360°
Powered by Tempus

Android 360° Assessment Programme

Q3 2026

MRG Effitas

Copyright © 2026 MRG Effitas Ltd.

MRG Effitas Ltd.

MRG Effitas is a world-leading, independent IT security efficacy testing & assurance company. We are trusted by antimalware vendors across the world.

Management team:
Chris Pickard
Chief Executive Officer

Zsombor Kovacs
Chief Technical Officer

Website:
www.mrg-effitas.com

Email:
contact@mrg-effitas.com

Twitter:
@mrgeffitas

Contents

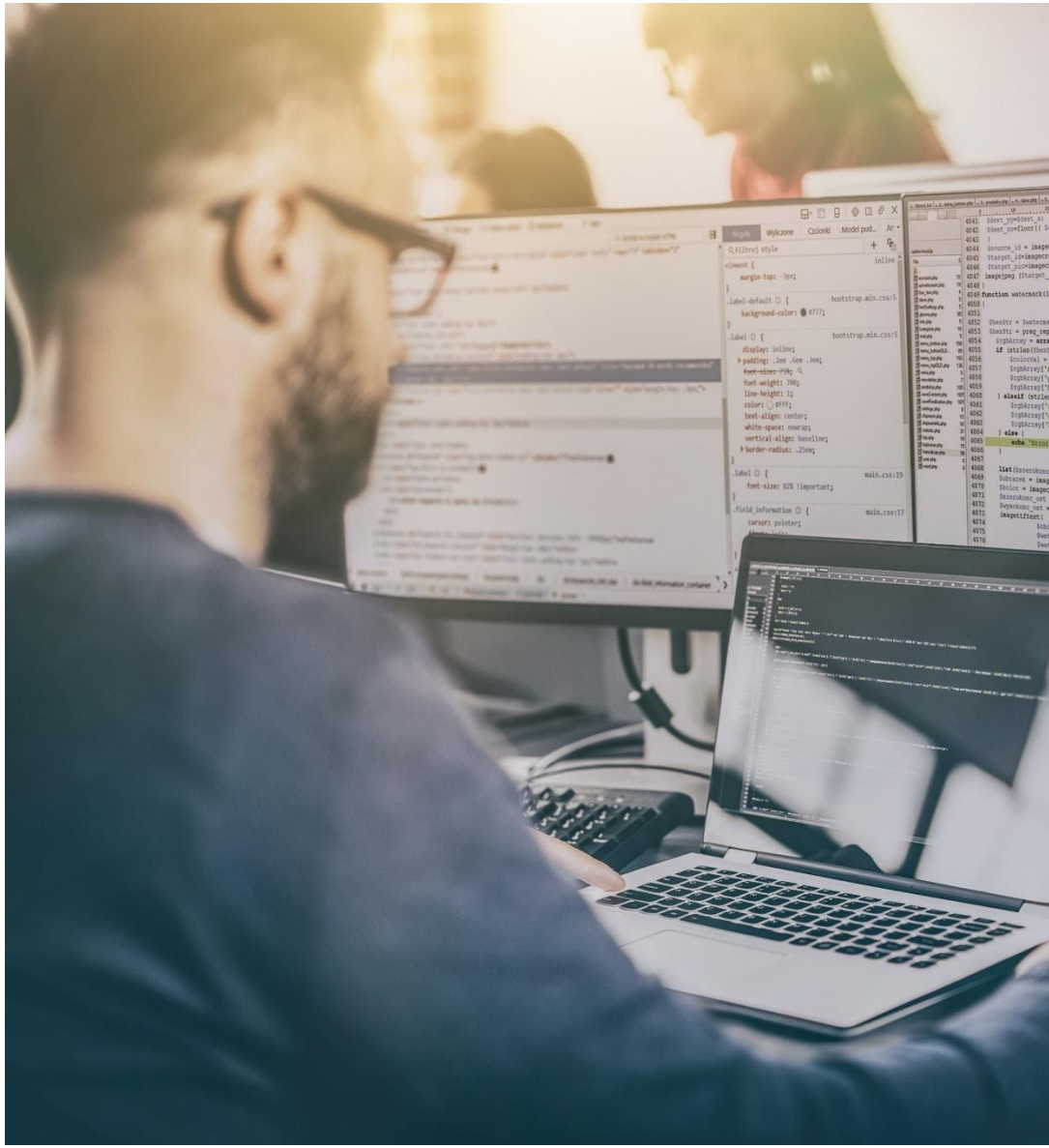
Introduction 3
Our Mission 4
Tests Applied 5
Testing Methodology 5
False Positive Tests 6
Samples 6
Malicious In-The-Wild Samples 6
Simulator samples 7
False positive samples 8
Security Applications Tested 8
Test Results 9
Overall non-PUA Detection 9
PUA Detection 10
Trojan Detection 11
Banking Detection 12
SMS Detection 13
Spyware Detection 14
Simulator Detection 15
False positive tests 16
Summary 16
Improvements in Our Test Bed 17
Conclusions 17

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Introduction

MRG Effitas is an independent IT security research company, with a heavy focus on applied malware analysis. Besides conventional AV efficacy testing and providing samples to other players in the AV field, we regularly test APT detection appliances and enterprise grade IT security products, simulating realistic attack scenarios.

Android devices are used by over 3.1 billion people on this planet, making Android one of the most widespread IT systems. As the overall platform philosophy allows an easy-to-opt in platform with no mandated central application distribution platform, Android-based malware has been on a constant rise since the early Gingerbread days. As a result, the market for Android AVs is heaving with applications that promise loud taglines with '100% security'. A quick search on the Play Store for Antivirus products reveals literally hundreds of results – our test aims to help user decisions with a complex test regime with both In-The-Wild (ITW) and artificially crafted simulator samples and results that reflect the real-life efficacy of our test participants.



Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder



Our Mission

In providing quarterly certifications, the MRG Effitas Android 360 Programme is the de facto standard by which security vendors, financial institutions and other corporations can attain the most rigorous and accurate determination of a product's efficacy against current financial malware attacks.

We test over twelve months beginning in Quarter 2 and ending in Quarter 1, at which point (or shortly after) we publish our results. As with all our certification testing, we work with vendors, offering feedback and helping them to improve their product as we go.

Products that pass all tests during a quarter will receive the MRG Effitas certification for Android Efficacy Protection.

More information about the compliance status of this test can be found on the AMTSO website.

https://www.amtso.org/tests/mrg-effitas-q3-2026-360-android-assessment-and-certification/

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Tests Applied

MRG Effitas performed an in-depth test of several Android AV applications. The level of protection provided was measured in real-life scenarios with in-the-wild pieces of malware as well as some benign samples to map the shortcomings of the applied detection mechanisms. This report summarises the results of our efficacy tests.

Testing took place on physical Pixel devices with Android version 16.
To ensure the cleanliness of the testing process, the Play Protect feature has been disabled.

Testing Methodology

The testing approach reflects a grounded and realistic take on what is usually a series of test batch runs in a simulated environment. To reflect the actual performance of Android AV products, we follow the following flow for each sample[1]. With this revised methodology, we aim to provide a better understanding of how the individual AV products provide protection and what the limits and potential problems might be.

1. We make sure that the AV product is updated, provided with the latest signatures, and the device is connected to the Internet. Prior to testing, we make sure that the default Play Protect is disabled.
2. Using an explicit intent, the default browser on the device is navigated to a web site with neutral reputation and instructed to download the sample .apk All browser security features are turned off, URL reputation warnings are dismissed.
3. The package is downloaded, and an automated sequence is initiated to install the downloaded package. All warnings are dismissed, and all appearing dialogs are accepted.

Should the AV display a warning or an alert...

a. ...in the download phase, the test case is counted as "Detection during download".
b. ...after the download has finished, but the application install has not yet started, the test case is counted as "Detection before install".
c. ...after the application install has finished, the test case is counted as "Detection after install".

Should the AV not display a warning or alert to the user, the test case is counted as a Miss.

It should be noted that on Android, installation of a piece of malware does not necessarily mean unwanted consequences for the user, as it is the first launch that kicks in any actual malicious code within. Having started the sample, however, it can have detrimental consequences from a security perspective. After the first launch, a piece of malware, after having requested SYSTEM_ALERT_WINDOW permission, can continuously display a Device Administrator or an Accessibility Admin request screen to the user. In such cases, the user is unable to get rid of the application as they have no

[1] A full AMTSO-approved test plan can be found on https://www.amtso.org/wp-content/uploads/2026/09/AMTSO-Test-Plan-MRG-Effitas-360-Android-Q3-2026-V_1_1.pdf

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

access to the launcher, the application drawer, or the Settings application to perform an uninstall[2].

False Positive Tests

To cover all aspects of the efficacy of the participants, a limited set of samples are selected. The samples have been downloaded from a well-known 3rd party app store, exhibiting no malicious behaviour but requiring a varying range of permissions.

Samples

Malicious In-The-Wild Samples

Testing used an initial 165-sample malware set. All samples have been categorized using the following labels.

- **SMS Payment.** The application provides features to send SMS messages to premium rate numbers. Most of the selected samples were able to 'auto-send' messages, as they usually opted for the SEND_SMS permission, resulting in a direct financial loss for the victim.
- **Trojan.** Trojans are applications that display a certain set of features within their description and their overall appearance suggests some expectations regarding their functionality. However, the implemented modules require a wider range of permissions, which do not belong to the advertised functionality. A typical example is a flashlight app that can read the contact list, location information, and send them to the Internet.
- **Spyware.** We classify a sample Spyware if it leaks information that could be used to track the user (as most security-conscious users do not wish to be tracked). Ironically, most ad-propelled applications using aggressive frameworks qualify as spyware, as they leak IMEI, phone number, phone vendor and model etc. to the ad provider network.
- **Financial/banking.** This type of malware aims for direct financial abuse. A typical financial piece of malware detects if the user is logged in to a mobile banking session using either a browser or mobile banking application and, for example, might attempt to display a matching phishing site or to draw an overlay window to fool the user into thinking that the session has ended and that they need to re-authenticate. Typically, such samples use permissions to get the task list, combined with the SYSTEM_ALERT_WINDOW permission.
- **PUA.**[3] The term 'Potentially Unwanted Applications' denotes applications, which perform actions that are not in alignment with the security-conscious user's intentions. For instance, applications provided with aggressive advertisement modules usually make it possible for ad campaigners to track individual users, even to assign the device with the user's demographic properties through social network ad services. Effitas claims that security-conscious users are sensitive regarding their privacy, and possibly no application feature can make up for the users' private data and browsing habits to be sold over the Internet. A decent AV should let the user know if such an application is about to be installed.

[2] Please note that to mitigate this kind of typical malware behaviour, the Android API design team reviewed the Device Administrator and the Accessibility Admin Request screens to include a checkbox that can be used to prevent the OS from displaying the screen again. This feature however, made its way only to recent revisions of the Android API.

[3] Android applications with a social network integrated advertising module often fall into a kind of 'grey zone' from a detection perspective, as any application can be turned into a PUA, should the developers include an aggressive advertising module. Hence, we included charts, which handle PUA and non-PUA samples separately.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Note that most samples implement several kinds of operation, therefore most samples fall into several categories. An example would be a typical piece of malware that serves malicious ads and, where possible, attempts to obtain the SEND_SMS permission to send premium rate messages.

Our ITW samples are obtained using several sources. As we strive to use fresh malware, the actual mix of samples used in test batches is highly dependent on the then-current activity of malicious threat actors. As a result, in many batches one or more families are represented with several samples, all of them fresh at the time of testing. Consequently, failing to detect that family of samples will result in multiple Misses.

Figure 1. depicts the distribution of test samples.

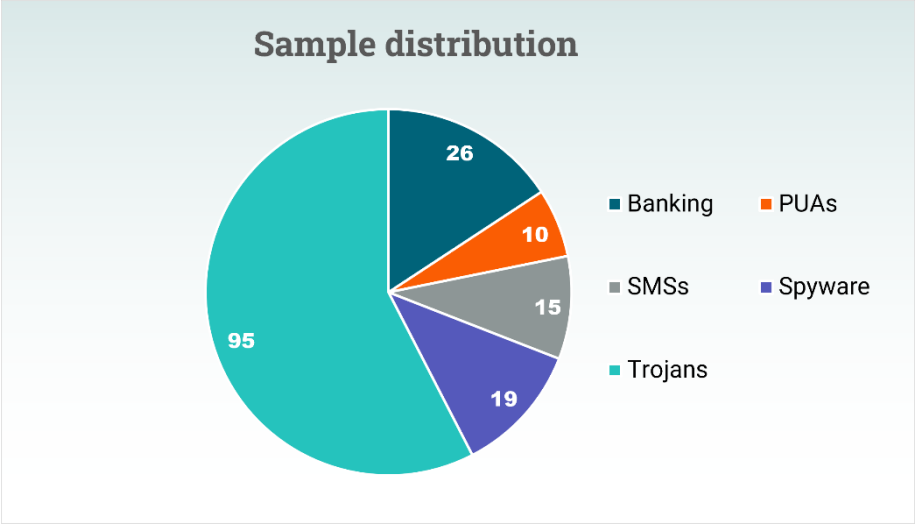


Figure 1. In-the-wild sample distribution

Simulator samples

Simulators are custom samples, introduced into the testing process to put the sophistication of the detection routines to the test. Our simulators were created to simulate the attack model of a "malicious 3rd party app store providing backdoored applications" type of scenario, which means that counterfeit versions of legitimate applications are provided to the victims (many times pirated application versions can be downloaded free-of-charge). The counterfeit versions are backdoored versions of popular applications, which, while retaining the functionality of the original application, also include malicious modules.

The samples have been created using a proof-of-concept engine using static smali byte code injection techniques, making no effort to obscure the malicious actions of the injected modules. All the simulator samples have been modified to implement SMS related features, which is a common trait for several malware families.

For testing, we used 5 custom created samples. It is important to stress that these samples have not been collected or observed In-The-Wild. All our custom samples implement the same well-known method for stealing the SMS. Our samples were counterfeit versions of legitimate Android applications, but including a malicious SMS service, which tries to steal all currently stored SMS on the device.

The purpose is to assess the general detection capability of the antivirus solutions across varied contexts without introducing a truly unique or separate threat.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

False positive samples

For false positive testing, a 5-sample set was used, retrieved from non-malicious 3rd party applications stores. The applications have been selected to cover a wide range of permissions and functionality.

Security Applications Tested

The following security suites have been selected for testing. Besides well-established vendors with considerable reputation and track history, we select smaller vendors with less market share. As the Play Store is heaving with Android security applications, we tend to select AV products with a considerable number of downloads.

Product Name	Caption	Play Store URL
Avast One: Antivirus, Security	Avast One	https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity
Avira Security Antivirus & VPN	Avira	https://play.google.com/store/apps/details?id=com.avira.android
Bitdefender Mobile Security	Bitdefender	https://play.google.com/store/apps/details?id=com.bitdefender.security
ESET Mobile Security Antivirus	ESET	https://play.google.com/store/apps/details?id=com.eset.ems2.gp
F-Secure Mobile Security	F-Secure	https://play.google.com/store/apps/details?id=com.lookout
G DATA Mobile Security	G Data	https://play.google.com/store/apps/details?id=de.gdata.mobilesecurity2g
Malwarebytes - Mobile Security	Malwarebytes	https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware
McAfee Security: Antivirus VPN	McAfee	https://play.google.com/store/apps/details?id=com.wsandroid.suite
Norton360: Virus Scanner & VPN	Norton360	https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity

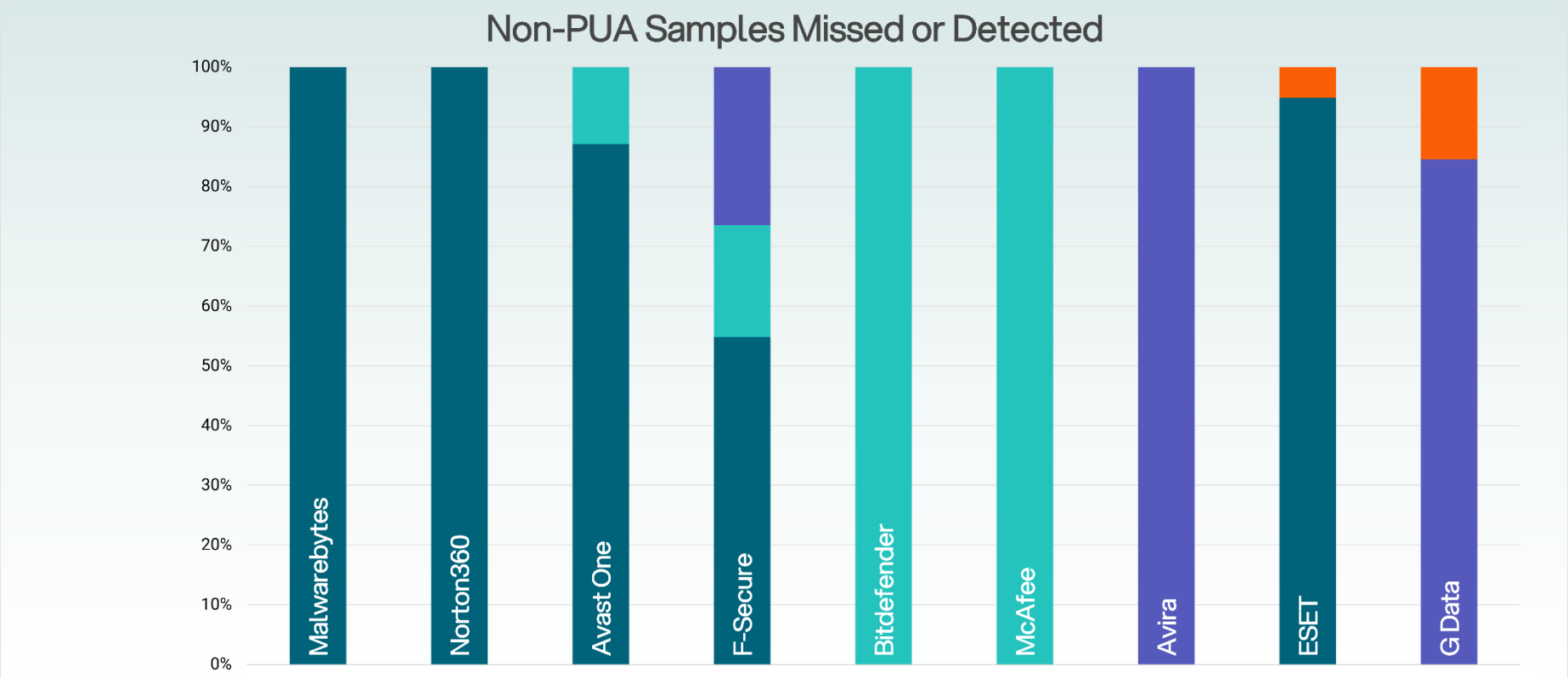
Figure 2. Test participants[4]

[4] During testing this quarter, several technical issues were encountered and subsequently resolved during the dispute phase. To ensure transparency, a detailed list is provided in the "Conclusions" section.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Test Results

Overall non-PUA Detection

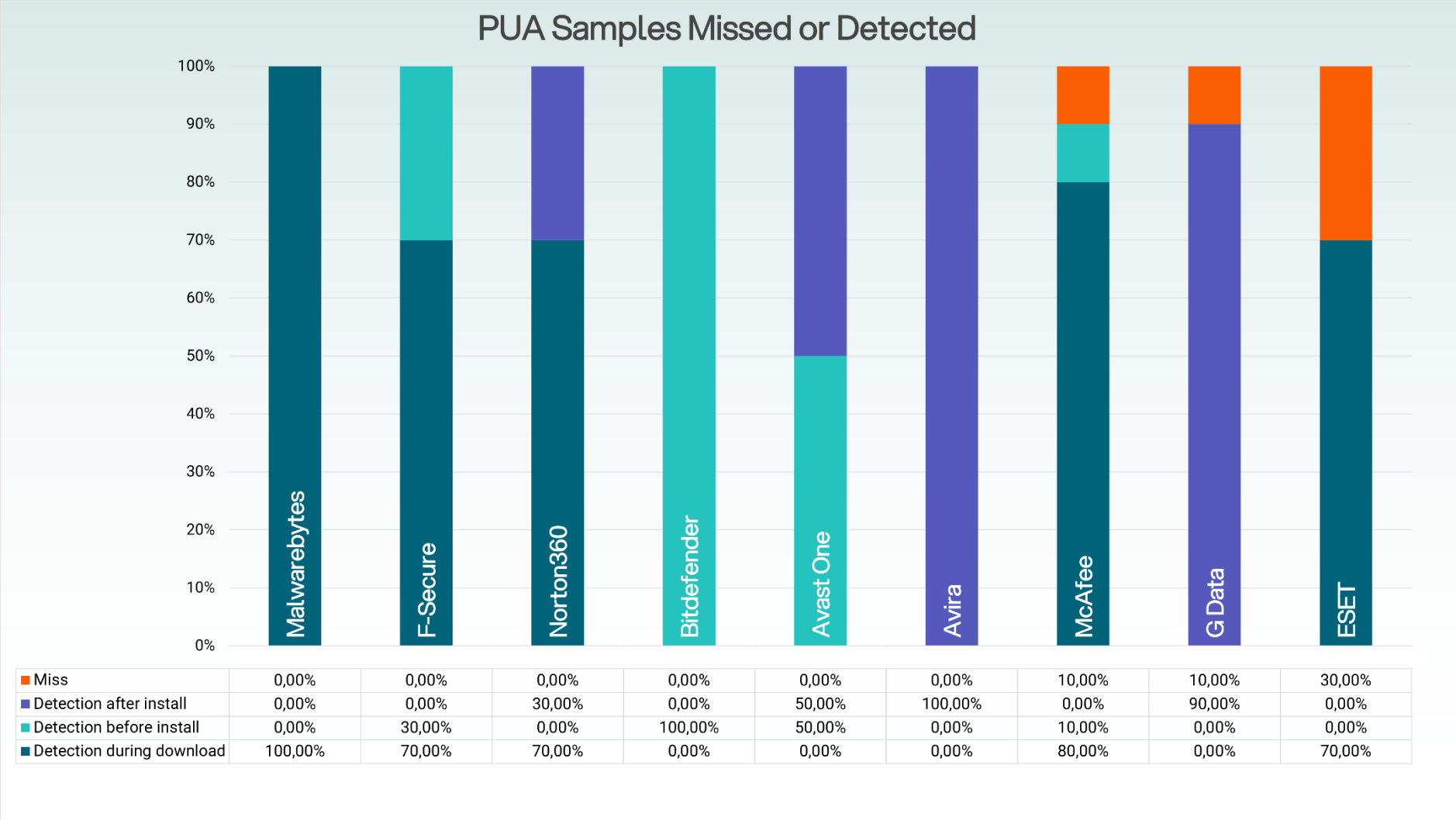


	Malwarebytes	Norton360	Avast One	F-Secure	Bitdefender	McAfee	Avira	ESET	G Data
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	5,16%	15,48%
Detection after install	0,00%	0,00%	0,00%	26,45%	0,00%	0,00%	100,00%	0,00%	84,52%
Detection before install	0,00%	0,00%	12,90%	18,71%	100,00%	100,00%	0,00%	0,00%	0,00%
Detection during download	100,00%	100,00%	87,10%	54,84%	0,00%	0,00%	0,00%	94,84%	0,00%

Figure 3. Summary, Non-PUA samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

PUA Detection

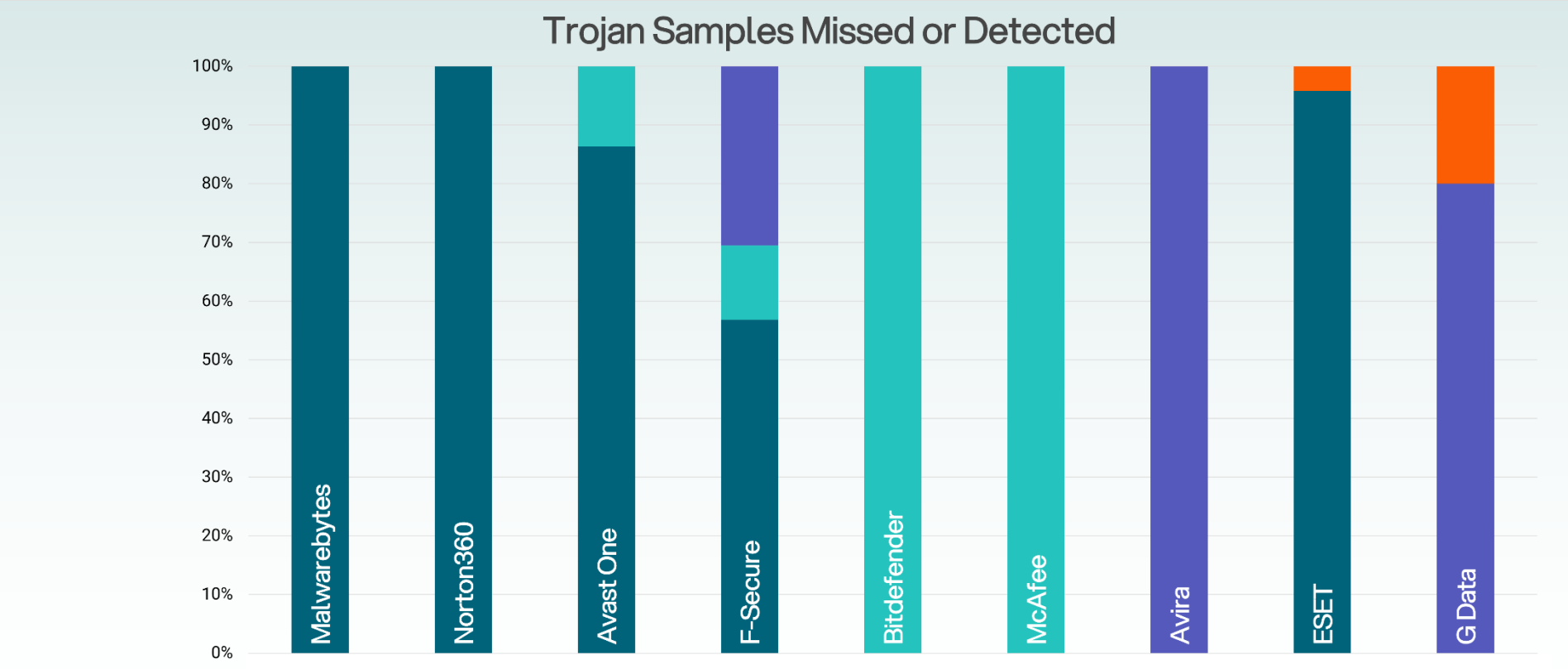


	Malwarebytes	F-Secure	Norton360	Bitdefender	Avast One	Avira	McAfee	G Data	ESET
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	10,00%	10,00%	30,00%
Detection after install	0,00%	0,00%	30,00%	0,00%	50,00%	100,00%	0,00%	90,00%	0,00%
Detection before install	0,00%	30,00%	0,00%	100,00%	50,00%	0,00%	10,00%	0,00%	0,00%
Detection during download	100,00%	70,00%	70,00%	0,00%	0,00%	0,00%	80,00%	0,00%	70,00%

Figure 4. Summary, PUA Samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Trojan Detection

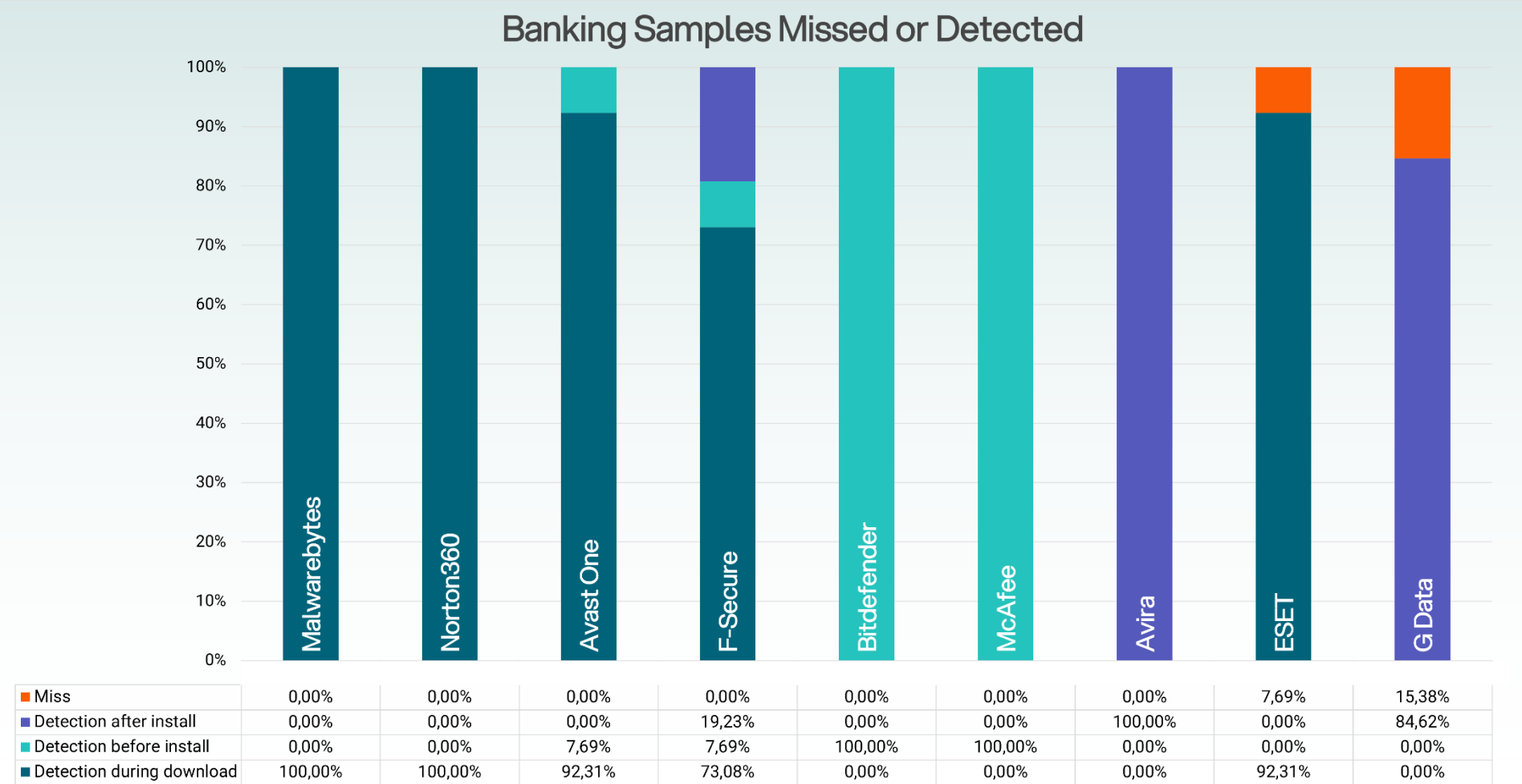


	Malwarebytes	Norton360	Avast One	F-Secure	Bitdefender	McAfee	Avira	ESET	G Data
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	4,21%	20,00%
Detection after install	0,00%	0,00%	0,00%	30,53%	0,00%	0,00%	100,00%	0,00%	80,00%
Detection before install	0,00%	0,00%	13,68%	12,63%	100,00%	100,00%	0,00%	0,00%	0,00%
Detection during download	100,00%	100,00%	86,32%	56,84%	0,00%	0,00%	0,00%	95,79%	0,00%

Figure 5. Summary, Trojan Samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Banking Detection

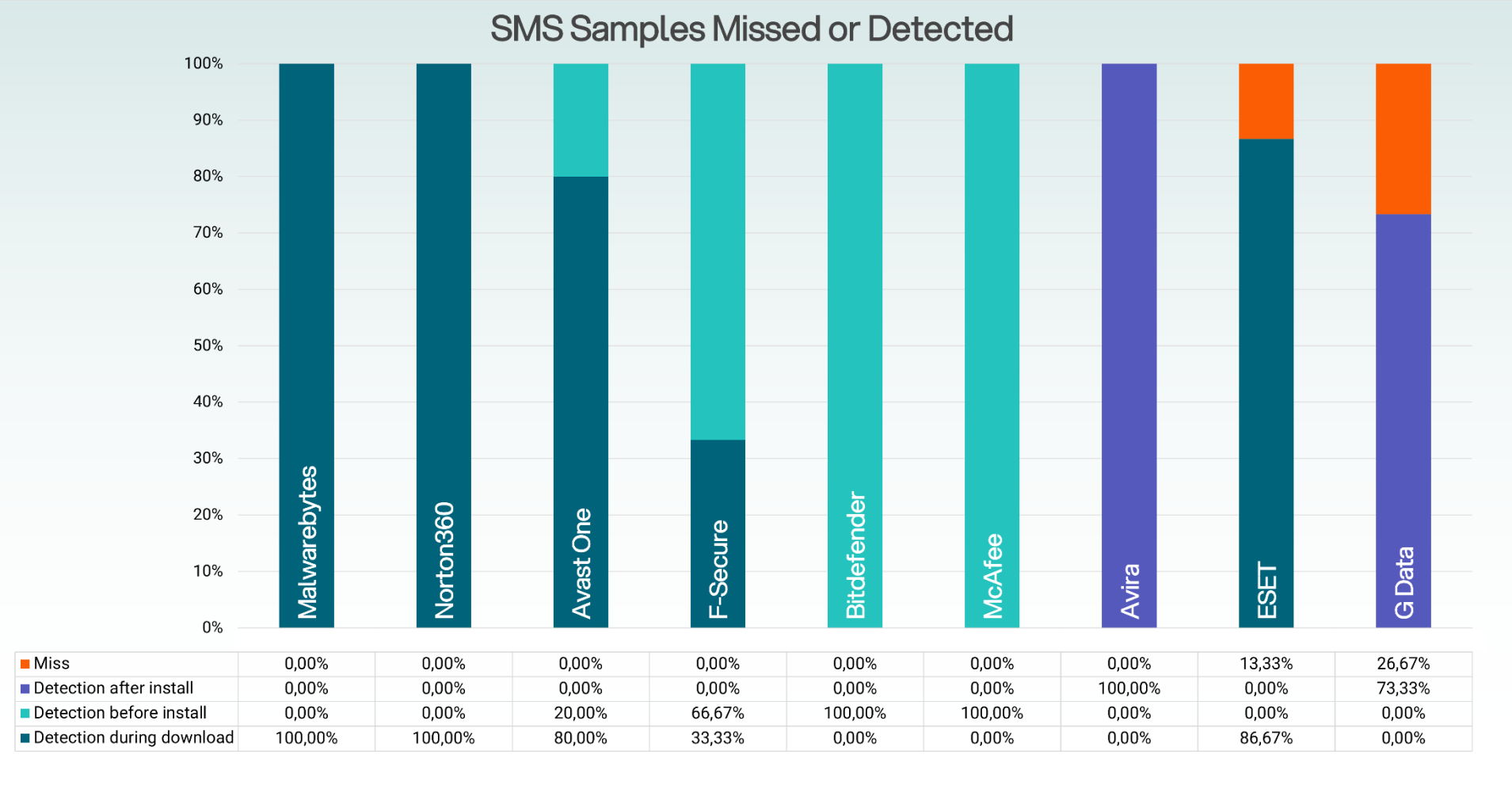


	Malwarebytes	Norton360	Avast One	F-Secure	Bitdefender	McAfee	Avira	ESET	G Data
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	7,69%	15,38%
Detection after install	0,00%	0,00%	0,00%	19,23%	0,00%	0,00%	100,00%	0,00%	84,62%
Detection before install	0,00%	0,00%	7,69%	7,69%	100,00%	100,00%	0,00%	0,00%	0,00%
Detection during download	100,00%	100,00%	92,31%	73,08%	0,00%	0,00%	0,00%	92,31%	0,00%

Figure 6. Summary, Banking Samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

SMS Detection

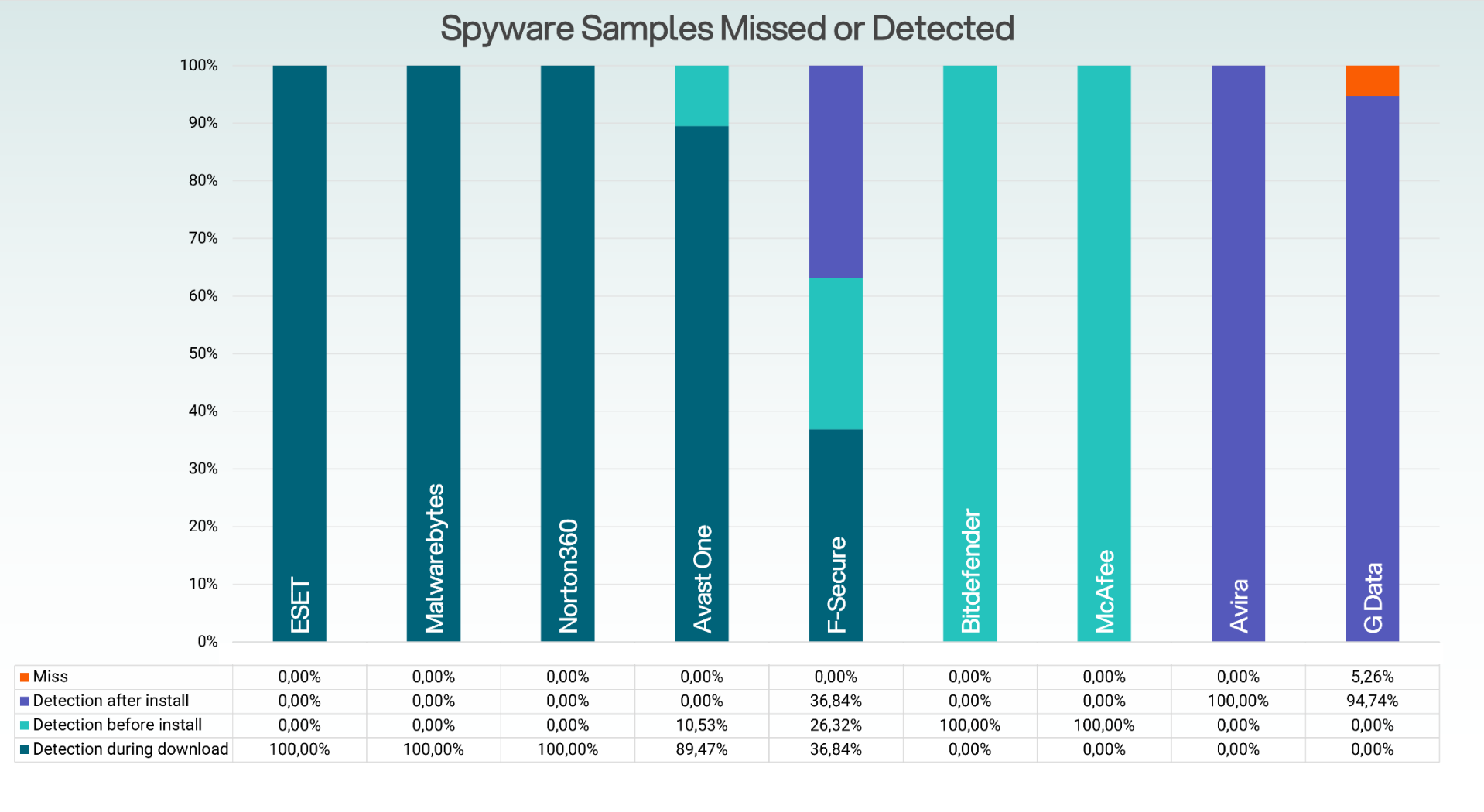


	Malwarebytes	Norton360	Avast One	F-Secure	Bitdefender	McAfee	Avira	ESET	G Data
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	13,33%	26,67%
Detection after install	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	100,00%	0,00%	73,33%
Detection before install	0,00%	0,00%	20,00%	66,67%	100,00%	100,00%	0,00%	0,00%	0,00%
Detection during download	100,00%	100,00%	80,00%	33,33%	0,00%	0,00%	0,00%	86,67%	0,00%

Figure 7. Summary, SMS samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Spyware Detection

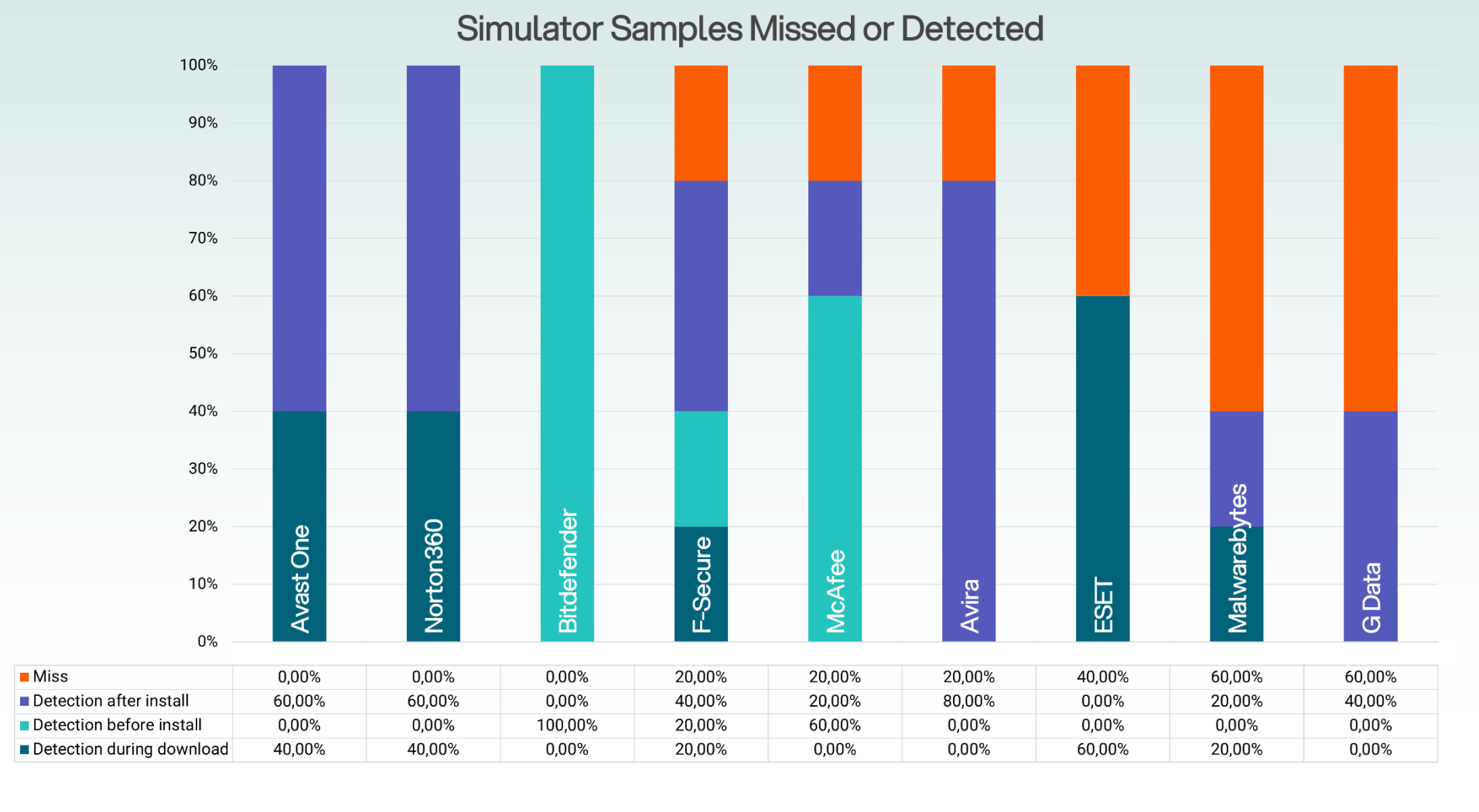


	ESET	Malwarebytes	Norton360	Avast One	F-Secure	Bitdefender	McAfee	Avira	G Data
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	5,26%
Detection after install	0,00%	0,00%	0,00%	0,00%	36,84%	0,00%	0,00%	100,00%	94,74%
Detection before install	0,00%	0,00%	0,00%	10,53%	26,32%	100,00%	100,00%	0,00%	0,00%
Detection during download	100,00%	100,00%	100,00%	89,47%	36,84%	0,00%	0,00%	0,00%	0,00%

Figure 8. Summary, Spyware samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Simulator Detection



	Avast One	Norton360	Bitdefender	F-Secure	McAfee	Avira	ESET	Malwarebytes	G Data
Miss	0,00%	0,00%	0,00%	20,00%	20,00%	20,00%	40,00%	60,00%	60,00%
Detection after install	60,00%	60,00%	0,00%	40,00%	20,00%	80,00%	0,00%	20,00%	40,00%
Detection before install	0,00%	0,00%	100,00%	20,00%	60,00%	0,00%	0,00%	0,00%	0,00%
Detection during download	40,00%	40,00%	0,00%	20,00%	0,00%	0,00%	60,00%	20,00%	0,00%

Figure 9. Summary, simulator samples

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

False positive tests

In False Positive tests, all participants achieved a perfect score.

Summary

The following AV engines reached a near-perfect rounded 99% detection rate in a non-PUA sample set, therefore, they have been awarded with the MRG Effitas Certificate. Note that in the certification process, no distinction is made on where the detection has taken place, i.e. to be awarded, the rounded MISS rate needs to be 1% or less.

- Avast One
- Avira
- Bitdefender
- F-Secure
- Malwarebytes
- McAfee
- Norton360



Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Improvements in Our Test Bed

During testing of past quarters, several technical issues were encountered and subsequently resolved during the dispute phase.

In several instances, the tested AV apps failed to connect to the cloud at critical moments following the installation of a sample. The primary concern was the lack of visual feedback to the user; in some cases, the detection interface even displayed reassuring messages, potentially giving users a false sense of security. In order to tackle this problem, the test bed has been modified to permanently monitor unhindered network connectivity.

Conclusions

As a result of our testing efforts, a couple of conclusions can be drawn from our time with the AV engines and samples in our test lab.

Detection mechanisms

Our tests confirmed that most AVs use different methods for detection before and after installation. This is because prior to installation, a different set of metadata is available for the AV engine of a file that is stored on an SD card, than what is available after its installation.

This updated methodology clearly highlights a trend of detection mechanisms and their temporal operation. Some AV products detect threats as soon as they are downloaded, others put the emphasis on post-installation detection.

The earlier an AV detects a threat, the better it is from a user perspective. Nevertheless, given that even a successful malware installation can be saved, provided the user is warned before the first tap on the launcher icon and detection takes place shortly after installation, the test case is counted as a Pass in every scenario, where the AV displays a warning to the user.

Vendor reputation and extra services

As of 2026, most of the well-established vendors reached a perfect or near-perfect score in the In-the-Wild categories. From a user perspective, this is all good news as several viable options are provided, some even without a subscription fee. In the future, we expect that the extra features (VPN, family locator, connections with desktop AV licenses etc.) have a significant effect on user choice.

‘AV as another app’

Testing led us to the conclusion that detection for many AVs relies heavily on the metadata of installed packages (hashes, developer certificates, etc.), meaning that, unlike in a Windows based environment, an AV is unable to get an insight into the actual activity of other applications. This behaviour is in alignment with the basic Android security principles, as “AV is another app”. As a result, having already started the freshly installed samples, it is quite hard to get rid of some samples in the In-The-Wild test set, making timely and properly displayed detection an absolute must for AV engines.

Simulator detection

Our test lab has been contacted on several occasions with claims that the simulators we utilise, do not present a lifelike challenge for an AV engine. However, field reports show the presented scenario – when an adversary patches an existing Android application to perform hidden spying activity – is well known technique that has been used for almost a decade. The most

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

famous campaigns using this approach is still the Dark Caracal APT[5], with an excellent analysis by Lookout[6]. For more details on the story, check out the corresponding episode of Darknet Diaries (ep. 38)[7].

Detection notifications and notification spam

While undertaking the 360° Android tests, we have noticed that there are significant differences in terms of user notification. When it comes to a successful detection, efficient and clear user notification is an essential part of both the efficacy of the AV application and the overall user experience.

The tested AVs choose one of the following approaches.

1. A separate activity is launched, usually with a bright red background and a couple of lines describing the nature of the threat presented by the application in question.
2. The Android notification subsystem is utilised to issue an important notification, usually displayed in the status bar, accompanied by an audible signal.

Both approaches have their merits. A separate activity like the first method is harder to dismiss or overlook, and the second method offers a more streamlined Android experience. However, Android provides a lot of options for users to customise notifications, therefore it is possible for the notification to get lost in the clutter. As a result, many of the tested apps opt for the first approach.

Furthermore, applying too many or too frequent notifications in the notification bar might result in important notifications getting lost in the noise. For instance, an AV might wish to inform the user that some background activity is taking place and to make it apparent that the device is provided with protection. However, should the user be accustomed to seeing AV notifications all the time, they might just automatically dismiss the notification as not important. As always, this is a matter of finding the right balance.

As for the wording, the overall design of the displayed notification and the consequent user choice description, there is a significant room for improvement in many apps. The Android way is to communicate as much information to the user as possible, just enough so that they can make a responsible decision. However, a responsible user must read and process the text displayed on the screen, which presents a significant mental load, especially for the less tech-savvy. As a result, a well-designed GUI can make all the difference for the everyday user, making users' choices more responsible and consequently, their devices more secure.

We see a worrying trend in the user experience of Android AVs. During this test, we encountered several instances of AVs issuing an unnecessary amount of user notifications, effectively "spamming" the notification bar. Albeit understandable from a marketing point of view, we think this adds unnecessary noise.

Changes in Android API and Android Malware

Android 14 introduced several API changes that significantly reduce the threat surface for malware, making it harder for malicious apps to exploit

[5] https://en.wikipedia.org/wiki/Dark_Caracal

[6] https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_es-kf_20180118_uk_v.1.0.pdf

[7] https://darknetdiaries.com/episode/38/

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

vulnerabilities and to perform malicious actions on a device. One of the most impactful changes is the restriction on outdated API levels. Apps targeting older Android versions (specifically before Android 6.0) are no longer installable, closing off attack vectors that rely on older, less secure permissions models. This change prevents malware from bypassing modern security enhancements such as runtime permissions, scoped storage, and background activity limitations. By enforcing higher API targets, Android 14 ensures that all apps adhere to the latest security best practices, making it more difficult for attackers to exploit legacy vulnerabilities.

Another critical improvement in Android 14 is its enhanced runtime execution restrictions. The update introduces stricter background activity limitations, preventing unauthorized apps from executing stealthy operations in the background. This curbs common malware tactics, such as accessibility service abuse, which cybercriminals use to capture user input or perform actions on behalf of users without their knowledge. Additionally, Android 14 refines dynamic code loading restrictions, limiting the ability of apps to load unverified external code at runtime. This directly mitigates the risk of code injection attacks, which are commonly used by malware to alter app behaviour or evade detection.

Android 15 also strengthens app integrity and communication security through its tightened inter-process communication (IPC) mechanisms and stricter data-sharing policies. With new restrictions on implicit and exported intents, malicious apps have fewer opportunities to intercept or manipulate data exchanged between applications. Additionally, the platform enhances its security against privilege escalation attacks by restricting access to certain system APIs and requiring explicit user consent for sensitive actions. Combined with ongoing improvements in Play Protect and app sandboxing, these API-level reinforcements make it significantly harder for malware to persist or spread across devices, leading to a more secure Android ecosystem.

Google and Sideloading

Google's 2025 announcement[8] regarding mandatory developer verification for Android applications represents a fundamental architectural shift in the Android threat landscape, though it's important to clarify that developers will continue to sign applications with their own certificates—the change mandates that developers verify their real-world identity and register their package names and signing keys with Google before apps can install on certified Android devices. From a malware analysis perspective, this verification requirement introduces a critical accountability layer that significantly alters the attack economics for threat actors. While Google cites data showing sideloaded applications contain over 50 times more malware than Play Store distributions, the verification mandate creates a double-edged security scenario: it raises barriers for opportunistic malware authors who rely on rapid deployment cycles and anonymity, but simultaneously establishes a high-value target in the form of developer credentials that could enable sophisticated supply chain attacks.

The security implications extend well beyond simple distribution control and fundamentally impact malware research methodologies and threat intelligence operations. The net security benefit will largely depend on Google's implementation rigor around identity verification processes, the security posture of the verification infrastructure itself (which becomes a critical single point of failure), and whether enforcement mechanisms can

[8] https://android-developers.googleblog.com/2025/08/elevating-android-security.html

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

effectively distinguish between legitimate independent developers and malicious actors employing increasingly sophisticated social engineering and credential compromise techniques. Additionally, the introduction of a "warn mode" for power users to bypass verification, while addressing legitimate use cases, creates a potential social engineering vector where malware could manipulate users into enabling this mode, essentially recreating the current threat landscape through a different attack path.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

MRG Effitas

Copyright © 2026 MRG Effitas Ltd.