

Antivirus Apps for Smartphones: Useful or Unnecessary Protection?

As mobile endpoints, smartphones and tablets offer attackers gateways into companies' networks. This is why many people turn to antivirus or security apps. In our e-book, you can find out whether they are worth using.

How do antivirus apps for smartphones and tablets work?

Antivirus apps for smartphones work in a similar way to antivirus programs on a PC, but are adapted to the special features of mobile operating systems such as **Android** or **iOS**.



Basic features of antivirus apps on smartphones

1. Scanning for malware

- The app scans installed apps, files and downloads for known viruses, Trojans, spyware, adware or ransomware.
- For Android, the app code (APK files) in particular is scanned, as Android apps from third-party providers can be installed.
- iOS is much more restrictive here, so malware scans are less relevant there (see below).

Base features of antivirus apps on smartphones

2. Real-time protection

- Many antivirus apps offer background protection that automatically checks new downloads or app installations.
- Some apps also check whether dangerous websites are being accessed while surfing (phishing protection).

3. Security features (mostly additional features with extra costs)

- Theft protection (localization, remote blocking, data deletion in the event of theft).
- VPN for secure surfing.
- App lock to additionally secure certain apps with a PIN or fingerprint.
- WiFi security check to detect unsecure networks.

Android vs. iOS: Differences in functionality

Android

- Antivirus apps can interfere deeply with the system, as Android allows more freedom.
- A virus scanner is therefore useful here, especially if you install apps from **non-official sources** (outside the Play Store).

iOS

- Apple does not allow antivirus apps access to system files or other apps, so real virus scanners do not work on iPhones in the classic sense.
- iOS antivirus apps usually only offer security tips, data protection reports or phishing warnings in the browser - in other words, more “security advice” than virus protection.



How useful are antivirus apps on the smartphone?

Antivirus apps can scan apps that are already installed and warn of dangerous downloads or websites. For this reason, they already offer a certain level of protection. However, this protection is not enough for companies because they have to comply with the strict requirements of the GDPR. It is important to always bear in mind what security apps can actually do and in what context they should be used. **That's why it is not advisable to use a mobile security app as the sole solution for securing devices.**



How useful are antivirus apps on the smartphone?



In the corporate context, antivirus apps can therefore only be a **supplement to strict, preventative measures** such as MDM (mobile device management) software. Another aspect of antivirus and security apps is that they can increase the end user's **sense of security**. Especially for people who are unsure about using technology, this can help them feel more comfortable using mobile devices for work. Warnings via the antivirus apps can also prevent end users from behaving carelessly. **Awareness of potential threats** can also be raised.

All-round security against viruses, malware and attacks with MDM and security apps

In principle, the additional use of antivirus and security apps can do no harm to security in the company and contribute to the security of mobile devices. Moreover, the use of an MDM is mandatory for most companies. The reason for this is that only through an MDM can comprehensive security precautions be taken on company mobile devices. For example, guidelines prevent certain apps from being downloaded or the use of unauthorized WiFi connections.

The IT admin can use an MDM to create an app catalog that only lists apps that meet the company's compliance guidelines. This also ensures that no apps are used on the devices that require too much access to the end user's data. In addition to the security features, MDM also facilitates simplified device management, for example by allowing apps to be installed remotely, the operating system to be updated automatically or wallpapers to be distributed centrally.



How MDM and antivirus apps can help

SMS phishing

- An MDM can ban certain phone numbers, e.g. 0800 numbers
- Incoming text messages can be blocked via MDM
- An antivirus app detects suspicious links in text messages

Installation of apps from third-party sources (sideloading)

- An MDM can prevent apps from being downloaded outside the Play Store and the App Store
- If this is permitted, an antivirus app can scan the app file during download and warn of malware

Data security

- With the help of an MDM, devices can be divided into two areas: the private profile and the work profile, which keeps important data cleanly separated
- A security app can also indicate if a recipient appears dubious when sharing and sending documents, images and other files

How MDM and antivirus apps can help

Securing the internet connection

- An MDM can specify which security standards WiFi connections must meet before they can be used
- WiFi connections outside the company can also be completely blocked
- An antivirus app can also scan WiFi connections and draw attention to security risks

Secure communication

- An MDM can prevent the sharing of files between private and business areas
- MDM can be used to install secure messaging apps that comply with the GDPR

Protection of passwords and access to the device

- An MDM can set password requirements, without which the device cannot be used
- A security app can ensure that passwords are stored securely

About the authors

IOTIQ GmbH is an international IT company based in Leipzig. We have been offering customized software solutions, especially for SMEs, since 2017.

Our goal: to drive digitalization in Germany - with the best software for your smartphone. Companies of all sizes should be able to benefit from the advantages of digitalization: from tailor-made app development to hardware consulting and procurement. We believe that mobile devices are the key to digital advancement.

The author of this article is Customer Care & Marketing Manager at IOTIQ GmbH and a certified Android expert.



Android
Enterprise

Silver partner