Awake

Bitdefender
Mobile Security

Scanning Android Market for potentially malicious software is exactly what the Bitdefender Mobile Security service does. If the Android Market was a club, you could think of it as a resident detective, there to find and sort out troublemakers the bouncer inadvertently let in.
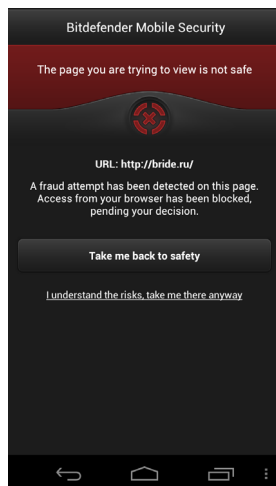
Bitdefender Mobile Security provides smart antivirus and web security for devices running Android. Its in-the-cloud scanning technology detects even the latest threats without putting a strain on the battery.

Bitdefender Mobile Security also provides information about billable services and applications' requirements for access to Internet or private user data, helping users make informed choices about their privacy and data security.

Here's a full list of what **Bitdefender Mobile Security** can do. Please note that features marked premium are only available upon purchase:
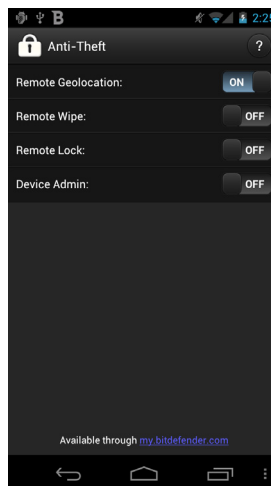
Anti-TheftPREMIUM

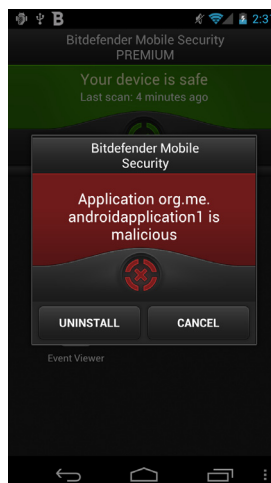The Anti-Theft module provides options to remotely locate, lock, wipe or send a message to the Android device.

Web SecurityPREMIUM

The Anti-Theft module provides options to remotely locate, lock, wipe or send a message to the Android device.

On-Install Scanning
FREE & PREMIUM

Bitdefender Mobile Security makes sure the Android device stays clean by automatically scanning any application immediately after its install. This also helps users stay informed and protected whenever they try a new application.
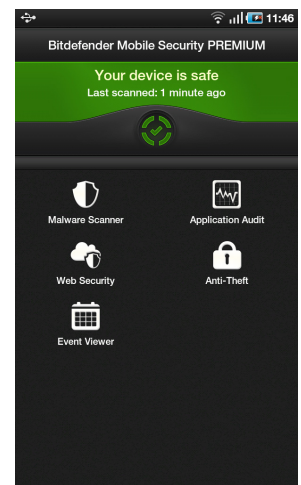

If you read an analyst report about 'viruses' infecting ios, android or rim, you now know that analyst firm is not honest and is staffed with charlatans. There is probably an exception, but extraordinary claims need extraordinary evidence.

Chris DiBona, Google Open Source Programs Manager, Nov. 6 2011

Today we're revealing a service we've developed, codenamed Bouncer, which provides automated scanning of Android Market for potentially malicious software without disrupting the user experience of Android Market or requiring developers to go through an application approval process.
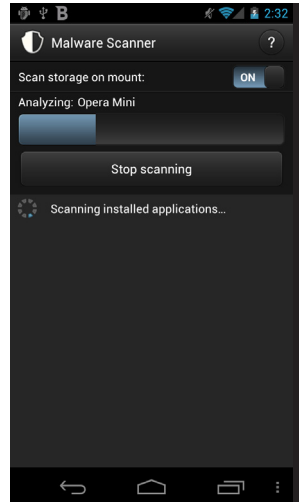
Hiroshi Lockheimer, VP of Engineering, Android, February 2, 2012
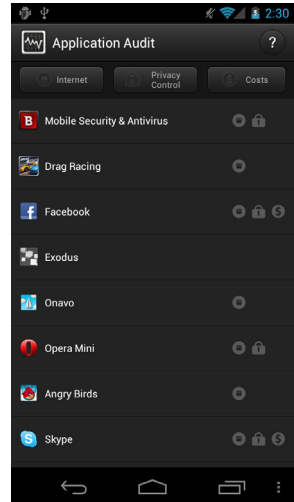

Bitdefender®

Bitdefender®

On-Demand Scanning FREE & PREMIUM

An on-demand scan may be run at any time to make sure all applications on the device are legitimate and all applications installed or kept in the phone's storage are legitimate and safe.

Application Audit FREE & PREMIUM

Bitdefender Mobile Security for Android allows users to keep track of each application's permission requirements, displaying which applications try to access the Internet or sensitive data (Contacts list, Messages, Calendar entries, Photo gallery). It will also indicate what applications have been granted the permission to access billable device functions such as making phone calls or sending text messages.

Full Speed & Low Battery Impact

Thanks to its cloud-based threat detection and top-of-the-line security services, Bitdefender Mobile Security for Android secures your browsing and prevents installation of malicious applications with virtually no battery life impact.

The main services

a. websecurity

Android device users enjoy can download and install application packages from the Web, by simply clicking a link or snapping a QR code. **Bitdefender Mobile Security** checks links that the device default browser tries to access, by sending it to a Bitdefender server. The link is then checked for known threats, and a verdict is sent back to the browser, alerting the user if the link points to a phishing- related page, a fraud attempt or to a page that hosts malware

b. antimalware

The actual on-demand scanning process is three-step: the application packages of installed apps and any apks which may be stored on the device's removable storage are fingerprinted, the fingerprints are sent to a Bitdefender server which picks out known malicious fingerprints and the results of the server-side analysis are returned to the device. The user then gets a recommendation to uninstall any malicious apps found.

Whenever an application is installed, **Bitdefender Mobile Security**

automatically scans it using in-the-cloud technology. If the application is found to be malicious, an alert will appear prompting the user to uninstall it.

Removable storage is also automatically scanned on mount, to cover the scenario where application packages are copied from a computer to the device

c. application audit

The application audit feature neatly groups legitimate apps based on their potential to perform potentially undesired actions, thus helping users to make informed security decisions. This regards apps which can trigger charges (by initiating a phone call or sending an sms), access the Internet or can access private data.

d. anti-theft

Bitdefender Mobile Security anti-theft service is based on Google's push notifications system, which was designed to allow Google and, by extension, Google users to send messages to specifically selected Android devices, which must be connected to the Internet for the service to work.

Upon installation, **Bitdefender Mobile Security** requests Google's access token. If the token is unavailable, the anti-theft function cannot be started.

When a locate request is sent via MyBitdefender, the Bitdefender server notifies a Google server which in turn passes a location request to the device. The device subsequently tries GPS and Wi-Fi positioning and replies with a location, which is then passed back to the MyBitdefender server and ultimately to the user.

 User initiated requests to play a sound, display a message, remotely lock or remotely wipe the device are passed in the same manner. Of course, Internet access for the device is required in all these scenarios.

However, due to the way Google sets up the security policies on Android devices, administration rights need to be explicitly granted to Bitdefender Mobile Security before requiring a full remote wipe. Only some data will be wiped if the user chooses not to grant admin rights to **Bitdefender Mobile Security**.