TESTING GROUND

RIGOROUS. REAL. TRUSTED.

Android Malware Detection Test

Independent assessment of 4 enterprise security solutions against 1,368 real-world Android malware samples.

TEST PERIOD	TEST DATE	REPORT VERSION	PUBLISHED
August 2026	2026.08.29	1.1	2026.10.06

4	1,368	500	4
PRODUCTS TESTED	MALWARE SAMPLES	CLEAN APPLICATIONS	5-STAR AWARDS

5-Star Monthly Award • August 2026

All 4 tested enterprise products achieved 5-star ratings. ESET and Kaspersky achieved a perfect score of 100.00 with zero false positives across 1,368 malware samples.

NAVIGATION

Table of Contents

01 Background

02 Test Process & Software

03 Tested Results

04 Test Summary & Award

05 Compliance

06 Rights & Disclaimer

v1.1 · 2026.10.14	AMTSO compliance review completed; Compliance chapter updated. Report restyled to the current Testing Ground Labs visual identity. Disclaimer item 4 clarified. Test data and results unchanged.
v1.0 · 2026.10.06	Initial publication of the August 2026 Enterprise 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.

Kaspersky's quarterly telemetry offers a useful reference point for the current threat landscape. In the second quarter of 2026, more than 304,000 malicious installation packages were detected, a volume that remained steady compared with the previous quarter. At the same time, the number of attacks blocked on devices declined to about 2.0 million, from 2.7 million in Q1. The picture is therefore one of stable malware production alongside continuous adaptation, rather than of simple growth or decline.

BANKING TROJANS REMAIN THE LEADING CATEGORY

Trojan-Banker was the most prevalent category of mobile malware in Q2 2026, accounting for about 31% of detected applications, including more than 93,500 banking Trojan packages. This follows a strong 2025, in which Kaspersky recorded a 56% year-over-year increase in banking Trojan attacks on Android and roughly 255,000 new banking Trojan packages. The Mamont family continues to dominate real-world attack metrics, with newer variants steadily replacing older ones — a sign of active, ongoing

development. Meanwhile, the growing share of Creduz builds among newly identified samples, despite modest victim telemetry, suggests that operators are iterating on new builds ahead of broader campaigns.

DROPPERS, LOADERS AND STORE-REVIEW EVASION

A notable shift in Q2 2026 was the rising share of users targeted by droppers, driven in part by banking droppers. Several banking Trojans are now distributed in packed form and are therefore classified as droppers, which partly explains the movement between categories. Researchers also found malicious loaders on Google Play, including a trojanized PDF reader that presented a fake update prompt in order to stage the Anatsa banking Trojan. Another loader, found in an app named Cleanova, used SDK telemetry about the installation source and returned a payload only to selected targets, remaining dormant elsewhere and thereby avoiding app store scanners. Such techniques make static review of an app at publication time less informative on its own, and highlight the value of behavioral and on-device protection.

PRE-INSTALLED AND SUPPLY-CHAIN THREATS

Backdoors embedded in device firmware, such as Triada and Keenadu, continue to appear in telemetry; a Triada variant was again the most frequently detected malware type in Q2 2026. On a more encouraging note, Kaspersky observed a decline in attacks driven by certain pre-installed strains, a shift likely linked to the rollout of patched vendor firmware. Because these threats ship with the device itself, they are generally removable only by reflashing a clean firmware image.

SPYWARE AND DATA THEFT

Spyware families also featured in the quarter's rankings, with Trojan-Spy.AndroidOS.Btmob.e appearing in the top 20 for the first time. Once installed, such tools exfiltrate contacts, messages, photos and other personal data, which may subsequently be used for fraud, account takeover or extortion.

PLATFORM AND POLICY DEVELOPMENTS

On the platform side, Google's Android developer verification program entered its first enforcement phase on September 30, 2026. In Brazil, Indonesia, Singapore and Thailand, apps installed on certified Android devices must now come from developers

registered with Google, with an advanced installation flow retained for power users; a broader global roll-out is planned for 2027. Google has described the initiative as a response to malware spread through unofficial APK distribution, and it has also reported that Google Play Protect identified more than 27 million malicious sideloaded apps in 2025. 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.

For organizations, these developments matter in two ways. Managed fleets and BYOD programs frequently include devices on older OS releases or from regional vendors, where firmware patching is slower. And enterprise users are exposed to the same banking, spyware and credential-theft families as consumers — often on devices that also hold corporate email, messaging and identity applications. Mobile endpoint protection is therefore best assessed on the same real-world samples as consumer products.

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 enterprise security solutions for the Android OS.

Sources: Kaspersky Securelist, “IT threat evolution in Q2 2026. Mobile statistics” (10 Aug 2026) and “Mobile malware evolution in 2025” (Mar 2026); StatCounter Global Stats (mobile OS and Android version share, Jun—Sep 2026); Google Android developer verification documentation and Google Security Blog; Android 17 release information.

CHAPTER 02

Test Process & Test Software

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

TEST DEVICE **Samsung Galaxy S22**	OPERATING SYSTEM **Android 14**
TEST DATE **2026.08.29**	PRODUCTS TESTED **4 enterprise**
MALWARE SAMPLES **1,368 in-the-wild**	CLEAN APPLICATIONS **500 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 1,368 recent, in-the-wild malware samples and 500 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

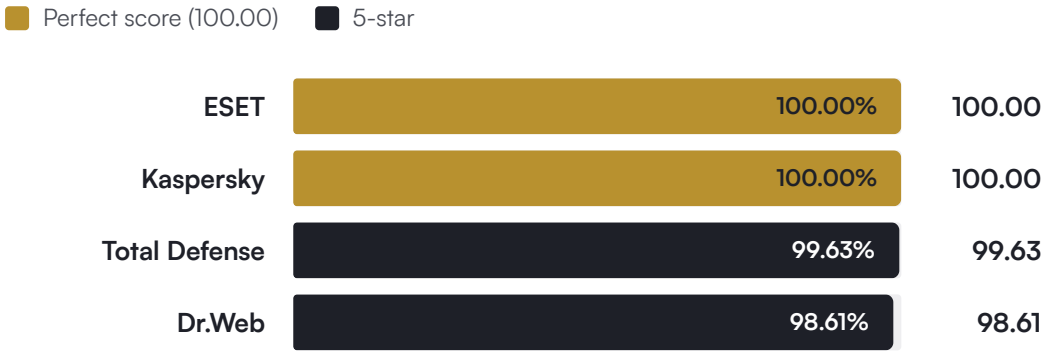
VENDOR	SOFTWARE	VERSION
Dr.Web	Dr.Web Mobile Security Suite	`12.9.11(2)`
ESET	ESET Endpoint Security for Android	`v 6.4.10.0-0`
Kaspersky	Kaspersky Endpoint Security for Mobile	`10.58.1.38`
Total Defense	Total Defense Mobile Security	`16.4.3`

CHAPTER 03

Tested Results

Android Malware Detection Rate — Enterprise Products

August 2026 • Testing Ground Labs • Total Samples: 1,368



VENDOR	TOTAL	MISSED	DETECTED	DETECTION RATE	FALSE POSITIVES	FINAL SCORE
ESET	1368	0	1368	100.00%	0	★ 100.00
Kaspersky	1368	0	1368	100.00%	0	★ 100.00
Total Defense	1368	5	1363	99.63%	0	99.63
Dr.Web	1368	19	1349	98.61%	0	98.61

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

$$\text{Final Score} = (\text{Detection \%}) \times 100 - 0.2 \times \text{FP}$$

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

All 4 tested enterprise products achieved 5-star ratings in the August 2026 Android Malware Detection Test from Testing Ground Labs. ESET and Kaspersky achieved a perfect score of 100.00 with zero false positives across 1,368 malware samples.

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

ESET	Kaspersky	Total Defense	Dr.Web

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

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

CONFIRMED COMPLIANT · AMTSO STANDARD V1.3

This test was conducted in accordance with the requirements of the AMTSO Testing Protocol Standard v1.3 (https://www.amtso.org/standards/), and AMTSO has confirmed it as compliant with the Standard.

The test record, including the published test plan and AMTSO's compliance information, is available on the AMTSO website: AMTSO test record.

`AMTSO Test ID: AMTSO-LS1-TP212`

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.

CHAPTER 07

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 is the judgment made by TG Labs to the product characteristics as of the date the 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 or client relationship between the reader and TG Labs. TG Labs does not accept any legal liability as the readers' customer.
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.