

Independent Tests of Anti-Virus Software



Mobile Security Review 2019

TEST PERIOD: JUNE- JULY 2019
LANGUAGE: ENGLISH
LAST REVISION: 22ND JULY 2019

WWW.AV-COMPARATIVES.ORG

Contents

INTRODUCTION	3
GOOGLE ANDROID	4
PROTECTION AGAINST ANDROID MALWARE	6
AVC UNDRROID ANALYZER	6
SECURITY FEATURES	7
PRODUCTS TESTED	8
OVERVIEW	9
MALWARE TEST SET & RESULTS	10
BATTERY DRAIN TEST RESULTS	11
AVAST	12
AVG	14
AVIRA	16
BITDEFENDER	18
F-SECURE	20
G DATA	22
GOOGLE	24
KASPERSKY	26
MCAFEE	28
SECURION	31
TREND MICRO	32
FEATURE LIST	34
COPYRIGHT AND DISCLAIMER	35

Introduction

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

In January 2019, we conducted a malware protection test¹ with 250 Android security apps. One purpose of this test was to distinguish genuine and effective apps from dubious/ineffective ones, and it used highly prevalent malware from the previous year. The test described in this report was much more in-depth and demanding, as it used very recent malware samples, and also investigated additional security features and battery drain. Consequently, it allowed the tested apps to demonstrate their effectiveness against current threats, along with their all-round security capabilities and performance.

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

On the following pages, we summarise the new features and changes in the latest operating system version *Android Pie*, and discuss the restrictions that were introduced in the Google Play Developer Policy in October 2019, which are crucial for the future development of Android apps. Furthermore, we will argue why it is not advisable to rely only on the built-in malware protection provided by Play Protect, but instead install a third-party anti-virus app. After that, we talk about the current risks facing smartphone users, and give recommendations for achieving better protection. At the end of the introduction, we give a short summary of common security features and main sub-components of typical Android security apps. In the main section of this report, we present the participating security products, along with the results of the malware protection tests, the battery drain test, and the detailed reviews of the individual products. For a product's anti-theft component, we comment on each function briefly and use the following symbols in the table to indicate how well it worked in our tests.



no issues



minor issue(s)

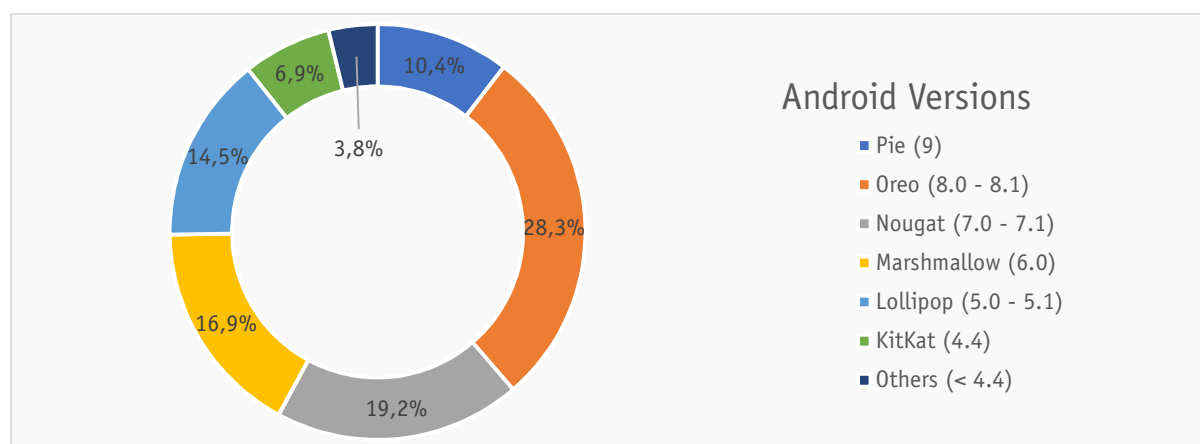


major issue(s)

¹ <https://www.av-comparatives.org/tests/android-test-2019-250-apps/>

Google Android

With the introduction of run-time permissions in Android 6.0 (Android Marshmallow), Google started to give the user more control over which information and private data is shared with, or exposed to, individual apps installed on his or her device. Also, apps were prevented from removing existing accounts, such as the main Google device account, from the phone. Android Marshmallow still runs on about 17% of all Android devices worldwide as the ring chart of Android versions in May 2019 below shows².

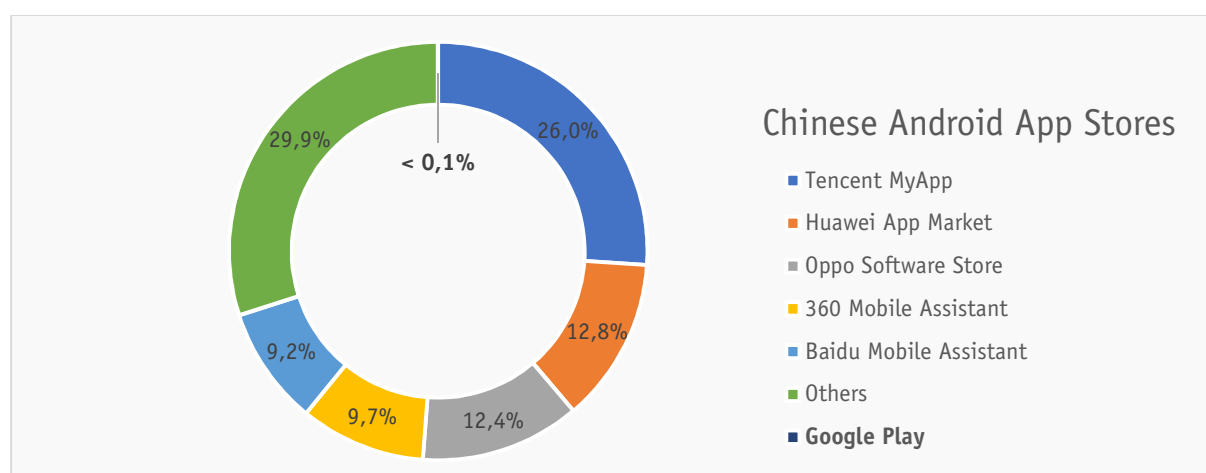


Since Android 8.0 (Android Oreo), notifications must be specifically assigned to notification channels in order to receive app notifications on the device. The global security setting “Install from unknown sources” became a run-time permission that needs to be granted for each app once. In addition, *Play Protect* is preinstalled on devices running Android 8.0 or later, to provide current Android devices with built-in malware protection. Since August 2017, Play Protect has also been available on older Android devices with Google Play Services 11 or later installed. It checks apps and APK files when they are downloaded from Google Play or third-party sources and constantly monitors the device and all installed apps for any signs of malware. Functions for device loss (*Find My Device*) and safe browsing (for Google Chrome) were integrated as regular components as well. Android Oreo runs on about 28% of all Android devices. In August 2018, Android 9 (Android Pie) was officially rolled out, and included behaviour changes and improvements regarding power management, privacy (e.g., restricted access to call logs, phone numbers, Wi-Fi location and connection information), and security (e.g., cryptographic algorithms). Currently, Android Pie is only installed on every tenth device (10.4%). In October 2018, new restrictions were added to the Google Play Developer policy³ that influence future Android app development. Apps are no longer allowed to access the call log or SMS log on Android devices. They must be actively registered as the default Assistant, Phone, or SMS handler in order to request the necessary permissions (e.g., `READ_CALL_LOG`, `WRITE_CALL_LOG`, `READ_SMS`) and to retrieve the aforementioned data. Violation of the policy may lead to the app being removed from Google Play. These changes were noted and taken seriously by those anti-virus vendors who updated their mobile security products, or completely removed the affected features from their apps. More information can be found in the upcoming chapter “Security Features” and the single product reviews. At that point, one might think that third-party anti-virus apps are no longer so important for Android devices, due to Google’s built-in malware and protection features. However, this can only be true for Android devices that have installed Google Play and Services along with Play Protect.

² <https://developer.android.com/about/dashboards>

³ <https://play.google.com/about/privacy-security-deception/permissions/>

Other devices based on modified Android OS versions (e.g., FireOS, LineageOS) do not run Google apps by default; hence, there is no built-in malware protection. In regions such as the United States and Europe, only two official app stores dominate the mobile app market: Google Play and Apple App Store. The risk of inadvertently downloading and installing malware from Google Play is very small, as the app store is regularly checked for fraudulent and dangerous apps. However, in many Asian countries, especially China, the risk of being infected by malware is much higher. There are many app stores provided by various third-party vendors, and many smartphones are rooted as well. Furthermore, over 787 million of China's total population of 1.4 billion use mobile devices, and about 75% of them run Android as the operating system⁴. The most-used Android app stores are shown in the ring chart below. With a market share of about 26%, Tencent MyApp is by far the most widely used app store, whereas Google Play lags far behind, and is used by almost no one (<0.1%). This is because Google Play and most of Google's services are inaccessible in mainland China.



This year's test results show that Google Play Protect performed better than last year (although with a higher rate of false alarms). However, it still lacks effective and sufficient malware protection. It surely has the potential to become better in the future, as Google has the data and resources to improve its algorithms. 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.

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

⁴ <https://www.appinchina.co/>

Protection against Android malware

Cyber-attacks on mobile devices are becoming more and more sophisticated, with fraudulent applications attempting to steal users' data or money. To reduce the risk of this happening, we suggest you follow the advice given here. Only download apps from official app stores like Google Play or stores of reputable app makers; avoid third-party stores and side-loading⁵. Assess requests for irrelevant access rights or permissions by questionable apps critically. Of course, not every app that shows strange behaviour is necessarily malicious, but it is good to consider whether it is genuine and worthy of use.

A quick look at the reviews in the app store before installing an app might help. Avoid apps with predominantly bad or dubious reviews. Rooting the smartphone increases the potential that malicious apps will take control of the device. Furthermore, it is not legally clear-cut for some manufacturers whether the warranty is still valid if the phone is rooted. Public Wi-Fi networks (e.g., coffee shop, airport) are popular targets for attackers to steal and comprise sensitive data.

Whenever connecting to a potentially risky Wi-Fi hotspot, we suggest using a secure VPN connection. Always be careful with sensitive data (user credentials, Wi-Fi passwords, bank/credit card information, etc.) that should not be shared with others.

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

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

However, we must point out that "low risk" is not the same as "no risk". The threat situation can change quickly and dramatically. It is better to be ready for this, and to install appropriate security software on the smartphone. Currently, we would say that in western countries, protection against data loss in the event of the phone being lost or stolen is more important than malware protection.

AVC UnDroid Analyzer

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



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

⁵ <https://en.wikipedia.org/wiki/Sideloadng>

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* which protects the user against the inadvertent installation of malicious apps on his or her device. Like anti-virus programs for Microsoft Windows, mobile security apps for Android use a number of different protection features. The *real-time protection* checks new apps during the setup process. This prevents the device being compromised by the installation of a malicious program.

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

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

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

Usually, the anti-theft component is controlled via a web interface, or (rarely) using a second phone that has the same security app installed. As the call log and text messages are no longer accessible (see chapter "Google Android"), anti-theft commands sent via SMS and other features that are related to accessing this data (e.g., call/SMS filter, text anti-phishing, SMS notifications, call log/SMS backups) are no longer fully supported by Android security apps. Vendors have either completely removed the affected features from their apps or kept them with only limited functionality.















































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

A *privacy advisor* is also included in some of the tested products, which typically scans the installed apps for possible privacy violations. In other words, apps are analysed for uncommon, unnecessary, or inappropriate app permissions, such as access to contacts, calendar, files on internal storage, GPS position, or the camera, which could lead to the user's private sphere being breached. As a result of this scan, some security products advise the user to uninstall "risky" apps.

Products tested





The products included in this year's test and review are listed below. We congratulate the third-party security vendors, who have demonstrated in this test that their solutions are effective and reputable, and helped to raise the standard for all mobile security solutions.

The latest products⁶ were taken from the Google Play Store at the time of the test (June 2019). After the products were tested, manufacturers had the opportunity to fix any flaws we found. Any problems that have already been solved are noted in the report.

Vendor	Product Name	Version	Features
 Avast	Mobile Security	6.21	   
 AVG	AntiVirus	6.19	   
 Avira	Antivirus Security	5.8	   
 Bitdefender	Mobile Security	3.3	   
 F-Secure	SAFE	17.6	   
 G DATA	Internet Security	26.5	   
 Google	Play Protect & OS Features	15.3	   
 Kaspersky	Internet Security	11.23	   
 McAfee	Mobile Security	5.2	   
 Securion	OnAV	1.0	   
 Trend Micro	Mobile Security	10.3	   

Symbols

To provide a simple overview of the features of a product, we use the same symbols as those on our website. At the beginning of every report, you will see these symbols; those in orange represent features the product has, while those in grey represent features that are not included. All symbols apply to Android 9.0 only, which we used in our test.

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

⁶ <https://www.av-comparatives.org/list-of-mobile-security-vendors-android/>

Overview

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

Ten of this year's products qualify for our "Approved Mobile Product" award, by providing reliable and effective core functions and solid malware protection.



Avast Mobile Security provides well-developed security features and device monitoring tools as well as app customizations which leave no wishes unfulfilled.



AVG AntiVirus offers a wide range of security and non-security features along with extensive configuration options for almost any use case.



Avira Antivirus Security is a solid anti-malware app for Android that provides a clean user interface and remote device control using web or in-app commands.



Bitdefender Mobile Security is an easy-to-use mobile security product which provides elaborated device protection and further privacy features.



F-Secure SAFE is an anti-malware solution developed for several platforms that adds safe browsing via a separate browser app and parental control rules.



G DATA Internet Security provides a robust anti-malware app for Android with additional safe browsing, app protection, and parental control features.



Google Android includes built-in security features for malware detection, device loss or theft, and safe browsing for free. However, Play Protect does not yet provide effective protection.



Kaspersky Internet Security is a comprehensive and easy-to-use mobile security app with a broad range of features including anti-malware, anti-theft, and anti-phishing.



McAfee Mobile Security comprises basic protection functions for every use case including anti-malware and anti-theft as well as several tools to optimize device performance.



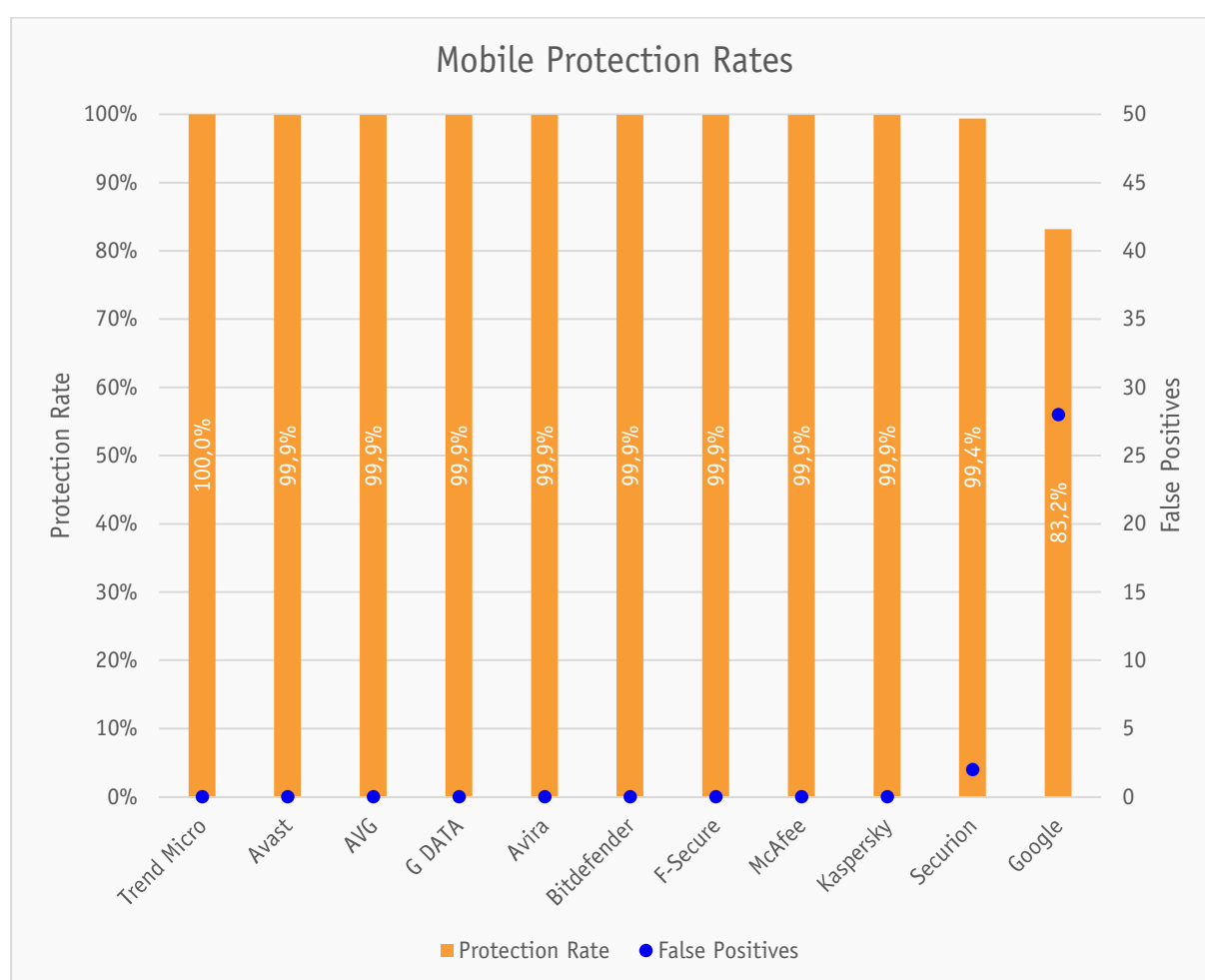
Securion OnAV is a very basic mobile security app with focus only on malware protection.



Trend Micro Mobile Security is a well-developed app offering malware protection, anti-theft commands via a neat web interface, and other helpful features for device management.

Malware Test Set & Results

The malware used in the test was collected by us in the few weeks before the test. We used **3,601** malicious applications, to create a representative test set. Apps with the same certificates and/or the same internal code were removed, in order to have a test set of genuinely unique samples. So-called "potentially unwanted applications" (PUA) were excluded. The security products were updated and tested on the 25th June 2019. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of APK files. An on-demand scan was conducted first. After this, every undetected app was installed and launched. We did this to allow the products to detect the malware using real-time protection. A false-positives test was also carried out by downloading 500 popular apps from various popular app stores. The results can be seen below (sorted by Malware Protection and number of False Alarms; products with identical scores are sorted alphabetically).



Mobile Protection Rates		
	Protection Rate	False Positives
Trend Micro	100%	0
Avast, AVG, Avira, Bitdefender, F-Secure, G DATA, Kaspersky, McAfee	99.9%	0
Securion	99.4%	2
Google	83.2%	28

Battery Drain Test Results

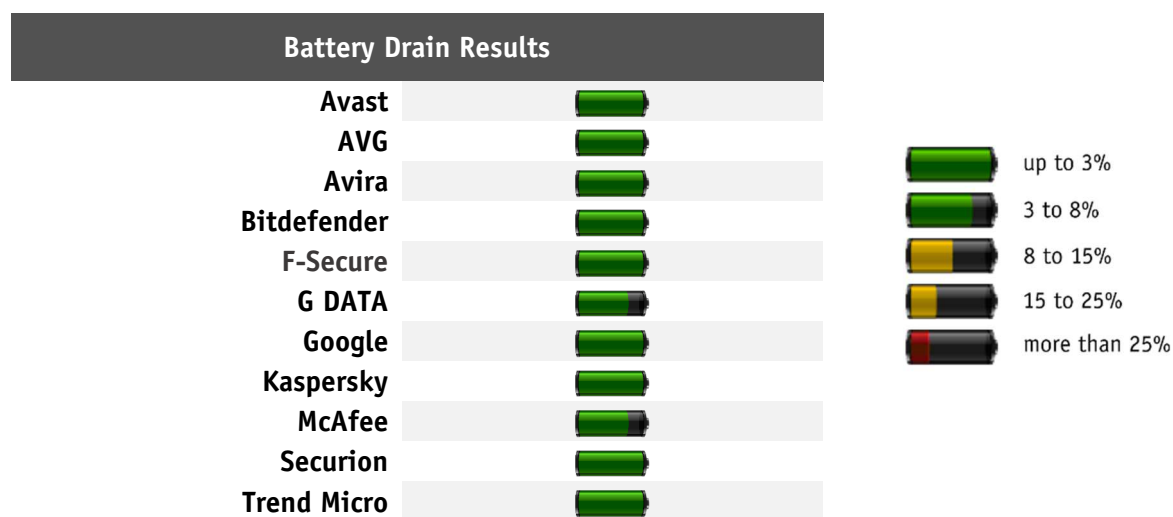
As in our previous reports, we measured the additional power consumption of an installed mobile security product. Testing the battery usage of a device might appear to be very straightforward at first glance. If one goes into more detail, the difficulties become apparent. Particularly with mobile phones,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

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

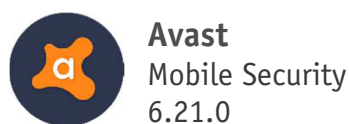
The test determined the effect of the security software on battery use for the average user. The following daily usage scenario was simulated:

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

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

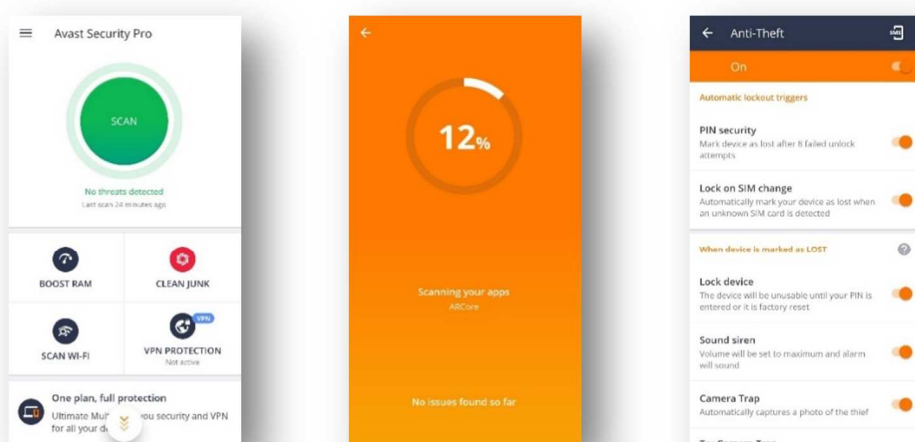


In general, we were able to give the tested security suites high marks regarding power usage. Two products in this year's test showed a slightly increased battery drain: **G DATA** and **McAfee**.



Introduction

Avast Mobile Security gives the user a good level of overall protection with important security features, including malware scan, Wi-Fi security, app audit, a photo vault, and a firewall feature. The free, ad-supported version comes with a 14-day trial to test the premium features such as anti-theft and app locking. Other, non-security related features are provided as well, aimed at improving device performance and monitoring data usage.



Usage

After accepting the EULA and Privacy Policy, the user is asked to either stay on the free and ad-supported version, or upgrade to the pro version immediately with a yearly or monthly subscription. After that, the main screen of the app shows up.

Anti-Malware

The malware scan is kept very simple, as all options to adjust the scan process are hidden in the app settings. First, the device is checked for any vulnerabilities, and an app-only scan is started afterwards. From the settings, the user can decide if files in the internal storage should be scanned in addition. A custom file/folder scan can be triggered from the menu via File Scanner. Protection against malicious apps and files, PUAs, as well as apps with a poor security level, is enabled by default. Furthermore, scans can be scheduled for any day and time.

Anti-Theft

Anti-theft commands can be sent from the web interface only. In the initial setup, the user has to configure an app-specific PIN, pattern, or fingerprint (if supported by the device), and an Android lock screen. Pictures taken of the thief, and recorded audio, can be downloaded from the web interface, or optionally uploaded to Google Drive. After 8 failed unlock attempts or when the SIM card is changed, the device is automatically set to a lost state, which triggers actions like Locate, Lock, Siren, and Camera Trap.

In the settings of the web interface, the Avast PIN, protection behaviour (lock phone, siren on lock), and lock screen text can be changed. However, it is still not obvious to first-time users how to find all backup files. They are in fact hidden behind the "Info" button and the "Notifications" tab.

Web, Wi-Fi & VPN Protection

Advanced web protection for various browsers needs to be activated first in order to protect the user against phishing websites. The app provides tools to scan and monitor Wi-Fi networks for security threats, and to test the speed of the currently connected Wi-Fi network. A VPN feature is also included to protect online activity from eavesdropping. However, it is only available for devices with an Ultimate or Ultimate Multi subscription.

App Audit

The App Permissions feature from earlier app versions is now part of App Insights. It categorizes the installed apps into three permission groups (high, average, low). The user can view detailed information about a specific app, such as usage of memory, battery, and mobile data, as well as the granted permissions. Furthermore, App Insights shows general statistics about app usage, monitors mobile data usage of apps, and alerts if the configured data limit is exceeded.

Additional Features

The App Locking feature restricts access to selected apps by locking an app with the Avast PIN, pattern, or fingerprint. The timeout for how long an app is unlocked can be configured in the settings. If photos are moved to the Photo Vault, they are encrypted and hidden for other users. Finally, Avast offers a Firewall (for rooted Android devices), which blocks Internet access for individual apps.

Conclusion

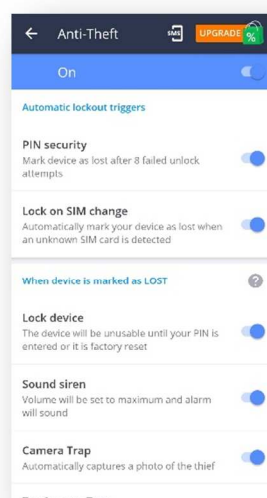
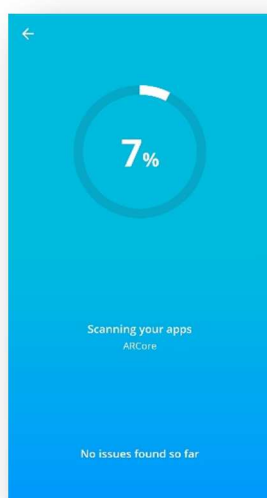
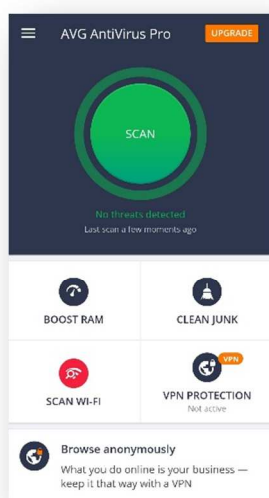
Avast provides an app with a comprehensive set of security functions, tools for optimizing and monitoring the device's performance and activity, and additional features. The user-friendly interface discreetly hides away all configuration options, and the tools are self-explanatory. The anti-theft commands worked flawlessly in our functionality test.

Anti-Theft Details		
Commands Web		
Locate	✓	Displays location on <i>Google Maps</i> map. Tracking the device can be enabled.
Mark as Lost	✓	Triggers configured actions like tracking, lock, siren, and camera trap.
Siren	✓	Activates/deactivates the phone siren.
Lock	✓	Locks/unlocks the phone.
Wipe	✓	Triggers a factory reset and wipes external storage.
Record Audio	✓	Records audio for a pre-defined duration of 1-5 minutes.
Take Picture	✓	Takes a picture with the front camera. Optional: The camera is triggered when the screen is turned on the next time.
Get Data	✓	Backs up contacts from the device in HTML format.
Message	✓	Sends and shows an on-screen message on the device.
Call	✓	Initiates a hidden phone call on the device to a given phone number.
Additional Features		
SIM Change Protection	✓	Sets the phone status to lost.
Camera Trap	✓	Takes a picture with the front camera.



Introduction

AVG provides a wide range of security features, among them malware scan, web protection, plus app and Wi-Fi checks, and a photo vault. The free version is ad-supported and comes with a 14-day trial of the pro version, which includes anti-theft and app locking. Further functions improve device performance, e.g. free up memory, delete temporary files, extend battery life, and monitor app and mobile data usage. A firewall feature allows selective control of Internet access on rooted devices.



Usage

After installation, the user must accept the Terms of Service and Privacy Statement. Next, the user can either upgrade to the pro version via an annual or a monthly subscription, or continue with the free and ad-supported version. On the app's main screen, the device status and important functions can be found.

Anti-Malware

Besides scanning all installed apps and the internal storage for malware, the app also checks the device's settings for vulnerabilities, and gives recommendations on how to remedy any that it finds. The scan settings can be adjusted to toggle the real-time protection, schedule automated daily scans, treat PUA as malware, and warn about apps with a poor reputation.

Anti-Theft

Upon setting up the anti-theft feature, an app-specific PIN – which can later be replaced by a pattern or fingerprint – must be configured, and all device permissions including device admin rights must be given to the app. The app must be linked to an existing AVG account in order to receive commands from the web interface. The device takes pictures of a thief with the front camera, and records audio on suspicious device activities (e.g., multiple failed unlock attempts or SIM card change). Pictures and audio records are uploaded to the web interface or Google Drive optionally. Furthermore, the phone's last known location is sent to the web interface when battery charge is critically low.

The AVG PIN, the protection behaviour (lock phone, siren on lock) as well as the lock screen text can be customized in the settings of the web interface. However, the backup data is hard to find as it is hidden behind the “Info” button and “Notifications” tab.

Web, Wi-Fi & VPN Security

The Web Shield can be enabled in the app settings and provides protection against phishing websites for different browser apps. To achieve more security, the currently connected Wi-Fi network can be checked for security threats and the VPN protection feature can be activated for an additional monthly or yearly license.

App Audit

The App Insights combines tools for analysing app permissions and usage for certain time periods. Apps are ranked by the risk categories “low”, “average”, and “high” depending on the permissions and private data they access. A custom mobile data plan can be set up to limit the mobile data consumption.

Additional Features

The app provides a feature to lock sensitive apps against unauthorized access using the AVG PIN, pattern, or fingerprint. In the options, the locking timeout for the protected apps can be changed. The Photo Vault provides similar functionality, enabling protection for photos specifically by hiding and encrypting them. For rooted devices, a Firewall restricts access to the Internet for individual apps.

Conclusion

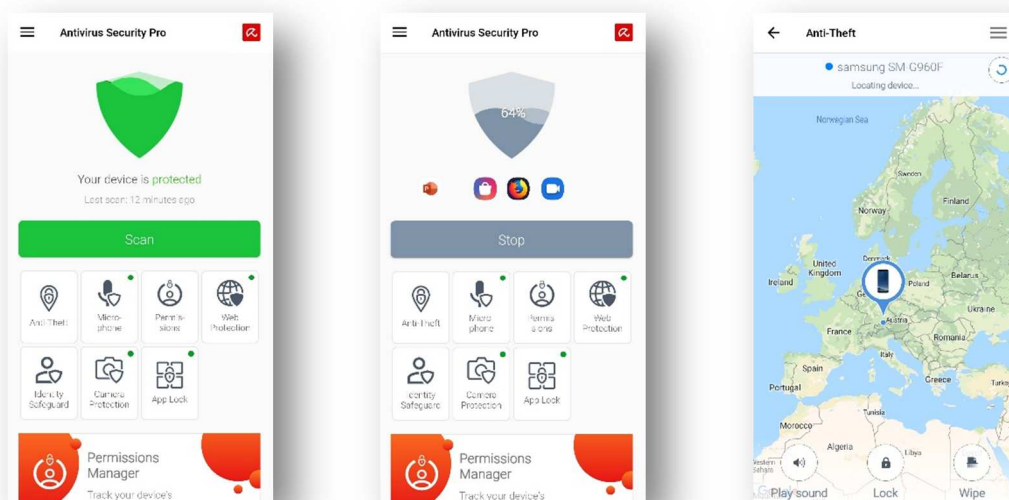
AVG AntiVirus is packed with both security and non-security features, which are easy to use and can be extensively customized via the app settings. The app interface is well designed and all the functions, especially the anti-theft commands, worked as intended.

Anti-Theft Details		
Commands Web		
Locate	✓	Displays location on <i>Google Maps</i> map. Tracking the device can be enabled.
Mark as Lost	✓	Triggers configured actions like tracking, lock, siren, and camera trap.
Siren	✓	Activates/deactivates the phone siren.
Lock	✓	Locks/unlocks the phone.
Wipe	✓	Triggers a factory reset and wipes external storage.
Record Audio	✓	Records audio for a pre-defined duration of 1-5 minutes.
Take Picture	✓	Takes a picture with the front camera. Optional: The camera is triggered when the screen is turned on the next time.
Get Data	✓	Backs up contacts from the device in HTML format.
Message	✓	Sends and shows an on-screen message on the device.
Call	✓	Initiates a hidden phone call on the device to a given phone number.
Additional Features		
SIM Change Protection	✓	Sets the phone status to lost.
Camera Trap	✓	Takes a picture with the front camera.



Introduction

Avira provides a comprehensive product that is available in a free (ad-supported) and a pro version. The free version comes with a malware scanner, anti-theft feature, Identity Safeguard, and Permissions Manager. An upgrade to the pro version adds more-frequent database updates, App Lock, as well as Web, Camera and Microphone Protection. Additional functions like VPN, password manager, and safe QR code scanner are offered as separate Avira apps that are accessible from within the main app.



Usage

After installation and accepting the EULA as well as the Privacy Policy, the user can either consent to continue with targeted or generic ads in the free version, or choose to upgrade to the pro version immediately. Starting with version 5.8.2, all available features are accessible from the main screen. We recommend creating an Avira account beforehand to enable most functions.

Anti-Malware

An app-only scan can be started from the main screen. To scan all files on the internal storage, the corresponding setting needs to be enabled first. The scan itself gives no information on what is actually being scanned. The results only show the number of scanned files and if issues were found. The scan settings can be customized to include adware, PUA and

riskware, to specify flexible schedules, and to start a scan when storage is mounted or a USB cable is unplugged.

Anti-Theft

After all necessary permissions and device admin rights have been granted, the anti-theft commands can be issued from within the app, or from the web interface under "Family Locator". The in-app commands Lock/Unlock and Wipe are restricted, as they are intended only to be executed on a remote device that also has the Avira app installed. A list of registered devices is shown, and the current selected device can be located on Google Maps. The web interface states that the device will only be locked if a lock screen has been set up in the Android settings. All commands worked flawlessly and as expected in our functionality test.

Web & Privacy Protection

The Web Protection feature blocks harmful websites while the user is surfing the web. Camera Protection and Microphone Protection restrict app access to the device camera and microphone, respectively. For the first, the user can mark apps as trusted which are then permitted to access the camera using the Avira Camera Protection widget. For Microphone Protection, either all listed apps or none get access to the microphone. In version 5.8.2, the Permissions Manager lists the installed apps by the permissions they access, and allows you to uninstall apps. Finally, the Identity Safeguard checks a given email address for data leaks or other threats.

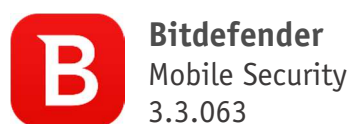
Additional Features

With the App Lock, the user can protect sensitive apps using a pre-defined pattern. Optionally, a PIN or fingerprint can be set up. Further settings are available to adjust the locking behaviour, when or where to lock individual apps, and showing a fake crash, if someone tries to access a locked app.

Conclusion

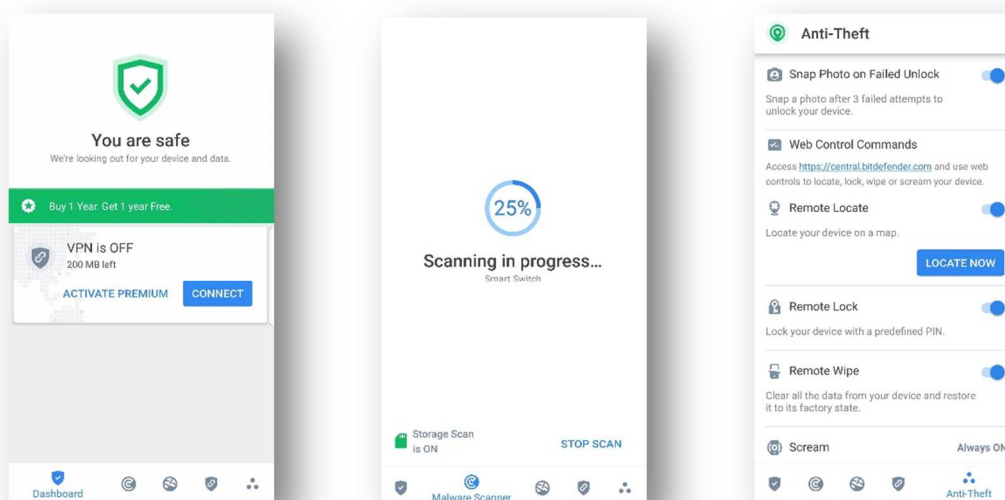
Avira Antivirus Security is a well-developed anti-malware application which provides protection against malware, device theft and loss, and phishing. Its anti-theft features can be used in-app as well as from the web interface, which enables more flexibility. Additional Avira apps can be downloaded separately to provide further device security and privacy.

Anti-Theft Details		
Commands App & Web		
Locate	✓	Displays location on <i>Google Maps</i> map.
Lock	✓	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.
Wipe	✓	Triggers a factory reset and wipes external storage (only executable remotely).



Introduction

Bitdefender Mobile Security is a well-designed and easy-to-use mobile security application. It comes with a 14-day trial period, during which the full potential of the app can be tested for free. After that, the user can continue by paying a yearly or monthly subscription. The features provided are malware scanning, anti-theft, web protection as well as application locking, account privacy, and basic VPN protection. The Autopilot function shows recommendations for security and privacy issues. Weekly summary reports and activity logs can also be viewed within the app.



Usage

On the first start, the user must either sign in to his or her Bitdefender account or create a new one. A quick setup follows in order to enable web protection and to start an initial file scan before the first usage. After that, the user is taken to the app's main screen where the security status and various suggestions to enhance security are shown. The bottom bar can be used to navigate through the app.

Anti-Malware

The malware scanner performs scans on all installed apps, additionally checks files on the internal and external storage if enabled, and automatically scans apps after they have been updated or installed. Suspect-app information is uploaded to Bitdefender by default to provide in-the-cloud detection.

Anti-Theft

After choosing a PIN and providing device admin rights, various anti-theft commands such as Locate, Lock, Alert, and Wipe are enabled and ready to be sent from the web interface. The app suggests activating Snap Photo to silently take a picture with the front camera whenever someone fails to unlock the device, which are instantly uploaded to the web interface. In the web interface, the IP address of the located device can be shown on request. If no Android lock screen is set up prior to issuing the Lock command, the device gets locked with a 4-digit PIN chosen in the web interface. If a lock mechanism (e.g., PIN, pattern, fingerprint) is already configured, the device is locked using the existing method and the PIN in the web interface is ignored.

Safe Browsing & VPN

The Web Protection component blocks malicious, fraudulent, and dangerous websites, and warns about associated risks. Right now, the Google Chrome, Dolphin, Firefox, Opera, and Opera Mini browser apps are supported.

The app allows the use of Bitdefender's VPN, which encrypts and anonymizes the user's web traffic. The basic subscription includes 200 MB of encrypted data per device, per day. An additional subscription provides unlimited traffic and the ability to connect to any of the available servers. In addition, the app can show a notification when connecting to an open Wi-Fi.

App Lock

After giving the necessary permissions, the user can lock sensitive apps with a 4-8-digit PIN. Several options are available to change the locking behaviour (e.g., unlock every time, unlock until screen off, lock after 30 seconds). For more convenience, trusted Wi-Fi networks can be set up, which keep apps unlocked while connected, and the fingerprint can optionally be used to unlock protected apps. If activated, the Snap Photo function is triggered after 3 failed unlock attempts in succession.

Account Privacy

This tool regularly checks pre-added email accounts for any known data leaks. On setup, the ownership must be confirmed via a confirmation code sent to that particular email address. If an online account is compromised, the user will be notified and prompted to change the password, and can mark the identified breaches as solved.

Conclusion

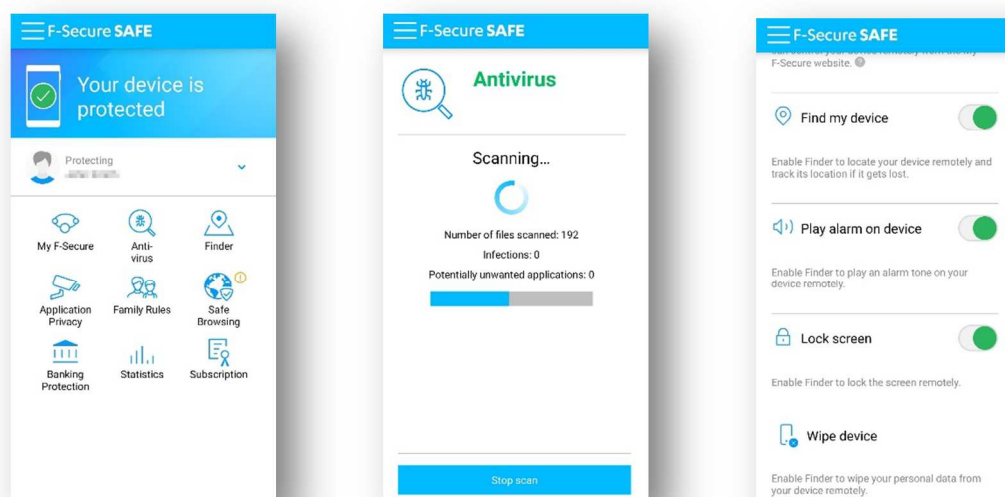
Bitdefender offers a well-designed and comprehensive mobile security solution for Android devices. Subscribed users can rely on a convenient and user-friendly web interface to remotely control a lost or stolen device. Further privacy is guaranteed by using app locking, email account checks, and Bitdefender's VPN.

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



Introduction

SAFE is F-Secure's solution to protect multiple devices (PC, Mac, Android, iOS) against malware and other threats. It offers an extensive parental control feature to restrict Internet and app access for children. The Android app comes with a 30-day trial, and includes a malware scanner, anti-theft feature, app audit feature, and its own Safe Browser app which secures online banking connections.



Usage

After accepting the EULA and granting all necessary permissions, the user must sign in to his or her F-Secure account or create a new one. Then, the app (and consequently the device) can be set up for an adult profile without any restrictions, or for a child profile by configuring Family Rules in the next step. These rules control the access to all installed apps and the device usage. Finally, the app starts an initial file storage scan.

Anti-Malware

Newly installed apps and memory cards, when they are inserted, are automatically scanned. Scans can be scheduled to run at regular intervals or whenever the device is restarted.

Anti-Theft

The anti-theft feature, called Finder, requires device admin rights and a lock screen PIN, password, pattern, or fingerprint for later validations. Commands like Locate, Alarm, Lock, and Wipe are available and can be executed from the corresponding web interface, but need to be enabled in the app first. In the web interface, you can easily switch between user profiles and devices associated with them.

Safe Browsing

Safe Browsing is only provided via a separate Safe Browser app which protects against fraudulent websites and identity theft. In addition, the browser notifies the user when accessing trusted online banking websites.

App Audit

The Application Privacy feature lists apps that might compromise privacy, e.g. if they can access messages or contacts, determine device location, or use camera and microphone for video and audio recordings. These apps are ranked according to the number of permissions they acquire, and the user is able to uninstall suspicious apps.

Parental Controls

As mentioned before, the user can set up child profiles to restrict app access and control device usage via the Family Rules. These rules can be remotely changed via the web interface anytime and include app control, time limits (device use limits, bedtime intervals), and content filtering for the Safe Browser app.

Conclusion

F-Secure SAFE provides an anti-malware solution to protect multiple devices against viruses and other security threats. The app and its functions are intuitive and easy to use. Basic anti-theft commands allow for remotely controlling the device. Several profiles and rules can set up the device appropriate for children. All functions worked as intended in our functionality test.

Anti-Theft Details		
Commands Web		
Locate	✓	Displays current or last-known location on <i>Google Maps</i> map.
Lock	✓	Locks the device with the pre-configured lock mechanism.
Wipe	✓	Triggers a factory reset and wipes external storage.

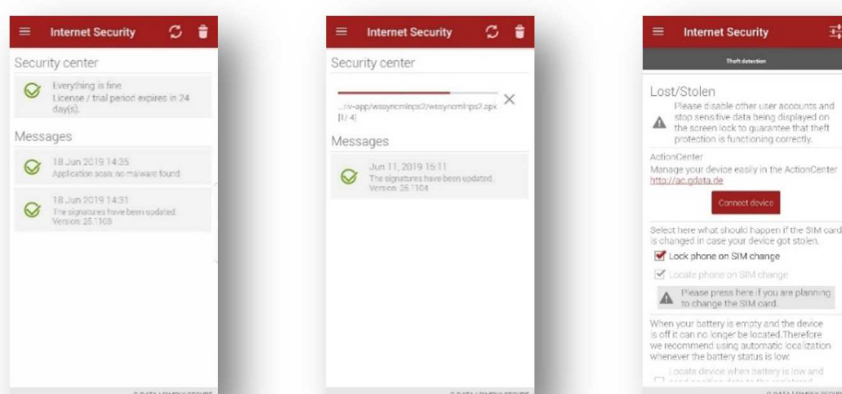


G DATA
Internet Security
26.5.6



Introduction

G DATA provides a mobile app with a number of security-related features such as malware scan, theft protection, web protection, and app restriction. The parental control function includes comprehensive settings to create protected environments for children, where only approved apps and websites are accessible. All premium features can be tested for 30 days. After that, only malware scan and app permissions are still available, unless a yearly license is purchased.



Usage

In order to use the app, the user must create a G DATA account first. After the user successfully logs in and accepts the EULA, the main screen appears and a database update is started. The screen looks very clean, and shows the license status as well as latest messages. All features are contained in the menu in the upper left-hand corner.

Anti-Malware

The app differentiates between a quick scan of all installed apps and a full system scan. By default, the app scans newly installed apps and periodically checks the device for any malware. Besides many other options, the user can decide how frequently the device will be scanned (1-30 days), if the background scan will only run while the device is on charge, and how often a signature update should run.

Anti-Theft

First, a maintenance PIN is required to activate anti-theft on the device. 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. Basic and additional commands can be issued from the G DATA ActionCenter once the device is connected to it. Moreover, the ActionCenter lets you start device scans and adjust in-app settings. At the time of testing, the web interface still showed SMS commands, although none of these were functional any more. G DATA have now removed these redundant commands from the interface. Each time a command is successfully executed, a reply mail is sent to a pre-configured email address. For the Lock command, an arbitrary PIN can be entered in the web interface to lock the device. If no additional PIN is set, the device is locked using the maintenance PIN. On SIM change and removal, the app locks the device and sends the current location to the registered email address.

In addition, permission to trigger a defined subset of anti-theft commands from the web interface can be given to other users. The chosen user receives an invitation link by email and will prompt to create an account for the web interface to gain access.

Safe Browsing

The web protection feature prevents phishing attacks while using the Android or Google Chrome browser app. Furthermore, G DATA provides its own Secure Browser app to securely surf the Internet, but it is very basic, with minimal surfing options. In the app settings, additional checks and rules for connected Wi-Fi networks can be activated.

App Audit & Protection

The Permissions feature lists apps grouped by the permissions they acquire and allows the user to uninstall apps or mark them as protected apps. App Protection prohibits unauthorized access to protected apps, which require the maintenance PIN to be entered.

Parental Controls

The app is equipped with an extensive parental control feature, with which the user can set up two device modes. The Children's Corner provides a child-oriented home screen with very limited functionality. Here, parents can create white- and blacklists for websites, select approved apps, and restrict the use of the device to specific locations and times. Further settings are switching off Wi-Fi, locking volume control, and adding time limits for device usage. The Teenager Corner just restricts the access to approved apps and the device usage to specific locations and time intervals.

Conclusion

G DATA provides a solid and well-programmed anti-malware app for Android. Necessary anti-theft commands can be sent from the web interface to remotely control the device. All functions worked properly in our functionality test, and the parental control feature includes many options to set up protected device environments suitable for children. As a result of our review, G DATA are in the process of updating the app's descriptions, websites, and the ActionCenter, and removing outdated and confusing information, such as old manuals and factsheets.

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

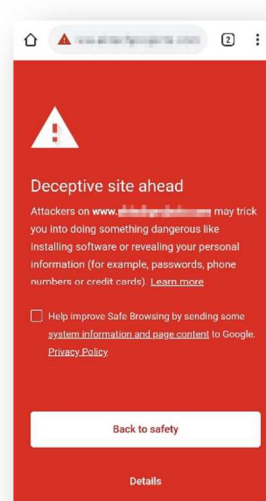
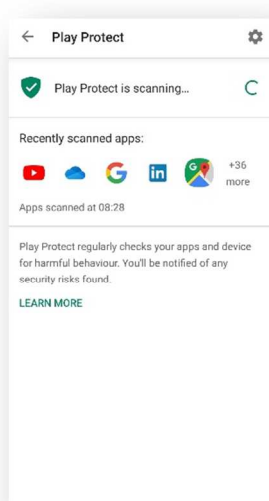


Google
Play Protect & OS Features
15.3.14



Introduction

Google's built-in malware protection for Android regularly checks installed apps for security threats, as well as apps and .APK files before they are downloaded and installed from Google Play or third-party sources. Besides the malware scan, Google provides anti-theft functions via a standalone app or web interface, and protection against phishing websites included in the Google Chrome browser app. For specific device models, Android profiles can be defined to create user workspaces, with custom settings and apps. Backups of user data, media files, apps, etc. can be created and uploaded to the Google cloud.



Usage

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

Anti-Malware

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

Anti-Theft

After logging in to the Google account, the anti-theft feature, called Find My Device, is accessible using the standalone app from Google Play, or the web interface. Both variants allow the user to view the current or last-known device location and to trigger an alarm on the target device for up to 5 minutes. If no lock screen is set up, the device is locked with a new PIN entered here. Otherwise, the pre-configured security mechanism (e.g., PIN, password, pattern, fingerprint) will be used. 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 erased permanently from the device.

Safe Browsing

Google Chrome contains a safe browsing feature, to detect and block phishing websites while the user is surfing the Internet.

App Audit

Since Android 6.0 was introduced, the user has had more control over the permissions granted to individual apps. These options are accessible from Settings → Apps. The access to certain apps can be restricted by creating custom user profiles. However, this feature may be different for each device manufacturer or not even be available.

Conclusion

Google continuously improves the security and threat protection for Android devices. Today, Play Protect runs on almost every new Android device that has Google Play Store and Services installed. The built-in malware protection along with other security-related features like anti-theft, safe browsing, and data backup can be carried out ex works and for free using a Google account.

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

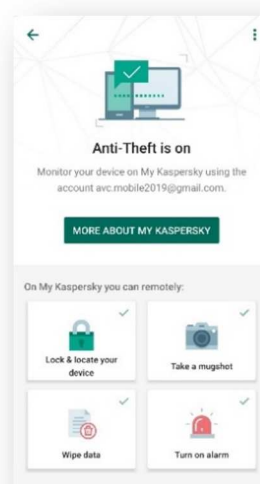
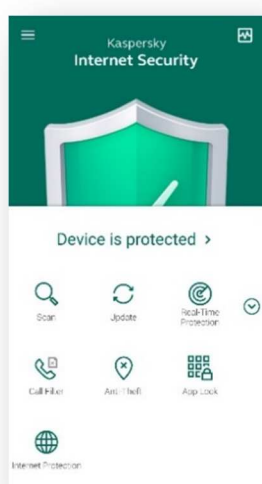


Kaspersky
Internet Security
11.23.4



Introduction

Kaspersky Internet Security provides the most important security functions, such as malware protection, theft protection, web protection, app lock, and call filter, in a very clean user interface. A 30-days trial allows you to test out all available features and get familiar with the app. Additional features like VPN protection, parental control, and password manager are offered as separate Kaspersky apps.



Usage

On first usage, the app requests a few permissions which are necessary for the initial configuration. After confirming the terms and conditions, the user can immediately buy a monthly or annual license for the app, assign an existing license to the current device, or completely skip this step and continue to the app's main screen. An initial virus signature update and a quick scan are started automatically.

Anti-Malware

The real-time protection monitors file activity 24/7 and scans newly installed apps before initial execution, under recommended settings. However, various options allow you to customize the scan and detection behaviour of the real-time protection, as well as that of an on-demand scan. Either all files, or apps and archives only, can be scanned, and protection

against adware and other unwanted apps is enabled by default. The user can choose between three different scan scopes: Quick Scan to scan all installed apps, Full Scan to run a scan for the entire device, or Folder Scan to check a specific device folder. Infected files can be moved to quarantine, deleted or skipped, or the user can be prompted for action. Finally, scheduled scans and database updates can be adjusted to the user's needs.

Anti-Theft

To use anti-theft properly, the app requires several permissions, device admin rights, and a secret code with 4-6 digits to be configured. Optionally, a pattern or fingerprint can be added and used instead of the secret code. The device can be remotely controlled using the web interface. Commands for Lock & Locate, Alarm, Mugshot, and Data Wipe can be issued only if they are enabled in the app first.

For each command except for Data Wipe, a custom lock screen text can be set. In addition, the Lock command is triggered, and an email notification is sent. If no Android device lock is already set up, the pre-configured Kaspersky secret code is used instead. Locking the device when the SIM card is removed or changed works, as does the protection against deinstallation of the app.

When the user activates “Do not disturb” (DND) on their device, KIS immediately prompts him/her for permission to sound the alarm while the device is in DND mode. In our test, we gave this permission, and found that the function worked as expected.

It is also possible to give KIS permission to sound the alarm while the system sound is muted. However, there is no alert shown by KIS when you mute the sound, and surely very few users would think to provide permissions here without being prompted.

If the Alarm command is sent but KIS has not been given permission to play sounds in DND/mute mode, the phone is still locked. In the web interface, the command is shown as pending until the app gets the permission and the device is online the next time.

Safe Browsing

Internet Protection blocks dangerous websites accessed by the Google Chrome browser app. According to the app’s help page, it may also work for pre-installed browsers of some devices, such as Samsung Internet on Samsung devices.

Additional Features

The App Lock component protects selected apps with the previously configured secret code, pattern, or fingerprint. The Call Filter blocks incoming calls of blacklisted contacts and manually entered numbers.

Conclusion

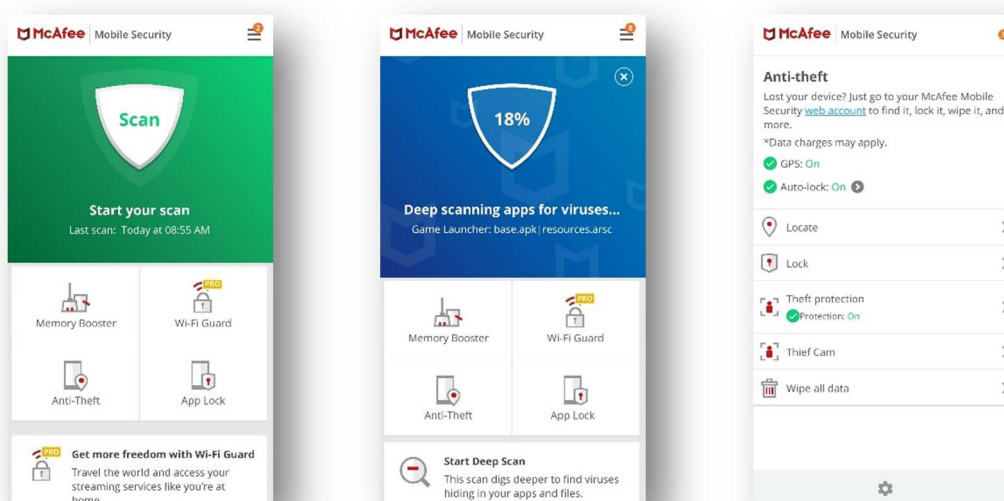
Kaspersky Lab’s product provides a great variety of features for mobile security in a clear user interface. A brief and helpful explanation is given on the very first use of every function and leaves no question unanswered. This product is recommended to users who like to keep things simple while also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

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



Introduction

McAfee is available in a free version, which provides an extensive selection of components for malware protection, theft protection, privacy control, Wi-Fi security, data backups, and tools for power and memory management. We strongly recommend creating a McAfee account in order to use the full potential of all security and privacy features. An upgrade to the paid-for Standard version removes ads, adds phishing protection, app lock, user profiles, and allows the user to backup media files like photos and videos. An additional VPN protection feature (Wi-Fi Guard) is only available with the Plus payment plan.



Usage

After the EULA and privacy notice are accepted, an initial setup process is started. The user is asked either to continue with the free and ad-supported version, to upgrade to the premium version by selecting a payment plan, or to log in with his or her McAfee account if one already exists. Afterwards, all required permissions need to be granted to modify and monitor the device, and a 6-digit PIN must be configured if not already done. The main screen shows the most important features and recommendations to improve device security.

Anti-Malware

Users can scan either apps only, or start a deeper scan of apps and internal files with pre-defined settings. The scan settings can be adjusted to schedule real-time scans and toggle automatic updates. The user can change the scan behaviour to scan all apps, potentially unwanted programs, as well as files in both internal and external storage. The app can also warn the user about malicious apps being installed or malicious files being transferred to a SD card.

Anti-Theft

After logging in to the McAfee account and enabling all necessary settings, anti-theft commands like Locate, Lock, Alarm, and Wipe can be sent using the web interface. If enabled, the device is locked when the airplane mode is activated, the SIM card is changed or removed, or no network connection is available. The latter did not work in our test when we deactivated Wi-Fi and the mobile data connection.

The web interface is still divided into two parts, which makes it rather confusing. “Find device” has a modern web view that provides all anti-theft commands, allowing the user to take action immediately when a device is lost or stolen, and shows the current location on Google Maps. “My device” and “My data” show a legacy page that supports the basic anti-theft commands and further options for Lock, Alarm, Thief Cam, Backup, and Wipe. Here, the backup data is accessible and can also be downloaded. For “Backup and Wipe”, the user can decide what action should be performed if the backup fails due to a network connection loss (e.g., don’t wipe, wipe without backup).

A click on “I lost my device” triggers the lock, locate, and thief-cam commands. The latter takes a photo with the front camera if someone enters multiple incorrect lock screen PINs. In addition, the location and the thief-cam photo are sent by email. The web interface also states that customizing a message for the lock screen does not work anymore. But, we were able to change the text on the lock screen via the app and web interface in our test.

The app and the web interface both state that the Wipe function will remove data from a SD card or storage card. However, we find this misleading and strongly suggest McAfee to improve this wording, as the Wipe only supports internal mounts/phone storage.

Safe Browsing

The Safe Web component provides browser protection against dangerous websites for Google Chrome, Samsung Internet, Opera Mini, and Firefox.

App Audit

The app contains several features regarding privacy. The Privacy Check rates and lists apps based on how much personal information and how many permissions they access. The App Lock feature locks certain apps with the pre-defined 6-digit PIN. The Guest Mode lets the user set up a guest profile with restricted access to pre-defined apps and functions.

Additional Features

The app can only save contacts to the cloud and restore them. In the premium version, it is also possible to back up media files. Automatic backups or notifications, when there is a new contact to back up, can be enabled as well.

Several tools can improve the power and performance of the device. The Storage Cleaner deletes junk, temporary, cached files, and obsolete apps. A Memory Booster frees up RAM, and a Battery Booster extends battery lifetime by turning off device settings (e.g., Wi-Fi, auto sync, screen timeout). Finally, a monitoring tool tracks and limits the mobile data usage of apps.

Conclusion

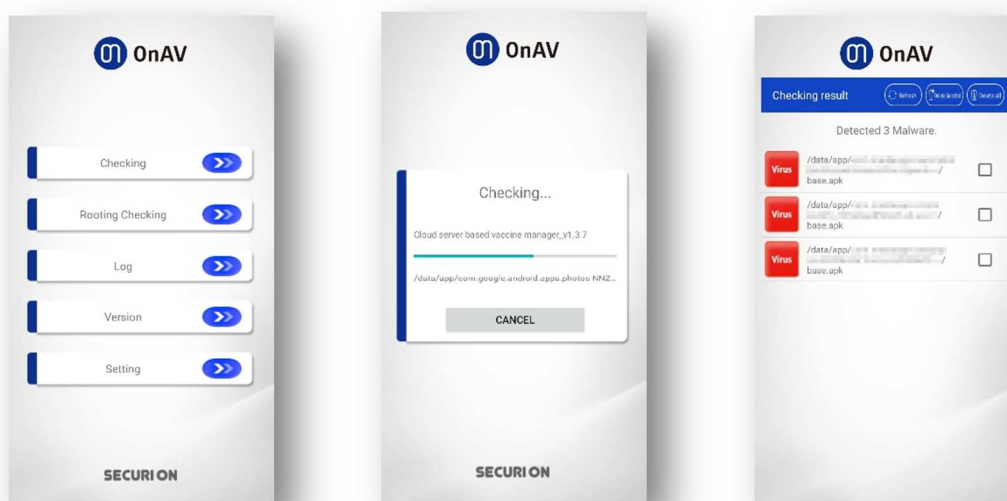
Besides malware detection, McAfee’s security product comprises an anti-theft and anti-phishing component, plus additional features to optimize the device’s performance. Except for a few minor issues, the anti-theft commands work as intended, and users are able to backup and wipe in one go. As we mentioned last year, the web interface, which is still split up into two separate pages, remains counter-intuitive.

Anti-Theft Details		
Commands Web		
Locate	✓	Displays location on <i>Google Maps</i> map.
Lock	✓	Locks the device with or without alarm.
Thief Cam	✓	Plays an alarm, shows a prompt, and takes a picture of the thief.
I lost my device	✓	Triggers lock, locate, and thief cam; if the phone is set to "It's still lost", the additional functions track, backup, wipe and factory reset can be used.
Track	✓	Tracks the phone for one or six hours continuously.
Backup	✓	Backs up contacts only. Backup of media files is only possible in-app.
Wipe	✓	Deletes contacts, photos, videos, and files on internal storage.
Factory Reset	✓	Triggers a factory reset and wipes external storage.
Additional Features		
SIM Change Protection	✓	Locks the device if the SIM card is removed or changed.
Uninstall Protection	✓	Locks the device if device administrator rights are removed from the app.
Thief Cam	✓	Takes a picture with the front camera after multiple failed unlock attempts.



Introduction

Securion OnAV is a free and slim application that only provides a virus scanner and a “Rooting Checking” function. We are not sure what exactly the latter feature is supposed to do. We assumed that it checks if the device is rooted. However, the function produced the result “No rooting detected” on both a non-rooted and rooted device. After we informed Securion about this bug, they removed this feature and told us that they will work to improve it.



Usage

After installation, the app asks for storage and phone permissions only. According to the Google Play entry, both permissions are required to perform a file scan and to use the unique device ID, respectively.

Anti-Malware

If “Checking” is selected from the main screen, the app starts a full virus scan of the internal storage. Trying to cancel the scan by tapping on “Cancel” or the “Back” button did not work in our functionality test. We had to kill the app using the task manager. Securion have since fixed this issue due to our feedback. Real-time protection can be switched on/off in the settings, and results of previous scans are located in “Log”.

Conclusion

Securion OnAV is a very basic mobile security app which focuses on malware protection only, and does not offer additional security-related features. The scan results do not provide any further virus information. We also found that the English translation of the very few menu terms was not optimal, and indeed rather confusing. This has also been improved now.

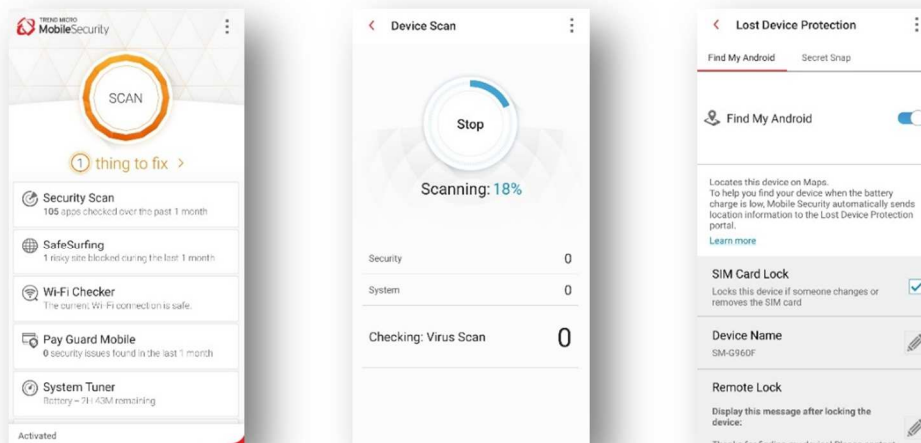


Trend Micro
Mobile Security
10.3.0



Introduction

Trend Micro's app has a free version which offers malware protection, system optimization and social media privacy tools. Starting the 14-day trial of the premium version, or purchasing a yearly licence for this, activates additional security features like anti-theft, web protection, Wi-Fi scanner, and parental controls.



Usage

After installation, the user is asked to accept the Privacy and Data Collection Notice, as well as the license agreement. Next, the user has to either sign in to an existing Trend Micro account, or create a new one, in order to continue. Meanwhile, an initial scan is started in the background. On the main screen, the device status and all features are readily accessible.

Anti-Malware

By default, an app-only scan is performed. The scan settings can be adjusted to set the level of threats the user will be notified about to low, normal, or high. Further options enable real-time scanning, pre-installation scanning of apps downloaded from Google Play, and scanning of the internal storage. Automatic updates are performed by default, but can be triggered manually and 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.

Anti-Theft

The Lost Device Protection component provides the anti-theft functionality for the device. Remote commands can be sent from a web interface and include Locate, Lock, Alarm, Wipe, and Reset. In addition, the phone can automatically be locked when the SIM card is changed or removed. The Uninstall Protection requires the Trend Micro account password to successfully uninstall the app. The Secret Snap feature takes a photo with the front camera if someone is trying to unlock the device, locked apps, or uninstall the app. The photos are stored on the device and sent to a pre-configured email address.

The Reset command allows you to force all running apps to stop or to reset the lock screen password. Unfortunately, the latter did not work properly in our test, as the web interface always stated "Unable to reset lock screen password".

Safe Browsing

The Safe Surfing feature checks and blocks malicious websites and links in listed browsers and other apps. The level of protection can be set to high, normal, or low. The user can also define a black- and whitelist of websites. A VPN protection is also available for supported apps.

Parental Controls

This feature is divided into two parts. First, it allows locking specific apps with the Trend Micro account password. Second, the website filter blocks pages inappropriate for children, pre-teens, or teens. A black- and whitelist of websites can also be defined.

Additional Features

The app contains a Wi-Fi Checker to scan the currently connected network for security risks, a System Tuner with several options to optimize device memory and battery charge, and a Social Network Privacy component that checks Facebook and Twitter account settings for possible privacy issues. The App Manager allows you to remove and disable installed apps to save resources. The Pay Guard Mobile feature monitors financial transactions of installed banking/shopping apps.

Conclusion

Trend Micro Mobile Security comprise a variety of security and privacy features to protect against threats on the device and manage the device remotely in case it is lost or stolen. The user interface is kept clean although several settings are provided to customize each function. Besides one minor issue, all anti-theft commands worked flawlessly.

Anti-Theft Details		
Commands Web		
Locate	✓	Displays location on <i>Bing Maps</i> map.
Lock	✓	Locks the device until either the Trend Micro password or a one-time unlock key from the web interface is entered.
Wipe	✓	Triggers a factory reset and wipes external storage.
Share	✓	Posts a <i>Bing Maps</i> link with the current location on Facebook.
Reset	✗	Forces all running apps to stop or resets lock screen password.
Additional Features		
SIM Change Protection	✓	Locks the device if the SIM card is removed or changed.
Uninstall Protection	✓	Locks the device if device administrator rights are removed from the app.
Secret Snap	✓	Takes a picture with the front camera.

Feature List Android Mobile Security (as of July 2019)											
Product Name	Android OS	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	Securion OnAV	Trend Micro Mobile Security
Version Number	9.0	6.21	6.19	5.8	3.3	17.6	26.5	11.23	5.2	1.0	10.3
Supported Android versions	built-in	5.0 and higher	5.0 and higher	4.4 and higher	4.0 and higher	5.0 and higher	4.1 and higher	4.2 and higher	4.2 and higher	4.1 and higher	4.1 and higher
Supported Program languages	All	English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese	English, Arabic, Belorussian, Bengali, Bulgarian, Catalan, Chinese, Croatian, Czech, Danish, Dutch, Estonian, Farsi, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukranian, Urdu, Vietnamese	English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish	English, Czech, Dutch, French, German, Greek, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Thai, Turkish, Vietnamese	English, Bulgarian, Croatian, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Chinese, Slovenian, Spanish, Swedish, Turkish, Vietnamese	English, Arabic, Chinese, Dutch, French, German, Hungarian, Italian, Japanese, Polish, Portuguese, Russian, Spanish, Turkish	English, Russian, German, French, Italian, Spanish, Portuguese, Turkish, Polish, Czech, Danish, Finnish, Hungarian, Norwegian, Dutch, Swedish, Arabic	English, Arabic, Bulgarian, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovak, Spanish, Swedish, Thai, Turkish, Vietnamese	English, Korean	English, Chinese, Dutch, French, German, Hebrew, Italian, Korean, Portuguese, Spanish, Turkish, Vietnamese
Anti-Malware											
On-Install scan of installed apps	●	●	●	●	●	●	●	●	●	●	●
On-Demand scan	●	●	●	●	●	●	●	●	●	●	●
On-Access scan of apps	●	●		●				●	●	●	
Automatic (scheduled) scan		●	●	●		●	●	●	●		●
Scan requires online cloud connection	●				●	●					
Privacy Advisor (audit app permissions)	●	●	●	●		●	●		●		
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●	●	●		●
Supported browsers (Safe Browsing)	Google Chrome	Google Chrome, Dolphin, Firefox, Opera	Google Chrome, Dolphin, Firefox, Opera	Google Chrome, Dolphin, Edge, Firefox, Opera, Opera Mini, Samsung Internet	Google Chrome, Dolphin, Firefox, Opera, Opera Mini, Samsung Internet	own Safe Browser only	Google Chrome, Firefox, Opera, Samsung Internet, own Safe Browser	Google Chrome, Samsung Internet	Google Chrome, Firefox, Opera Mini, Samsung Internet		Google Chrome, Samsung Internet
User account needed to use product	●				●	●	●		●		●
Anti-Theft											
Web Interface for controlling Anti-Theft commands	●	●	●	●	●	●	●	●	●		●
Remote Locate, Lock & Wipe (Factory Reset)	●	●	●	●	●	●	●	●	●		●
Thief Cam		●	●		●			●	●		●
Lock on SIM Change		●	●				●	●	●		●
Anti-Theft Alarm (cannot be muted by thief)		●	●		●		●	●			
Locate-Phone Alarm only (can be muted)	●			●		●			●		●
Remote Unlock		●	●	●					●		
App settings protected with password					●		●	●			●
Uninstallation Protection (password required for uninstallation)	n/a							●	●		●
Parental Control											
App Lock		●	●	●	●	●	●	●	●		●
Safe Web Browsing (content filtering)						●	●				●
Time Limits (device use limits, bedtime intervals)						●	●				
Additional Features											
Battery Monitor (track battery usage)	●	●	●						●		●
Wi-Fi Security		●	●				●		●		●
VPN		●	●		●				●		●
Task Manager (manage installed apps)	●	●	●								●
Network Monitor (track data usage)	●	●	●						●		
System Optimizer		●	●						●		●
Account Privacy				●	●						
Backup	●								●		
Anti-Spam (Whitelist / Blacklist Phone calls)	●							●			
Other Features		Photo Vault	Photo Vault				Panic Button				Social Network Security
Support											
Online Help & FAQ	●	●	●	●	●	●	●	●	●		●
User Forum	●	●	●	●	●	●		●	●		●
Email Support		●		●	●		●	●	●		●
Phone Support				●	●	●	●	●	●		●
User Manual (PDF)	●			●	●		●	●	●		
Online Chat					●	●		●	●		
Supported languages of support	All	English, Czech, German, French, Japanese, Spanish, Portuguese, Russian	English, Czech	English, Dutch, French, German, Indonesian, Italian, Japanese, Korean, Portuguese, Russian, Spanish	English, French, German, Italian, Dutch, Japanese, Portuguese, Romanian, Spanish, Turkish	English, Danish, Dutch, Finnish, French, German, Italian, Japanese, Norwegian, Polish, Swedish	English, Chinese, Dutch, French, German, Italian, Japanese, Polish, Portuguese, Spanish	English, French, German, Italian, Portuguese, Russian, Spanish	English, Chinese, Czech, Danish, Dutch, French, German, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Spanish, Suomi, Swedish, Turkish	English, Korean	English
In-App List Price (may vary)											
Price 1 Device / 1 Year (USD/EUR)	FREE	USD 8 / 8 EUR	USD 8 / 8 EUR	USD 10 / 8 EUR	USD 15 / 10 EUR	USD 18 / 15 EUR	USD 16 / 16 EUR	USD 20 / 17 EUR	USD 30 / 25 EUR	FREE	USD 36 / 30 EUR



Copyright and Disclaimer

This publication is Copyright © 2019 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
(July 2019)