Independent Tests of
Anti-Virus Software

Stalkerware Test 2025

TEST PERIOD: AUGUST – SEPTEMBER 2025
LAST REVISION: 3RD NOVEMBER 2025

IN COOPERATION WITH: EFF

WWW.AV-COMPARATIVES.ORG

Contents

Introduction

Digital devices hold our most private conversations, photos, and movements. For many years, a particularly insidious threat has turned these trusted tools into instruments of surveillance in personal relationships: *stalkerware*. Although detection reports showed a decline after a peak in 2020, recent research confirms that technology-enabled abuse through stalkerware remains widespread[1].

What Stalkerware Is and Why It Matters

Stalkerware is software that monitors an electronic device, such as a computer, tablet, or smartphone, without the owner's knowledge or consent, giving an abuser continuous access to the victim's private life. Typical capabilities include reading text messages, viewing photos, tracking GPS location, recording phone calls, logging keystrokes, and monitoring app and screen activity.

Its danger lies in the veneer of legitimacy under which it is distributed. Many stalkerware functions also exist in parental-control or employee-monitoring tools, creating a grey market where applications marketed for legitimate use are exploited for abuse. Reports from domestic-violence shelters and researchers show that stalkerware is still common in intimate-partner abuse cases[2]. This has fostered a profitable "stalkerware-as-a-service" industry, offering subscriptions, technical support, and affiliate programs. Vendors are fully aware of the dual-use nature of their products, which are deliberately engineered for stealth.

Legal and Regulatory Context

The legality of stalkerware varies by jurisdiction. While it may be legal to buy and sell such software, using it to monitor someone without their knowledge is often a crime. Vendors typically include disclaimers in their terms and conditions, requiring customers to obtain permission before installation, yet design their apps to remain hidden and untraceable. Such warnings are therefore largely meaningless.

Installation and Persistence

Most stalkerware cannot be installed remotely; for most products, the abuser requires unrestricted physical access to the victim's device. Once installed, stalkerware typically removes its app icon, runs silently in the background, and sends collected data to an online dashboard accessible via the vendor's website. The scope and frequency of monitoring depend on the product and purchased license. Furthermore, stalkerware is often designed to resist removal, for example, by blocking access to system settings or requiring a password set by the abuser to uninstall.

Platform Mitigations and Limitations

Google has introduced several countermeasures on Android, including banning stalkerware from Google Play, using Google Play Protect to warn and block apps, and making it harder for apps to automatically hide themselves after setup. While these efforts improve detection, they are not foolproof. Most stalkerware apps are now *sideloaded* directly from developer websites, often with instructions to disable built-in protections and third-party antivirus or hide the app. Even with the latest security updates, users are not fully immune.

[1] https://stopstalkerware.org/2024/12/12/understanding-technology-enabled-abuse-in-modern-relationships/

[2] https://pmc.ncbi.nlm.nih.gov/articles/PMC10486147/, https://www.cdc.gov/nisvs/media/pdfs/stalking-brief.pdf

Data Security Risks

Security research has shown that stalkerware vendors frequently operate insecure servers. Consequently, the sensitive data collected from victims, including messages, photos, contacts, browsing histories, and locations, is not only accessible to abusers but also vulnerable to public leaks. In multiple cases[3], compromised backend systems have exposed this information on the open Internet, and some breaches even forced vendors to discontinue their businesses. Stalkerware is therefore not only a tool of intimate-partner abuse but also a significant cybersecurity and data-protection risk.

About This Report

This report is a collaborative effort between AV-Comparatives and the Electronic Frontier Foundation (EFF)[4] to evaluate the ability of mobile security products to detect commercial stalkerware apps for Android.

EFF is a non-profit organisation that defends civil liberties such as privacy and free speech in the digital world through legal action, policy analysis, and activism. Together with cybersecurity companies, digital rights organisations, and survivor-support groups, EFF was one of the founding members of the Coalition Against Stalkerware (CAS)[5] in November 2019 to address the growing misuse of such tools in domestic violence and abuse. The coalition's objectives include defining best practices, raising awareness, providing training, strengthening the technical capacity of support organisations, and improving the cybersecurity industry's response through sample sharing and consensus-based detection criteria.

In addition to assessing product performance, this report provides empirical data to support EFF's key recommendations for the cybersecurity industry. Security products should not only detect stalkerware but also label it clearly, rather than using generic terms such as "Potentially Unwanted Application". Detections should also be handled carefully: products should not allow stalkerware onto safe lists, should notify users through a secure channel, and should give them an informed choice about removal, since deletion may alert the abuser. Our test results show which products meet these standards and provide a benchmark for further improvement.

The report's Appendix outlines best practices for the detection, removal, and prevention of stalkerware, building on the guidelines of CAS and extending them with additional recommendations.

[3] https://techcrunch.com/2024/05/28/pctattletale-spyware-shutters-data-breach/
https://techcrunch.com/2024/02/02/phonespector-highster-stalkerware-shut-down/
https://techcrunch.com/2023/06/27/letmespy-hacked-spyware-thousands/
https://techcrunch.com/2022/12/12/xnspy-stalkerware-iphone-android/

[4] https://www.eff.org/

[5] https://stopstalkerware.org

Test Procedure

This test, conducted in September 2025, evaluated the ability of mobile security products to detect and alert on commercial stalkerware apps for Android. **Seventeen** popular stalkerware apps, selected together with EFF, were tested on a non-rooted Samsung Galaxy A36 running Android 15 with Google Chrome and an active Wi-Fi connection. The latest app versions available at the time of testing were used. For every stalkerware product, the highest-tier license was purchased to enable the full feature set, and a new user account was created.

Installation was performed in accordance with each vendor's instructions. Since stalkerware is typically distributed through sideloading, the option to install unknown apps was enabled in the Android security settings. In several cases, vendors advised disabling on-device protections such as Google Play Protect to avoid installation interference. Each app was then installed and configured, with all requested permissions granted, including device administrator rights. When suggested, the app icon was hidden and forensic traces were removed after setup (e.g., browser history, downloaded APK files, recent apps, and notifications). The aim was to replicate a realistic scenario from a victim's perspective.

Once the stalkerware was in place, the mobile security products were evaluated sequentially. For each product, a user account was registered, a license was activated to unlock the full protection feature set, and the app was installed from Google Play. Testing consisted of up to three scan stages to give each security product the best opportunity to identify the stalkerware:

1. **Initial scan:** the default scan prompted at first launch, which varied by product between an app-only or full-device scan.
2. **Full scan:** a manual full-device scan with default settings, initiated if not already included in the initial scan.
3. **Advanced full scan:** a repeat full-device scan at the highest possible protection level, with additional detection options enabled (e.g., potentially unwanted applications, adware, riskware, or system apps). In some cases, these settings were already active by default or unavailable to users.

A stalkerware app was considered detected if the mobile security product displayed a clear, user-facing warning or detection message during any of these scans. Where detections occurred, the quality of the information provided, and the options offered for mitigation were evaluated. After each product test, the device was reset to factory settings before the next stalkerware testcase was installed.

Tested Products

We examined **thirteen** well-known mobile security apps for Android. The products, selected in collaboration with EFF, and their respective versions at the respective time of testing (September 2025) are listed below.

Product	Version
Avast Mobile Security	25.17
Avira Antivirus Security	7.28
Bitdefender Mobile Security	3.3
ESET Mobile Security	11.0
F-Secure Total Security	5.8
G Data Mobile Security	29.2
Google Play Protect	48.0
Kaspersky Mobile Security[6]	11.124
Malwarebytes Mobile Security	5.18
McAfee Mobile Security	9.8
Norton 360 Mobile Security	5.121
Sophos Intercept X for Mobile	9.7
Trend Micro Mobile Security	17.1

Test Results

The stalkerware apps used in this assessment are not named. This decision serves both to avoid promoting such products and to prevent potential abusers from identifying which mobile security solutions may fail to detect their preferred software.

The objective of this test is to encourage vendors to strengthen stalkerware detection generally, rather than to focus narrowly on the specific testcases included in a single test. For this reason, vendors are not informed in advance which stalkerware apps are being evaluated or when testing will occur. Updated versions of previously tested stalkerware may be reused in subsequent assessments to verify whether detection capabilities are being maintained or improved over time.

The table below summarizes the results for each mobile security product, including detections of the selected stalkerware testcases and the overall detection rate. Results are based on **full scans**, with the exception of Google Play Protect, which only scans installed apps. Performing advanced full scans did not change the outcomes or lead to additional detections.

[6] Currently not available on Google Play. Downloaded and installed from the official vendor website.

Testcase	Avast	Avira	Bitdefender	ESET	F-Secure	G Data	Google	Kaspersky	Malwarebytes	McAfee	Norton	Sophos	Trend Micro
Stalkerware 1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 2	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗
Stalkerware 3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Stalkerware 4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗[7]	✓	✓
Stalkerware 5	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗
Stalkerware 6	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✗
Stalkerware 7	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗
Stalkerware 8	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗
Stalkerware 9	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✗
Stalkerware 10	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 11	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
Stalkerware 12	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓
Stalkerware 13	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 14	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✓
Stalkerware 15	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Stalkerware 16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Stalkerware 17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Detection Rate	**88%**	**88%**	**94%**	**94%**	**88%**	**65%**	**53%**	**94%**	**100%**	**94%**	**82%**	**82%**	**59%**

✓ Stalkerware detected ✗ Stalkerware not detected

[7] Stalkerware prevented mobile security app from working properly.

Detection Results

The results show clear differences in performance between mobile security products. **Malwarebytes** stood out by detecting all stalkerware testcases, achieving a 100% detection rate. **Bitdefender**, **ESET**, **Kaspersky**, and **McAfee** followed closely with 94% each, showing consistently high effectiveness. **Avast**, **Avira**, and **F-Secure** also performed well, identifying 88% of the test set, while **Norton** and **Sophos** achieved moderate coverage, detecting around 82%. At the lower end, **G Data** (65%), **Google** (53%), and **Trend Micro** (59%) missed a substantial portion of the stalkerware.

The test also revealed that some stalkerware can actively interfere with security software. One testcase prevented Norton's app from functioning properly, showing that resilience against manipulation is as important as detection itself.

During testing, it became apparent that some stalkerware apps are essentially variations of the same underlying product. In several cases, they were simply rebranded versions that reuse components such as payment systems, backend infrastructures, admin dashboards, or APK files. To avoid redundancy, testcases with identical APK file hashes were treated as one product in the result table.

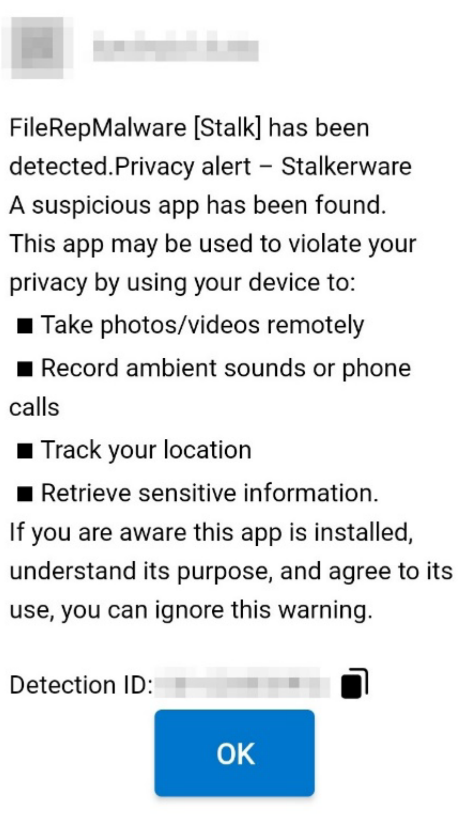
Threat Reporting

Beyond detection rates, the way security products report stalkerware to users is equally important. The clarity, accuracy, and safety of alerts determine whether victims can respond appropriately without putting themselves at greater risk. When a security product detects stalkerware it should provide clear warnings, contextual information, and safe removal options. Ideally, alerts should explain the potential capabilities of the detected app, such as monitoring calls, taking photos, recording audio, or tracking location, and warn that immediate removal may alert the perpetrator, thereby increasing the victim's risk. For this reason, automatic removal is inappropriate; removal options should only be offered after the victim has seen the warning and can make an informed choice.

In this test, a few products labelled the detected threat as stalkerware or provided descriptions that pointed towards it, using terms such as "spyware", "monitor app", or "this app can spy on you". These alerts included brief explanations of the threat's capabilities and were clearer for users. However, most products displayed only generic alerts such as "Malware detected", "Threat detected", or "Potential unwanted app detected". These provide limited context and make it difficult for victims to understand the risks or the nature of the application. Security vendors may face challenges in unambiguously identifying stalkerware, as its features overlap with legitimate tools, but greater clarity is still essential for supporting victims. Figure 1 shows examples of more informative and responsible detection alerts.

None of the tested products removed stalkerware automatically, which is appropriate. All allowed users to initiate uninstallation when they considered it safe. However, most products recommended immediate removal without explaining the potential risks of doing so. Only **Kaspersky** included a warning about possible consequences of immediate uninstallation, aligning with best practices.

As further recommended by CAS, the use of secure notification channels (e.g., email) to inform the user about a detection is not currently implemented in any of the tested products. Instead, alerts are shown immediately in the app or via push notifications. This approach risks exposing the detection event to the abuser if they are monitoring the device in real time through screen recordings, screenshots, or intercepted notifications.



[redacted]

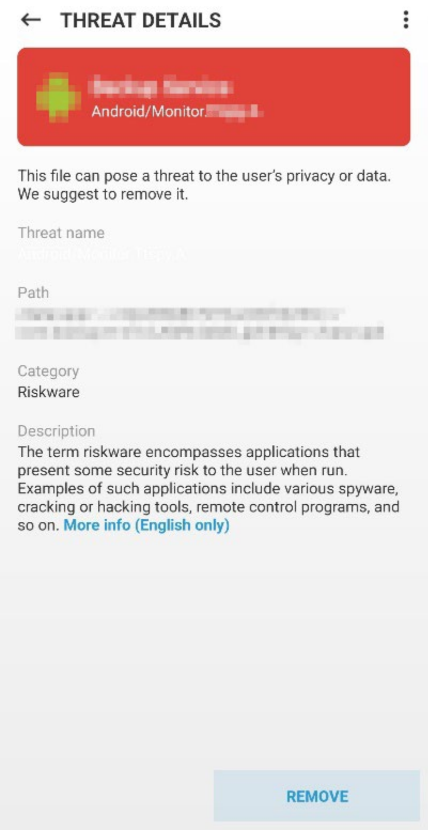
FileRepMalware [Stalk] has been detected.Privacy alert – Stalkerware

A suspicious app has been found. This app may be used to violate your privacy by using your device to:

- Take photos/videos remotely
- Record ambient sounds or phone calls
- Track your location
- Retrieve sensitive information.

If you are aware this app is installed, understand its purpose, and agree to its use, you can ignore this warning.

Detection ID: [redacted]



[redacted]
Android/Monitor.[redacted]

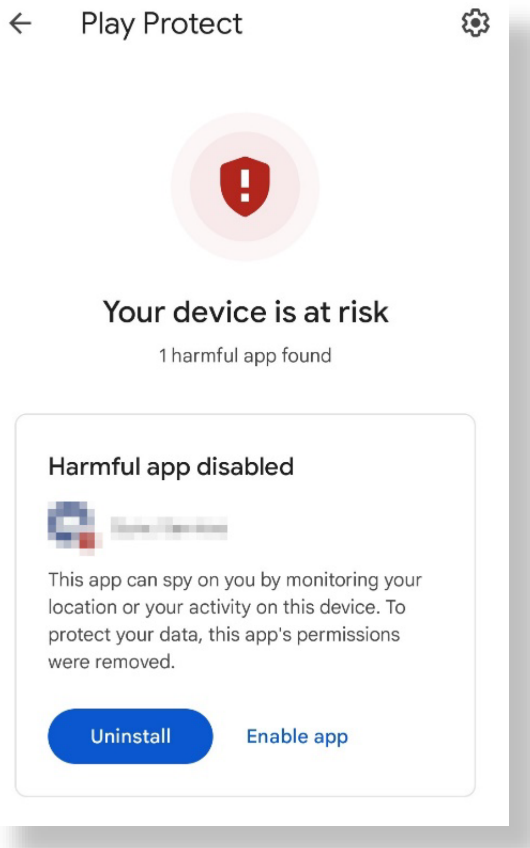
This file can pose a threat to the user's privacy or data. We suggest to remove it.

Threat name
[redacted]

Path
[redacted]

Category
Riskware

Description
The term riskware encompasses applications that present some security risk to the user when run. Examples of such applications include various spyware, cracking or hacking tools, remote control programs, and so on. More info (English only)



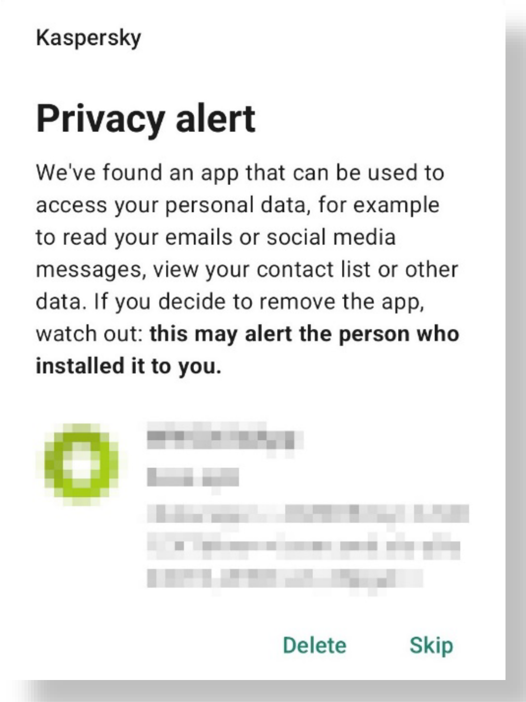
Your device is at risk

1 harmful app found

Harmful app disabled

[redacted]

This app can spy on you by monitoring your location or your activity on this device. To protect your data, this app's permissions were removed.



Kaspersky

Privacy alert

We've found an app that can be used to access your personal data, for example to read your emails or social media messages, view your contact list or other data. If you decide to remove the app, watch out: **this may alert the person who installed it to you.**

[redacted]

Figure 1 Examples of Stalkerware Detections on Android

Conclusion

This test has demonstrated that stalkerware remains a persistent digital threat, with significant variation in how effectively mobile security products detect and report it. While some solutions, such as **Bitdefender**, **ESET**, **Kaspersky**, **Malwarebytes**, and **McAfee**, achieved very high detection rates, others showed notable gaps, and even the strongest performers did not always deliver clear or context-rich warnings to victims. Generic alerts and immediate removal recommendations, without consideration of victim safety, remain common.

The findings underline two key points. First, victims cannot rely solely on built-in protections such as Google Play Protect, which detected only around half of the used stalkerware. Second, responsible handling of detections, including clear labelling, transparent explanations of potential risks, and safe removal options, is equally important to protect users in vulnerable situations.

Security vendors are encouraged to adopt consensus-based detection criteria and improve threat reporting in line with the recommendations of the Coalition Against Stalkerware. They should monitor publicly available lists of known stalkerware and indicators of compromise (IoCs) to strengthen detection capabilities. In addition, vendors should explore the use of secure, out-of-band notifications and ensure their products are resilient against tampering by stalkerware. By doing so, vendors can provide victims with both the technical means to detect surveillance and the necessary context to respond safely.

For users and victims of surveillance, strong mobile security products, combined with careful device practices and support from trusted organisations, remain the best defence. The best practices outlined in the Appendix provide practical guidance for detection, removal, and prevention of stalkerware.

Appendix

This appendix provides practical guidance on recognising, removing, and preventing stalkerware on mobile devices. It is intended both for users who may be at risk of surveillance and for practitioners supporting them. The recommendations build on the work of the Coalition Against Stalkerware (CAS) and related initiatives, and they are extended here with additional measures for device security and victim safety.

Best Practices on Stalkerware Detection

Stalkerware is designed to operate covertly, but certain technical and behavioural signs may indicate that a device has been compromised. The following indicators should raise suspicion and prompt further investigation:

- Unusual battery drain or high data usage.
- Unknown or suspicious apps listed in the device settings (*Settings* > *Apps*).
- Irregular device behaviour, such as screen captures, camera or microphone activity, unexpected notifications, or overheating while idle.
- New *Device Admin* profiles (Android) or unknown configuration profiles (iOS).
- Unfamiliar accounts or online dashboards linked to your device's data (e.g., device backups, sync services).

Best Practices on Stalkerware Removal

If stalkerware is suspected, it is important to proceed carefully. Taking action directly on the compromised device may alert the abuser. Only attempt to remove stalkerware if it is safe to do so.

Initial steps should be carried out from a safe device, such as a trusted computer or a separate phone. The following measures can help contain the threat and regain control:

- Change passwords for important accounts (e.g., email, Apple/Google accounts, banking, social media) and enable two-factor authentication. Use strong, unique passwords that cannot be guessed, and do not allow apps (other than a trusted password manager) to save them.
- On the suspected phone, review and remove unknown apps or profiles.
- On Android, revoke *Device admin rights* for suspicious apps before uninstalling them.
- Boot the Android device into Safe Mode, which prevents many stalkerware apps from running and makes them easier to uninstall.
- Run a reputable, independently tested anti-malware/anti-stalkerware solution with advanced detection settings enabled.
- If removal fails or compromise appears deep (e.g., hidden processes, root/jailbreak), back up essential data, perform a factory reset, reinstall only trusted apps from official stores, and reconfigure accounts securely.
- Preserve evidence (e.g., screenshots, logs) if you plan to report the incident, and seek assistance from local authorities or domestic violence/tech-safety organisations.

Best Practices on Stalkerware Prevention

Installing stalkerware generally requires physical access to the device. The following practices can reduce that risk and restrict access to sensitive data:

- Lock the device with a strong PIN, password, or biometric method known only to you, and configure it to lock quickly when not in use.
- Do not leave the device unattended or lend it to others, even briefly, as stalkerware can often be installed in less than a minute.
- Be cautious with new or gifted devices. Even shrink-wrapped smartphones may contain pre-installed stalkerware.
- Regularly check device security settings to ensure that "install from unknown sources" (Android) remains disabled.
- Regularly review installed apps and uninstall those you do not recognise or no longer need.
- Install apps only from trusted, official stores and avoid sideloading from unverified websites.
- Keep the device's operating system and apps updated to the latest versions.
- Keep built-in protections such as Google Play Protect active and perform regular scans.
- Consider running a trusted mobile security solution with stalkerware-detection capabilities for ongoing protection.

Further Resources

EFF's *Surveillance Self-Defense* guide provides step-by-step advice on securing devices and communications against surveillance, including measures relevant for stalkerware[8]. In addition, security vendors and public resources maintain detailed indicator lists that can be consulted for confirmation[9]. CAS also offers further recommendations and links to local authorities and support organisations that assist victims of threats and cyber violence[10].

[8] https://ssd.eff.org

[9] https://github.com/AssoEchap/stalkerware-indicators

[10] https://stopstalkerware.org/

TÜV AUSTRIA
ZERTIFIZIERT
ISO 9001:2015
20100141369414
TÜV AUSTRIA GMBH

Copyright and Disclaimer

This publication is Copyright © 2025 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
(November 2025)