Independent Tests of
Cybersecurity Solutions

Mobile Security Review 2026

TEST PERIOD: MAY 2026

LAST REVISION: 9TH JUNE 2026

WWW.AV-COMPARATIVES.ORG

Contents

Introduction

In this report, we aim to help readers evaluate both the built-in security measures of Android and various third-party mobile security apps. Our report covers results from malware protection and battery consumption tests, along with reviews assessing the functionality, design, and overall usability of each security app. While some of the tested apps may offer additional features such as an app manager, network monitor, or system optimizer, our primary focus is on security aspects, including anti-malware, anti-theft, web protection, and privacy protection.

Mobile security products are designed primarily to safeguard mobile users and their devices from threats such as malicious apps, phishing URLs, fraudulent emails, and other harmful links. In 2025, we also evaluated how well some security apps for Android protect against **stalkerware**[1]. This type of software operates covertly, enabling unauthorized users to spy on device owners without their knowledge or consent. While the lines between stalkerware and legitimate software, such as parental controls, can sometimes be blurred, Google Play has implemented stricter policies in recent years to combat this issue. Consequently, stalkerware is typically installed through sideloading[2] since it is not available on Google Play.

Google Play regularly updates its policies to maintain a high standard of security and user trust. App developers must verify their identity, digitally sign their apps, meet minimum API level requirements[3], disclose how they handle user data, and ensure that any integrated third-party SDKs do not sell personal or sensitive information. Additionally, all apps undergo multiple review processes, including privacy checks by Google, before being approved and listed on Google Play.

As Android's built-in security features continue to evolve, it remains essential to ensure that third-party solutions provide effective malware protection. Given the prevalence of rogue antivirus apps offering inadequate security[4], independent testing and certification are more important than ever. We appreciate the vendors who participated in our tests and achieved certification, highlighting their dedication to maintaining high standards of mobile security. Our comprehensive certification process affirms the effectiveness and reliability of these products. Some manufacturers might prioritize other platforms or operating systems, believing Google's security features for Android (e.g., Play Protect, Find My Hub) provide sufficient protection. However, we encourage continued vigilance and innovation in mobile security solutions.

Another advantage of continuous independent testing is that it supports vendors' quality-assurance efforts by helping to identify issues that may otherwise go unnoticed.

[1] https://www.av-comparatives.org/tests/stalkerware-test-2025/
[2] https://en.wikipedia.org/wiki/Sideloading
[3] https://developer.android.com/google/play/requirements/target-sdk
[4] https://www.av-comparatives.org/tests/android-test-2019-250-apps/

Key Features in Android Mobile Security Apps

In this section, we provide a concise overview of key security components commonly found in mobile security products for Android. At the beginning of each product review, a set of symbols can be found which indicate whether a feature is supported (orange) or not supported (grey). Please note that all symbols apply specifically to Android 16.

The primary component is the M*alware Scanner* or *Anti-Malware* which safeguards users from unintentionally installing malicious apps on their device. Similar to antivirus programs for Windows, mobile security apps for Android incorporate other protection features: The R*eal-time Protection* actively scans newly installed and/or downloaded apps for any malicious behaviour. The O*n-demand Scanner* examines the device for already installed malicious apps or malicious app installers on the internal storage and/or SD card. Keeping malware definitions up to date is a critical factor in effective protection, especially for apps that primarily rely on them for detecting malware. Certain tested products offer a cloud-assisted malware scanner to ensure access to the very latest definitions. Definition updates are either retrieved automatically by the app at specified time intervals or triggered manually by the user.

The A*nti-Theft* component is designed to remotely control a lost or stolen device. Android already includes core anti-theft features such as device lock, locate, and alarm. The tested security products extend this functionality with features such as location tracking, taking pictures of the thief using the device's cameras, or triggering actions in response to suspicious device activities (e.g., locking the device when the SIM card is changed or trying to uninstall the security app, capturing pictures after multiple failed unlock attempts). This component is typically managed via a web interface.

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

App Lock is another useful security feature, enabling users to safeguard selected apps from unauthorized access. Users can set up a locking mechanism, such as PIN, password, pattern, or biometrics (e.g., fingerprint or face recognition on supported devices), which is required to launch a protected app. Furthermore, they might be able to customize the app locking behaviour, such as unlocking when connected to a trusted Wi-Fi or locking based on location or time schedule.

A *Privacy Advisor* or *App Audit* feature is also included in most of the tested products, which typically scans the installed apps for possible privacy violations. This analysis examines app permissions that are uncommon, unnecessary, or inappropriate, as they may pose a risk to the user's privacy. Based on this result, some security apps advise uninstalling "risky" apps.

Built-in Security Measures in Google Android

Since the introduction of the runtime permission model in Android 6.0 (Marshmallow), Google has continuously enhanced Android's privacy and security architecture. With each version, new features have been introduced to give Android users more control over their devices and the data accessed by third-party apps.

At the core of Android's security system is *Google Play Protect*, a built-in malware scanner that checks apps during installation from Google Play or third-party sources and regularly scans the device for potential threats. With real-time code-level scanning, it prompts users to scan apps it has not previously encountered. Additionally, it includes live threat detection powered by on-device AI to identify suspicious app behaviour without compromising user privacy.

The *Safe Browsing* API protects users against malware and phishing links while browsing in Google Chrome. Google's *Find Hub* (formerly *Find My Device*) offers anti-theft functions to lock, locate, alarm, or wipe lost or stolen phones. With Android 15, advanced theft-protection features[5] such as "Theft Detection Lock" and "Offline Device Lock" were added, and existing functionalities such as "Remote Lock" and "Factory Reset" were improved, making it harder for thieves to gain device access, change sensitive settings, or reset the device. Android includes several *app auditing* features that let users review and adjust privacy settings, such as permissions and notifications, and monitor app activity, such as mobile data usage, battery use, and storage space.

Android 16 introduces several new privacy and security features[6]. A new runtime permission gates access to the local network, requiring apps to declare this permission explicitly. The platform also strengthens protection against intent redirection attacks. Wi-Fi location ranging on devices supporting IEEE 802.11az is secured with AES-256 encryption, providing protection against man-in-the-middle (MITM) attacks. A new embedded photo picker API allows developers to integrate media selection directly into an app's layout, maintaining process isolation and eliminating the need for broad storage permissions. To counter theft, Android 16 conceals one-time passwords on the lock screen in higher-risk scenarios, such as when the device is not connected to Wi-Fi and has not been recently unlocked. Finally, Android 16 incorporates the latest Privacy Sandbox iteration and introduces a new API to facilitate secure key sharing.

Limitations and the Role of Third-Party Security Apps

With each new feature and behaviour change, Android may impose tighter restrictions on third-party security apps, limiting their ability to control the device, monitor activity, or access sensitive user data. As a result, some security vendors have removed certain features from their apps, e.g., remote wipe of devices running Android 14 or higher[7]. However, the availability of Google's security features and third-party mobile security apps can vary depending on the device model, Android version, or regional restrictions. For example, in mainland China and on devices running modified Android-based systems, such as HarmonyOS, FireOS, or LineageOS, Google apps and services including Play Protect, are typically unavailable thus lacking built-in malware protection.

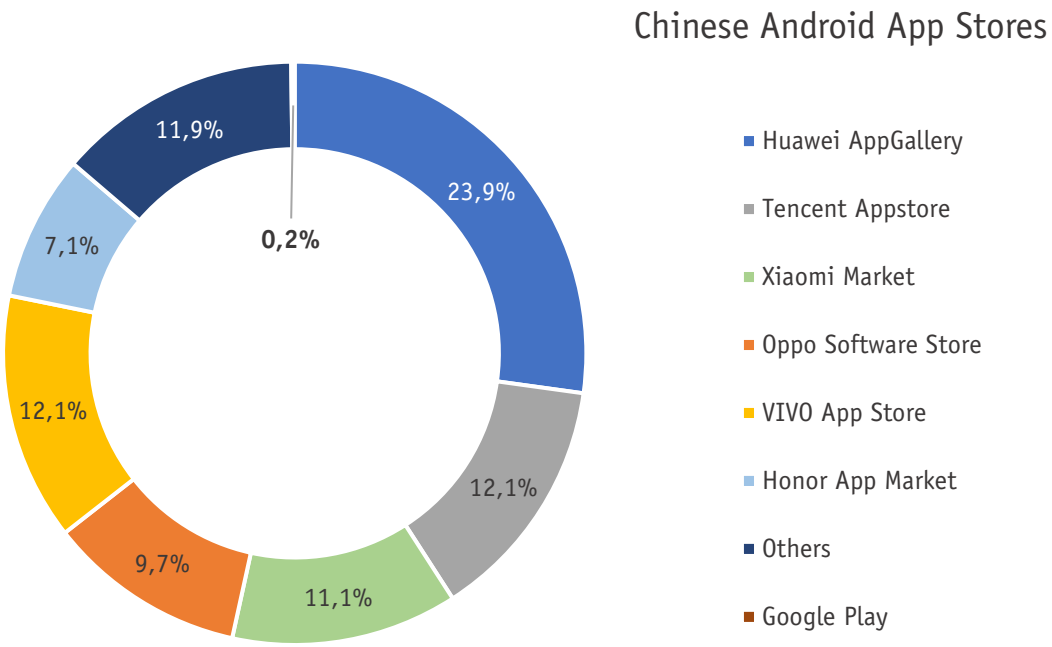
[5] https://security.googleblog.com/2024/10/android-theft-protection.html

[6] https://developer.android.com/about/versions/16/summary

[7] https://developer.android.com/reference/android/app/admin/DevicePolicyManager#wipeData(int,%20java.lang.CharSequence)

In regions such as the United States and Europe, the mobile app market is largely dominated by two official app stores: *Google Play* and *Apple App Store*. The risk of inadvertently downloading and installing malware from Google Play is relatively low, as the app store is regularly checked for fraudulent and dangerous apps. In contrast, many Asian countries like China face a significantly higher risk of malware infections due to the widespread use of third-party app stores and the prevalence of rooted devices. There exist approximately 1.83 billion[8] active mobile devices in China, with around 71%[9] running Android.

The ring chart below highlights the most used Chinese Android app stores[10]. Notably, Google Play is used by almost no one (0.2%). This is largely due to a U.S. Executive Order[11] signed in November 2020, which prohibits American companies from doing business with blacklisted Chinese telecommunication firms. As a result, Google apps and services including Play Protect are no longer available on newer device models from affected Chinese manufacturers.



For users without access to Android's built-in security features, there is a very strong argument for using a third-party security app. Even users with full access to Google's protections may benefit from the additional layers of defence these apps offer. Unlike Play Protect, which primarily focuses on scanning installed apps, third-party security solutions often provide more comprehensive coverage by also scanning files, folders, and device storage. This proactive approach helps identify and mitigate malicious apps before they are installed or executed. It is important to note that third-party security apps for Android supplement, rather than replace, Android's native security features.

[8] https://datareportal.com/reports/digital-2026-china
[9] https://gs.statcounter.com/os-market-share/mobile/china
[10] https://www.appinchina.co/market/app-stores
[11] https://ofac.treasury.gov/media/49616/download

Best Practices for Enhancing Mobile Security

Smartphones are now commonly used as popular PC substitutes for a variety of daily tasks including online shopping, banking, instant messaging, video conferencing, and emailing. However, with the increasing sophistication of cyberattacks, mobile devices are becoming a prime target, particularly through fraudulent apps and phishing websites that aim to steal user data or money. These malicious apps often disguise themselves as fake versions of popular apps that have been downloaded by millions of users from Google Play[12].

To minimize the risk of falling victim to these threats, we recommend the following:

- Download apps only from official app stores like Google Play or reputable app makers and avoid third-party stores and sideloading.
- Check app reviews before installation and avoid those with predominantly negative or suspicious feedback.
- Be wary of opening links that you receive via e.g., text messages, emails, instant messenger chats, or social media, and block/delete unknown senders or spam.
- Pay attention when granting apps permissions or excessive access rights and question unnecessary requests.
- Keep your Android and third-party apps up to date with the latest patches.
- Use a certified[13] antivirus app to provide an additional layer of protection.
- Regularly back up your data using common backup solutions.
- Regularly evaluate the legitimacy, usefulness, and data handling practices of apps, whether online or on Google Play.
- Do not root your smartphone, mitigating the risk of malware infection and keeping the warranty.
- Disable unused settings and device sharing functions that could be potential attack vectors such as Bluetooth, NFC, or Wi-Fi calls.

How High is the Risk of Malware Infection with an Android Smartphone?

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

[12] https://www.scworld.com/brief/novoice-android-malware-steals-whatsapp-data-via-google-play-apps

[13] A list of antivirus apps for Android can be seen here: https://www.av-comparatives.org/list-of-mobile-security-vendors-android/

Tested Products

The following products were reviewed and tested for this report. We congratulate the third-party security vendors who have demonstrated that their solutions are effective and reputable and helped to raise the standard for all mobile security solutions. The latest products were taken from Google Play at time of testing (May 2026). After the test, manufacturers had the opportunity to fix any flaws we discovered[14]. Any problems that have already been solved are noted in the reviews. The versions listed below apply to the updated product reviews.

Vendor[15]	Product Name	Version	Features
Avast	One Free	26.6	
AVG	AntiVirus Free	26.6	
Bitdefender	Mobile Security	3.3	
G DATA	Mobile Security	29.4	
Google	Play Protect & OS Features	50.9	
Kaspersky	Premium for Android	11.131	
Norton	360 Deluxe	26.5	
Securion	OnAV – Global	1.0	
Tencent	腾讯手机管家	16.1	

For this report, the unmodified version of Android 16, currently the most recent Android release, was used to avoid potential issues caused by modifications from hardware manufacturers or mobile carriers. For each product's anti-theft component (see *"Key Features in Android Mobile Security Apps"*), brief comments are provided for each function. The following symbols indicate its performance in our tests:

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

[14] Any bugs or issues discovered during the review that we consider critical must be fixed, and an updated app version must be published on Google Play within three weeks of reporting the issue.

[15] **Avast, AVG,** and **Norton** are products of Gen Digital and use the **Avast** engine. **G DATA** uses the **Ikarus** engine.

AV-Comparatives' Approved Mobile Product Award

No mobile security product is ideal for every user. As with Windows products, we recommend drawing up a shortlist of suitable candidates after reading the reviews and noting the advantages and disadvantages of each. Free trial versions of the shortlisted products can then be installed and tested one at a time over a few days to help inform the final decision. It is worth noting that for Android security products in particular, new versions with improvements and new functions are constantly being released.

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

Avast One Free is an ad-supported mobile security application that provides a range of security, privacy, and device optimisation features.

AVG AntiVirus Free is an ad-supported mobile security application that offers a range of security, privacy, and device optimisation features.

Bitdefender Mobile Security integrates a wide range of tools to monitor and protect device security and user privacy, all within a clean and navigable user interface.

G DATA Mobile Security offers a straightforward user interface with a solid set of security and privacy features.

X **Google Android** provides built-in malware protection, anti-theft, safe browsing, and advanced app auditing features. Google narrowly missed the certification threshold.

Kaspersky Premium for Android delivers extensive, fully configurable security and privacy features within an approachable and navigable app interface.

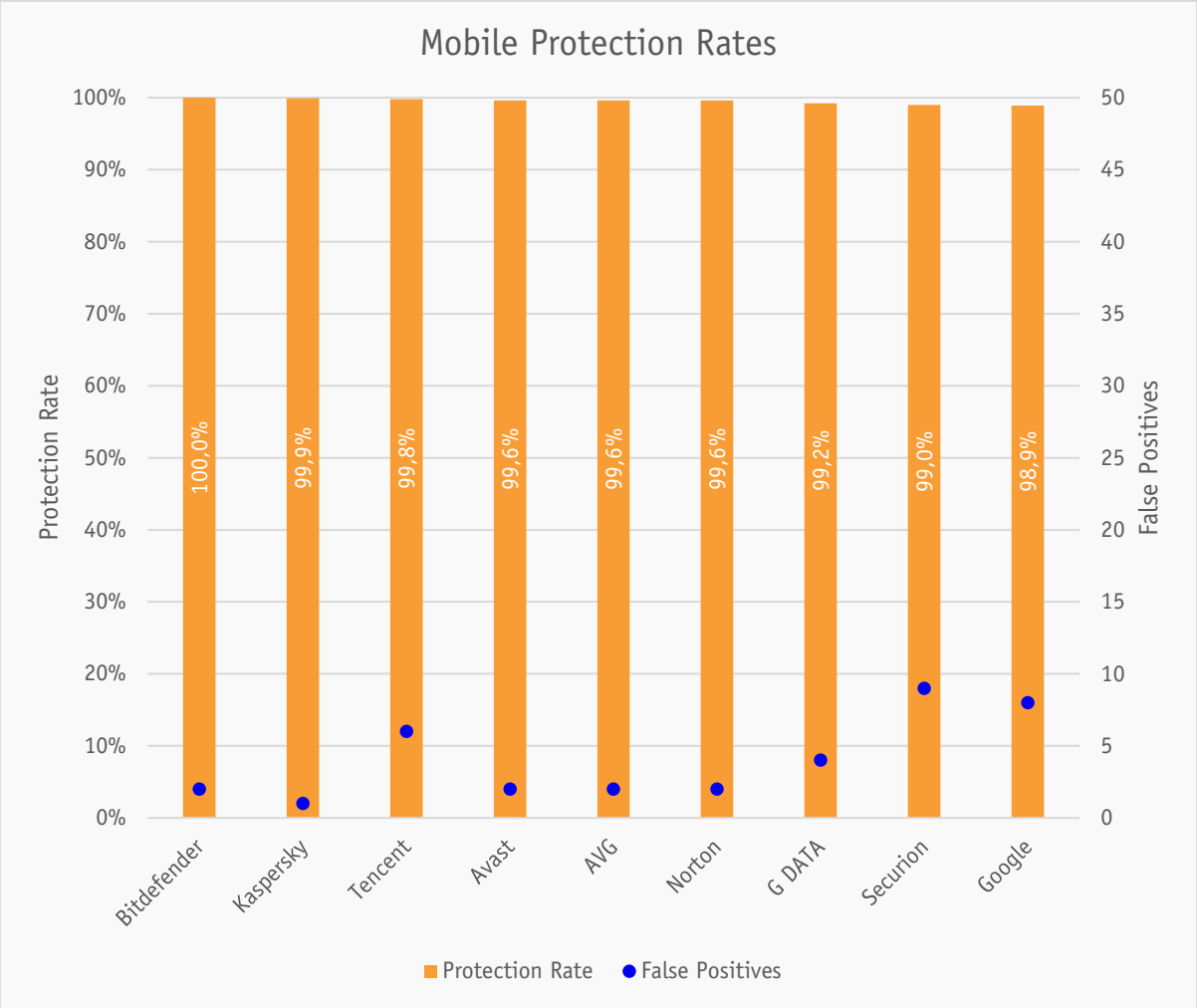
Norton 360 Deluxe offers a variety of security and privacy features including an AI-powered scam check within a modern, navigable user interface.

Securion OnAV – Global is a free, lightweight mobile security application focused on providing essential malware protection.

Tencent 腾讯手机管家 is a free mobile security and device optimisation application developed for the Chinese market, offering malware protection, privacy tools, and a range of additional device management features.

Malware Protection Test Results

The malware used in the test was collected by us in the few weeks before the test. We used **3,156** malicious applications, to create a representative test set. Apps with the same certificates and/or the same internal code were removed, in order to have a test set of genuinely unique samples. The security products were updated and tested begin of May 2026. The test was conducted with an active Internet connection on genuine Android smartphones (no emulators were used). The test set consisted exclusively of APK files. If available, an on-demand scan was conducted first. After this, every undetected app was installed and launched. We did this to allow the products to detect the malware using real-time protection. A false-positives test was also carried out using 500 clean apps. The results can be seen below (sorted by Malware Protection and number of False Positives; products with identical scores are sorted alphabetically).



Mobile Protection Rates		
	Protection Rate	**False Positives**
Bitdefender	**100%**	2
Kaspersky	**99.9%**	1
Tencent	**99.8%**	6
Avast, AVG, Norton	**99.6%**	2
G DATA	**99.2%**	4
Securion	**99.0%**	9
Google	**98.9%**	8

Battery Drain Test Results

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

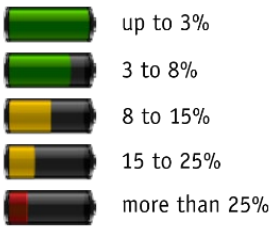
Some use the multimedia functions extensively, others view a lot of documents, while some use only the telephone functions. We need to differentiate between power users who take advantage of all the possible functions in the device and traditional users who merely make and receive phone calls.

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

- 67 minutes using social media apps (such as YouTube)
- 40 minutes telephony
- 35 minutes surfing the Internet using the Google Chrome browser
- 22 minutes looking at photos
- 13 minutes watching videos saved on the phone itself
- 2 minutes sending and receiving mails using the Google Mail client
- 1 minute opening locally saved documents

In our test, we found that all the tested mobile security products had only a minor influence on battery life, as outlined in the table below. In general, we were able to give the tested mobile security apps high marks regarding power usage.

Battery Drain Results	
Avast	
AVG	
Bitdefender	
ESET	
G DATA	
Google	
Kaspersky	
Norton	
Securion	
Tencent	



Review Format

The following product reviews are structured consistently across all mobile security apps. Not every section is applicable to every product, as individual apps offer different feature sets. Only features integrated directly within the product are included. Standalone companion apps are covered only where they are installed automatically alongside the main security app; those requiring manual installation are not included. Reviews are limited to two pages.

Introduction: A concise overview of the product, stating its price model and highlighting up to five key security and privacy features, indicated by the symbols in the top-right corner of each review, along with up to five additional features considered noteworthy. Standardised terms from the feature list at the end of this report are used throughout for easier comparison across products.

Usage: A brief description of the initial app launch, setup process, and navigation to the main app features. Note that all third-party security apps require users to agree to the vendor's data protection policies and grant necessary permissions, such as full file access, location, camera, and device administrator rights, either during setup or when activating specific features.

Anti-Malware: The available scan options, including quick, full, and scheduled scans, where applicable. Any suggestions shown to the user following the initial scan are noted, as are settings related to detection behaviour and any notable findings where malware is detected.

Anti-Theft: Where applicable, the setup procedure, available remote commands, and how to trigger them. Any additional settings, command failures, or unexpected behaviour during testing are noted. A summary table of available anti-theft commands is provided at the end of each applicable product review.

Web & Wi-Fi Protection: Where applicable, the available protection capabilities against web-based threats and Wi-Fi vulnerabilities, such as anti-phishing, VPN, and Wi-Fi scanning.

App Lock & Audit: Where applicable, the app locking feature and its settings for restricting access to selected apps, and/or the functionality for reviewing installed apps with respect to permissions, data usage, and storage consumption.

Parental Control: Where applicable, the available tools for monitoring and regulating children's device usage and restricting access to inappropriate content, such as app locking, web filtering, and daily usage limits.

Privacy Protection: Where applicable, available features that contribute to user privacy, such as call filtering, data leak checkers, social network privacy scanners, and protection against scam or malicious links in notifications and text messages.

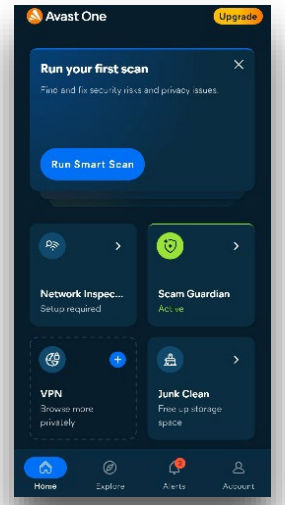
Additional Features: Additional app features that do not fall within the preceding categories and are considered worth noting, such as system optimisation or task management tools.

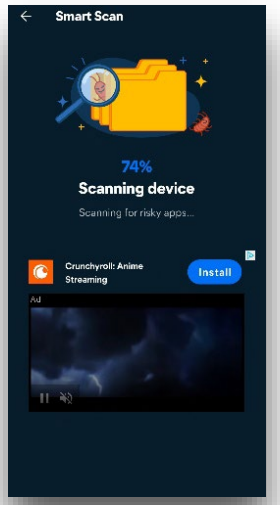
Conclusion: A brief summary of the product and the testing experience, including a statement on any reviewed feature that did not function as expected and was not resolved prior to publication.

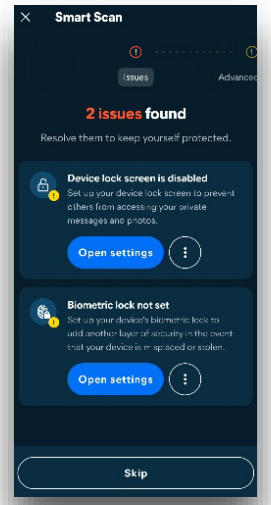
Avast
One Free
26.6.0

Introduction

Avast One Free is an ad-supported application offering a broad range of privacy and security tools, including anti-malware, safe browsing, app auditing, scam protection, Wi-Fi protection, a data leak checker, and a photo vault. Avast commissioned us to test and review the free tier. It is also worth noting that since Avast owns AVG, their respective Android apps deliver near identical functionality, with only minor variations in their user interfaces.







Usage

Upon opening the application, users must first agree to Avast's Privacy Policy and User Agreement. Following a brief overview of main features, users are prompted to allow notifications and select a free or paid tier. The app then initiates a preliminary scan, necessitating permissions to finish. Various tools are accessible via the bottom navigation bar, but any features locked behind a premium subscription will show a banner suggesting an upgrade.

Anti-Malware

Once the preliminary scan is complete, the application prompts users to address potential security vulnerabilities, like activating or establishing a screen lock. Users may then opt to initiate a further scan at their discretion.

Web & Wi-Fi Protection

Web Guard protects against malicious URLs and phishing websites across different browser apps. The Wi-Fi scan detects vulnerabilities on the currently connected Wi-Fi network.

App Audit

App Insights details the permissions each application requires, letting users adjust access rights or delete apps directly. Additionally, it categorizes applications based on the permissions they request, assigning them a "low", "average", or "high" risk designation relative to their overall access demands.

Privacy Protection

Hack Alerts notifies users if any accounts associated with their email addresses have been involved in a data breach.

The Scam Guardian feature adds an extra layer against deceptive practices, while the Privacy Advisor provides actionable guidance on securing private information across the apps installed on the device.

Additional Features

With Photo Vault, users can safely lock away a maximum of ten pictures behind a unique PIN. The Wi-Fi Speed Test can be used to evaluate the speed and reliability of the current network.

The integrated Junk Cleaner works to scan for and eliminate unnecessary digital clutter. My Statistics displays a summary of Avast's security measures, such as the total number of threats successfully blocked.

Conclusion

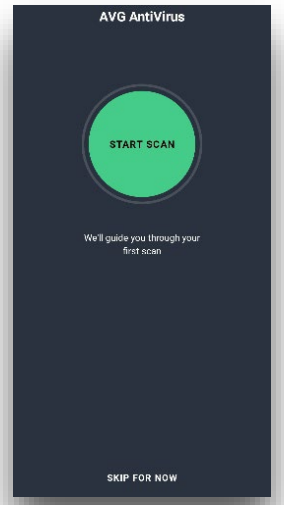
Avast One Free is a well-crafted anti-malware application that delivers a variety of security features, though with certain restrictions. It additionally features optimization and privacy-boosting tools, offering step-by-step walkthroughs to help configure each function.

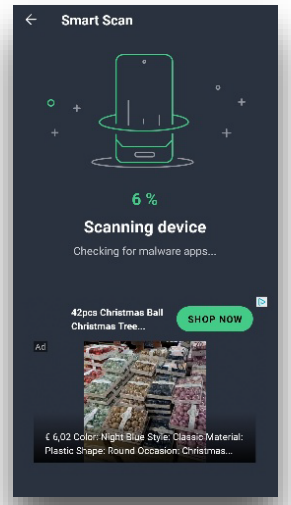
AVG

AntiVirus Free
26.6.0

Introduction

Operating as an ad-supported security application, AVG AntiVirus Free delivers a broad range of privacy and protection capabilities. These tools feature anti-malware, Wi-Fi security, safe browsing, app auditing, a data leak checker, and a secure photo vault. At AVG's request, we evaluated the free tier of their app. It is worth noting that Avast is the parent company of AVG; consequently, their respective Android applications function near identically, differing only slightly in their user interfaces.





Usage

When launching the application, users are required to agree to AVG's Privacy Policy and User Agreement. Following a short summary of primary features, the app requests notification permissions and prompts the user to choose a premium subscription. Next, an introductory scan begins, necessitating full file access. If opting for the free, ad-funded tier, users must also consent to personalized advertising. Every feature can be accessed through the bottom navigation bar.

Anti-Malware

Following the preliminary scan, the application recommends addressing possible security vulnerabilities, such as activating web protection and configuring a screen lock. Users have the option of a deep scan, which evaluates all storage and device configurations, or a file scan, which targets specifically chosen files and folders.

Web & Wi-Fi Protection

Web Shield protects against malicious URLs and phishing websites across different browser apps. The Wi-Fi scan detects vulnerabilities on the currently connected Wi-Fi network.

App Audit

App Insights displays the permissions required by each app, enabling users to manage app permissions or uninstall apps directly. Apps are also grouped by the permissions they request and labelled with risk levels "low", "average", or "high", based on their access requirements.

Privacy Protection

Hack Alerts notifies users if any accounts associated with their email addresses have been involved in a data breach.

A *Privacy Advisor* supplies tutorials on enhancing personal data protection across multiple applications.

Additional Features

The Photo Vault enables users to safely hide up to ten images, requiring a custom PIN to unlock them. The Wi-Fi Speed Test evaluates the performance of the current network. My Statistics delivers an overview of AVG's protective measures on the device, such as the total number of threats blocked.

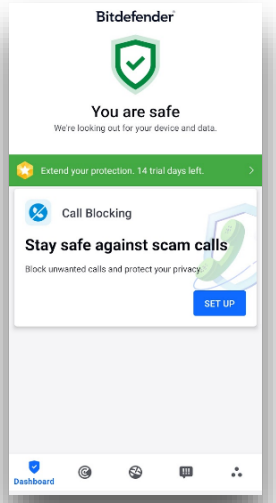
Conclusion

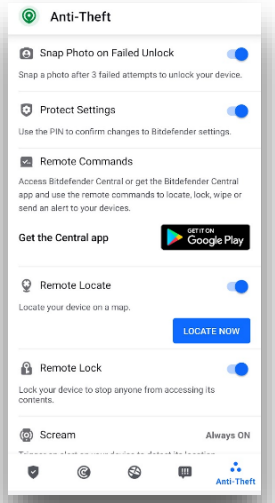
AVG AntiVirus Free is an intuitively crafted anti-malware application, providing an array of security capabilities, despite certain restrictions. It additionally features utilities for optimization and privacy enhancement. The app supplies a step-by-step walkthrough to configure every function.

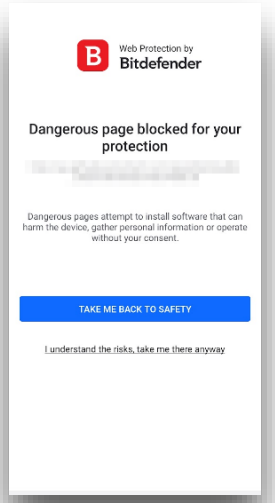
Bitdefender
Mobile Security
3.3.295

Introduction

Bitdefender Mobile Security is a paid-for security solution for Android. The app includes additional security features such as anti-theft, safe browsing, app lock, data leak checker, scam protection for SMS and instant messages, and a basic VPN service. Device activity can be controlled and monitored remotely via the Bitdefender Central app or web interface at *central.bitdefender.com*.







Usage

Upon opening the app for the first time, users must agree to Bitdefender's subscription agreement, and either log in with an existing account or create a new one with a 14-day trial period. Users are then asked to grant notification permission and guided through the configuration of the necessary features, such as Malware Scanner and Web Protection. At the end of the setup process, users are prompted to run a first scan of their device. All functions are accessible via the bottom navigation menu.

Anti-Malware

Users are prompted to activate additional security features. The App Anomaly Detection setting monitors apps for malicious behaviour in real-time. Apps downloaded from non-official stores are scanned before installation.

Anti-Theft

Anti-theft components are listed in the table below. Users are asked to set up a device lock and an app-specific PIN to protect the anti-theft and app-lock settings. The remote commands *Locate*, *Lock*, and *Scream* can be sent to all connected devices from either the Bitdefender Central app or web interface. The *Snap Photo* feature takes a photo with the front camera, stores it on the device, and uploads it to Bitdefender Central if an incorrect PIN has been entered three times in a row.

During our testing, anti-theft commands sent from both the Bitdefender Central app and web interface failed to execute on the target device. However, after we reported the issue to Bitdefender, it was promptly resolved.

Web & Wi-Fi Protection

The Web Protection feature blocks malicious URLs and phishing websites in various browser apps and displays a notification upon visiting banking pages. The app also includes a VPN service, providing up to 200 MB of data traffic per day while connected to an automatically chosen server. By default, the app warns users each time the device connects to an open Wi-Fi network and recommends activating the VPN.

App Lock

The App Lock feature limits access to chosen apps, requiring a predefined PIN or biometrics (e.g., fingerprint, face recognition) to open them. The lock behaviour can be customized, and apps can remain unlocked while connected to trusted Wi-Fi networks. The Random Keyboard setting shuffles the number position on the keyboard each time the lock screen appears. When Snap Photo is enabled, the front camera automatically captures a photo after three failed unlock attempts.

Privacy Protection

The Account Privacy featured allows users to check if email addresses are included in known data breaches. Additional email accounts must be verified before being monitored. Chat Protection monitors incoming messages and app notifications for potential scam or spam links. This functionality is also available in supported messaging apps. The Scam Radar warns users when certain types of fraud become more common in their area. The app also includes a call blocking feature which automatically blocks calls from known scam and spam numbers as well as individual phone numbers.

Conclusion

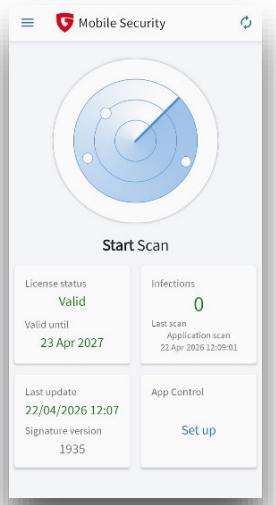
Bitdefender Mobile Security integrates a wide range of tools to monitor and protect device security and user privacy, all within a clean and intuitive user interface.

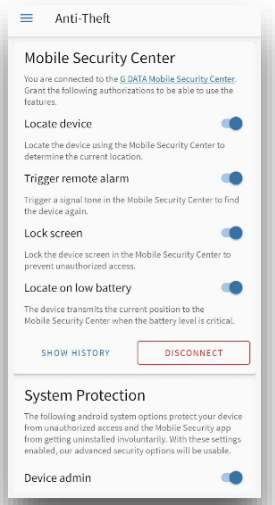
Anti-Theft Details		
Commands App & Web		
Locate	✔	Displays the device location of all registered devices on *Google Maps*.
Alert/Scream	✔	Sounds an alarm and optionally shows a custom message on the unlocked device. Alert cannot be switched off if the device is locked.
Lock	✔	Locks the device if a pre-defined Android lock screen is configured.
Additional Features		
Snap Photo	✔	Takes a picture with the device's front camera after 3 failed unlock attempts.

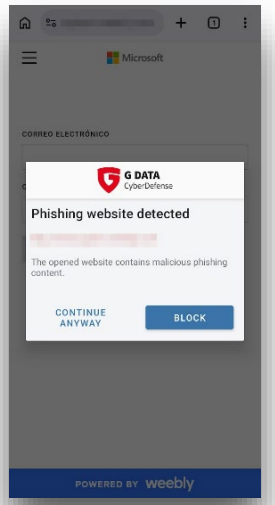
G DATA
Mobile Security
29.4.0

Introduction

G DATA Mobile Security is a paid-for security solution that incorporates various security- and privacy-related features such as malware scan, anti-theft, web protection, app lock, and app audit.







Usage

When first launching the app, users must accept the EULA and Privacy Policy and decide whether to share anonymous and/or malware-related data. After logging into their account, users are guided through a quick tour of the app's main components and asked to grant notification permission. Next, they can adjust scan-related settings and must grant the app access to all files and folders. Once setup is complete, the app opens the main screen. This dashboard shows app and license information and features a prominent scan button at the top of the page. Additional features can be accessed via the menu in the upper-left corner.

Anti-Malware

Users can set the scan type to App Scan or System Scan, checking installed apps only or all files stored on the device. Scheduled scans can also be configured. Signature updates can be set to run manually or at user-defined intervals, and there is also the option to restrict updates to Wi-Fi connections.

By default, G Data analyses newly installed apps and performs periodic scans.

Anti-Theft

Anti-theft commands are listed in the table below. To activate anti-theft, the device must be connected to the G DATA Mobile Security Center at *msec.gdata.de*, and the necessary permissions must be granted. Available features include device location (*Locate device*), remote alarm (*Trigger remote alarm*), and remote screen lock (*Lock screen*). The latter requires admin rights and a device lock screen to be set. Additionally, SIM card protection and locating the device on low battery can be enabled. The web interface allows users to issue remote commands, view and adjust app settings as well as access general device information along with a history of actions performed by the app.

Web & Wi-Fi Protection

When enabled, the Web Protection feature blocks phishing and malicious URLs in supported browser apps. It can be configured to activate only when connected to a Wi-Fi network.

App Lock & Audit

To enable App Control, users must create a PIN, which is required to open protected apps, set a security question, and provide a recovery email address. The feature also shows all permissions granted to an app and allows users to uninstall apps directly.

Conclusion

The G DATA Mobile Security app offers a simple, user-friendly interface with a solid set of security and privacy features. In our testing all anti-theft features worked flawlessly.

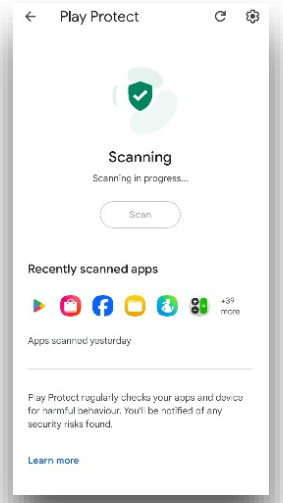
Anti-Theft Details		
Commands Web		
Locate device	✔	Displays the device location on *Google Maps*.
Trigger signal tone	✔	Sounds an alarm on the device. The alert is stopped, when the device is unlocked.
Lock screen	✔	Locks the device if a pre-defined Android lock screen is configured.
Additional Features		
SIM card protection	✔	Locks the device and sounds an alarm if the SIM card is removed or changed.

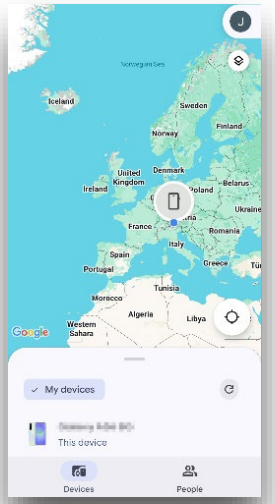
Google

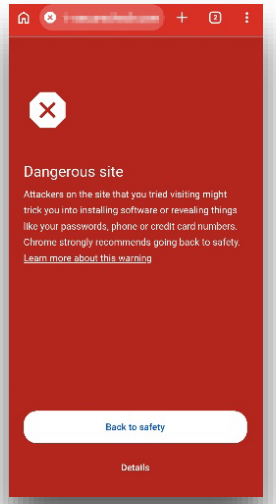
Play Protect & OS Features
50.9.23

Introduction

Android devices certified by Google are pre-equipped with Google Mobile Services (GMS) and Google Play Services, providing crucial APIs and apps that grant seamless access to Google platforms (e.g., Chrome and Gmail) via a unified account. Included in this ecosystem, Google Play Protect supplies native malware defence by constantly observing the device for harmful applications. Additionally, user privacy and security are fortified by anti-theft tools, safe browsing, and app auditing.







Usage

Play Protect is integrated into Google Play and available on supported, certified Android devices. Users can access it either via the Google Play app or Android system settings.

Anti-Malware

Utilizing both cloud-based analysis and on-device scanning, Play Protect identifies potentially harmful applications (PHAs) installed from either Google Play or external, third-party sources. Such applications might obscure critical details or abuse permissions to extract private data, thereby breaching Google's established policies. The system automatically inspects installed apps daily, though users maintain the ability to trigger manual scans at any time. If a PHA is discovered, the user receives an alert advising deletion, simultaneously preventing any future installations of that specific app.

Users also have the option to forward unfamiliar applications directly to Google for deeper evaluation. Both the scanning process and the submission of unknown apps can be toggled off within the Play Protect settings menu.

Anti-Theft

Anti-theft commands are listed in the table below. To issue commands to a lost or stolen device, users can use the Google *Find Hub* (formerly *Find My Device*) web interface at *google.com/android/find* or the dedicated app on a second Android device. Once a Google account is added to a new device, Find Hub features are enabled by default but can be changed via Android's security settings. The interfaces display the device's current or last-known location, battery level, time, and connection details (Wi-Fi name). The device can only be locked if a lock screen was previously configured.

Issuing the lock command signs the user out of the Google account and removes stored Google Wallet payment information. If the device is lost, users can provide a custom message and phone number which is displayed on the lock screen. A remote factory reset deletes all data from the internal and external device storage. Advanced screen lock features (e.g., automatic locking when theft is detected, device goes offline or remotely locking by a verified phone number) provide enhanced protection against theft. The opt-in feature "Identity Check" lets users lock critical Google and device settings (e.g., passkeys, passwords, changing unlock PIN or pattern, disabling Find Hub) behind biometric authentication, providing an additional layer of defence.

Web Protection

Google Chrome for Android incorporates Safe Browsing automatically. Utilizing "Standard Protection", users are warned about malicious downloads and risky websites. By switching to "Enhanced Protection", web links are forwarded to the cloud for comprehensive evaluation. Additionally, Chrome alerts users whenever their login credentials appear in recognized data breaches.

App Audit

The system settings within Android offer comprehensive details regarding installed applications, encompassing the download origin, version number, notification preferences, permission configurations, and resource consumption (e.g., mobile data, battery life, and storage). Users can uninstall or force-stop applications, as well as modify specific app permissions. The Permission Manager, alongside the "Special access" menu, categorizes applications based on their requested privileges (e.g., location, camera, contacts, device administrator rights, full file access, display over other apps, and installing unknown apps), thereby granting users greater control over their privacy. Furthermore, permissions for applications that remain unused for several months might be revoked automatically.

Conclusion

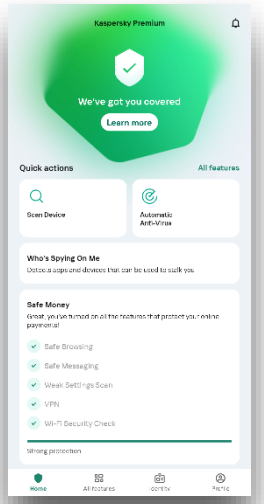
Google Play Protect comes preinstalled on certified Android devices as part of the broader GMS suite. Depending on the device manufacturer, additional security features may be offered that complement or overlap with pre-existing GMS apps such as Google Chrome and Find Hub. All anti-theft commands worked flawlessly.

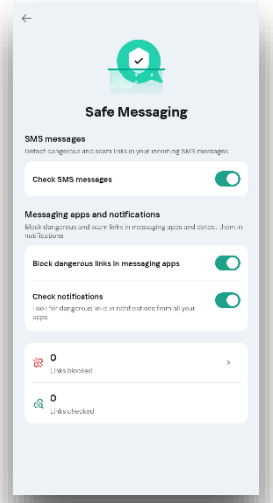
Anti-Theft Details		
Commands App & Web		
Locate	✔	Displays the current or last-known location of all registered devices on *Google Maps*.
Play Sound	✔	Plays the device's currently configured ring tone.
Secure device	✔	Locks the device with the pre-defined locking mechanism and signs out from current the Google account. A message and/or phone number can be displayed on the locked device screen.
Factory reset	✔	Triggers a factory reset and wipes the external storage.

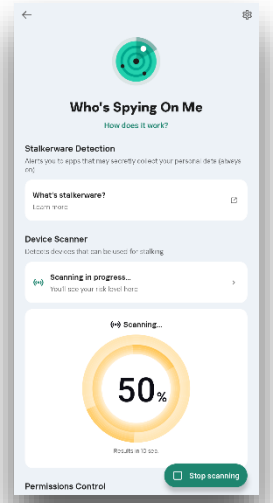
Kaspersky
Premium for Android
11.131.4

Introduction

Kaspersky Premium for Android is a well-rounded, paid mobile security solution. It offers a comprehensive set of tools to protect against malware, phishing, theft, and privacy violations. The app functionality is extended by additional features such as app lock, app audit, unlimited VPN, data leak checker, identity theft check, stalkerware protection, and notification protection. The Premium plan also includes licenses for separate Kaspersky apps, such as password manager and parental control (*Safe Kids*). Kaspersky apps are currently not available on Google Play. Users must download them from alternative sources, i.e., the Samsung Galaxy Store, Huawei AppGallery, Xiaomi GetApps, Transsion, RuStore, V-Appstore, Oppo Store or directly from Kaspersky's official website[16].







Usage

Upon initial launch, users must agree to Kaspersky's EULA and Privacy Policy. They can also optionally join the Kaspersky Security Network and consent to marketing data processing. Next, users may purchase a new license, activate a current subscription, or proceed using the restricted free version. Following a preliminary scan, the application prompts users to establish security configurations and device settings. The main dashboard provides shortcuts to update databases and execute quick scans, with all application features conveniently accessible through the bottom navigation menu.

Anti-Malware

When starting a scan, users may select a quick scan for installed applications, a full scan of all internal and external storage, or a targeted scan of specific files and folders. The configuration options provide granular control over scan frequency, update cycles, and operational behaviour. Out of the box, the application identifies adware and auto-dialers while examining both active apps and APK files.

Enabling the advanced anti-virus setting activates continuous monitoring of all file and app activities, with custom responses to detected threats. Users may also establish an automated scanning routine.

[16] https://support.kaspersky.com/common/beforeinstall/16085

Anti-Theft

Anti-theft commands are listed in the table below, located within the app's *Where Is My Device* section. Initial setup requires establishing a secret code, pattern, or fingerprint. Users may additionally activate *SIM Watch* and *Uninstallation Protection*. Through the *my.kaspersky.com* web portal, users can issue remote actions like *Lock & Locate*, *Alarm*, and *Mugshot*, including a personalized lock screen message. An email confirmation is dispatched upon the successful execution of a *Lock & Locate* or *Mugshot* command. The online dashboard also displays device metrics, such as battery life, active security tools, vulnerable settings, and captured photos, while providing a unique recovery code to restore access if biometrics fail or the unlock method is forgotten. All gathered data is automatically purged from the interface after 30 days.

Web & Wi-Fi Protection

The Safe Browsing component safeguards users from visiting phishing/scam websites in supported browser apps. When enabled, any in-app links will be opened in Chrome. Users must accept Kaspersky's VPN statement before using the unlimited VPN service. It then auto-selects the server closest to the device's location, but users can manually select other locations. Advanced features such as Split Tunnelling, Kill Switch, and auto-connect for unsecured networks can be configured via the VPN settings. Wi-Fi Security analyses the current network for vulnerabilities, prevents the device from connecting to unsecured Wi-Fi networks, and gives security advice. Smart Home Monitor notifies users when new devices join the current Wi-Fi network.

App Lock & Audit

App Lock secures sensitive apps using the same code, pattern, or fingerprint configured for anti-theft. The My Apps feature categorizes apps by permissions, displaying data and storage usage, while highlighting rarely used apps for quick uninstallation.

Privacy Protection

Safe Messaging evaluates links in SMS and instant chats for potential threats. Call Filter automatically rejects incoming calls from designated blacklisted numbers. Weak Settings Scan audits device configurations to uncover security flaws. *Identity Protection* includes a Data Leak Checker and Identity Theft Check to monitor connected emails and phone numbers for compromised information as well as the Identity Protection Wallet, providing an encrypted local storage for sensitive ID documents such as passports. The anti-stalking feature (*Who's Spying On Me*) helps identify potential stalking threats. Finally, Social Privacy assists in reviewing the privacy configurations of linked social media profiles to further enhance online security.

Conclusion

Kaspersky Premium for Android delivers extensive security and privacy features, which are clearly explained during setup and fully customizable. All anti-theft commands worked flawlessly.

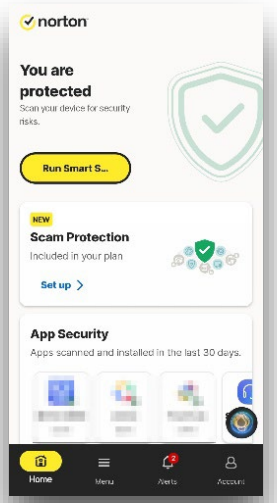
Anti-Theft Details		
Commands Web		
Lock & Locate	✔	Locks the device, displays the location on *Google Maps*, and sends the location in an email.
Mugshot	✔	Locks the device and takes several pictures using the front camera.
Alarm	✔	Locks the device and rings an alarm.
Additional Features		
SIM Watch	✔	Locks the device if the SIM card is removed or changed.
Uninstallation Protection	✔	Locks the device if device admin rights are removed from the app.

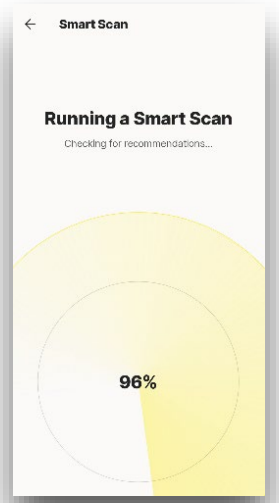
Norton

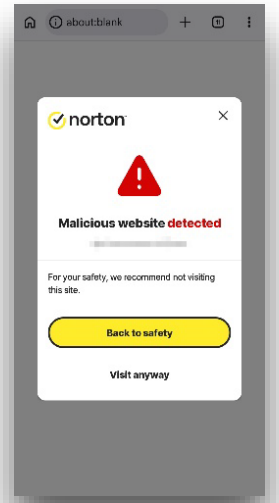
360 Deluxe
26.5.0

Introduction

As a premium mobile security solution, Norton 360 Deluxe protects Android devices with a broad spectrum of defences, from anti-malware and app auditing to safe browsing and scam protection. It extends to privacy with a built-in VPN, secure Wi-Fi capabilities, and active data leak monitoring. The Deluxe plan includes full access to standalone Norton apps for private browsing, parental controls and password management.







Usage

Upon first launching the app, users are required to accept Norton's subscription agreement. Activation involves selecting a subscription plan, inputting a product key, or signing in with an existing account. The app then leads users through a guided setup, prompting them to grant the necessary permissions to enable each security feature. Once complete, all tools are easily accessible from the bottom navigation bar.

Anti-Malware

By default, starting a scan from the main menu scans only apps installed by the user. However, security settings allow users to include system apps and files on internal or external storage. New installations are scanned automatically, and users can set up recurring scans.

Web & Wi-Fi Protection

Safe Web shields against malicious websites in supported browsers, Outlook, and Facebook. To protect connections, Wi-Fi Security analyses the active network for risks like weak encryption; this scanning can be automated if extended location permissions are granted. Furthermore, the native VPN includes manual server selection, a kill switch, split tunnelling, ad-tracker blocking, and auto-connect capabilities for unsecured Wi-Fi networks.

App Audit

In addition to app permissions, Norton reviews the privacy policies of installed apps and highlights the types of data they collect. The Device Security feature identifies potentially insecure Android system settings and provides recommendations to mitigate risks.

Privacy Protection

The Safe SMS feature analyses incoming texts for malicious links. In the Identity hub, users can check for data breaches involving sensitive information like emails, phone numbers, passports, and credit cards. Lastly, the Privacy Monitor helps users discover if data broker platforms are hosting and sharing their personal information.

Additional Features

Norton Genie utilizes AI detection technology to check user-provided content, including images, URLs, and text messages, for potential scams.

Conclusion

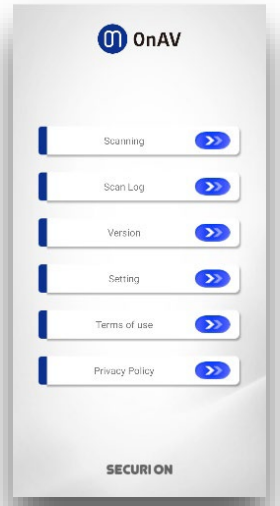
Norton 360 Deluxe offers a variety of security and privacy features in a modern, intuitive user interface. The app provides clear, step-by-step setup guidance for each feature.

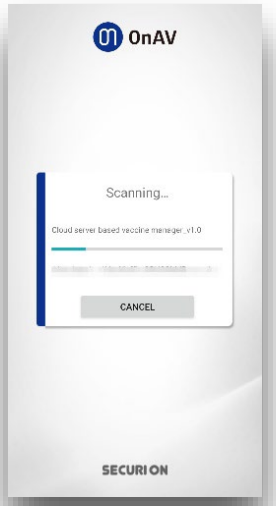
Securion

OnAV – Global
1.0.42

Introduction

Securion OnAV is a free, lightweight mobile security application dedicated primarily to defending devices against malware. This review evaluates the app's global edition, which is distinct from its original Korean release.





Usage

Upon initial startup, users must agree to the EULA, Terms and Conditions, and Privacy Policy. The app bypasses user registration entirely. Instead, it generates a distinct device ID to stop duplicate sign-ups. All features and data can be easily accessed through the clean, straightforward main dashboard.

Anti-Malware

The automatic real-time protection can be turned on and off via the app settings. The on-demand scanner checks the internal storage for malicious apps and files. Scan results display detected threats along with their full file paths, allowing users to review and delete items selectively. Previous scan results are stored in the Scan Log.

Conclusion

Securion OnAV is a free, straightforward mobile security app that offers essential malware protection without requiring registration.

Tencent

腾讯手机管家

16.1.38

Introduction

腾讯手机管家 is a free mobile security and device optimisation application developed for the Chinese market. The app is not available on Google Play and can only be downloaded from Chinese app stores (e.g., Tencent AppStore) or directly from the vendor's official website[17]. The user interface is exclusively in Chinese. During both the protection test and product review, a VPN connection to a server in Hong Kong was required in order to properly access and evaluate all supported features, including malware protection. Please note that this review reflects the Chinese market version of the product, and that the test results may not be representative of a potential international version of the product.

Usage

Once downloaded from the official website, the app requires users to agree to the EULA and grant device permissions. Users can initiate an optional scan, which cleans the system and flags any potentially unsafe settings, before gaining full access to the remaining app features.

Anti-Malware

Within the settings, the app provides options for a full scan, a quick scan, and a smart scan that identifies malware and insecure device or network configurations. Notably, no option is offered to scan specific files or individual folders.

Parental Control

The app features a Child Protection mode (umbrella icon at the top). Within this section, users can find a combination of content monitoring tools, configurable alerts and reminders, along with device management settings to oversee how the smartphone is used. The device can be configured for a parent or a child, and use of the feature requires a WeChat account.

[17] https://m.qq.com/

Privacy Protection

腾讯手机管家 provides built-in tools to detect and block spam calls and text messages. The app also offers an AI-powered call assistant to WeChat-/QQ-registered users that can answer and screen incoming calls on the user's behalf. Additionally, a privacy cleaning feature removes personal data and metadata from photos and messages.

Additional Features

The app includes a range of additional features beyond its core security functions. Remote connectivity tools allow users to link their mobile device to a computer for file and photo sharing, as well as remote control of the PC, including screen lock and shutdown. The app further provides file and storage management tools and a system optimisation function. Several of these features require a WeChat or QQ account.

Conclusion

腾讯手机管家 is available exclusively in Chinese and is tightly integrated with Tencent's QQ and WeChat platforms. It provides useful security and device optimisation features within a clear interface.

Feature List Android Mobile Security (as of May 2026)									
Product Name	*Android OS*	Avast One Free	AVG AntiVirus Free	Bitdefender Mobile Security	G DATA Mobile Security	Kaspersky Premium for Android	Norton 360 Deluxe	Securion OnAV - Global	Tencent 腾讯手机管家
Version Number	*16*	26.6	26.6	3.3	29.4	11.131	26.5	1.0	16.1
Supported Android versions	*built-in*	10 and higher	10 and higher	6.0 and higher	8.0 and higher	8.0 and higher	10 and higher	7.0 and higher	16 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, Chinese, Czech, Dutch, French, German, Greek, Hungarian, Italian, Japanese, Korean, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thailandese, Turkish, Vietnamese	English, Dutch, French, German, Italian, Japanese, Polish	English, Arabic, Bulgarian, Czech, Danish, Dutch, Finnish, French, German, Hungarian, Italian, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Thai, Turkish, Vietnamese	English, 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	Chinese
Anti-Malware									
On-Install/On-Update scan of installed apps	●	●	●	●	●	●	●	●	●
On-Demand scan	●	●	●	●	●	●	●	●	●
Scan requires online cloud connection	●			●					●
Can detect malware sitting on external SD card				●	●	●	●		
Safe Browsing (Anti-Phishing & Anti-Malware)	●	●	●	●	●	●	●		
Manual local database update possible (beside automatic updates)		●	●		●	●	●		●
User account needed to use product				●	●	●			
Customizable automatic (scheduled) scan					●	●	●		
Anti-Theft									
Web Interface for controlling Anti-Theft commands	●			●	●	●			
Remote Locate & Lock	●			●	●	●			
Remote Wipe (Factory Reset)	●								
Anti-Theft Alarm (cannot be muted by thief)				●	●	●			
Locate-Phone Alarm only (can be muted)	●								
Thief Cam				●		●			
App settings protected with password	●			●		●			
Uninstallation Protection (password required for uninstallation)						●			
Lock on SIM Change					●	●			
Additional Features (selected by AV-Comparatives)									
Hack Alerts / Data Leak Checker	●	●	●	●		●	●		
System Settings Checker	●	●	●			●	●		●
Wi-Fi Security / Smart Home Security		●	●	●		●	●		●
Privacy Advisor (audit app permissions)	●	●	●		●	●	●		
Task Manager (manage installed apps)	●				●	●			
Notification/Scam/Link Protection	●			●		●	●		
System Optimizer	●	●	●						●
App Lock				●	●	●			
Call Blocker/Filter	●			●		●			●
VPN				●		●	●		
VPN is limited / not available for users in the following countries				Belarus, China, Iran, Iraq, North Korea, Oman, Russia, Turkey, Turkmenistan, Uganda, United Arab Emirates		Belarus, China, India, Iran, Oman, Pakistan, Qatar, Russia, Saudi Arabia	Belarus, Cuba, Iran, North Korea, Syria, Russia		
Support									
Online Help & FAQ	●	●	●	●	●	●	●		●
User Forum	●	●	●	●		●	●		●
Email Support				●	●	●	●		
Phone Support				●	●	●	●		
Online Chat				●		●	●		
Supported languages of support	All	English, Czech, Dutch, French, German, Italian, Japanese, Polish, Portuguese, Russian, Spanish	English, Czech, Dutch, French, German, Italian, Japanese, Polish, Portuguese, Spanish	English, Chinese, Dutch, French, German, Italian, Portuguese, Romanian, Spanish, Swedish	English, Dutch, French, German, Italian, Japanese, Polish	English, Chinese, Czech, Dutch, French, German, Hungarian, Italian, Japanese, Portuguese, Romanian, Russian, Spanish, Turkish, Vietnamese	English, Chinese, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Turkish		Chinese
In-App List Price (without discounts; prices may vary)									
Price 1 Device / 1 Year (USD/EUR)	FREE	FREE	FREE	USD 29 / 29 EUR	USD 10 / 10 EUR	USD 90 / 80 EUR	USD 60 / 55 EUR	FREE	FREE

Copyright and Disclaimer

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

AV-Comparatives
(June 2026)