

# Anti-Virus Comparative



## Mobile Security Review 2018

Language: English  
July 2018

Last Revision: 7<sup>th</sup> August 2018

[www.av-comparatives.org](http://www.av-comparatives.org)

# Table of Contents



Introduction	3
Products tested	7
Overview	8
Malware Test Set & Results	10
Battery Drain Test Results	11
Alibaba	12
Avast	14
AVG	17
Avira	20
Bitdefender	22
F-Secure	24
G Data	26
Google	29
Kaspersky Lab	31
McAfee	33
Tencent	36
Trend Micro	37
Feature List	39
Copyright and Disclaimer	40

## Introduction

This report provides test results and reviews of security products for smartphones running Google's Android operating system. Amongst other things, this report aims to help readers decide whether they would benefit from the more comprehensive and sophisticated security features provided by a third-party security app.

Besides the reviews, which cover the user experience of the apps, the results of comprehensive tests on malware protection rates and battery consumption are provided as well. Additionally, a short table at the end of each product report gives an overview of any anti-theft functions included in that product. Many of the reviewed and tested apps have components which are not security-related, such as power and memory optimizers and data backup tools.

The review mainly focuses on the security features – anti-malware, anti-theft, and privacy – and only mentions further functionalities briefly. The structure of each product report is identical, allowing readers to compare products easily.

The main purpose of a mobile security product is to protect users and their devices from potential harm inflicted by malicious apps, fraudulent mails, or phishing URLs. Readers should note that recent Android versions incorporate some basic anti-malware features. For example, Google's built-in malware scanner *Play Protect* checks apps during installation from the Google Play store or a third-party source and scans the device continuously for any threats. Google's *Safe Browsing API* protects against malware and phishing links when the user is surfing the Internet using the Chrome browser. Furthermore, an anti-theft component in a security app could be used to find a lost or stolen phone, and/or prevent access to any personal data stored on the device. Basic anti-theft features (lock, locate, alarm, and wipe) are already provided by recent versions of Android via Google's *Find My Device* function.

On the following pages, we provide a brief overview of the risks facing smartphone users from malware and the loss or theft of their device, and discuss the benefits of security apps. We start by recapping *Android Oreo's* new features and security behaviour changes. Furthermore, we will argue why it is not advisable to rely only on built-in malware protection features (all latest and newer Android devices are already equipped with such functions), but instead install a third-party anti-virus app to be better protected against security threats. After that, we give a short summary of security features and their main sub-components commonly implemented in typical security apps for Android.

At the end of the introduction, we list the participating security products, and present the results of the malware and battery drain tests. Detailed reviews of the individual products follow, in which we will shed light on the layout and usage of the features. In the table representing a product's anti-theft features, we comment on each function briefly and use the following symbols to indicate how well it worked in our tests.



everything worked fine



minor issue(s)



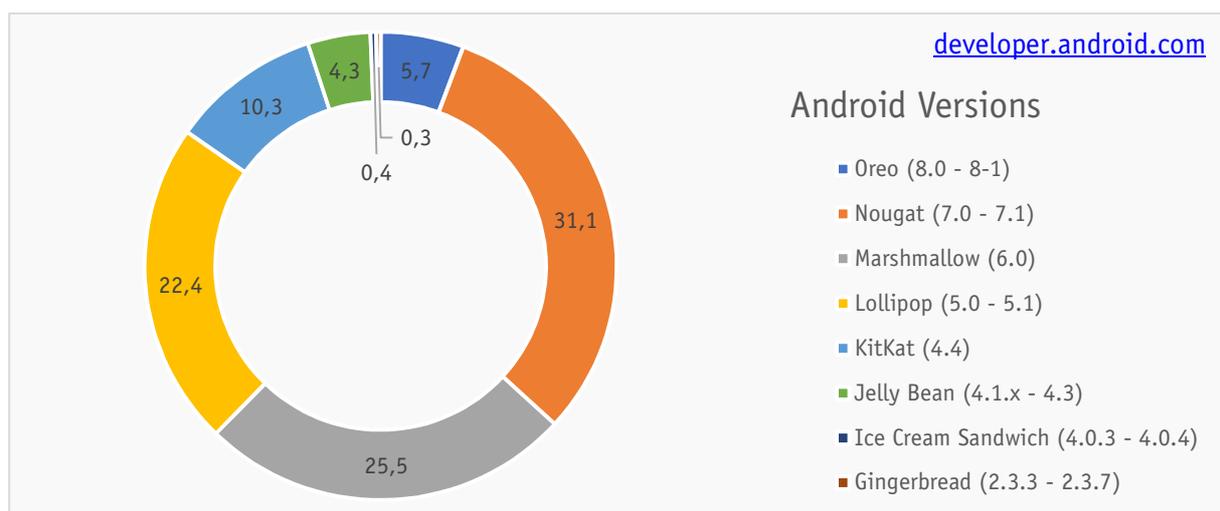
major issue(s)

## Google Android

In last year's report, we tested anti-virus apps for devices with Android 6.0 (Android Marshmallow). At that time, it was the most commonly used Android version, running on around 31% of all Android devices. Android 6.0 introduced run-time permissions where an app will request a specific permission the first time it needs it, which gives the user more control over the permissions granted to/removed from individual apps. Additionally, the account management was restricted, so as to deny apps permission to remove existing accounts (such as the main Google account) from the phone. As the ring chart of Android versions in May 2018 below shows, Android Marshmallow still runs on more than 25% of all Android devices.

With the release of Android 7.0 (Android Nougat) in August 2016, Android devices received seamless system updates (e.g., better multitasking, new JIT compiler, dual system partition), improvements for the storage manager, and overall performance improvements that extend battery life, reduce RAM usage, and speed up app installation and execution. Many manufacturers upgraded the operating system for their older phones and Android Nougat is currently running on almost every third Android device (31.1%).

Android version 8.0 (Android Oreo) was officially released in August 2017. Besides notable changes in the notifications system (e.g., notification channels) as well as enhanced security in web browsing, the system performance (e.g. limited background services, battery life) and the user interface were improved. Compared to Android 7.0 and 7.1, the biggest change was the revised architecture of the Android system (*Project Treble*) to separate device-specific and low-level vendor software implementations from the Android OS Framework. This makes it easier, faster and less costly for manufacturers to update devices to a new Android version. Furthermore, the global security setting "Install from unknown sources" became a run-time permission that needs to be granted every time an app requires it. Currently, Android 8.0 and 8.1, the recent Android versions, are only installed on a few brand-new devices (5.7%) but updates will be available for older devices gradually.

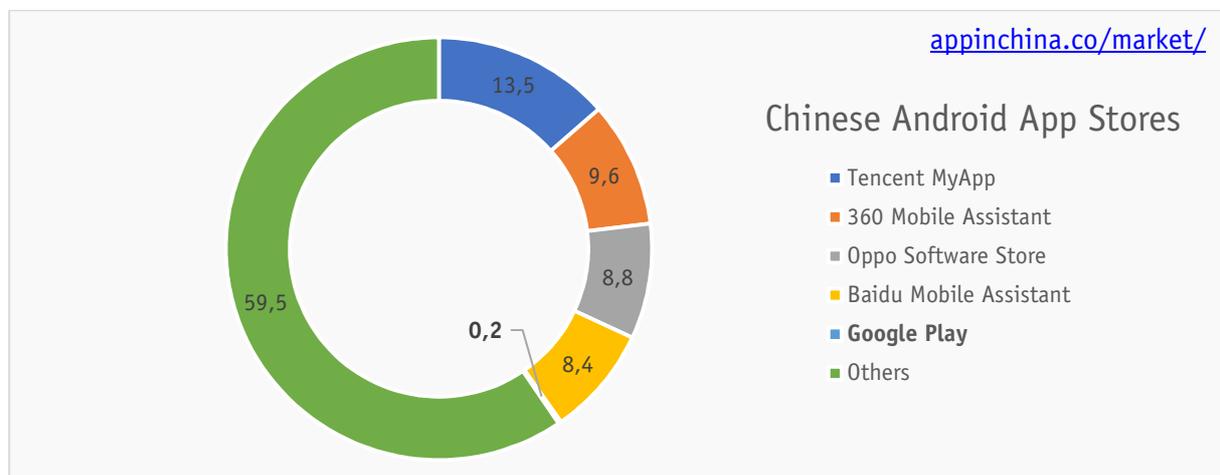


We decided to use Android Oreo for this review, even though it is currently only available on a limited number of devices. There are no major changes relative to the previous version, Android Nougat, that would prevent current anti-virus apps installing or working properly. However, testing with Android Oreo enables the apps to make full use of the new functionality in the latest OS. We used the unmodified version of Android Oreo, as provided by Google, in order to avoid potential problems with hardware manufacturers' or mobile carriers' modifications.

## Google Play Protect

In May 2017, Google announced its new built-in malware protection for Android, *Play Protect*, which checks apps and APK files when they are downloaded using the Google Play store app or third-party sources. Since August 2017, it has been available on all Android devices with Google Play Services 11 or later, and is preinstalled on devices with Android 8.0 and later. Play Protect constantly monitors the device and all the user's data, and notifies the user of any security risks found. It also scans the Google Play store and all installed apps for any signs of malware, and includes the three functions malware scanner, device loss (*Find My Device*), and safe browsing.

One might think that third-party anti-virus apps are no longer necessary for Android devices, due to Google's built-in malware and protection features. This might be true for Android devices with Play Protect integrated into the preinstalled Google Play store app. However, some Android devices (e.g., Amazon's Fire line) do not benefit from the built-in malware protection of Play Protect as they do not run Google apps by default<sup>1</sup>.



In western countries where official stores like Google Play are mostly used, the risk of being infected by malware is much lower than in many Asian countries, especially China. Many rooted phones and third-party app stores can be found there, increasing the chance of installing a dangerous app. About 750 million of China's total population of 1.4 billion use mobile devices, and almost 80% of them (about 600 million) run Android as the operating system<sup>2</sup>. In China, there are over 400 Android app stores available, and the ring chart above shows a summary of the top used ones. The Tencent MyApp store is by far the most widely used app store, with a market share of 13.5%, whereas Google Play lags far behind, and is used by almost no one (0.2%). The reason for this is that most Google services are currently inaccessible in mainland China, and most smartphones sold in China have neither Google Play nor the Google Services framework installed.

In our tests, Google Play Protect did not perform very well, as can be seen in the test results (further on in this report). Play Protect surely has the potential to become better in the future, as Google has the data and resources to improve its algorithms and systems, as Microsoft did with its Windows Defender. However, Play Protect as a cloud-based malware scanner would still suffer from inaccessibility of Google services from mainland China, even if it might in future protect better against Android threats.

<sup>1</sup> <https://arstechnica.com/gadgets/2018/03/google-starts-blocking-uncertified-android-devices-from-logging-in/>

<sup>2</sup> <https://www.appinchina.co/market/>

## Security Features

In this section, we give a short 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. This protects the user against the inadvertent installation of malicious apps on his or her device. Similarly to anti-virus programs for Microsoft Windows, mobile security apps for Android use a number of different protection features. The *real-time scanner* checks new apps during the setup process. This prevents the device being compromised by the installation of a malicious program. *On-demand scanners* search 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. As with Windows desktop security applications, keeping malware 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. We noticed that many 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 after a certain time or can be downloaded by the user manually.

A major component in various security apps is the anti-theft module. It is designed to execute commands on a target device that has been lost or stolen. As mentioned in previous sections, Android includes core anti-theft features such as remote device lock, location, wipe, and an alarm sound. Many of the security products we tested extend this base functionality with additional features such as taking pictures of the thief using the built-in front and/or back camera of the device, location tracking, or automatic notification in the event of a SIM card change. Usually, the anti-theft components are controlled via a web interface, but several apps also support text-message commands. The latter have the advantage that they work even if no Internet connection is available, but they are less convenient to use. For example, if the Android OS is not appropriately configured by the user, text messages will be shown as notifications just before the screen locks or on the lock screen itself. Therefore, texts containing e.g. the unlock code could be read by a thief. With Android 4.4 and later, app developers are no longer able to programmatically delete text messages as they arrive. Hence, they can no longer prevent the text messages used for their commands being seen on the screen when they appear. To get around this issue, some manufactures have developed their own custom binary SMS. This function is provided by the anti-theft feature of the security app itself, meaning the same app has to be installed on the friend's/relative's phone used to send the anti-theft SMS commands.

Several security products offer browser protection, which prevents the user from unintentionally downloading malicious apps or accessing phishing websites while surfing the Internet. Some apps support a variety of different browsers, including those made by third-party app developers. This is an important question, as many smartphone users like to use their preferred browser on their smartphones.

A privacy advisor is also included in many of the tested products. This 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, text messages, emails, 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 any apps that have given themselves such inappropriate permissions.

## Products tested

The products included in this year's test and review are listed below. The latest products<sup>3</sup> were taken from major app stores like Google Play at the time of the test (July 2018). After the product review, 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
 Alibaba	Ali Money Shield	5.8	     
 Avast	Mobile Security & Antivirus	6.11	     
 AVG	Antivirus for Android Security	6.10	     
 Avira	Antivirus Security	5.2	     
 Bitdefender	Mobile Security & Antivirus	3.3	     
 F-Secure	SAFE	17.4	     
 G DATA	Internet Security for Android	26.4	     
 Google	Play Protect & OS Features	10.7	     
 Kaspersky Lab	Internet Security	11.17	     
 McAfee	Mobile Security	5.0	     
 Tencent	WeSecure	1.4	     
 Trend Micro	Mobile Security & Antivirus	9.5	     

## Symbols

To provide a simple overview of the features of a product, we use symbols like those on our website. At the beginning of every report, you will see all these symbols; those in orange represent features the product has, while those in grey represent features that are not included.

<b>Anti-Malware</b>		includes a feature to scan against malicious apps
<b>Anti-Theft</b>		includes remote features in case the smartphone gets lost or stolen
<b>Safe-Browsing</b>		includes a web filtering feature to block dangerous sites
<b>App Audit</b>		includes features to audit installed apps
<b>Anti-Spam</b>		includes features to block unwanted calls and/or SMS
<b>Backup</b>		includes a feature to backup files on the smartphone

<sup>3</sup> A comprehensive overview of the mobile security products available on the market can be seen on our website: <https://www.av-comparatives.org/list-of-mobile-security-vendors-android/>

## Overview

The perfect mobile security product does not yet exist. As with e.g. Windows products, we recommend drawing up a short list 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; this should make the decision easier. With Android security products in particular, new versions with improvements and new functions are constantly being released. As this report shows, we found some degree of malfunction in some of the tested products. The manufacturers of the affected products have taken these problems seriously and are already working on solutions. Nine of this year's participants qualify for our "Approved Mobile Product" award, by providing reliable and effective core functions and solid malware protection.



**Alibaba** Ali Money Shield is a free anti-malware product available in Chinese language only. It has a clear focus on security and payment protection for users with a Taobao account.

**X**

**Avast** Mobile Security and Antivirus provides well-developed features for almost any use case. Unfortunately, because of a bug it fell just short of the minimum malware protection level for certification.

**X**

**AVG** AntiVirus offers full access to a wide range of security and device customization features. However, a bug meant that it unfortunately just missed the malware protection level for certification.



**Avira** Antivirus Security is a well-developed app including malware detection, an anti-theft component with in-app text-message commands, and additional security features.



**Bitdefender** Mobile Security and Antivirus is an easy-to-use product which provides malware protection, as well as a flawlessly working anti-theft feature that lets you control the device via SMS or the web interface.



**F-Secure** SAFE is an anti-malware solution for multiple devices, including Android smartphones. It contains a malware scanner, as well as basic anti-theft and parental control features.



**G DATA** Mobile Internet Security is a solid anti-malware app for Android with protection against malware, plus anti-theft commands sent by SMS or the web interface, and an extensive parental control feature.

**X**

**Google** equips all its recent Android devices with built-in anti-theft features and a malware scanner, but the latter does not yet provide effective protection.



**Kaspersky** Internet Security is a comprehensive mobile security app, with a variety of features for mobile security including anti-malware and anti-theft, presented in a clean and user-friendly interface.



**McAfee** Mobile Security has been completely redesigned and provides a great security product with malware detection and a comprehensive anti-theft component.



**Tencent** WeSecure represents a free, basic, straightforward anti-malware application that omits anti-theft features, but is extensible with other useful tools.



**Trend Micro** Mobile Security is a comprehensive app offering malware protection, an anti-theft module, and additional, helpful features for managing the device.

## 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, follow the advice given here. Only download apps from official app stores like Google Play or stores of reputable app makers, and avoid third-party stores and side-loading<sup>4</sup>. Irrelevant access rights are another indicator of untrustworthy apps. For example, an app that counts the steps the user takes every day has no need to access the phone book or call log. Of course, even if an app behaves like this, it does not necessarily mean that it is malicious, but it makes sense to consider whether it is genuine and worthy of use. A quick look at the reviews in the app store before installing an app is also a guide; avoid apps with predominantly bad or dubious reviews. Rooting the smartphone may gain the user more functionality on the phone, but also increases the risk that malicious apps will take control of the device. Furthermore, it is not legally clear-cut whether the warranty is still valid if the phone is rooted. With some manufacturers, the warranty will be considered null and void. Public Wi-Fi networks without appropriate security are opportunities for malware to steal or comprise sensitive personal data. Whenever connecting to a public Wi-Fi hotspot e.g. in a coffee shop, be aware of the security risks when sharing information. Never expose data (user credentials, Wi-Fi passwords, bank/credit card information, etc.) that shouldn't be shared with others. This holds not only for Android devices but also for other portable devices from any manufacturer.

### 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 the previous sections, official stores such as Google Play are mostly used in western countries, where the risk of infection is very low. In Asian countries, where rooted devices and large number of third-party app stores can be found, the chance of installing a dangerous app is greatly increased. In many parts of Asia, the smartphone is often used as a replacement for the PC, and so is frequently employed for online banking. There is a high risk involved in receiving the TAN code on the same phone that is used to carry out the subsequent money transfer. Nowadays, banking apps have also become popular in Europe and the USA. Assuming you stick to official app stores and don't root your phone, we would say the risk of the smartphone becoming infected in western countries is still relatively low. However, we must point out that "low risk" is not the same as "no risk". In addition, 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 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.



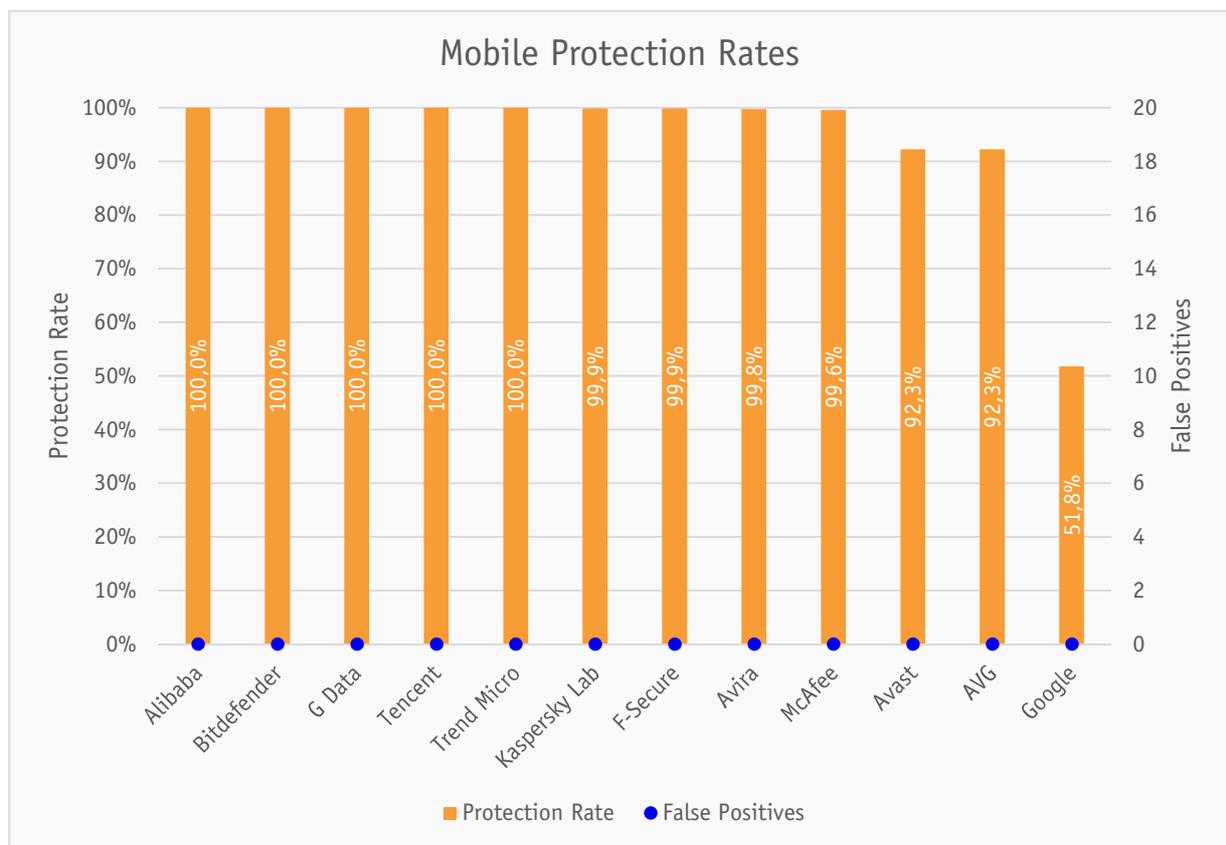
We invite readers to try it out: <https://www.av-comparatives.org/specials/undroid/>

---

<sup>4</sup> <https://en.wikipedia.org/wiki/Sideloading>

### Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **2,604** malicious applications, to create a representative test set. Apps with same certificates and/or same inner-code were removed to have a more unique set. So-called "potentially unwanted applications" (PUA) were not included. The security products were updated and tested on the 4<sup>th</sup> July 2018. 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 third-party app stores. The results can be seen below (sorted by Malware Protection and number of False Alarms).



Mobile Protection Rates		
	Protection Rate	False Positives
Alibaba, Bitdefender, G DATA, Tencent, Trend Micro	100.0%	0
Kaspersky Lab, F-Secure	99.9%	0
Avira	99.8%	0
McAfee	99.6%	0
Avast, AVG	92.3% <sup>5</sup>	0
Google	51.8%	0

<sup>5</sup> Unfortunately, Avast and AVG had a bug in their apps, which resulted in lower detection rates. The bug meant that on Android 7.0 or later, the apps did not query their respective cloud services under certain circumstances. We reported the observations to Avast and AVG, who have since found and corrected the bug.

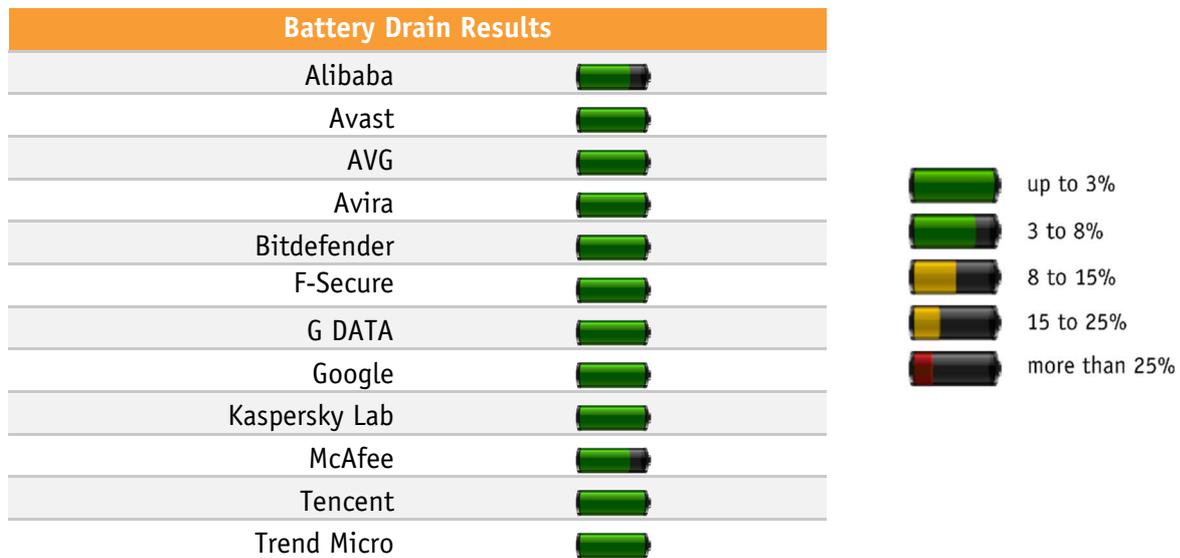
## Battery Drain Test Results

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. Two products in this year's test showed a slightly increased battery drain: **Alibaba** and **McAfee**.



**Alibaba**

Ali Money Shield

5.8.4



## Introduction

Alibaba's Ali Money Shield is a free application which includes a variety of performance and security features with a focus on secure money transfer. Currently, the app is only available in Chinese language.



## Usage

After agreeing to the Terms and Conditions, the user is taken to the app's home screen, from where the most important features of the app can be accessed. At the top of the screen, a security rating ranging from 0 to 100 is presented. This can be improved by taking any recommended actions, such as performing a scan or giving needed permissions to the app.

## Security Check

The security check rates the device's protection status and gives an updated security rating each time it is performed. After each check, it gives a list of recommended actions for the user to perform, which include performing a malware scan, creating a Taobao account, and enabling other features of the app.

## Anti-Malware

The scanning tool can be started directly from the home screen. The user can choose to perform either a quick scan, which only scans installed applications, or a full scan, which also scans other files. Virus signature database updates are performed automatically.

## Fraud & Nuisance Blocker

Alibaba's Phone Intercept feature allows call blocking according to a few different rulesets, as well as automatically detecting malicious URLs received via SMS. The user has the option to create a blacklist and whitelist of phone numbers, as well as to enable automatic filtering of unknown or suppressed callers, strange numbers and harassment calls. It is possible to create a schedule of times during which only whitelisted calls will be allowed.

### Phishing Intercept & Application Lock

The Phishing Intercept tool reroutes network traffic over a VPN after user confirmation, allowing the app to automatically block all browsers from visiting phishing websites. An option to also block gambling websites is available. After setting up a touch pattern, as well as a security question in case the pattern is forgotten, the user can utilize the Application Lock feature to selectively lock access to chosen apps.

### Tool Box

The tool box covers a wide range of other useful components and applications, from improving device performance by cleaning up RAM and storage, to allowing secure transfer of money via Alibaba's services. Also notable are the notification manager and the fraud reporting features.

The anti-theft feature, which was part of the app when we did our mobile test last year, seems to have been deprecated. Only a function preventing normal uninstallation is present in the app. References to Anti-Theft can still be found in the manual and on the website. However, it could not be enabled either in the app version downloaded from the Play Store (8.5.4) or from the web interface (8.5.3).

### Task Bar & Widget

The app comes with a taskbar that is displayed in the Android notification area. From there, small features like an OCR scanner, a flashlight, and several clean-up functions can be quickly accessed.

In addition, a small widget is displayed on the screen. Dragging it to the bottom of the screen performs a quick security check-up and clean-up of the device's RAM.

### Conclusion

Ali Money Shield is an easy-to-use product with a clear focus on payment protection. In addition to the usual security features, it contains a wide array of additional tools and components. However, the anti-theft function, which was present in our last year's review, has since been removed completely and no replacement has been added, leaving the user to rely on Android's built-in anti-theft features.



## Introduction

Avast offers a comprehensive app with all the important security features, including malware scan, anti-theft, Wi-Fi security, app locking, app permissions, photo vault, call blocker, and a firewall feature (root rights required), that will give the user a good level of overall protection. The free and ad-supported version comes with a 14-day trial for some premium features in the anti-theft and app-locking component. Many other, non-security related features are provided as well aimed at improving device performance and monitoring data usage.



## Usage

After installing the app and accepting the EULA, the user can decide if he or she wants to stay on the free version, or upgrade to the pro version with either a yearly or a monthly subscription. Afterwards, the home screen of the app shows up.

### Anti-Malware

The malware scan is kept neat and very simple, as all options to adjust the scan process are hidden in the app settings. There, the user can manually set the protection against malicious apps, phishing websites accessed by various browsers, malicious URLs via text messages, PUAs, as well as applications and data with a poor security level. Furthermore, scans can be scheduled for any day and time, and the user can decide if files in the internal storage should be scanned.

### Anti-Theft

The feature provides both web-based and text-message commands. On the initial setup, the user has to set up a PIN, pattern, or fingerprint (if supported by the device), required to send the SMS commands and to unlock the screen. Pictures taken of the culprit, as well as recorded audio and backup data, can be found and downloaded via the web interface, or optionally uploaded to Google Drive. SMS Remote Control allows you to send anti-theft commands from a friend's phone – which must also have the app installed – to your own phone if this is lost or stolen. The message exchange between the two phones happens behind the scenes. The text messages are not displayed on the receiving phone, so that the thief does not see what is happening or gain any useful information.

During the feature tests, some bugs and issues were detected in both the app itself and the web interface. These are listed below

- In the web interface, the “Get data” function can fetch a list of calls, SMS, and contacts from the device, and should be able to store them in HTML or XML format. However, only HTML was possible at the time of testing.
- It is not obvious to the first-time user how to find all the backup files in the web interface. They are in fact hidden behind the “Info” button and the “Commands” or “Notifications” tab.
- When the device status is shown as “Attention”, insufficient details about the reason for/cause of the problem(s) are displayed.
- When testing the anti-theft feature, we found some connectivity issues. For example, the info dialog in the bottom right of the page does not always provide useful or correct information, e.g., after executing a command successfully it still states “Trying to contact your device”.

### Wi-Fi Security & VPN Protection

This tool scans and monitors currently connected Wi-Fi networks and other available networks for threats, and determines whether they are safe. After a scan, information about the network is revealed and a speed test can be performed in addition.

The latest version of the app also includes a VPN feature to protect online activity from eavesdropping. However, it is only available for devices with an Ultimate or Ultimate Multi subscription.

### App Locking & Photo Vault

The App Locking feature restricts access to selected apps by locking an app with the previously set PIN, pattern or fingerprint. If photos are moved to the Photo Vault, they are protected against unauthorized access, i.e., they are encrypted and hidden.

### Call Blocker

The call blocking feature allows the user to block either all unknown or hidden numbers, or to add specified numbers to the blacklist (manually or from the contacts). Incoming calls from blocked numbers are displayed as a notification for a few seconds, then suppressed. The phone does not ring at all.

### App Permissions & Firewall

The App Permissions feature categorizes all installed apps into three permission groups: high, average, and low. The user can see detailed information about an app and the granted permissions.

Avast offers a firewall for rooted Android devices, which allows the user to control Internet access for individual apps. However, as no rooted device were available during the tests, we were unable to test this feature.

### Conclusion

Avast provides an app with a wide range of security features and additional gimmicks for optimizing and monitoring device performance. The user-friendly interface focuses on the main functions, and discreetly hides away the extensive configuration options for the scan process. The tools are self-explanatory and function well, and the establishment of the in-app SMS Remote Control is really convenient.

Anti-Theft Details		
Commands Web		
<b>Locate</b>	✓	Displays location on <i>Google Maps</i> map. Tracking the device can be enabled.
<b>Mark as Lost</b>	✓	Triggers configured actions like tracking, lock, siren, ...
<b>Forwarding</b>	—	Forwards all incoming calls and/or SMS to a given phone number. Forwarding calls does not work however, a text message is send to the receiving device to notify that the sending device is receiving a phone call.
<b>Siren</b>	✓	Activates/deactivates the phone siren.
<b>Lock</b>	✓	Locks/unlocks the phone.
<b>Wipe</b>	✓	Triggers a factory reset and wipes external storage.
<b>Record Audio</b>	✓	Records audio for a pre-defined duration of 1-5 minutes.
<b>Take Picture</b>	✓	Takes a picture with the front or back camera. Optional: The camera is triggered when the screen is turned on the next time. On a device with face-recognition, the camera can also be triggered upon detecting a face after unlock.
<b>Get Data</b>	✓	Fetches data (calls, SMS, contacts) from the device. Data can be downloaded from the web interface afterwards.
<b>Message</b>	✓	Sends and shows an on-screen message on the device.
<b>Call</b>	✓	Initiates a hidden phone call on the device to a given phone number.
Commands SMS		
<b>Message</b>	✓	
<b>Lost</b>	✓	SMS commands are sent from within the app's SMS Remote Control. This enables the usage of binary SMS which can't be read on the receiving phone. To get SMS answers from the receiving phone (e.g. the location), SMS responses have to be explicitly activated in the anti-theft settings. In our test, all commands worked as expected.
<b>Found</b>	✓	
<b>Lock</b>	✓	
<b>Unlock</b>	✓	
<b>Siren</b>	✓	
<b>Locate</b>	✓	
<b>Locate Stop</b>	✓	
<b>Call</b>	✓	
<b>Forward</b>	—	
<b>Wipe</b>	✓	
Additional Features		
<b>SIM Change Protection</b>	✓	Sets the phone status to lost.



## Introduction

AVG provides a comprehensive application with a wide range of security features, among them anti-theft, malware scans, app permission checker, call blocker and a firewall feature. The free version is supported via fairly non-intrusive ads and comes with a 14-day trial for the pro version. The pro version is completely ad-free and contains some additional functionality related to anti-theft and application locking. In addition to its extensive security tools, the app offers functionality to improve device performance, e.g. free up RAM, delete junk files, extend battery duration, and monitor mobile data usage.



## Usage

After installation, the user is asked to accept the Terms of Service as well as the Privacy Statement. Following that, an upgrade to the pro version is offered via either an annual or a monthly subscription. Next, the user is taken to the app's main screen. Necessary permissions are acquired case-by-case whenever the user activates a feature.

## Anti-Malware

Besides scanning all installed apps, the malware scan also checks the device's settings for any threats and gives recommendations how to remedy them. The options menu includes settings to scan all files in the internal storage, schedule automated daily scans, treat PUA as malware, block visiting malicious websites, and warn about malicious URLs in text messages.

## Anti-Theft

Upon first opening the anti-theft feature, a security PIN – which can later be replaced by a pattern or fingerprint – must be set up, and a set of permissions including device admin rights must be given to the app. Optionally, the web control interface can be configured by linking to an existing AVG account. Once this is done, the phone can receive several different commands either via text messages or the aforementioned web interface.

Commands via text messages can be sent using a second phone with the AVG app installed, and are hidden on receiving on the target phone. The easy-to-use web interface provides additional commands and lists information about the status of the selected device.

During testing of the web interface, we came across some minor issues with misleading notifications - for example "Command cannot be processed" - although in all cases the respective commands were successfully executed.

In the pro version, the user can configure the device to be marked as lost upon failed unlock attempts or upon detecting a new SIM, and has the option to send the phone's last known location to the web interface when battery life becomes critically low.

### Wi-Fi Security

This feature checks the currently connected Wi-Fi for security vulnerabilities and gives recommendations for how to fix them. It also tests the respective upload and download speeds of the network.

### App Locking & Photo Vault

App Locking is a tool exclusively available to the pro version, which allows you to secure selected apps with either a PIN, pattern, or fingerprint. The photo vault provides similar functionality, enabling you to protect photos and other images specifically.

### Call Blocker

This feature enables creation of a blacklist of phone numbers to block, either by manual selection or by choosing to block all hidden/unknown numbers.

### App Permissions & Firewall

The App Permissions tool analyses the permission requirements of all installed applications, and ranks them as either high, average, or low-permission. For rooted devices, a firewall is offered, which allows selective control of Internet access by installed apps. However, as we did not have access to a rooted device, we did not test this feature.

### Conclusion

AVG AntiVirus comes with a wide range of security features, which are easy to use, but still allow for some amount of customization. The interface is well designed and all tools function as intended. Despite not having access to the full range of features, the free version of the app still provides an extensive arsenal of tools, and only shows a limited number of ads.

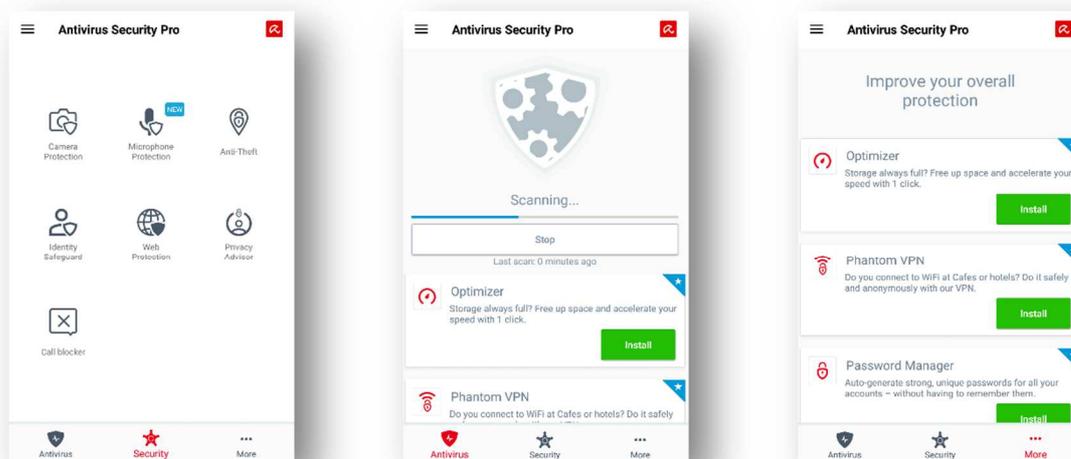
Anti-Theft Details		
Commands Web		
<b>Locate</b>	✓	Displays location on <i>Google Maps</i> map. Tracking the device can be enabled.
<b>Mark as Lost</b>	✓	Triggers configured actions like tracking, lock, and siren
<b>Forwarding</b>	—	Forwards all incoming calls and/or SMS to a given phone number. Forwarding calls does not work, however, a text message is sent to the receiving device to indicate that the sending device is receiving a phone call.
<b>Siren</b>	✓	Activates/deactivates the phone siren.
<b>Lock</b>	✓	Locks/unlocks the phone.
<b>Wipe</b>	✓	Triggers a factory reset and wipes external storage.
<b>Get Data</b>	✓	Fetches data (calls, SMS, contacts) from the device in HTML format. Data can be downloaded from the web interface afterwards.
<b>Message</b>	✓	Sends and shows an on-display message on the device.
<b>Call</b>	✓	Initiates a hidden phone call on the device to a given phone number.

Commands SMS		
Message	✓	
Lost	✓	SMS commands are sent from within the app's SMS Remote Control. This enables the usage of binary SMS which can't be read on the receiving phone. To get SMS answers from the receiving phone (e.g. the location), SMS responses have to be explicitly activated in the anti-theft settings. In our test, all commands worked as expected. The Lost and Found commands mark the device as lost and found respectively. The Locate command enables the tracking of the device in the web interface and sends its current location to the phone that triggered the command (if specified in the settings). The Locate Stop command deactivates the location tracking.
Found	✓	
Lock	✓	
Unlock	✓	
Siren	✓	
Locate	✓	
Locate Stop	✓	
Call	✓	
Forward	✗	
Wipe	✓	



## Introduction

Avira provides a comprehensive product that has a refreshed user interface since our test last year. It is available in free (ad-supported) and pro versions, whereby the free version comes with an anti-theft feature, Identity Safeguard, Privacy Advisor, and Call Blocker. An upgrade to the pro version adds more-frequent database updates, Web Protection, as well as Camera and Microphone Protection. Further functions like App Lock+ and a Password Manager are offered in separate Avira apps.



## Usage

After installation, the user can either consent to continuing with personalised or non-personalised ads in the free version, or choose to upgrade to Pro immediately. The user interface is kept clean, and the user can navigate through the different functions via the navigation bar at the bottom (previous version used a tab layout with swipe gestures). The two main features are Antivirus and Security. Most of the functions are only available after creating an account, so we recommend doing so beforehand.

### Anti-Malware

The app provides a one-click scan of applications and internal files, which can be further customized in the settings. What has actually been scanned is hidden; only the number of files, and if something was found, is shown. In the settings, the scan process can be adjusted to include adware, potentially unwanted applications and riskware.

In addition, a scan can be scheduled for any time, and started when storage is mounted or a USB cable is unplugged.

### Anti-Theft

In an addition since the last test, the anti-theft functions can now be used in-app as well as from the web interface. However, Lock/Unlock and Wipe are restricted in-app on the tracked phone, as they are intended only to be executed on a remote device that also has the Avira app installed. A list of registered devices can be viewed, and the current selected device can be located on Google Maps. All commands except for Lock/Unlock worked fine. A 4-digit PIN has to be entered in order to lock/unlock the device. More than 4 digits can be defined to lock the device, but please note the device cannot then be unlocked later on as only 4 digits are allowed to be entered on the lock screen. Finally, the device can only be unlocked using the web interface after 3 failed attempts.

The web interface provides all anti-theft functions under the *Family Locator*. The Wipe command is still not available. As in the app, the device's current location is displayed on demand on Google Maps map. Locking requires a 4-digit PIN, a message to display on the lock screen, and an alternative contact number optionally. While the device is locked, one can call the previously defined contact number with a simple button tap. Dialling is successful but on Google Pixel 2 with Android 8.1, the call cannot be ended on the calling device. Furthermore, an alert can be sounded for 20 seconds using the Play Sound command (formerly "Yell"). Avira told us that they will fix the two aforementioned issues in the next app updates.

### Additional Features

Two functions that were added since the last test, and are accessible in the pro version only, are Camera Protection and Microphone Protection. These restrict app access to the device camera and microphone respectively. In Camera Protection, the user is able to mark apps as trusted, and these are permitted to access the camera while protection is active. In order to use trusted applications, the user has to launch them from the Avira Camera Protection widget. For Microphone Protection, either all listed apps or none have access to the microphone.

Other functions that are included in the app are: Identity Safeguard, which checks a given email address for hacks, vulnerabilities, or other threats; Web Protection, which protects the user from harmful websites while surfing; Privacy Advisor, which rates the installed apps according to the number of permissions they access; and Call Blocker, which can blacklist unknown numbers and/or unwanted callers from the contacts list or call log.

### Conclusion

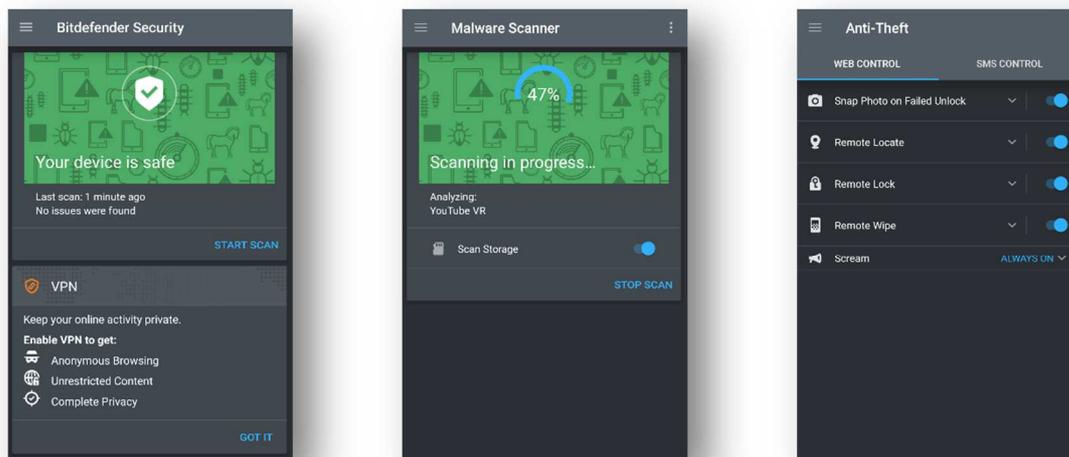
Avira Antivirus Security is essentially a well-developed anti-malware application which provides protection against malware, plus additional security features. Its functionality and interface has been greatly improved, as anti-theft features can now be used in-app as well as from the web interface, which enables more flexibility. The two new features for protecting the camera and microphone are convenient too. The web interface did not receive an update regarding the Wipe command, and some minor issues in the anti-theft features were detected as well.

Anti-Theft Details		
Commands App		
<b>Locate</b>	✓	Displays location on <i>Google Maps</i> map.
<b>Lock</b>	—	Locks the device with a 4-digit PIN and shows a message on the lock screen (only executable remotely). Optional: Call the phone number entered.
<b>Wipe</b>	✓	Triggers a factory reset and wipes external storage (only executable remotely).
Commands Web		
<b>Locate</b>	✓	As for the corresponding app command.
<b>Lock</b>	—	Locks the device with a 4-digit PIN and shows a message on the lock screen. Optional: Call the phone number entered.



## Introduction

Bitdefender Mobile Security & Antivirus is a well-polished and easily usable mobile security application. It comes with a 14-day trial period during which the app can be used for free, and after that the user can continue with a paid subscription. The features provided by the app include malware scanning, anti-theft, web protection as well as application locking functionality.



## Usage

On the first start of the application, the user must either sign in to a Bitdefender account or create a new one. At this point, the user is taken to the app's home screen and the 14-day free trial begins, which can be extended to a monthly or yearly subscription immediately. The app asks for permissions whenever one of its features is accessed.

## Anti-Malware

The malware scanner component performs a scan on all installed apps with the option to also check all files on the internal and external storage. Additionally, the autopilot feature automatically scans applications after they have been updated or installed in the background.

## Anti-Theft

After you set up the anti-theft protection by choosing a PIN and providing device admin rights, a number of protective features like Locate, Lock, and Wipe are enabled. The app can be configured to silently take a picture with the front camera whenever someone fails to unlock the device. You can also set up a trusted phone number, which will automatically be notified if a SIM card change is detected. The phone can be remotely controlled via SMS or a web interface.

## Web Protection & VPN

The web security feature monitors browser usage and gives a warning when a malicious, fraudulent, or phishing website is accessed. Currently, the Chrome, Dolphin, Firefox, Opera, Opera Mini, and Samsung Internet browser apps are supported.

The app allows the usage of Bitdefender's VPN, which encrypts and anonymizes the device's web traffic. The basic subscription includes 200 MB per device, per day. An additional subscription offers unlimited traffic and the ability to connect to any of the available servers. However, we were not able to use this feature in our test; the traffic limit appeared to have been reached already, even though we had installed and used the app for the first time on our test devices. Bitdefender is aware of this issue and is already working on a solution.

### App Lock

This feature allows you to selectively lock certain apps with a PIN and to hide their notifications. Several options are provided to configure when apps should be locked (e.g., each time the app is accessed). Trusted Wi-Fi networks can be set up, which will keep the apps unlocked as long as the device is connected, and optionally, a photo can be snapped once there have been three incorrect attempts at unlocking.

### Account Privacy

This tool will check email addresses for any known data leaks, after the user confirms their ownership via a pre-sent confirmation mail. The user will be notified and prompted to change their password if an online account is compromised, and will have the ability to mark the secured accounts as dealt with after changing the password, so as to keep track of the privacy status.

### Conclusion

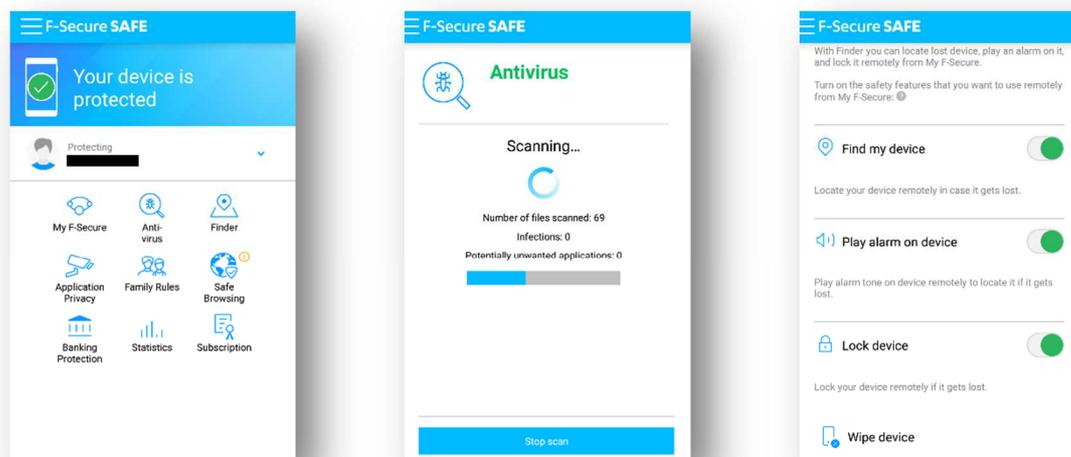
Bitdefender offers a well-designed and comprehensive mobile security solution for Android devices. Despite missing app audit and a call blocker, its anti-malware and anti-theft features work flawlessly and can be used freely for 14 days before requiring payment. Controlling the device via the web or SMS anti-theft commands is really convenient and user-friendly.

Anti-Theft Details		
Commands Web		
<b>Locate</b>	✓	Displays location on <i>Google Maps</i> map.
<b>Alert</b>	✓	Message can be displayed on screen. Optional: Alarm sound.
<b>Lock</b>	✓	Locks the device with the Android lock screen. The PIN is set in the web interface.
<b>Wipe</b>	✓	Triggers a factory reset and wipes external storage.
Commands SMS		
<b>Locate</b>	✓	Link to <i>Google Maps</i> is sent.
<b>Lock</b>	✓	Locks the device with the Android lock screen.
<b>Wipe</b>	✓	As for the corresponding web command; only allowed by the trusted number/contact.
<b>Scream</b>	✓	Sounds an alarm on the device.
<b>CallMe</b>	✓	Dials the phone number from which the command was sent with the speaker turned on.
<b>Help</b>	✓	Sends the usable commands.
Additional Features		
<b>SIM Change Notification</b>	✓	Sends a SMS to the trusted number whenever the SIM card is changed.
<b>Snap Photo</b>	✓	Takes a picture of the thief using the device's front camera on failed unlock attempts and uploads it to the web interface.



## Introduction

SAFE is F-Secure's solution to protect multiple devices (PCs, Macs, smartphones, tablets) against viruses, malware, and other threats. It also secures online banking connections and offers a parental control feature to restrict Internet and app access for children. The Android app comes with a 30-day trial including malware scanner, anti-theft feature, and its own Safe Browser app.



## Usage

On first use, the user has to accept the EULA and grant permissions to the app. Then the user can set up the app either for his or her current profile, or for a child profile by configuring Family Rules in the next step. These rules can be adjusted via the web interface anytime. The app starts with an initial scan.

## Anti-Malware

F-Secure SAFE automatically scans apps during installation, and memory cards when they are inserted, as well as manually scanning files on internal storage. The user can define scheduled scans to run at regular intervals, or enable a boot scan on device start.

## Anti-Theft

The anti-theft feature, called *Finder*, requires device admin rights and either a PIN, password, pattern, or fingerprint for later validations. Commands like Find, Alarm, Lock, and Wipe need to be enabled in-app first before being executed on the corresponding web interface. Optionally, a trusted phone number can be defined which will receive a notification if the SIM card of the protected device is changed. All commands worked as expected. An alarm command is available which is intended to help find the device at home, rather than if it is lost or stolen. The alarm can be turned off on waking up the screen e.g. by pressing the power button.

## Safe Browsing

The separate Safe Browser app protects against fraudulent web sites and identity theft while surfing on the Internet. The browser shows a notification when opening a trusted online banking website.

## Privacy

The Application Privacy feature lists and ranks apps that might compromise privacy, i.e. if they can access messages (SMS or emails), detect location via network or GPS, or use camera or microphone for video or audio recordings. Via the web interface, the user can remotely change the Family Rules settings for child profiles. These include app control, time limits (device use limits, bedtime), and content filtering for the Safe Browser app.

## Conclusion

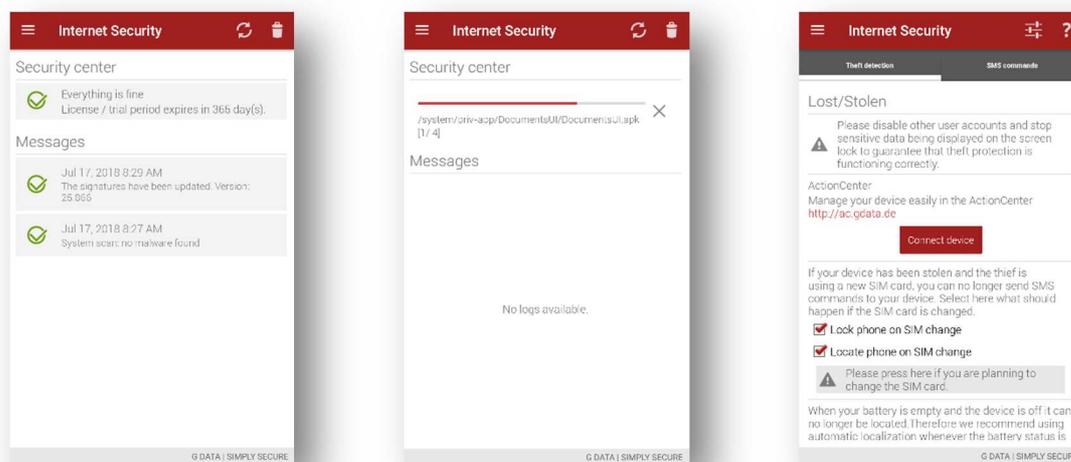
F-Secure SAFE provides an anti-malware solution to protect multiple devices like PCs, Macs, and smartphones against viruses and other security threats. The simple Android app is easy to use and contains a malware scanner, basic anti-theft features for remotely controlling the device, and a parental control function that is configurable via the web interface. All functions worked as intended.

Anti-Theft Details		
Commands Web		
<b>Locate</b>	✓	Displays current or last-known location on <i>Google Maps</i> map.
<b>Lock</b>	✓	Locks the device with the pre-configured lock mechanism.
<b>Wipe</b>	✓	Triggers a factory reset and wipes external storage.
Additional Features		
<b>SIM Change Notification</b>	✓	Sends a SMS to the trusted number whenever the SIM card is changed.



## Introduction

G Data provides a mobile app with a number of security-related features like malware scan, theft protection, web protection, app restriction, and a call/SMS filter. In addition, the *parental control* function includes comprehensive settings that create a protected environment for children where only suitable apps and websites are available to them. All premium features can be extensively tested within the first 30 days. After that, only basic features such as malware scan and app permissions are still available unless the user purchases an upgrade.



## Usage

A G Data account is required in order to use the app. After successful login to the account, the app performs a database update, and the main screen appears which shows latest messages. The screen looks very clean, as all features are hidden inside the menu in the upper left-hand corner.

## Anti-Malware

By default, the app scans newly installed applications and checks the device for viruses periodically. The user can decide how frequently the device will be scanned (1-30 days), whether to perform a quick scan of installed apps or a full system scan, and if the background scan will only run while recharging.

## Anti-Theft

Anti-theft commands can be send via SMS to the target device to remotely control it. All available SMS commands are listed in the app and require a pre-configured PIN. Responses to SMS commands are immediately sent to the device that issued the command, and can be forwarded to a given email address in addition. On SIM change, the app locks the device and/or sends the Locate command to the registered phone number/email address. The user can also receive position data when battery is low, and enable an alarm whenever the headset is disconnected.

As notifications of incoming text messages can no longer be hidden by other apps in Android 4.4 and later, G Data explicitly advises the user to turn on the system option "Hide sensitive information content" on the lock screen to use the anti-theft feature properly.

It is possible to manage the device from the G Data ActionCenter after connecting the device to it. Here, the user is able to view the device status and settings, and to send anti-theft commands (similar to SMS commands). All commands worked as intended in our test.

### Web & Wi-Fi Protection

This feature prevents phishing attacks while using the Android or Google Chrome browser app. Optionally, G Data provides its own Secure Browser app to securely surf the Internet, but this is very basically implemented and offers minimal surfing options. However, the app settings allow you to configure the feature and set additional checks and rules for connected Wi-Fi networks.

### App Audit & Protection

The Permissions feature lists apps grouped by the permissions they acquire. App Protection prevents unauthorized persons from launching protected apps, which require a password on launch. Protected apps remain unlocked for 60 seconds after the app is terminated.

### Call Filter

The app also provides a call and SMS filter, as well as a feature to hide sensitive contacts. Unfortunately, we could not test the call filter as it is not available for patch levels 2018-05-01 or later. The Hide Contacts feature seemed not to work correctly in our test, as we could still access hidden contacts in the Contacts app and see their call logs in the Phone app.

### Parental Controls

The app is equipped with extensive parental control features, with which the user can set up restricted and protected environments for children using the device. The Children's Corner is a restricted area with a child-oriented home screen powered by G Data. Here, the user can define whitelists/blacklists for websites the child can visit, select approved apps, and restrict the use of the device to specific locations at specific days and times. Further settings like switching off Wi-Fi, blocking incoming calls, and time limits for device usage are available. The Teenager Corner environment just restricts the access to approved apps and the device usage to specific locations and time intervals. Furthermore, it can use basic G Data functions.

### Conclusion

G Data provides a solid and well-programmed anti-malware app for Android. The focus on the anti-theft feature lies on SMS commands, as they can be issued even without an active network connection. However, a web interface is also provided, where the user can access and send anti-theft commands. All functions worked well, except for the Call Filter which we were not able to use with our test devices. We are very impressed by the parental control feature as it provides extensive options to set up protected device environments suited to children.

Anti-Theft Details		
Commands Web		
<b>Locate device</b>	✓	Displays current or last-known location on <i>Google Maps</i> map and sends email notification with link to <i>Google Maps</i> .
<b>Delete personal data</b>	✓	Triggers a factory reset and wipes external storage.
<b>Trigger signal tone</b>	—	Rings an alarm on the device. Alarm can be muted while locked, and is switched off when device is unlocked and app is launched.
<b>Mute device</b>	✓	Mutes the device.
<b>Lock screen</b>	✓	Locks the device with the pre-configured PIN.
<b>Set lock screen password</b>	✓	Changes the lock-screen password.
Commands SMS		
<b>Locate</b>	✓	Sends text message with coordinates of current location.
<b>Locate fine</b>	✓	As "Locate" command but more precise and takes significantly longer.
<b>Wipe</b>	✓	
<b>Ring</b>	—	
<b>Mute</b>	✓	As for the corresponding web command.
<b>Lock</b>	✓	
<b>Set device password</b>	✓	
<b>Remote password reset</b>	✓	As "Set device password" command, but must be sent from the registered phone number.
Additional Features		
<b>SIM Change Protection</b>	✓	Sends a message to the registered number and/or email address whenever the SIM card is changed. Additionally, locks the device.
<b>Headset Protection</b>	✓	Locks the device and rings an alarm whenever the headset is disconnected.



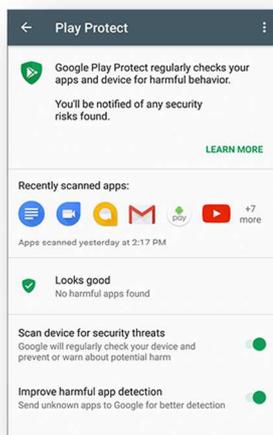
**Google**

Play Protect & OS Features  
10.7.19



## Introduction

Google's built-in malware protection for Android has been available on all Android devices with Google Play Services 11 or later since summer 2017. It checks apps and .APK files before they are downloaded and installed from Google Play or third-party sources. Furthermore, it constantly monitors the device and user data for harmful apps and other security threats. Besides the malware scan, Google provides anti-theft features via a web interface or the standalone app "Find My Device", protection against phishing websites included in Google Chrome, and text-message and call-blocking functions. Access to certain apps can be restricted by defining user profiles (for Android 5.0 or newer and some manufacturers only) and backups of data and apps can be created and uploaded to the Google account as well.



## Usage

Play Protect is preinstalled on all new Android devices and older devices can be upgraded via the Play Store. It can be found either inside the Play Store under the Menu and "Play Protect", or Settings → Google → Security → Google Play Protect.

## Anti-Malware

In Play Protect, the status of the device, a list of recently scanned apps as well as the date and time of the last scan is shown. Here, the user can start a new device scan manually and decide to send unknown apps to Google to improve detection of harmful apps.

## Anti-Theft

After login to the Google account, the anti-theft features are accessible using either the web interface ([android.com/find](http://android.com/find)) or the standalone app "Find My Device", which is preinstalled on new devices. Both variants allow the user to view the current or last-known location of the device, to trigger the alarm on the target device for up to 5 minutes, and to lock the device with a given PIN or the configured security mechanism (PIN, pattern, password). The alarm can be muted and turned off on waking up the screen e.g. by pressing the power button. Optionally, a message and/or a phone number to contact can be defined and displayed on the device lock screen. Finally, all data including the Google account can be removed permanently from the device.

### Anti-Phishing

Google Chrome contains a safe browsing feature, to detect phishing websites on the Internet and prevent the user accessing them.

### App Audit

With the introduction of run-time permissions in Android 6.0, the user gains more control over the permissions granted to/removed from individual apps. This option is accessible from “Apps” in the Android system settings.

On devices with Android versions 5.0 or newer, the user is able to create user profiles with which the access to certain apps can be restricted. However, this feature may be different for each device manufacturer or not even be available.

### SMS & Call Blocking

With the rollout of Android 4.4, Google added the text message and call blocking function to its Messages and Phone app, in order to protect the user against spams and unwanted calls. The user can decide to either block individual numbers or numbers from the contacts.

### Conclusion

In recent years, Google has continuously improved the security and threat protection for devices running Android OS. With Play Protect, they have developed built-in malware protection that automatically scans the device for any security flaws in the background. Recent and current Android devices have security-related features like anti-theft, safe browsing, and all device management tasks can be carried out using the Google account.

Anti-Theft Details		
Commands Web & App		
<b>Locate / Track</b>	✓	Displays location on <i>Google Maps</i> map.
<b>Secure Device</b>	✓	Locks the device with a given PIN or the pre-configured PIN, pattern, or password. Optional: Displays a message and/or phone number to contact.
<b>Erase Device</b>	✓	Triggers a factory reset immediately or after next device restart when offline and wipes external storage.
<b>Enable Secure &amp; Erase</b>	✓	Activates lock and erase mechanisms.



**Kaspersky Lab**  
Internet Security  
11.17.4



## Introduction

Besides a malware scanner, Kaspersky Internet Security provides other important security functions such as theft protection, call blocker, app lock, privacy, and web protection. The user can either start with a 30-days trial to test out all available features, or immediately update to the pro version of the app. Additional features like Secure Connection, Safe Kids, and Password Manager are offered in separate apps.



## Usage

On first start-up, the app requests permissions that are necessary for the initial configuration. After the EULA has been accepted, a first scan is started automatically, whereby the user is still able to use the application while it is running.

### Anti-Malware

The app offers many options to customize scan behaviour. It allows for scanning either all files, or apps and archives only. The user can decide between three different scan scopes to manually scan installed apps (Quick scan), the entire device (Full scan), or a selected folder (Folder scan). Infected files can be moved to quarantine, deleted, skipped, or the user can be prompted for action. Scheduled scans and database updates are configured by default to the recommended timetables, but can be adjusted to the user's desires.

If Real-Time Protection is enabled, the app performs 24/7 background monitoring of file activity and scans newly installed apps before initial execution. Here, the user can choose from "Extended" mode, which monitors all actions with files and installed apps, "Recommended" mode, which only checks installed apps and installation packages from the Downloads folder, or completely turning off real-time protection. Protection against adware or other harmful apps is enabled by default but it can be turned off by the user.

### Anti-Theft

In order to use this feature properly, the app requires several permissions, as well as device admin rights, and requires a secret code with 4-6 digits to be configured. SMS commands were completely removed in version 11.17.4 hence, the device can be remotely controlled using the web interface on *My Kaspersky* only.

Here, commands for Lock & Locate, Alarm, Mugshot, and Data Wipe can be executed only if they are enabled in the app first. In our test, the alarm could not be triggered if the setting “Do not disturb” was enabled. Kaspersky Lab promptly fixed this issue. Due to technical limitations in Android 4.4 and later, text messages can no longer be deleted using the Wipe Personal Data command. Kaspersky Lab have told us that they will make clear in the GUI that wiping data on an external SD card is done in two steps, and so might take some time to complete (depending on the card size). In the first step, data is deleted, and the second step makes the data unrecoverable. The user can establish a SIM Watch, which locks the device if the SIM is replaced or removed. Hot change of SIM is covered, as is protection against deinstallation of the app.

### Internet Protection & Text Anti-Phishing

Internet Protection scans websites and blocks dangerous websites accessed by the browser app installed on the device. Google Chrome is the only browser that is shown in-app as protected by default. The Text Anti-Phishing tool checks incoming text messages for links to malicious and harmful websites which could lead to theft of financial/private data.

### Privacy Protection & App Lock

With Privacy Protection, it is possible to hide sensitive contact data and conversation history. This switches off Google account synchronisation while Privacy Protection is active. The App Lock component protects apps against unauthorized access. To unlock a protected app, the previously configured secret code needs to be entered.

### Call & Text Filter

This tool blocks unwanted incoming calls. The app clearly states that text-message blocking does not work for devices with Android version 4.4 or later. The user can create respective whitelists and blacklists of blocked and allowed phone numbers, by manually entering phone numbers or importing them from the call/text-message logs.

### Conclusion

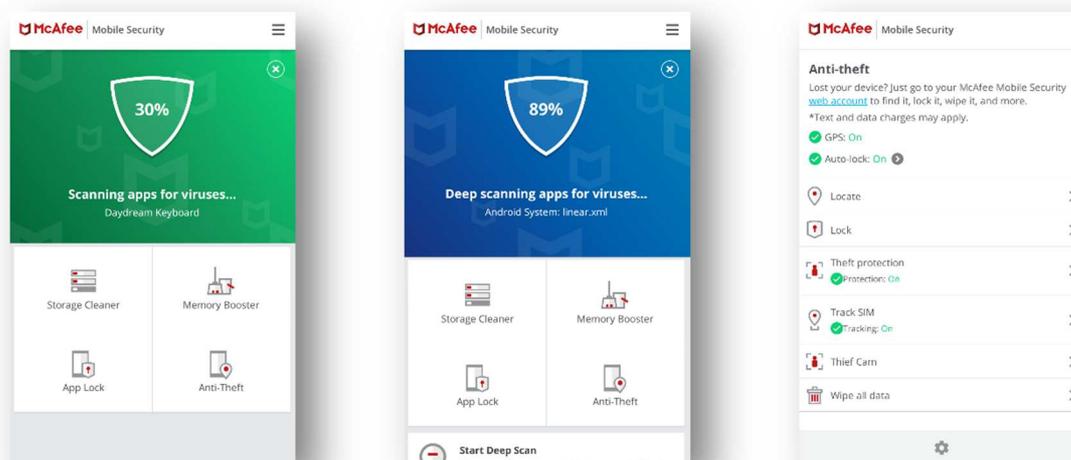
Kaspersky Lab’s product provides a great variety of features for mobile security in a clear user interface. A brief and helpful explanation is given on the very first use of every function and leaves no question unanswered. This product is recommended to users who like to keep it simple while also being protected effectively.

Anti-Theft Details		
Commands Web		
<b>Lock &amp; Locate</b>	✓	Locks the device, displays the location on <i>Google Maps</i> map, and sends the location in an email.
<b>Mugshot</b>	✓	Locks the device and takes several pictures using the front camera.
<b>Alarm</b>	✓	Locks the device and rings an alarm.
<b>Wipe Personal Data</b>	✓	Removes contacts, call log, calendar entries, and files on internal and external storage. Sync for the Google account is turned off.
<b>Wipe All Data</b>	✓	Triggers a factory reset and wipes external storage.
<b>Hide Data</b>	✓	Hides contacts listed as sensitive in the Privacy Protection.
Additional Features		
<b>SIM Watch</b>	✓	Locks the device if the SIM card is removed or replaced. Sends a text message with the new phone number to an alternate phone number specified in the Anti-Theft settings.
<b>Uninstall Protection</b>	✓	Locks the device if device administrator rights are removed from the app.



## Introduction

McAfee has released a brand-new version of its Mobile Security app, with a lot of visual and functional improvements. It still comes in a free and a premium version (with a 30-day free trial) and provides an extensive selection of components for malware protection, theft protection, privacy control and web security, as well as additional tools for power/memory management and backups. We strongly recommend creating a McAfee account in order to use the full potential of all security and privacy features. An upgrade to the premium version removes ads, allows to also backup photos and videos, and to access the McAfee's premium 24/7 phone support service.



## Usage

After accepting the EULA and an initial configuration, the user is asked to grant the app all required permissions to modify and monitor the device. The user can then either continue with the free and ad-supported version, or upgrade to the premium version instantly using his or her McAfee account. The main screen has received a nice visual update since the last test, and shows the most important features.

### Anti-Malware

Users can scan either apps only, or start a deeper scan of apps, messages, and internal files with pre-defined settings. The scan settings can be adjusted to toggle and schedule real-time scans and automatic updates.

Furthermore, the user can decide if all apps, potentially unwanted programs, text and multimedia messages, as well as files in both internal and external storage should be scanned. The app can also warn the user when malicious apps are installed or malicious files are transferred to the SD card.

### Anti-Theft

A McAfee account and all the necessary permissions for the device are required to use this feature. Anti-theft commands like Locate, Lock, Alarm, and Wipe can be sent using the web interface exclusively. SMS commands were completely removed. The alarm can be muted and turned off by pressing the on-display button or volume button on the device.

The web interface is basically divided into two parts, which makes it rather confusing. “Find device” has a modern web view that provides a map and anti-theft commands, allowing the user to take action immediately when a device is lost or stolen. “My device” and “My data” also have a legacy page that supports the basic anti-theft commands, further options to wipe and factory reset the device, and access to the backup data.

“Backup and Wipe” is evidently supposed to back up data and then wipe it from the device. The user can decide what action should be performed if the backup fails due to a network connection loss. A separate backup of text messages is supported, but not in combination with the wipe, which we find rather strange. The app and the web interface both state that the Wipe function will remove data such as contacts, call log, and media files, from a SD card or storage card. However, we find the latter misleading and strongly suggest McAfee to improve this wording, as the wipe feature only supports internal mounts/phone storage.

### Safe Web

The Safe Web component shows a list of supported browsers for which the user can enable/disable protection against dangerous websites.

### Privacy

The app contains several features regarding privacy. The Privacy Check rates apps based on how much personal information they access and shows details of this. The App Lock feature locks certain apps with the pre-defined 6-digit PIN. By activating the Kids Mode, the user can select apps that should be accessible for the pre-defined, restricted Kids profile. The Call Blocker maintains lists of allowed/blocked incoming and outgoing calls. However, blocking incoming calls did not work even with option “Block All Filter”. McAfee is currently investigating this issue.

### Performance & Backup

Tools for improving the power and performance of the device are included, such as Storage Cleaner for removing junk/temporary files, a memory booster that frees up RAM, a battery booster that extends battery life time by turning off device settings (e.g., Wi-Fi, auto sync, screen timeout), and a monitoring tool for tracking mobile data usage of apps. The app can save private data (text messages, call logs, and contacts) to the cloud and restore this data. It is possible to activate automatic backups or to be notified when there is a new contact or message to back up. In the premium version, it is also possible to back up media files.

### Conclusion

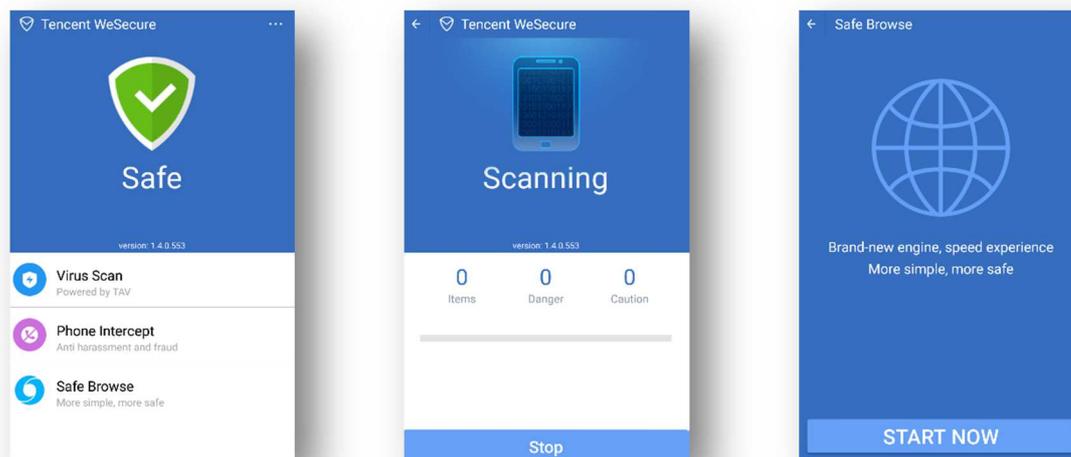
McAfee’s security product is largely well-designed and equipped with a comprehensive anti-theft component plus additional features to optimize the device’s performance and to backup data. All provided anti-theft features work as intended and users are able to backup and wipe in one go. Finally, we feel that the web interface, which is still split up into two separate pages, remains counter-intuitive.

Anti-Theft Details		
Commands Web		
<b>Locate</b>	✓	Displays location on <i>Google Maps</i> map.
<b>Lock</b>	✓	Locks the device with or without alarm.
<b>Thief Cam</b>	✓	Plays an alarm, shows a popup message, and takes a snapshot of the thief.
<b>I lost my device</b>	✓	Triggers lock, locate, and thief cam; if the phone is set to a <i>lost</i> state, the additional functions <i>track</i> , <i>backup</i> , <i>wipe</i> and <i>reset</i> can be used.
<b>Track</b>	✓	Tracks the phone for one or six hours continuously.
<b>Backup</b>	✓	Backs up personal data. Backup of media files is only possible in-app.
<b>Wipe</b>	✓	Deletes contacts, photos, videos, call log and files on internal storage.
<b>Reset</b>	✓	Triggers a factory reset and wipes external storage.
Additional Features		
<b>SIM Change Protection</b>	✓	Locks the device and notifies the user via email if the SIM card is changed.
<b>Uninstall Protection</b>	✓	Locks the device if device administrator rights are removed from the app.
<b>Capture Cam</b>	✓	Takes an automatic snapshot when the wrong login credentials are provided for the Android or McAfee lock screen.



## Introduction

Tencent's WeSecure is an easy-to-use application that is free to use, but nonetheless ad-free. Its core features include a virus scanning tool and automated phone-number blocking. Additional functionality like Safe Browse and Data Backup is offered via external tools.



## Usage

Upon opening the application for the first time, the user is prompted to agree to the Terms of Service and the Privacy Statement. Accepting everything takes the user to the main screen. Here the protection status of the device and version number are displayed.

### Virus Scan

When scanning the device, the user has the choice between doing a "Quick Scan", which only scans installed apps, or a "Full Scan" which includes all other files. Both of these scan the internal device storage as well as external storage media. Updates to the virus database are applied automatically in the background.

### Phone Intercept

This feature attempts to automatically block fraudulent or harassment calls. The ruleset by which this is done is based on Chinese phone numbers and allows no further customization.

### Safe Browse & Data Backup

The Safe Browse tool must be downloaded from a 3rd party source, requiring the user to manually enable installations from all unknown sources. It additionally requires permission to access the phone's Storage and Location and only supports Chinese language.

Likewise, the Data Backup tool must also be downloaded separately. It requires access to System Setting, Camera, Location, Phone, SMS and Storage. After setting up it allows the user to backup contacts, text messages and call logs in the cloud.

## Conclusion

Tencent WeSecure is a free and straightforward anti-malware solution which can be readily extended by downloading additional tools. While it does not provide anti-theft functions, users can rely on the built in anti-theft features of Android.

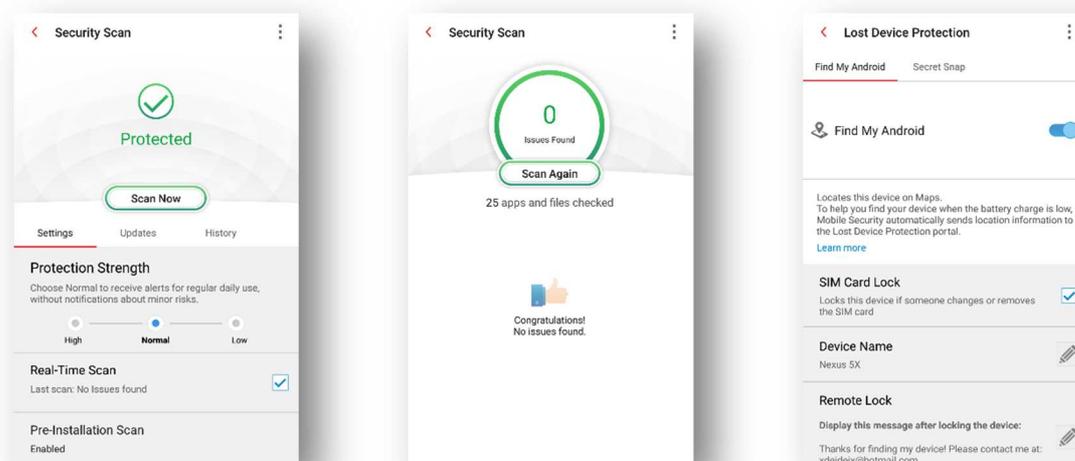


**Trend Micro**  
Mobile Security  
9.5.2



## Introduction

Trend Micro's app has free and pro versions. The former offers malware protection, system optimization and social media privacy tools, while the latter adds a wide range of additional security features including anti-theft, app locking and a call blocker. The pro version can be tried free of charge for 14 days, after which a monthly or yearly subscription is required.



## Usage

After installation, the user is asked to accept the Terms and Conditions as well the Privacy Statement. The app then asks for permission to collect data about installed apps and blocked websites, in order to improve their service. Next, the user is taken to the app's home screen, where he or she can either sign in to an existing Trend Micro account or create a new one. This screen makes all features readily accessible.

## Security Scan

The first scan is started in the background immediately after opening the app. There are three different scan settings available, which determine the level of threats the user will be notified about: high, medium, or low. Per default, only installed apps are scanned, but there is an option to include all other files as well.

Further options like real-time scanning, pre-installation scanning of apps downloaded from Google Play, as well as scanning external storage, can be chosen by the user. Updates and scans are performed automatically, but can be scheduled to run daily, weekly or monthly. In addition to the malware scan, the device's configuration and settings are also checked for possible vulnerabilities.

## Lost Device Protection

This tool provides anti-theft functionality for the device. It works in conjunction with a web interface that is accessible from the user's Trend Micro account, and from which remote commands can be sent to the protected device. In addition, the phone can automatically be locked on SIM change or removal, a photo will be taken with the front camera after a certain number of unsuccessful unlock attempts, and uninstalling the app will require a password.

The Partial Remote Wipe function did not work fully as described in the web interface. The contents of the SD card were left intact during our testing. Trend Micro informed us that they will remove the Partial Remote Wipe function in one of their next app updates. However, performing a Full Remote Wipe did wipe the external storage as expected.

### Network & Messenger Protection

The Safe Surfing feature monitors visited URLs and blocks malicious or fraudulent websites, with protection settings configurable either as high, normal, or low. The user can also set up both a blacklist and whitelist of websites that will always be blocked or allowed respectively. A Wi-Fi scanning feature allows checking the currently connected network for vulnerabilities and risks.

The Safe Surfing feature can also be extended to text messages, where it will scan message content for dangerous URLs. This feature shares the settings of the network protection features and currently supports the following messenger apps: Messages, WhatsApp, LINE, Messenger.

### Parental Controls

Parental Control allows selectively locking apps using either a PIN, a pattern, or the Trend Micro account password. In addition, a website filter blocks pages inappropriate for children. The filter can be configured to block sites for either children, preteens, or teens, and allows setting up a black- and a whitelist of websites.

### Call Blocking

This component allows blocking incoming phone calls according to one of three rules: blocking only blacklisted callers, allowing only approved callers, or allowing approved and anonymous callers. Blocked calls can either be rejected or silenced for the duration.

### Additional Features

In addition to the features listed above, the app contains a System Tuner to optimize phone performance, a Social Network Privacy component that checks Facebook settings for possible privacy issues, and an App Manager that allows the removing and disabling of apps to save resources.

### Conclusion

Trend Micro Mobile Security comes with a variety of security features that help to protect and manage the device. The user interface is clean and not overloaded with functions, and the web interface provides all necessary anti-theft commands.

Anti-Theft Details		
Commands Web		
<b>Locate / Track</b>	✓	Displays location on <i>Bing Maps</i> map.
<b>Lock</b>	✓	Locks the device until either the Trend Micro password or a one-time unlock key from the web interface is entered.
<b>Full Remote Wipe</b>	✓	Triggers a factory reset and wipes external storage.
<b>Alarm</b>	⚠	Sounds an alarm from the device which can be muted.
<b>Share Location on Facebook</b>	✓	Creates a post with a link.
<b>Reset</b>	✓	Forces all apps to stop or resets lock screen password.
Additional Features		
<b>SIM Change Protection</b>	✓	Locks the device if the SIM-card is changed or removed; device is unlocked automatically if the original SIM is inserted again.
<b>Uninstall Protection</b>	✓	Locks the device on uninstallation; part of the Parental Controls component.

Feature List Android Mobile Security (as of July 2018)	FREE	FREE	COMMERCIAL	FREE	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	COMMERCIAL	FREE	COMMERCIAL
Product Name	Android OS	Alibaba Ali Money Shield	Avast Mobile Security & Antivirus	AVG AntiVirus for Android	Avira Antivirus Security Pro	Bitdefender Mobile Security & Antivirus	F-Secure SAFE	G DATA Internet Security	Kaspersky Internet Security	McAfee Mobile Security	Tencent WeSecure	Trend Micro Mobile Security
Version Number	8.1	5.8	6.11	6.10	5.2	3.3	17.4	26.4	11.17	5.0	1.4	9.5
Supported Android versions	built-in	4.0 and higher	4.1 and higher	4.1 and higher	4.4 and higher	4.0 and higher	5.0 and higher	4.1 and higher	4.1 and higher	4.1 and higher	4.2 and higher	4.0 and higher
Supported Program languages	All	Chinese	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, Ukrainian, Urdu, Vietnamese	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, Ukrainian, Urdu, Vietnamese	Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Malaysian, Portuguese, Russian, Spanish	Czech, Dutch, English, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Thai, Turkish, Vietnamese	Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Lithuanian, Norwegian, Romanian, Russian, Chinese, Slovenian, Spanish, Swedish, Turkish, Vietnamese	Arabic, Chinese, Dutch, English, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, Spanish, Turkish	English, Russian, German, French, Italian, Spanish, Portuguese, Turkish, Polish, Hungarian, Norwegian, Dutch, Swedish	Arabic, Bulgarian, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Spanish, Swedish, Thai, Turkish, Vietnamese	English, Chinese	Chinese, Dutch, English, French, German, Hebrew, Italian, Korean, Portuguese, Spanish, Turkish, Vietnamese
<b>Anti-Malware</b>												
On-Install scan of installed apps	•	•	•	•	•	•	•	•	•	•	•	•
On-Demand scan	•	•	•	•	•	•	•	•	•	•	•	•
On-Access scan for apps	•	•	•	•	•	•	•	•	•	•	•	•
Scan requires online cloud connection	•					•						
Automatic (scheduled) Scan			•	•	•	•	•	•	•	•	•	•
Scan installed apps for (possible) privacy violations	•		•	•	•	•	•	•	•	•	•	•
Recommendations for Android settings	•	•	•	•	•	•	•	•	•	•	•	•
Safe Browsing (Anti-Phishing & Anti-Malware)	•		•	•	•	•	•	•	•	•	•	•
Supported browsers (Safe Browsing)	Google Chrome		Google Chrome, Firefox, Opera, UC Browser, Dolphin	Google Chrome, Firefox, Opera, Dolphin, UC Browser	Google Chrome, Firefox, Opera	Google Chrome, Dolphin, Firefox, Opera Mini, Opera, Samsung Internet	Google Chrome	Google Chrome	Google Chrome, Boat Browser, Opera Mini	Google Chrome		Google Chrome, Samsung Internet
<b>Anti-Theft</b>												
Remote Locate, Lock & Wipe	•		•	•	•	•	•	•	•	•		•
Webinterface for controlling Anti-Theft features	•		•	•	•	•	•	•	•	•		•
Notify on SIM Change (Email / SMS)			•			•			•	•		
Lock on SIM Change			•						•	•		•
SMS commands for controlling Anti-Theft features			•	•		•			•	•		
Remote Unlock			•	•	•				•	•		
<b>Anti-Spam</b>												
Whitelist / Blacklist Phonecalls		•	•	•	•				•	•	•	•
Whitelist / Blacklist SMS		•				•			•	•	•	•
Whitelist / Blacklist with wildcards			•	•					•	•	•	•
Blocking of SMS containing keywords		•							•	•	•	•
<b>Parental Control</b>												
Lock Apps		•	•			•	•	•	•	•	•	•
Safe Webrowsing (content filtering)						•	•	•	•	•	•	•
<b>Authentication</b>												
Uninstallation protection (password required for uninstallation)			•		•	•	•	•	•	•	•	•
Settings protected with password			•			•	•	•	•	•	•	•
User Account needed to use product	•				•	•	•	•	•	•	•	•
<b>Additional features</b>												
Task Killer	•		•	•							•	•
Battery Monitor	•		•	•							•	•
Network monitor			•	•							•	•
Backup	•										•	•
Local Wipe	•								•	•		
<b>Support</b>												
Online Help & FAQ	•		•	•	•	•	•	•	•	•	•	•
Email support		•	•	•	•	•	•	•	•	•	•	•
User Forum	•		•	•	•	•	•	•	•	•	•	•
User Manual	•	•			•	•	•	•	•	•	•	•
Phone Support					•	•	•	•	•	•	•	•
Online Chat						•	•	•	•	•	•	•
Supported languages of support	All	Chinese	English, Czech, Spanish, Portuguese, German, French, Japanese, Russian	Czech, English	Chinese, Dutch, English, French, German, Italian, Japanese, Korean, Malaysian, Portuguese, Russian, Spanish	English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish	Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Swedish	Chinese, Dutch, English, French, German, Italian, Japanese, Polish, Portuguese, Spanish	English, French, German, Italian, Portuguese, Russian, Spanish	Chinese, Czech, Danish, Dutch, English, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Swedish, Thai, Turkish, Vietnamese	Chinese, English	English
<b>Price (may vary)</b>												
Price 1 Android / 1 year (USD/EUR)	FREE	FREE	USD 8 / 8 EUR	FREE	USD 10 / 8 EUR	USD 15 / 10 EUR	USD 18 / 15 EUR	USD 16 / 16 EUR	USD 15 / 11 EUR	USD 30 / 30 EUR	FREE	USD 36 / 20 EUR

## Copyright and Disclaimer

This publication is Copyright © 2018 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 (August 2018)