | | |
| **Camera Trap** | ✔ | Takes a picture with the front camera. |

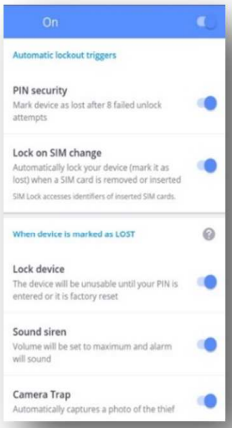
# AVG
AntiVirus
6.27.3

## Introduction

AVG AntiVirus is a freemium product with three versions: Free, Pro and Ultimate. All offer a comprehensive set of protection tools, including malware scan, anti-theft, web and Wi-Fi security, app audit, and a photo vault. Other, non-security related features aimed at improving device performance and monitoring data usage are provided as well. Pro features are App Lock, and some features within the anti-theft component. The Free version has a limit of 10 images inside Photo Vault. The Ultimate version includes a VPN on top of the Pro features.








## Usage

After installation, the user must accept the vendor's EULA and Privacy Policy and is asked whether to upgrade to the Pro version with a monthly, 6-monthly, or yearly subscription, or continue with the free, ad-supported version. The user is then redirected to the app's main screen, where the device status and important functions can be found.

## Anti-Malware

On the very first malware scan, the app asks for permission to access photos, media, and other files. It then checks the device's settings for vulnerabilities and starts a scan of the installed apps and user data. The option to scan the internal storage is also available and is disabled by default. The user can adjust the scan settings to treat PUA as malware, to be warned about apps with a poor reputation, and to schedule an automated scan at regular intervals. If one of the protection shields, aimed at guarding the device during the installation and download of apps and files as well as from malicious websites, is disabled, a notification appears on the main screen.

## Anti-Theft

Anti-theft commands are listed in the table below. In order to configure the anti-theft feature, the user has to choose an app-specific PIN, and give further permissions to the app, among which are device admin rights. For remote commands to work from the web interface *my.avg.com*, the app has to be linked to an existing AVG account and connected to the Internet. Recorded audio, and photos of the potential thief are uploaded automatically to the web interface and can be found under the "Notifications" tab, "Info" button. Optionally, the user can add his/her Google account to upload the aforementioned data to Google Drive.

The AVG PIN, the protection behaviour (lock phone, siren on lock), and the lock screen text can be customized in the web interface. The map in the web interface shows the phone's last known location when the device battery runs.

On detection of suspicious device activities (e.g. multiple failed unlock attempts or SIM card change), the device is marked as lost, which activates several protection mechanisms such as lock, locate, and alarm. At the time of testing, the SIM change protection did not trigger any action on our test devices. AVG tells us that this feature is not supported on Android 10 or later, and will remove it in an upcoming version of the app.

## Web & Wi-Fi Protection

The Web Shield provides protection against phishing websites for different browser apps. Wi-Fi Security and Wi-Fi Speed scan the currently connected Wi-Fi network for security threats, and measure connection speeds, respectively. The app offers a VPN service only as part of the Ultimate subscription plan.

## App Audit & Lock

App Insights monitors app permissions and usage over a day, week, or month. All installed apps are ranked using the risk categories "low", "average", and "high", depending on the private data and permissions they access. A custom data plan can be set up to limit mobile data consumption.

With App Lock, the user is able to lock sensitive apps against unauthorized access using the AVG PIN, pattern, or fingerprint, whereby the locking timeout for the protected apps can be configured.

## Additional Features

The Photo Vault encrypts and stores sensitive images, and controls access to them via the AVG PIN. Junk Cleaner helps to free up storage space by removing junk files.

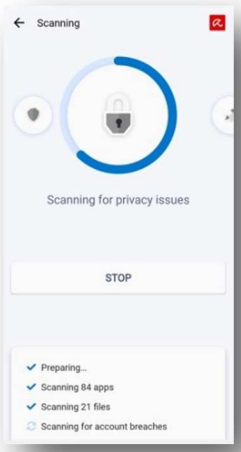
## Conclusion

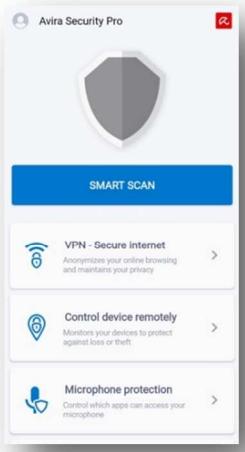
AVG AntiVirus provides a wide range of security functions and tools for optimizing and monitoring the device's performance and activity. All anti-theft commands from and to the device worked as expected.

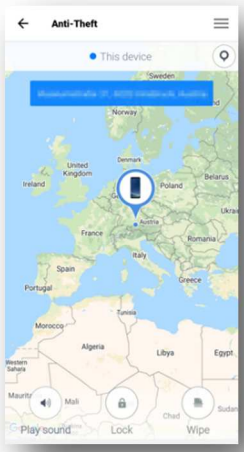
| Anti-Theft Details | | |
|---|---|---|
| **Commands Web** | | |
| **Locate** | ✔ | Displays location on *Google Maps*. Tracking the device can be enabled. |
| **Mark as Lost** | ✔ | Triggers configured actions like tracking, lock, siren, and camera trap. |
| **Siren** | ✔ | Activates/deactivates the phone siren. |
| **Lock** | ✔ | Locks/unlocks the phone. |
| **Wipe** | ✔ | Triggers a factory reset and wipes external storage. |
| **Record Audio** | ✔ | Records audio for a pre-defined duration of 1-5 minutes. |
| **Take Picture** | ✔ | Takes a picture with the front- or back camera. Optional: The camera is triggered when the screen is turned on the next time. |
| **Message** | ✔ | Sends and shows an on-screen message on the device. |
| **Call** | ✔ | Initiates a hidden phone call on the device to a given phone number. |
| **Additional Features** | | |
| **Camera Trap** | ✔ | Takes a picture with the front camera. |

## Avira
Antivirus Security
6.6.3

## Introduction
Avira Antivirus Security is a freemium product with three editions: Free, Pro and Ultimate. The Free version includes a VPN feature with limited data traffic, performance enhancement, app locking and permission monitoring, in addition to malware protection. The Microphone/Camera/Web Protection and Premium Support features are only available in the Pro version. The Ultimate edition offers unlimited data and a choice of servers for the VPN service, in addition to the Pro features.




## Usage
After installation, the user has to agree to the EULA and Terms and Conditions. After that, the user is redirected to the main screen, and prompted to start a scan to discover potential issues.

## Anti-Malware
When the user runs the first scan, the program asks for permission to scan the internal data storage, including media, photos, and other files. If the user grants these permissions, a full scan is run; otherwise only apps will be scanned. The options to scan for adware and PUA are enabled by default. After the first scan, the user is encouraged to check his/her email account for data breaches, and to optimize the device performance by freeing both memory and storage using the Optimizer.

Further scan-related settings include scanning for riskware, and starting a scan when storage is mounted or a USB cable is unplugged. The option to schedule a scan at any time is also offered.

## Anti-Theft
Anti-theft commands are listed in the table below. During setup of the anti-theft feature, the app requests access to the location, and further permissions such as device admin rights. Afterwards, the screen shows a map with the current device location, and displays the three commands *Play sound*, *Lock*, and *Wipe*, whereby the last two commands can only be executed remotely.

Unlike with previous versions of the product, the target device can now only be remotely controlled by a second device that has the Avira app installed and is linked to the same user account. The registered devices can be accessed and controlled from the menu in the top right corner of the anti-theft component.

## Web & Wi-Fi Protection

The Web Protection component blocks phishing and malicious websites while the user navigates the web. However, this feature did not work on our test devices, and we were able to visit phishing websites using Google Chrome and other popular browser apps. Avira tells that this issue will be fixed with the next version.

The Network Scanner informs the user about other devices connected to the same network. A VPN service with unlimited traffic and free choice of servers is available only for users with an Ultimate subscription. At the time of testing, the Pro and Free version displayed 1024 MB of daily traffic using the nearest VPN server. However, Avira responded to us that the daily traffic is limited to only 100 MB and they will fix this issue in a future version of the app.

## Privacy Protection

Microphone and Camera Protection list apps requiring access to the device's microphone and camera. If enabled, they restrict access to these functionalities to pre-selected apps. For Camera Protection, the user can mark an app as trusted, and subsequently access it only through the Avira Camera Protection widget. For Microphone Protection, either all apps or none, except for the pre-installed Phone Dialer app, obtain access to the device's microphone.

The Identity Safeguard checks a particular email address for data leaks and lists recently breached companies.

## App Audit & Lock

The Permissions Manager groups and lists the installed apps by the permissions they request, and allows the user to uninstall a specific app.

The App Lock component lets the user set up a pattern, PIN, or fingerprint to protect sensitive apps. The user can choose between different locking behaviours (lock always, lock by location, or lock by schedule), or an automatic lock, which locks the apps after a pre-defined time interval. There is also the possibility to show a fake crash message each time a locked app is accessed. If this is enabled, the user needs to press the OK button for a longer time in order to get to the unlock prompt.

## Conclusion

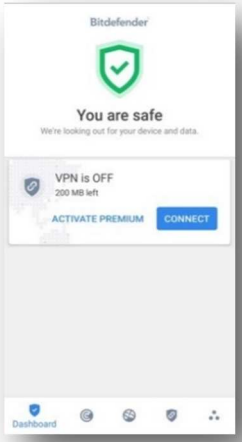
Avira Antivirus Security offers well-developed tools to enhance device security and protect a user against privacy leaks, device loss or theft. All anti-theft commands worked as expected, although the Web Protection feature did not block any phishing websites in our test.

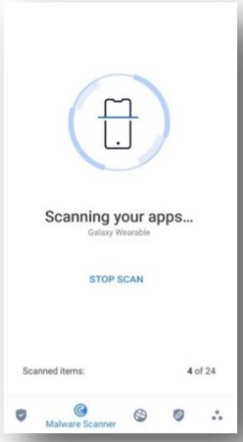
| Anti-Theft Details | | |
|---|---|---|
| **Commands App** | | |
| **Locate** | ✔ | Displays location on *Google Maps*. |
| **Lock** | ✔ | Locks the device with a 4-digit PIN (only executable remotely) |
| **Wipe** | ✔ | Triggers a factory reset and wipes external storage (only executable remotely).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

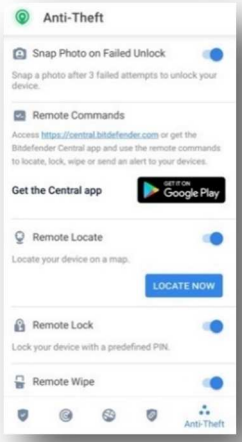
**Bitdefender**
Mobile Security
3.3.102

## Introduction

Bitdefender Mobile Security is a paid-for mobile security solution, which aims to improve the user's security and privacy. The vendor offers a 14-day trial, letting a potential buyer experience each functionality, and subsequently choose between a monthly and an annual subscription. The Autopilot feature helps the user monitor security and privacy issues. Weekly summary reports and activity logs are also generated and accessible within the app.




## Usage

First, the user has to consent to the subscription agreement and subsequently, sign into a Bitdefender account (or create a new one). The user is then asked to insert a license code, or to continue with a 14-day trial period. The app advises the user to activate Web Protection and to scan the device, before redirecting to the main screen. This gives a general overview of the security status of the device, and further suggestions for improving it.

## Anti-Malware

Upon the first scan, the app performs an app-only scan and if enabled, scans both the external and internal storage. The option to upload suspicious app information to Bitdefender is enabled by default. Additionally, a list of threats the app actively searches for during each scan is available, along with a brief description.

## Anti-Theft

Anti-theft commands are listed in the table below. In order to activate Anti-Theft, the user is prompted to select a PIN and grant permissions as well as device admin rights to the app. Besides the basic commands Locate, Lock, and Wipe, which are enabled by default, the feature includes a Snap Photo command, which silently takes a photo with the front camera after three failed unlock attempts, and uploads it to the remote command interface. Scream, which triggers an alarm on the device, is the only command that cannot be deactivated.

Remote commands can be sent either from the web interface *central.bitdefender.com* or the Bitdefender Central app. In either case, both the IP address and the location of the device can be seen on Google Maps.

Further information about the device such as the MAC address, device type, device manufacturer, and threats blocked in the last few days, is shown as well.

## Web & Wi-Fi Protection

Once enabled, the Web Protection feature identifies and blocks fraudulent and dangerous websites when using several mobile browser apps.

The basic subscription includes a VPN with up to 200 MB of daily traffic and automatic server selection. A warning informs the user each time the device connects to an open Wi-Fi, in which case a VPN connection is recommended.

## Account Privacy

The Account Privacy component allows the user to check any pre-added email address for known data leaks. During the setup process, the ownership of the email address needs to be verified with a confirmation code sent to that particular address.

## App Lock

After granting the necessary permissions, the App Lock component allows the user to select and lock sensitive apps with either a 4-8-digit PIN or the fingerprint reader. The user can designate a specific Wi-Fi network as trusted, in which case the protected apps remain unlocked while connected to it. In the settings, the app lock mode, i.e. when to lock/unlock an app, as well as the Random Keyboard option, which randomizes the number pattern on the keyboard each time a protected app is accessed, can be configured. After three failed subsequent unlock attempts, the Snap Photo function is triggered.

## Conclusion

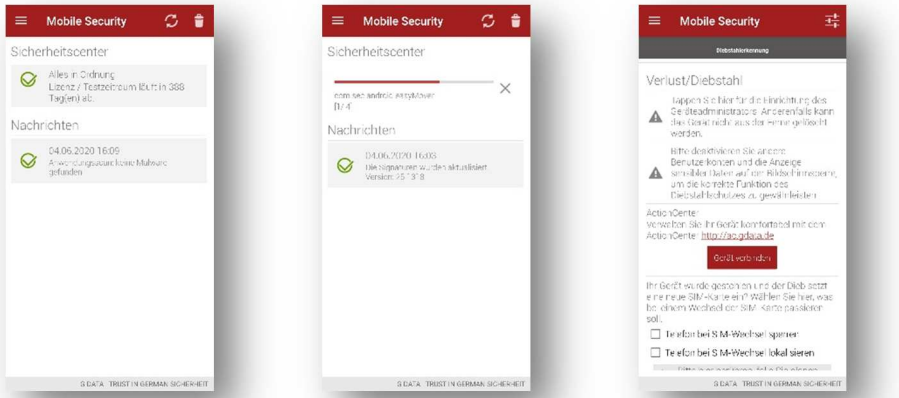
Bitdefender Mobile Security is a well-designed anti-malware application, which provides additional security by means of the anti-theft and web-protection components. Privacy-enhancing tools such as Account Privacy and App Lock are also available. All features worked flawlessly in our functionality test.

| Anti-Theft Details | | |
|---|---|---|
| **Commands App & Web** | | |
| **Locate** | ✔ | Displays location on *Google Maps*. |
| **Alert** | ✔ | Sounds an alarm on the device and/or shows a custom message. |
| **Lock** | ✔ | Locks the device with the Android lock screen. The PIN can be set in the command interface. |
| **Wipe** | ✔ | Triggers a factory reset and wipes external storage. |
| **Additional Features** | | |
| **Snap Photo** | ✔ | Takes a picture with the device's front camera on multiple failed unlock attempts and uploads it to the command interface. |

**G DATA**
Mobile Security
26.6.4

## Introduction

G DATA Mobile Security is a freemium app. The premium version has an annual subscription, and offers multiple security-related features such as malware scan, theft protection, web protection, and app restriction. There is also a parental control function, which allows the user to set up protected environments for children, where only approved apps or websites are accessible, and time limits can be defined. The free version only provides access to the malware scanner and app permissions. All the premium features can be tested for 30 days.




## Usage

A G DATA account must first be created in order to use the app. After the user has accepted the EULA and logged in, the main screen appears and a database update is started. The main screen has a clean layout, which shows the license status and the latest notifications. All other features are accessible from the menu in the upper left-hand corner.

## Anti-Malware

The app offers a quick scan of all installed apps, and a full-system scan after the required permissions have been granted. Apps are scanned upon installation, and the device is regularly checked for malware. The settings offer fine-grained control of scanning frequency and signature updates, and the user can set background scans to run only while the device is charging or has full battery.

## Anti-Theft

Anti-theft commands are listed in the table below. To use Anti-Theft on the device, the necessary permissions need to be granted, and a PIN as well as a security question must be set up. G DATA explicitly advises the user to choose a secure PIN, and to turn on the system option “Hide sensitive information content” on the lock screen. After the device has been connected to the G DATA ActionCenter (*ac.gdata.de*), web commands can be sent to the device, whereby a notification is sent to a pre-configured email address each time a command has been successfully executed. The user can remotely start device scans, and adjust in-app settings, in the web interface. For the Lock command, an arbitrary PIN can be entered in the web interface to lock the device.

There are options to locate the device when the battery is low, and to sound an alarm when a headset is disconnected.

The SIM change protection did not work in our test; the device was not locked, and no email notification was received. G DATA confirmed this issue and will release a fix in the upcoming version.

Other users can also be invited to use the web interface and granted access to a subset of anti-theft commands.

## Web & Wi-Fi Protection

The Web Protection feature blocks phishing websites when using Google Chrome or Firefox. G DATA also provides its own Secure Browser app to securely surf the Internet. However, it is very basic with minimal features. Additional checks and rules for connected Wi-Fi networks can be activated in the app settings.

## App Audit & Lock

The Permissions menu displays all apps grouped by their permissions, and allows the user to uninstall apps. Apps can be marked as protected, which then require the maintenance PIN to launch.

## Parental Controls

The app offers an extensive parental control component, where the user can set up two device modes: Children's Corner and Teenager Corner. The first one provides a child-oriented home screen with very limited functionality, and only shows allowed apps. Parents can create white- and blacklists for websites, and restrict the device usage to specific locations and times. The Teenager Corner just restricts the access to approved apps and the device usage to specific locations and time intervals.

In our test, the website filter of the Children's Corner only worked with G DATA's Secure Browser app. We were unable to set location-based restrictions, as the app accepted neither a typed-in address nor a location selected on the map.

## Conclusion

G DATA Mobile Security provides a well-developed security solution for Android, with an easy-to-use interface. Except for the SIM change protection, all anti-theft commands behaved as expected. The parental control feature includes many options for managing children's use of the device.

| Anti-Theft Details | | |
|---|---|---|
| **Commands Web** | | |
| **Locate device** | ✔ | Displays the current or last-known location on *Google Maps*, and sends an email notification with a link to *Google Maps*. |
| **Trigger signal tone** | ✔ | Rings an alarm on the device, which is switched off when device is unlocked and app is launched. |
| **Lock screen** | ✔ | Locks the device with the pre-configured PIN. |
| **Delete personal data** | ✔ | Triggers a factory reset and wipes external storage. |
| **Mute device** | ✔ | Mutes all sounds on the device. |
| **Set lock screen password** | ✔ | Changes the lock-screen password. |
| **Additional Features** | | |
| **SIM Change Protection** | ▬ | Locks the device and sends the current location to the registered email address whenever the SIM card is changed. |
| **Headset Protection** | ✔ | Locks the device and rings an alarm when the headset is disconnected. |

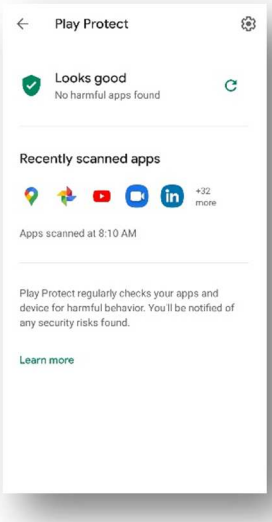
## Google

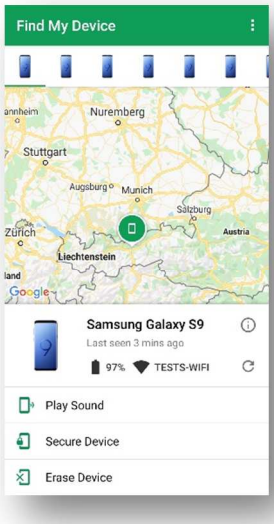
Play Protect & OS Features

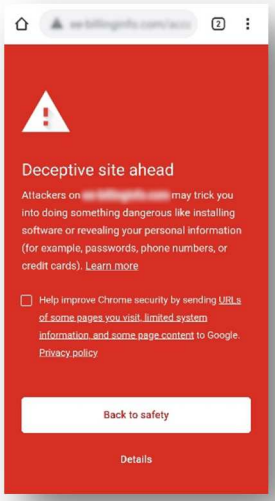
20.4.18

## Introduction

Google's built-in malware protection checks installed apps for security threats on a regular basis. It scans apps, as well as APK files before these are downloaded and from Google Play or a third-party source. Google also offers anti-theft functionality via a standalone app and a web interface. Both can be used to find devices attached to the same Google account. The Google Chrome browser provides protection against phishing websites via the Google Safe Browsing API. Some specific Android devices also support profiles with custom settings and apps. Backups of user data, media files, apps, etc. can be created and uploaded to the Google cloud.




## Usage

Play Protect is preinstalled on all new Android devices and can be found either via Play Store > Menu > Play Protect, or via Android Settings > Google > Security > Google Play Protect.

## Anti-Malware

Play Protect shows the list of recently scanned apps, as well as the scan status. Here, the user can manually start a new app scan, and adjust a few settings.

## Anti-Theft

Anti-theft commands are listed in the table below. Before using anti-theft commands within the standalone *Find My Device* app or the web interface *google.com/android/find*, the user must log in with his or her Google account. Once logged in, all devices connected to that account are displayed. Selecting a device shows the current or last-known location, the battery level, and the currently connected Wi-Fi network. There are options to play an alarm on the target device, log out of the Google account and lock the device, and completely wipe the device by removing all data including the Google account. If no lock screen is configured, a PIN has to be set in the command interface. Optionally, the user can display a message and phone number on the lock screen.

## Web Protection

Google Chrome includes a safe browsing feature, which detects and blocks phishing websites when browsing the internet.

## App Audit

Since Android version 6.0, users have had more control over the permissions granted to individual apps. Within the Android settings, the apps can be viewed grouped by their permissions, and these permissions can also be revoked from here. The access to certain apps can also be restricted by creating custom user profiles. However, different device manufacturers may implement this feature differently, or may not even include it all.

## Conclusion

Google Play Protect comes preinstalled on every new Android device. Supported devices with older versions of the Google Play Store and Services installed will be updated automatically in the background, so that users enjoy the full functionality of Play Protect. The built-in malware protection, and all the other security-related features like anti-theft, web protection, and data backup, can be used free of charge with a Google account.

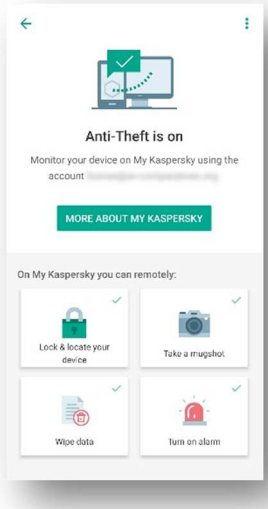
| Anti-Theft Details | | |
|---|---|---|
| **Commands App & Web** | | |
| **Locate / Track** | ✔ | Displays location on *Google Maps*. |
| **Secure Device** | ✔ | Locks the device with a given PIN or the pre-configured security mechanism. Optional: Displays a message and/or phone number to contact. |
| **Erase Device** | ✔ | Triggers a factory reset immediately, or after next device restart, and wipes external storage. |

**Kaspersky**
Internet Security
11.48.4

## Introduction

Kaspersky Internet Security is a well-designed, paid-for app that combines the most important security features, such as protection against malware, theft, and phishing, with an app lock and call filter. All the features can be tested out within a 30-day trial period. More functionality such as VPN, parental controls, or a password manager, is available through separate Kaspersky apps.






## Usage

On first usage, the app requests the necessary permissions for the setup process. After accepting the terms and conditions, the user can either purchase a license for the app, assign an existing license to the current device, or skip this step and start using the trial. The user is then redirected to the app's main screen, where an initial signature update and a quick scan are started automatically. After the first scan, the app advises the user to activate the web protection, configure the anti-theft feature, and run a full system scan.

## Anti-Malware

In the recommended mode, the real-time protection scans installed apps and packages in the Downloads folder, whereas the extended mode lets the app scan all file activities and installed apps regularly.

The user can fine tune when scheduled scans and updates take place, and customize the scan behaviour. For example, the user can decide whether to scan all files, or only apps and archives, whether to scan for adware and auto-dialers, and what action to take on detection. It is also possible to manually trigger a scan of either all installed apps, a certain folder, or the entire device.

## Anti-Theft

Anti-theft commands are listed in the table below. The anti-theft functionality needs permission to access the camera and location, and requires device admin rights. The users must also log into a My Kaspersky account and set up a secret code with 4-6 digits. This is used for unlocking the device if no other lock screen is set up, and for accessing the anti-theft settings.

Optionally, a pattern or fingerprint can be used instead of the secret code. Commands such as Lock & Locate, Alarm, Data Wipe and Mugshot can be issued from the web interface only if they have been activated in the app beforehand.

All commands except for Data Wipe lock the device, and can be sent with a custom lock screen message. In addition, the SIM Watch function and Uninstall Protection can be enabled within the app settings. Kaspersky explicitly asks for the respective permissions in order to sound the alarm while the device is in "Do not disturb" (DND) mode. The user can reset the secret code from within the web interface as well.

## Web Protection

The Internet Protection feature blocks phishing websites when using the Google Chrome and Samsung Internet browsers. In our test, we found that when we accessed phishing websites using the Samsung Internet browser on the Samsung Galaxy S9, the browser app crashed. Kaspersky have informed us that they are working on a fix for this. The Text Anti-Phishing feature scans incoming text messages for phishing links and warns the user of these.

### App Lock & Additional Features

The App Lock feature protects selected apps with the same secret code/pattern/fingerprint that is used for the anti-theft feature. The Call Filter blocks incoming calls of blacklisted contacts and manually entered numbers.

## Conclusion

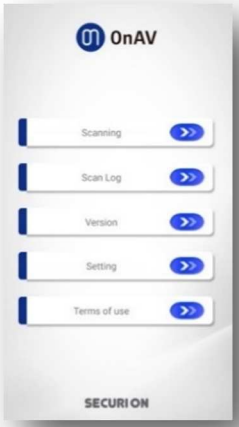
Kaspersky Internet Security offers a great variety of security features packaged in an easy-to-use and cleanly designed app. Its functionality can be expanded through additional apps. The simple explanations provided when each feature is used for the first time leave no questions unanswered. All the anti-theft commands worked flawlessly in our test, and the uninstall protection is a nice add-on to secure the device against deinstallation by an unauthorised user.

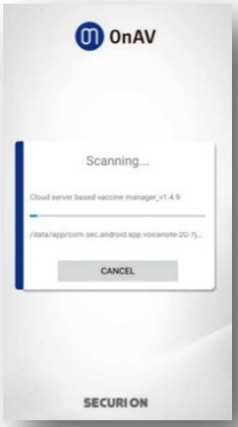
| Anti-Theft Details | | |
|---|---|---|
| **Commands Web** | | |
| **Lock & Locate** | ✔ | Locks the device, displays the location on *Google Maps*, and sends the location in an email. |
| **Mugshot** | ✔ | Locks the device, and takes several pictures using the front camera. |
| **Alarm** | ✔ | Locks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

**Securion**
OnAV
1.0.25

## Introduction

Securion OnAV is a very basic, free AV product that provides a virus scanner with real-time protection. No user account is required, although each device is assigned a unique ID in order to prevent double sign-ups. This review covers the English version of the app only, which differs from its original Korean counterpart.





## Usage

First, the user must accept the Terms of Service and the Privacy Policy. The app then asks for storage and phone permissions, to scan for files and assign the device a unique ID, respectively. All important functions, including Scanning, Scan Log, and Setting are accessible from the main screen [sic].

With Android versions from 6.0 onwards, users have been able to grant and revoke app permissions at any time. Thus, we tried to not give the requested permissions to the app in first place, which resulted in the app to crash every time the user launches it. Meanwhile, Securion fixed this issue in the latest app version.

## Anti-Malware

The Scanning option starts a full scan of the internal storage, which can be interrupted at any time.

Once the scan is completed, the results are displayed, and the user can select and delete potentially malicious files. Notice that external storage is not included in the scan.

Scan Log shows the results of previous scans, along with the number of detected and deleted malware apps. In Setting, the user can turn the real-time protection on or off.

## Conclusion

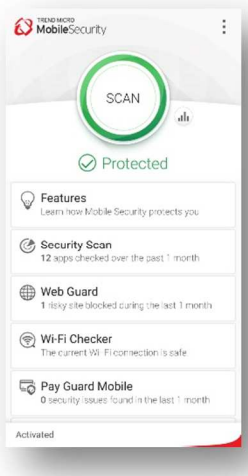
Securion OnAV is a slimline free app that provides malware protection only. The scan results list detected malware and lets you remove it, although no further details are provided.

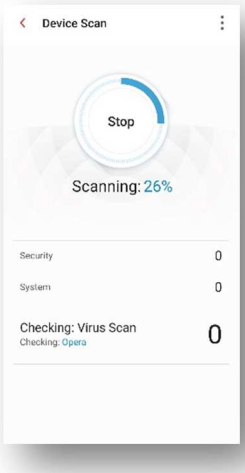
At the time of testing, the Play Store entry still mentioned a “Rooting Check” feature, and displayed a screenshot of this, even though the feature had already been removed from the app. Securion has updated the description and screenshots in the Play Store.

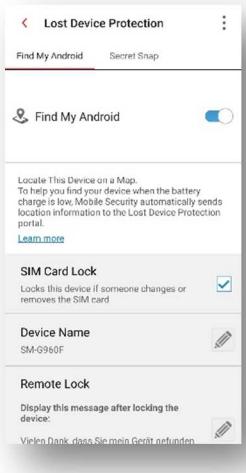
**Trend Micro**
Mobile Security
11.5.0

## Introduction

Trend Micro Mobile Security is a freemium product. The free version has malware protection, system optimization, and social media privacy tools. Starting the 14-day trial, or purchasing a monthly or yearly licence for the premium version, enables additional security features like anti-theft, web protection, Wi-Fi scanner, and parental controls.




## Usage

After installation, the user is prompted to accept the EULA and Privacy Policy. While the user is given a brief tour of the app, an initial scan runs in the background. The user can then buy/activate a license, or continue using the test version for 14 days. On the main screen, the device status and all the features are readily accessible.

## Anti-Malware

By default, an app-only scan is performed. The threshold for the threat level at which the user is notified can be changed in the scan settings. Further options allow toggling real-time scanning, pre-installation scans of apps downloaded from Google Play, and scanning of the internal and external storage. Signature updates can be scheduled as daily, weekly, or monthly, triggered manually, or completely turned off.

## Anti-Theft

Anti-theft commands are listed in the table below. The Lost Device Protection component offers the anti-theft functionality. The remote commands can be sent from the web interface at *mobilesecurity.trendmicro.com* and include Locate, Lock, Alarm, Delete, and Reset. There is also the option to share the device location directly as a Facebook post. An option to lock the device when the SIM card is changed or removed is also included. The Uninstall Protection requires the Trend Micro account password to successfully uninstall the app. The Secret Snap feature takes a photo with the front camera after a set number of failed unlock attempts (3, 5, or 7), and this is sent to a pre-configured email address.

The Reset command allows you to force all running apps to stop, or to reset the lock-screen password. Unfortunately, neither option worked properly in our test. In all cases, the web interface stated that our request could not be handled, and that we should try again later.

## Web & Wi-Fi Protection

The Web Guard checks and blocks malicious websites and links for supported browsers and apps. The level of protection can be set to low, normal, or high. The user can also define black- and whitelists of websites. For apps that are not directly supported, a VPN connection with its own web protection is provided. The Wi-Fi Checker scans the currently connected network for security risks.

## Parental Controls

This feature is divided into two parts. Firstly, it allows the locking of specific apps with the Trend Micro account password. Secondly, the website filter blocks pages inappropriate for children, pre-teens, or teens. There is an extensive set of categories which can be used for custom filtering of websites, as well as support for black- and whitelists of websites.

The VPN content-filtering function can be used by parents to control what their children see in apps that are not directly supported by the parental control feature. However, we were able to deactivate the VPN connection without opening the app (e.g. from the Android notifications area) on our Samsung Galaxy S9 devices. This would effectively circumvent the website filters.

## Additional Features

The app also includes a System Tuner, with several options for optimising memory usage, and extending battery life. There is also the Social Network Privacy feature, which checks Facebook and Twitter account settings for possible privacy issues. The App Manager allows users to uninstall or disable multiple installed apps at once. The Pay Guard Mobile feature monitors financial transactions made with installed banking and shopping apps.

## Conclusion

Trend Micro Mobile Security combines a variety of security and privacy features. These protect against threats on the device and while browsing the Internet, control the device remotely and limit access to apps and certain websites. The user interface is kept clean, while still allowing the user to customise each function. Apart from the Reset feature, all anti-theft commands worked flawlessly.

| Anti-Theft Details | | |
|---|---|---|
| **Commands Web** | | |
| **Locate** | ✔ | Displays location on *Bing Maps*. |
| **Lock** | ✔ | Locks the device until either the Trend Micro password or a one-time unlock key from the web interface is entered. |
| **Wipe** | ✔ | Triggers a factory reset and wipes external storage. |
| **Share** | ✔ | Posts a *Bing Maps* link with the current location on Facebook. |
| **Reset** | ▬ | Forces all running apps to stop, or resets lock-screen password. |
| **Additional Features** | | |
| **SIM Change Protection** | ✔ | Locks the device if the SIM card is changed. |
| **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 July 2020)** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Product Name | *Android OS* | Avast Mobile Security | AVG AntiVirus | Avira Antivirus Security | Bitdefender Mobile Security | G DATA Mobile Security | Kaspersky Internet Security | Securion OnAV | Trend Micro Mobile Security |
| Version Number | *10.0* | 6.29 | 6.27 | 6.6 | 3.3 | 26.6 | 11.48 | 1.0 | 11.5 |
| Supported Android versions | *built-in* | 5.0 and higher | 5.0 and higher | 5.0 and higher | 4.1 and higher | 4.1 and higher | 4.2 and higher | 5.0 and higher | 4.1 and higher |
| Supported Program languages | All | English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese | English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese | English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish | English, Czech, Dutch, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Thai, Turkish, Vietnamese | English, Arabic, Chinese, Dutch, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, Spanish, Turkish | English, Russian, German, French, Italian, Spanish, Portuguese, Turkish, Polish, Czech, Danish, Finnish, Hungarian, Norwegian, Dutch, Swedish, Arabic | English | English, Chinese, Dutch, French, German, Hebrew, Italian, Korean, Portuguese, Spanish, Turkish, Vietnamese |
| Anti-Malware | | | | | | | | | |
| On-Install scan of installed apps | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| On-Demand scan | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| On-Access scan of apps | ● | ● | | ● | | | ● | ● | |
| Can detect malware sitting on external SD card | | | | ● | ● | ● | ● | | ● |
| Automatic (scheduled) scan | | ● | ● | ● | | ● | ● | | ● |
| Scan requires online cloud connection | ● | | | | ● | | | | |
| Manual signature update possible (beside automatic updates) | n/a | ● | ● | | n/a | ● | ● | | ● |
| User account needed to use product | ● | | | | ● | ● | | | ● |
| Privacy Advisor (audit app permissions) | ● | ● | ● | ● | | ● | | | |
| Safe Browsing (Anti-Phishing & Anti-Malware) | ● | ● | ● | ● | ● | ● | ● | | ● |
| Supported browsers (Safe Browsing) | Google Chrome | Google Chrome, Dolphin, Firefox, Opera | Google Chrome, Dolphin, Firefox, Opera | Google Chrome, Dolphin, Edge, Firefox, Opera, Opera Mini, Samsung Internet | Google Chrome, Dolphin, Edge, Firefox, Opera, Opera Mini, Samsung Internet | Google Chrome, Firefox, Opera, Samsung Internet, own Safe Browser | Google Chrome, Samsung Internet | n/a | Google Chrome, Samsung Internet |
| Anti-Theft | | | | | | | | | |
| Web Interface for controlling Anti-Theft commands | ● | ● | ● | ● | ● | ● | ● | | ● |
| Remote Locate, Lock & Wipe (Factory Reset) | ● | ● | ● | ● | ● | ● | ● | | ● |
| Thief Cam | | ● | ● | | ● | | ● | | ● |
| Anti-Theft Alarm (cannot be muted by thief) | | ● | ● | | ● | ● | ● | | |
| Locate-Phone Alarm only (can be muted) | ● | | | ● | | | | | ● |
| Lock on SIM Change | | | | | | ● | ● | | ● |
| Remote Unlock | | ● | ● | ● | | | | | |
| App settings protected with password | | ● | ● | | ● | ● | ● | | ● |
| Uninstallation Protection (password required for uninstallation) | n/a | | | | | | ● | | ● |
| Parental Control | | | | | | | | | |
| App Lock | | ● | ● | ● | ● | ● | ● | | ● |
| Safe Web Browsing (content filtering) | | | | | | ● | | | ● |
| Time Limits (device use limits, bedtime intervals) | | | | | | ● | | | |
| Additional Features | | | | | | | | | |
| Wi-Fi Security | | ● | ● | | | ● | | | ● |
| VPN | | ● | ● | ● | ● | | | | ● |
| Task Manager (manage installed apps) | ● | ● | ● | | | | | | ● |
| Network Monitor (track data usage) | ● | ● | ● | | | | | | |
| System Optimizer | | ● | ● | ● | | | | | ● |
| Supports landscape mode | ● | | | | | ● | ● | | |
| Other Features | Backup, Battery Monitor, Call Block | Photo Vault | Photo Vault | Account Privacy | Account Privacy | Panic Button | Call Block | | Social Network Security, Battery Monitor |
| Support | | | | | | | | | |
| Online Help & FAQ | ● | ● | ● | ● | ● | ● | ● | | ● |
| User Forum | ● | ● | ● | ● | ● | | ● | | ● |
| Email Support | | ● | | ● | ● | ● | ● | | ● |
| Phone Support | | | | ● | ● | ● | ● | | ● |
| User Manual (PDF) | ● | | | ● | ● | ● | ● | | |
| Online Chat | | | | | ● | | ● | | |
| Supported languages of support | All | English, Czech, German, French, Japanese, Spanish, Portuguese, Russian | English, Czech | English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish | English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish | English, Chinese, Dutch, French, German, Italian, Japanese, Polish, Portuguese, Spanish | English, French, German, Italian, Portuguese, Russian, Spanish | n/a | English |
| In-App List Price (may vary) | | | | | | | | | |
| Price 1 Device / 1 Year (USD/EUR) | FREE | 20 USD / 20 EUR | 30 USD / 30 EUR | USD 10 / 8 EUR | USD 15 / 10 EUR | USD 16 / 16 EUR | USD 20 / 11 EUR | FREE | USD 30 / 20 EUR |

# Copyright and Disclaimer



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

AV-Comparatives
(July 2020)