TESTING GROUND

RIGOROUS. REAL. TRUSTED.

Android Malware Detection Test

Independent assessment of 10 consumer security solutions against 1,572 real-world Android malware samples.

TEST PERIOD	TEST DATE	REPORT VERSION	PUBLISHED
October 2026	2026.10.29	1.0	2026.11.22

10	1,572	288	8
PRODUCTS TESTED	MALWARE SAMPLES	CLEAN APPLICATIONS	5-STAR AWARDS



5-Star Monthly Award • October 2026

8 of 10 tested consumer products achieved 5-star ratings. Avast, Avira, F-Secure, Kaspersky, McAfee and NortonLifeLock achieved a perfect score of 100.00 with zero false positives across 1,572 malware samples. Dr.Web and AhnLab received 4-star ratings.

NAVIGATION

Table of Contents

01 Background

02 Test Process & Software

03 Tested Results

04 Test Summary & Award

05 Compliance

06 Rights & Disclaimer

v1.0 · 2026.11.22	Initial publication of the October 2026 Consumer Android Malware Detection Test report.

CHAPTER 01

Background

Android is a mobile operating system developed by Google, based on a modified version of the Linux kernel and other open-source software. It is the dominant OS for a wide array of devices including smartphones, tablets, televisions (Android TV), and automotive systems (Android Auto).

As of mid-2026, Android accounts for roughly 68—69% of worldwide mobile operating system usage, serving an estimated 3.9 billion users. Its reach is even greater in key growth markets: in countries such as India, Brazil, Indonesia, Vietnam, and Turkey, Android's share exceeds 85%. Google released Android 17 on June 16, 2026, yet adoption of any single release remains gradual — Android 16, the most widely used version, represented only about a quarter of Android traffic worldwide in June 2026 — so the installed base continues to be spread across many OS generations and patch levels. This scale and diversity keep the Android ecosystem a uniquely attractive target for cybercriminals.

VOLUME, GROWTH AND GEOGRAPHY

Zscaler ThreatLabz's 2025 Mobile, IoT and OT Threat Report, built on more than 20 million mobile threat-related transactions, recorded a 67% year-over-year rise in Android malware transactions, driven largely by spyware and banking Trojans. India was the most targeted country, receiving about 26% of mobile malware traffic (and 38% more attacks than a year earlier), followed by the United States (15%) and Canada (14%). Adware overtook the Joker family as the leading mobile threat at 69% of cases, while Joker fell to 23% from 38%. The same report counted 239 malicious apps on Google Play with a combined 42 million downloads, and documented a backdoor that infected 1.6 million Android-based TV boxes, primarily in India and Brazil.

BANKING MALWARE TARGETS ASIA-PACIFIC

Zimperium's 2026 Mobile Banking Heist Report tracked 34 active mobile malware families targeting 1,243 financial brands across 90 countries. Two-thirds of these families now enable full device control and 45% support financial extortion, including ransomware. In Asia-Pacific and Japan alone, 24 families were found targeting 214 core banking and fintech apps across 19 countries, according to a follow-up zLabs analysis published in September 2026. Regional campaigns continue to evolve: in October 2026, ThreatFabric reported a new Android banking remote access trojan, Hirudo, that replaces installed banking apps with patched copies to bypass their built-in security checks — with replacements identified for eight Indonesian banking apps, and credential targeting spanning Indonesia, China, India, Mexico, Morocco and Thailand. In August 2026, ThreatFabric also described Manic, a new family that blends banking-fraud functions with spyware and device-control features, targeting government institutions, banking applications and cryptocurrency wallets.

AI ACCELERATES THE ATTACKER SIDE

Zimperium's 2026 Global Mobile Threat Report, released on July 29, 2026, concluded that artificial intelligence is increasing the speed, scale and sophistication of mobile attacks, from more convincing phishing to malware development. The report cited LAMEHUG, an APT28 campaign that used AI to generate polymorphic malware on each execution, and PromptLock, the first identified AI-powered ransomware. For defenders, this reinforces the value of behavioral and machine-learning-based detection over purely static signatures.

STORE ENFORCEMENT AND THE SIDELOADING GAP

Google's 2025 ecosystem report shows both the scale of abuse and the effect of platform controls. Google prevented more than 1.75 million policy-violating apps from being published on Google Play and banned more than 80,000 developer accounts (down from 2.36 million apps and 158,000 accounts in 2024). Outside the store, Google Play Protect, which scans more than 350 billion apps daily, identified more than 27 million new malicious apps from non-Play sources in 2025, roughly double the 13 million found in 2024. Google's internal analysis found malware appears more than 90 times as often in apps installed from sideloaded sources as in apps from Google Play. Its enhanced fraud protection, which blocks risky sideloaded installs that request sensitive

permissions, now covers more than 2.8 billion devices in 185 markets and blocked 266 million installation attempts involving 872,000 unique high-risk apps in 2025; in Malaysia it is being rolled out with the National Cyber Security Agency.

PLATFORM AND POLICY DEVELOPMENTS

Google's Android developer verification program began with the Android Developer Verifier in system settings in April 2026, followed by limited-distribution accounts and an advanced sideloading flow worldwide in August 2026. The first enforcement phase took effect on September 30, 2026: in Brazil, Indonesia, Singapore and Thailand, apps installed on certified Android devices must now come from developers registered with Google. A broader global roll-out is planned from 2027, and Malaysia has announced that all apps on certified devices there must come from verified developers by 2027. Even so, dedicated security applications remain an important additional layer, particularly on older devices and in markets where apps are commonly obtained from multiple sources.

To protect users from this evolving threat landscape, dedicated Android security applications must be continuously evaluated against real-world threats. This test is designed to independently assess the efficiency of consumer security solutions for the Android OS.

Sources: Zscaler ThreatLabz, “2025 Mobile, IoT and OT Threat Report” and press release (Nov 2025); Zimperium zLabs, “2026 Mobile Banking Heist Report” (Mar 2026), “2026 Global Mobile Threat Report” (29 Jul 2026) and “Mobile Fraud in 2026” APJ analysis (1 Sep 2026); ThreatFabric Mobile Threat Intelligence, “Manic” (20 Aug 2026) and “Hirudo” (14 Oct 2026), as reported by The Hacker News; Google Security Blog, “Keeping Google Play & Android app ecosystem safe in 2025” (Feb 2026); Google Malaysia announcement on enhanced Play Protect; Infosecurity Magazine on Android developer verification; StatCounter Global Stats (mobile OS and Android version share, Jun 2026); Android 17 release information.

CHAPTER 02

Test Process & Test Software

This section outlines the methodology used for the test conducted in October 2026. The test environment and procedures were designed to ensure objectivity and reproducibility.

TEST DEVICE **Samsung Galaxy S22**	OPERATING SYSTEM **Android 14**
TEST DATE **2026.10.29**	PRODUCTS TESTED **10 consumer**
MALWARE SAMPLES **1,572 in-the-wild**	CLEAN APPLICATIONS **288 installers**

TEST ENVIRONMENT

- A Samsung Galaxy S22 was used as the primary testing platform.
- The device was running a clean installation of Android 14.
- Before each test run, the device was reset to a clean, pre-configured backup image to ensure a consistent state and prevent cross-contamination between tests.

TEST PROCEDURE

1. **Sample Collection:** A comprehensive test set was compiled, consisting of 1,572 recent, in-the-wild malware samples and 288 legitimate, clean application installers gathered from threat intelligence feeds and verified sources.
2. **Software Installation:** Each security application was installed on the test device using its default configuration settings.
3. **Signature Updates:** Prior to each scan, each application and its virus definitions were updated to the latest available versions to ensure peak detection capability.
4. **Static Analysis (On-Demand Scan):** A full file system scan was initiated. All detections and any false positives were recorded.
5. **Dynamic Analysis (Behavioral Test):** Each malicious sample not detected during the static scan was manually installed and executed. Behavioral or on-execution detections were recorded.
6. **False Positive Verification:** Clean applications were scanned only — not installed or executed — serving exclusively to measure the false positive rate.

TESTED PRODUCTS — SOFTWARE & VERSIONS

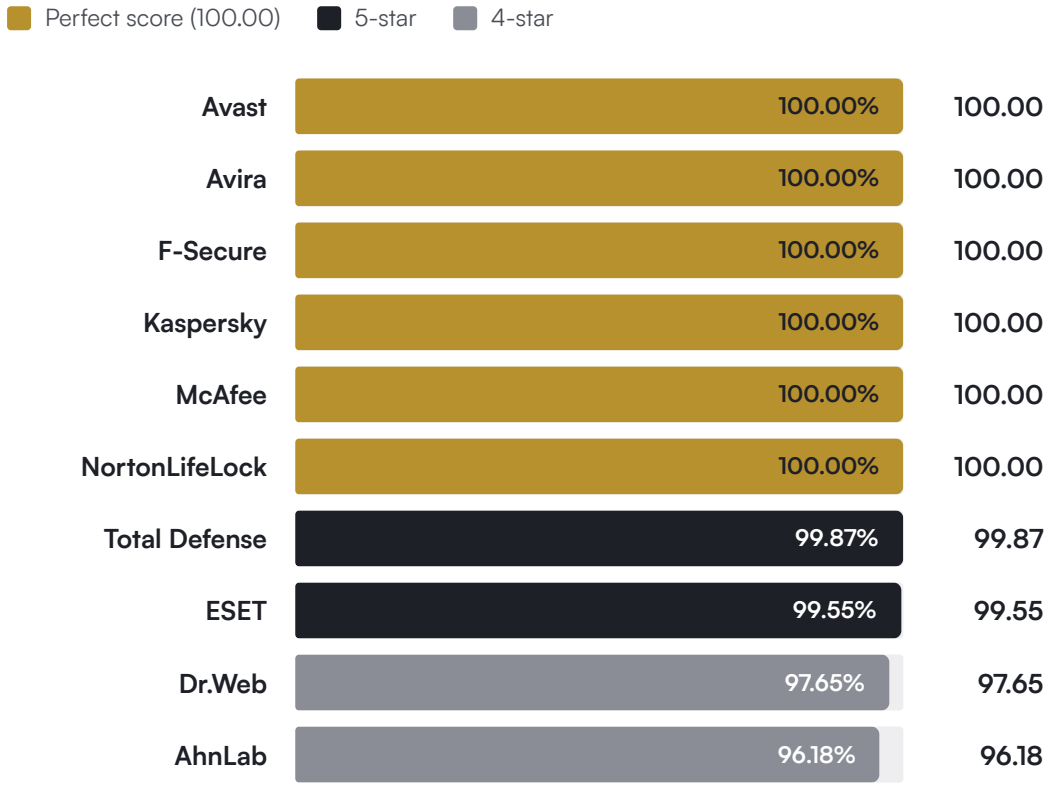
VENDOR	SOFTWARE	VERSION
AhnLab	AhnLab V3 Mobile Security	`3.14.0.2(Build 4313)`
Avast	Avast Mobile Security	`26.18.0.260925870`
Avira	Avira Antivirus Security for Android	`7.33.0 build No. 260908328`
Dr.Web	Dr.Web Mobile Security Suite	`12.9.12(2)`
ESET	ESET Mobile Security	`v. 12.0.17.0-15`
F-Secure	F-Secure Mobile Security	`26.9.1240618`
Kaspersky	Kaspersky Premium for Android	`11.133.4.15938`
McAfee	McAfee Mobile Security	`10.10.0.537`
NortonLifeLock	Norton 360 (Norton Mobile Security)	`26.18.0.260925980`
Total Defense	Total Defense Mobile Security	`16.4.3`

CHAPTER 03

Tested Results

Android Malware Detection Rate — Consumer Products

October 2026 • Testing Ground Labs • Total Samples: 1,572



VENDOR	TOTAL	MISSED	DETECTED	DETECTION RATE	FALSE POSITIVES	FINAL SCORE
Avast	1572	0	1572	100.00%	0	★ 100.00
Avira	1572	0	1572	100.00%	0	★ 100.00
F-Secure	1572	0	1572	100.00%	0	★ 100.00
Kaspersky	1572	0	1572	100.00%	0	★ 100.00
McAfee	1572	0	1572	100.00%	0	★ 100.00
NortonLifeLock	1572	0	1572	100.00%	0	★ 100.00
Total Defense	1572	2	1570	99.87%	0	99.87
ESET	1572	7	1565	99.55%	0	99.55
Dr.Web	1572	37	1535	97.65%	0	97.65
AhnLab	1572	60	1512	96.18%	0	96.18

For each security solution, a Final Score is calculated once the full test is performed:

$$\text{Final Score} = (\text{Detected} / \text{Total}) \times 100 - 0.2 \times \text{FP}$$

FINAL SCORE	MONTHLY AWARD
98.00 — 100.00	★★★★★ 5-star rating
95.00 — 97.99	★★★★ 4-star rating
90.00 — 94.99	★★★ 3-star rating

CHAPTER 04

Test Summary & Monthly Award

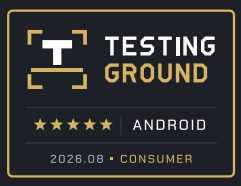
8 of 10 tested consumer products achieved 5-star ratings. Avast, Avira, F-Secure, Kaspersky, McAfee and NortonLifeLock achieved a perfect score of 100.00 with zero false positives across 1,572 malware samples. Dr.Web and AhnLab received 4-star ratings.

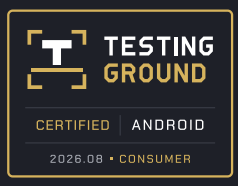
★★★★★ 5-Star Monthly Award — October 2026

Avast	Avira	F-Secure	Kaspersky
McAfee	NortonLifeLock	Total Defense	ESET

Gold outline = Perfect Score (100.00) with zero false positives

Dr.Web: 4-star rating (Final Score 97.65); AhnLab: 4-star rating (Final Score 96.18)





Products achieving 5-star ratings are entitled to display the Testing Ground Labs Monthly Award badge on their marketing materials, subject to the Rights Statement set out in this report.

CHAPTER 05

Compliance

AMTSO STANDARD V1.3 · COMPLIANCE REVIEW PENDING

This test was conducted in accordance with the requirements of the AMTSO Testing Protocol Standard v1.3 (https://www.amtso.org/standards/). AMTSO's compliance review of this test has not yet been completed; this chapter and the report version will be updated once AMTSO confirms the outcome.

`AMTSO Test ID: AMTSO-LS1-TP218`

CHAPTER 06

Rights Statement

Unless otherwise stated, Testing Ground Labs (hereinafter referred to as "TG Labs"), owns the copyright of this report. Without prior written consent of TG Labs, no other organization or individual shall have the right to alter the contents of this report and use it for commercial purposes by any means (including but not limited to transmission, dissemination, reproduction, excerpt, etc.).

Unless otherwise stated, TG Labs shall be the rightful owner of the trademarks and service marks used in the report. Any action of infringing upon the legal rights of TG Labs is prohibited. TG Labs shall have the right to pursue the legal liability of the infringer in accordance with the law.

Disclaimer

Before using this report issued by Testing Ground Labs (hereinafter "TG Labs"), please read and understand the following terms and conditions (the "Disclaimer") carefully, including provisions that limit or exclude TG Labs' liability and that restrict the rights of users. Use of this report constitutes acceptance of, and agreement to, all terms and conditions set forth herein.

1. The report is provided by TG Labs; all contents are provided for reference purposes only and shall not be construed as a recommendation, invitation, or warranty to choose, purchase, or use any products mentioned herein. TG Labs does not guarantee the absolute accuracy or completeness of the report's contents; readers should not rely solely on this report or substitute its findings for their own independent judgment.
2. The contents contained herein reflect TG Labs' assessment of the tested products' characteristics as of the date this report was published. TG Labs reserves the right to issue future reports containing different content or conclusions and is under no obligation to update this report or notify readers of any such updates.
3. The report may contain links to other websites provided solely for the readers' convenience. The contents of linked websites are not part of this report. TG Labs accepts no liability, direct or indirect, for any damages or losses arising from readers' access to or reliance on such linked websites.
4. TG Labs may have existing or future business relationships with companies whose products are mentioned in this report. Such relationships do not influence test methodology or results. Information on test funding and any material conflicts of interest is disclosed in the published test plan in accordance with the AMTSO Testing Protocol Standard.
5. Receipt of this report does not constitute the formation of any business, advisory, or client relationship between the reader and TG Labs. TG Labs does not owe any duty or accept any legal liability to the reader as a customer or client.
6. All products tested by TG Labs were procured through official and lawful channels. The findings of this report apply only to products obtained through equivalent channels, and not to products acquired through unofficial or unlawful means.
7. This report may reference trademarks, images, or intellectual property owned by third parties. If you believe your rights have been infringed, please contact TG Labs promptly.

TG Labs reserves the right to interpret, amend, and update this Disclaimer at any time.