AV-Comparatives


# 移动安全软件评测

语言：中文

2013年8月

最后修订：2013年8月18日

www.av-comparatives.org

# 目录

# 简介

智能手机象征着移动电话未来的发展方向。2013年4月，智能手机的市场占有量预计超过55%[1]，迟早会取代传统的手机。这种设备在许多人眼里已远远超过了普通的手机。可以用智能手机登录网上银行、脸谱（Facebook）、拍摄并保存照片，甚至安排全部的生活。但同时也带来了一些风险，某些功能在方便用户的同时，也同样引起罪犯的关注。恶意软件也会感染智能手机，敏感数据信息也可能被窃取。任何其他设备上遭遇的网络钓鱼攻击也会发生在智能手机身上。

您绝对不会允许自己的台式机或笔记本电脑，在不安装任何安全软件的前提下裸奔。而对于智能手机用户来说，尽管手机中或许已保存了重要的个人信息、私家照片，甚至还存有公司的数据，但大多数人尚不具备这种安全意识。由于电子邮件可以自动同步，甚至文件也能通过云存储服务来保存，所以手机中保存的信息比用户真正想要保存的还多。

手机虽小，但价格昂贵，这自然就成为窃贼的目标。手机安全软件必须增加窃贼对信息的访问难度，以减少被偷窃的可能。如果没有任何保护，窃贼就可以更加为所欲为。手机失窃后，窃贼一旦换掉手机中的SIM卡，那么失主就再也无法联系到失窃的手机。或者，窃贼也可能会直接使用手机中原有的SIM卡拨打电话，让失主为话费买单，或用它来从事更多的犯罪活动。所以，为了避免这些情况的发生，先进的移动安全产品为智能手机用户设计了各种不同的保护功能。

## 防盗保护

几乎所有测试的产品都提供防盗保护功能。最重要的功能之一是锁定功能，它可以通过密码来保护智能手机，从而防止未经授权的操作。远程删除数据也属于智能手机安全程序的标准功能。定位功能可以发现丢失手机的所在位置；我们注意到，在智能手机被盗的情况下，一些厂商告诫不要使用此功能来追捕小偷。

厂商提供两种不同的控制防盗保护功能的方法。首先是短信。从另一部手机发送指令来触发相关的操作。其次是web界面。这两种情况各有自己的优缺点。短信差不多是最能发挥作用的，即使使用应急联系电话在不同的国家也可以发送防盗短信。另一方面，网络界面使用起来非常直观，并且常允许您一个帐户进行多设备管理。短信命令的缺点是，用户需要发出短信通知，并且需要第二部发送短信的移动电话。如果要使用网络界面，必须将移动电话连接到网络。在某些情况下，例如，如果手机丢失时身在国外，有效的网络连接可能已被禁用。

定位功能非常有用，但也可能被滥用来跟踪常人。因为，任何人都可以在手机中安装安全软件，或直接选择一个已经预装了安全保护产品的手机，来跟踪某人的活动。当然，如果父母们是为了能够关注自己的孩子，使用这种功能是完全可以接受的，但在其他情况下使用，可能是完全不恰当的。

[1] http://www.comscore.com/ger/Insights/Presentations_and_Whitepapers/2013/The_Mobile_Shift

## 恶意软件防护

借助恶意软件的防护功能，可以对智能手机进行恶意软件扫描，发现恶意程序后即会被删除或隔离。如果要有效启动该功能，必须使恶意软件病毒库保持最新。当您在国外旅行时，需要注意避免产生高额的漫游费。

由于谷歌安卓操作系统高速增长的市场份额（目前已占74.4% [2] ），今年我们再次使用安卓操作系统进行安全软件的测试。在这份报告中，读者所看到的，都是那些领先的各厂商的产品功能的详细介绍，厂商选择后交由我们测试和评估。测试于2013年7月执行，使用的是运行安卓4.1.2版本的三星Galaxy S3迷你智能手机。

## 电池的使用

智能手机用户可能都有同感，“傍晚时，如果能有一个便携式的充电器就好了”。智能手机功能的多样性，即使省电处理也无法大幅降低电池的使用时间。GPS、电子邮件、互联网，特别是大多数智能手机的大屏幕显示器，都意味着需要大量的电源。所以，对智能手机的频繁使用，每到午后，电量用尽是常事。有三种方法可以防止这种情况的发生。用户可以有限制地使用智能手机；随身携带一个太阳能充电电池；或采取某些措施，在使用过程中尽可能地减少电量消耗。

- **显示设置：**显示屏，是智能手机的电量消耗大户。最好让显示屏自动调整亮度，或手工调设，以节省电源。当电池电量变低时，一些智能手机会自动降低屏幕的亮度。
- **定位：**关闭GPS。导航和定位手机（如带有地理位置的照片）都需要处理器进行高精度的计算，因为精确的地理位置需要不断地重新计算。只在确实需要使用GPS时再打开该功能。同样，WIFI和蓝牙功能也是只在必要的前提下才打开。这种设置适用于手机的所有功能；关掉不需要的功能，电池使用时间将明显延长。
- **多重任务：**在安卓系统下，应用程序可以在后台运行，在某些情况下，一些应用在很长一段时间内都不会用到。使用任务管理器关闭不适用的应用可以节省电源，因为这些未使用的应用会以其他方式耗电。在安卓系统中，只需按住“Home”按钮，就可以打开“任务管理器”。
- **邮件、Gmail：**不仅与互联网上的电子邮件和联系人同步，而且还更新脸谱（Facebook）和其他社交网站如LinkedIn的信息。可以关闭一些未知的后台运行服务或将同步计划改成不频繁进行。如果将邮件同步的时间从即时状态改为每45分钟同步一次，那么电池的使用时间可以延长三分之一。对于脸谱（Facebook）的状态更新也是一样。 Facebook的每一次更新都会打开显示屏，然后显示音频通知，两者都对电池的电量有不同程度的消耗。
- **安全软件：**许多用户始终认为，安卓智能手机中的安全软件是耗电大户。然而，我们的测试表明，这种看法也已不再属实。安全软件对电池的影响，几乎可以忽略不记。另一方面，备份、更新和恶意软件扫描，显然都会增加电池的消耗。但是，产品的优点是，可以对它们进行配置，即在手机充电时执行此类操作。

[2] http://www.gartner.com/newsroom/id/2482816

## 概述

还没有完美的移动安全产品。然而，本报告可以让您比较各产品的优缺点，缩小选择范围。在有可能的情况下，安装合适的试用版，这样更容易决定选择最佳的解决方案。尤其是那些在安卓安全产品领域，频繁发布具有完善和最新功能的新版本的产品。

通过参与本次测试，厂商们都表现出了为客户生产高品质手机安全软件的奉献精神。通过本报告发现的一些错误或作用不完善的功能，各厂商都非常重视，且纷纷采取措施，并已经开始着手解决这些问题。许多错误已经被修复。由于各测试产品的核心功能已经达到了一个很好的标准，我们很高兴为所有参与测试的产品提供评测认证。


AhnLab V3 Mobile 已经是成熟的产品。它能提供创新的功能，如文件加密和精心设计的网络监控功能。

avast! Mobile Security是一个功能全面、甚至可以免费使用的安全产品。去年已经拥有广泛功能的配套产品，现在还拥有一个网络界面。

移动安全市场的新人是只为中国用户免费提供的**百度安全管家**。除了安全功能外，它包含了一些体检功能，以提高手机的性能。

Bitdefender Mobile Security 给人的感觉是一款设计清新的安全产品。设计良好的Web界面，可用于管理多台设备，与众不同。

ESET Mobile Security在新版本中，在视觉设计方面进行了大幅度的修改。这增强了产品的实用性，这一设计值得举荐。该应用程序还提供良好的功能。

F-Secure Mobile Security 和 Trend Micro Mobile Security 提供最佳的家庭安全解决方案。除了传统的防盗保护功能外，两款产品都提供全面的家长控制功能，为儿童上网提供安全保护。

IKARUS mobile.security为用户提供设计清新的安全产品，其中包含了所有重要的功能。此外，个性化十足但有价值的功能，如URL拦截和USSD保护也包括在内。

Kaspersky Mobile Security允许用户通过隐藏短信、通话记录和联系人的方式来保护自己的隐私。今年产品版本最大的变化是加入了网络界面。

**金山手机毒霸**是只为中国用户提供的免费移动安全产品。产品设计简单易用，并提供一些有用的功能，如安全二维码扫描和广告拦截。

Lookout PREMIUM集成的备份功能可以将文件保存到云中，以防止数据丢失。测试过程中，配套的其他功能也给我们留下了深刻印象。

**奇虎360手机卫士**是一款免费的安全产品，目前主要用户为中国用户[3] 。该产品具有广泛的功能，包括防盗保护、各种优化工具、应用程序管理、网络管理以及垃圾邮件拦截。

第一次参加评测的 **Quick Heal Total Security**，其产品凭借其广泛的功能让我们着实吃惊不小。实用的备份功能和网络监控组件更令产品增色。

与去年相比， **Sophos Security and Antivirus** 也取得了质的飞跃。小程序已经发展成为一款全面的安全配套产品，它在视觉设计和功能方面给我们留下了深刻的印象。

**腾讯手机管家** 是一款中文的免费安全产品。精心设计的应用程序提供防盗保护、隐私保护以及其他各种创新的功能。

希望使用短信和网络界面两种方式发挥防盗保护功能的用户，不妨试试**Webroot SecureAnywhere Mobile** 。它的各种应用监控功能能帮助您找到耗费资源的应用程序。

[3] 英文版本将很快面市。

## 测试的产品

下列产品参与了本次测试。厂商或者为我们提供了各自的最新版产品，或确认最新的版本已经投放到谷歌商店（截至2013年7月）。测试结束后，厂商们有机会对测试中发现的其产品错误进行勘误。我们注意到，报告中提到的任何问题，随后已被修复解决。

- AhnLab V3 Mobile 2.1.0.3.178
- Avast!Mobile Security 2.0.4993
- 百度手机管家 2.0
- Bitdefender Mobile Security Premium 1.2.365
- ESET Mobile Security 2.0.766.0-0
- F-Secure Mobile Security 8.1.12262
- IKARUS mobile.security 1.7.13
- Kaspersky Mobile Security 10.4.47
- 金山手机毒霸2.3.2.775
- Lookout Premium 8.17-8a39d3f
- Sophos Security and Antivirus 3.0.1154(7)
- 腾讯手机管家4.1.1.986
- Trend Micro Mobile Security 3.1.0.1095
- 奇虎 360 手机卫士 4.0.1
- Quick Heal Total Security 1.01.063
- Webroot SecureAnywhere Mobile 3.3.0.5566


目前，百度、金山和腾讯的移动安全产品仅提供中文版，奇虎360的英文版也将/已经上市。因此，这4款产品的完整报告只包含在中文版评测报告中，详细请阅读我们的官方网站[4] 。

您可以通过下列链接，查看市场上现有的所有移动安全产品：
http://www.av-comparatives.org/list-mobile/

[4] http://www.av-comparatives.org/mobile-security/

## 电池的使用

测量手机电池的使用，乍一看似乎是很容易的。然而，当您仔细研究时，显然不是轻而易举的事情。特别是，它会因个人用户使用手机的方式不同，而对电量消耗产生很大的差异。有人使用手机的多媒体功能，有人使用手机阅读文档，同时，还有些人只是把它作为电话使用。我们需要将那些充分利用手机的技术性能和功能的用户，与“传统”的只是将智能手机当做电话使用的用户区分开。

为了了解用户对智能手机的使用情况，2012年4月我们进行了一次网上问卷调查。来自世界各地的超过千名的智能手机用户通过匿名的方式，接受并回复了我们的问题，告诉我们他们是如何使用自己的智能手机的。很显然，大多数用户选择充分利用自己智能手机所具备的先进功能。95%的用户使用智能手机上网和收发邮件，超过66%的用户收听网络音乐，或观看在线视频。另外值得注意的是，70%的用户从不关闭手机。

智能手机正变得越来越重要，而很少有用户会放过自己手机中的任何功能。智能手机的发展趋势，使它们正演变成一种无处不在的通信方式，甚至可能会成为电脑的替代品。用智能手机的电话功能越来越多的成为一种附属。其实，超过41%的用户用智能手机打电话所花费的时间只有10分钟或更少。29%的用户每天用智能手机上网超过一个小时。

我们所用的手机使用统计数据，都是来自（2012年4月的）手机安全网络问卷调查。根据此数据，我们整理并形成了智能手机每日典型的使用模式用于电池使用时间的测试。

### 测试环境

为了准确地测量电池的使用（电池电量的消耗），我们与x.test和安捷伦合作，在我们的测试中使用一台ISO标准的测量设备。这种高精密仪器，可以精确地测量电池电量的消耗。根据调查数据模拟真实用户，反复执行了多次自动化的标准测试。

### 外部环境影响

为了排除环境和技术因素的影响，我们煞费苦心，以确保每个设备都在完全相同的条件下完成测试，与ECMA-383兼容[5]。

天气条件的变化也很容易对3G和WiFi的的连接产生影响。为了尽量减少或消除这种波动，我们在自己的测试实验室建立了WiFi基站和我们自己的UMTS基站。因此，我们可以判断，建立无线连接所需的支持对每款产品是相同的。

电池的消耗自然也要取决于智能手机的型号。各种因素会影响电池的消耗，重要的一项就是显示屏。较大的手机屏幕的电池功率消耗肯定要大于较小的手机屏幕。另外还有显示屏的类型（LCD，OLED，AMOLED等）。所有被测试的安全产品使用同一款手机，使我们能够排除这种差异对测试的安全产品产生的影响。

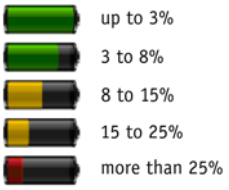
[5] http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-383.pdf

在对以下操作平均使用的基础上，我们对手机的电量消耗进行了测量（根据我们的手机使用情况调查）：

- **打电话** （每天30分钟）
- **查看图片** （每天82分钟）
- **浏览网站** （存储在本地服务器上，以避免互联网连接速度波动产生的影响;每天45分钟）
- 使用集成的YouTube应用程序**观看YouTube**视频 （每天17分钟）
- **观看存储在本地**设备上的**视频** （每天13分钟）
- 使用集成的Gmail邮件客户端**接收和发送邮件（每天2分钟）**
- **打开**存储在设备中的**文档**，如PDF和Word文档（每天1分钟）

我们在测试中发现，大多数移动安全产品对电池消耗的影响极小。

| 厂商 | 电量消耗 | 厂商 | 电量消耗 |
|---|---|---|---|
| AhnLab | | 金山 | |
| avast! | | Lookout | |
| 百度 | | Sophos | |
| Bitdefender | | 腾讯 | |
| ESET | | Trend Micro | |
| F-Secure | | 奇虎360 | |
| IKARUS | | Quick Heal | |
| Kaspersky | | Webroot | |




整体而言，对于涉及到的电量消耗，我们可以给移动安全产品的厂商们一个好评。不过，在今年的电量测试中，有两款产品没有达到最高水平：

- 例如**奇虎**360，当接听来电时，屏幕上出现五颜六色的动画画面。这看起来很漂亮，但却消耗处理器，这最终会对电池产生连锁反应。
- 对于**Webroot**，我们曾经查出是“ *执行盾（Execution Shield）* ”组件增加了电量消耗，这是一个实时防护组件，它能检测每一个执行恶意软件的应用，并将其散列值发送到云端。当关闭该功能后，电池消耗率下跌至3%以下。测试结束后，Webroot发布了新版本（3.4.0.5650）。应厂商的要求，我们使用这个版本重新进行了测试。虽然有小的改善，但电池消耗率一直在3%以上。

## 安卓恶意软件检测率

对智能手机攻击的方法越来越复杂。欺诈性应用程序试图窃取智能手机用户的信息或金钱。为了减少发生这种情况的风险，我们在此建议用户。只下载谷歌商店中的应用程序，或可信任的应用程序制造商自己的网上商店。避免使用第三方商店和Sideloading[6] 。不可信任的应用程序的另一种表现是需要无关的访问权限。例如，测量速度的一个应用程序，当您旅游时，已不再能访问您的电话簿或者通话记录。当然，即使某个应用程序做到了，它也没有明显的迹象表明，它就是恶意程序，但如果仔细的考虑一下这个程序是否是真正或应使用的程序，也不无道理。看看App Store中的评论也是一种帮助，尽量避免使用带有不良或可疑评论的应用程序。如果您ROOT您的智能手机，将实现手机的更多功能，但同样也为恶意程序的侵入提供了机会。还有一点要考虑的是保修条件。没有明确的法律条文规定，对于ROOTED的智能手机的保修是否仍然有效。在许多情况下，保修将被视为无效。

**安卓智能手机感染病毒的风险究竟有多大？**

这是个很难回答的问题，因为它取决于许多不同的因素。在西方国家，如果只使用开发厂商的官方商店，如Google Play，风险就要比许多亚洲国家低许多，特别是中国。有许多智能手机被刷机且使用的是非官方商店提供的应用程序，从而增加了安装危险应用程序的机会。在许多亚洲国家，智能手机被当做PC的替代品使用，且经常使用刷机后的手机登陆网上银行。在欧洲和美国，银行应用程序也越来越普遍。使用同一部用于汇款的手机接收mTan码会有很高的风险。在西方国家，如果您坚持使用官方应用程序商店，并且未经过刷机，那么相对来说，我们认为风险就会较低。但是，我们必须指出的是，“低风险”并不意味“无风险”。此外，威胁的情况可能发生迅速和显着的变化。最好为此做好准备，并在智能手机上安装安全软件。而目前，我们会说，如果手机丢失或被窃，防止失窃手机中的信息丢失比预防恶意软件更重要。

## AVC 安卓分析仪

基于这一点，我们向您介绍一种新的恶意软件分析工具-AVC安卓分析仪，用户可以免费使用。它是一个静态的分析系统，用于检测可疑的安卓恶意软件、广告软件并提供统计信息。用户可以上传apk文件，然后用各种分析机制看到分析结果。


我们诚挚的邀请读者进行体验：http://www.av-comparatives.org/avc-analyzer/

[6] http://en.wikipedia.org/wiki/Sideloading

## 测试集

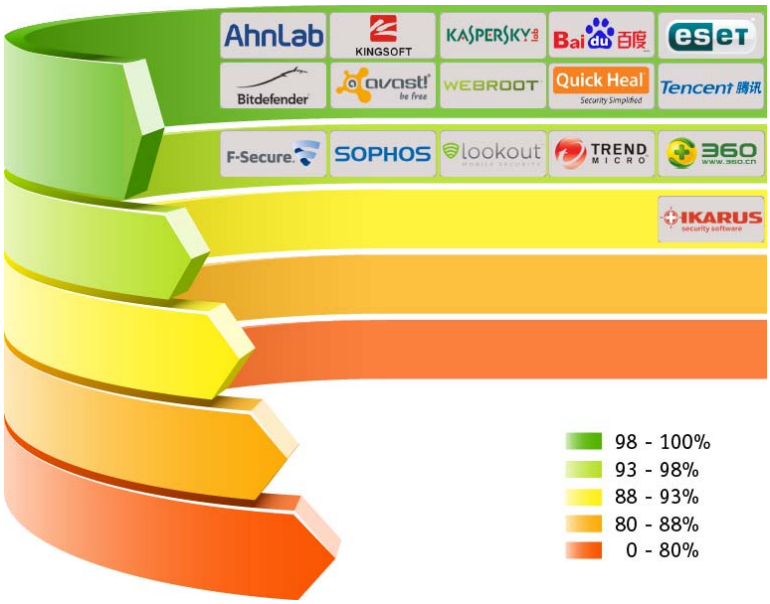
测试使用的恶意软件是在本次测试开始的前四周专门收集的。为了是测试集更具代表性，使用了2,947个恶意程序。所谓的“可能不受欢迎的应用程序”并不包括在内。2013年7月23日对所有测试的安全产品进行了更新和测试。

测试是在真实的安卓智能手机（没有使用虚拟机）上进行的。测试集含有专门的APK文件。每个单独的应用程序通过手动安装，这样做是为了测试每个安全产品所部署的反恶意应用程序技术。

我们还做了误报测试。使用的是谷歌商店里前100个不支持广告的应用。参加检测的所有产品对这100个常用的应用未产生任何的误报。

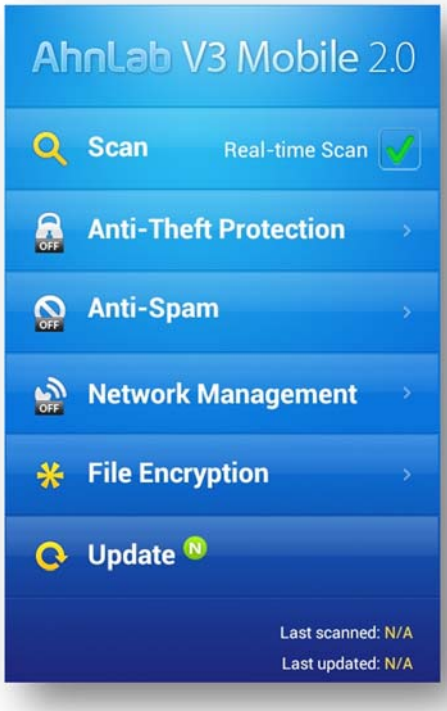
## 检测率

1. AhnLab，金山 99.9%
2. Kaspersky 99.7%
3. 百度，ESET 99.6%
4. Bitdefender 99.4%
5. avast! 99.0%
6. Webroot 98.9%
7. Quick Heal 98.6%
8. 腾讯 98.1%
9. F-Secure 97.1%
10. Sophos 96.3%
11. Lookout 96.0%
12. Trend Micro 95.6%
13. 奇虎360 93.6%
14. Ikarus 91.0%



## AhnLab V3 Mobile

AhnLab V3 Mobile是一款安卓安全产品，具有最重要的诸如恶意软件扫描、防盗和防垃圾短信功能。




### 安装

AhnLab为我们提供了AhnLab V3 Mobile 的APK文件。安装过程非常简单。接受使用许可协议后，我们需要先为手机进行注册，只花了几秒钟，并未要求输入任何更多的用户信息。随后，程序进入启动页面。

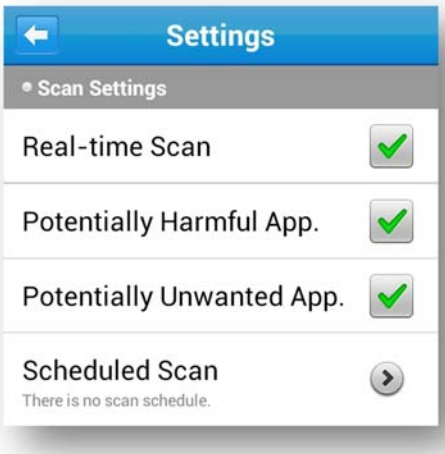
### 启动程序

没有关于 AhnLab V3 Mobile的产品介绍，用户只需进入程序，然后慢慢去研究发现所提供的功能。没有初始更新。默认情况下，实时保护已开启，可以从主屏幕直接开启或关闭。在本窗口中，也可以开启所有其他功能。在屏幕的右下角显示有详细的最后更新和扫描状态；安装一结束，两种状态都显示为“N/A”。

### 扫描

扫描模块允许用户运行两种不同类型的扫描：扫描所有已安装的恶意行为的*智能扫描*，和额外扫描手机中所有文件的*全面扫描*。最后一次*计划扫描*的详细信息和下次扫描时间也被显示。该设置可以在全局配置菜单更改。扫描间隔（每天或每周）可以设定，每天扫描的时间也能设定。

设置还包括敏感扫描选项。




### 防盗保护

要使用这个组件，需要设置一个4至10个字符的密码。该应用还必须以设备管理员的身份注册。总的来说，我们感觉设置步骤非常简单。防盗保护功能通过短信来控制，但没有web界面。指令以总览的形式列示，且可以测试。

### *锁定*

***短信指令：*** *“#lock〈密码〉〈短信〉“*

使用该指令可以锁定智能手机，防止未经授权的操作。此处需要使用先前设置的密码。我们喜欢的一项设计是，可以发送私人讯息在锁定的屏幕上显示。另一个加分点是，错误输入10个密码后，一条带有手机位置信息的短信将被自动发送给锁定命令的发送人。

需要减分的是，锁屏后不允许进行紧急呼叫。这样不是很安全。按下“主页”按钮会显示主屏幕；通过屏幕可以查找并查看已安装的应用程序。另外，仍然可以启动程序，虽然几秒钟后锁定屏幕会出现。因此，锁屏功能其实不能算是名副其实。

### *远程数据删除*

***短信指令：“#remove〈密码〉“***

这条指令将删除手机上的所有数据。手机没有被恢复到出厂设置，这意味着防盗软件仍然在并能发挥作用。虽然短信日志未被删除，但这项功能在很大程度上还是行之有效的。所有的联系人、文件、日历、浏览器历史记录和书签都被一扫而光。然而，使用普通的免费软件工具还是有可能恢复SD卡中的数据。

### *远程擦除重置*

***短信指令：“#kill〈密码〉“***

此命令将删除个人数据信息并重置手机到出厂设置。

与远程数据删除功能相反，这个功能的测试结果并不理想。无论是SIM卡上的联系人还是SD卡上的文件皆未被删除。我们可能建议先发送“远程数据删除”指令，然后使用“远程删除重置”指令。

### *远程定位追踪*

***短信指令：“#locate〈密码〉“***

当指令被发送后，短信发送者会及时地收到一条在谷歌地图上，带有完整坐标的手机位置链接短信。名词“追踪”的意思是连续的跟踪，而不是一次性的指出位置，所以，定位功能发挥的非常出色。

### *SIM卡监控*

如果SIM卡被更换，带有手机位置的详细信息的短信将被发送到受信任的电话号码上。

### 反垃圾短信

安博士的反垃圾短信功能允许将要拦截的通话和短信加入黑名单来完成。有几种可能的方式来添加电话号码到黑名单：从呼叫和短信记录中添加、从通讯录添加、或手动添加。对于每一个电话，可以只阻止呼叫，只拦截短信，或两者都阻止。

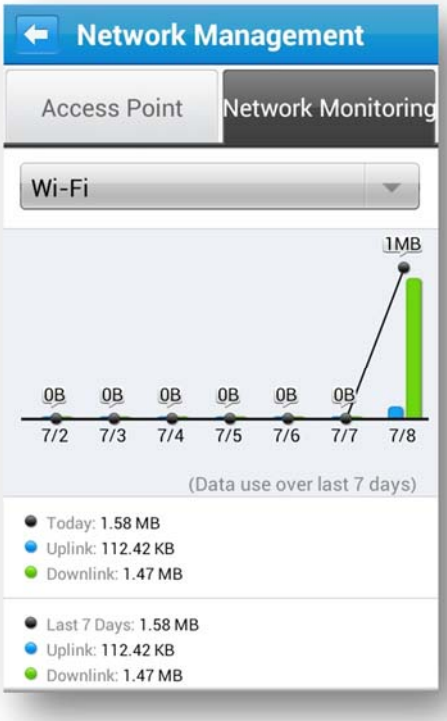
此外，还可以根据内容拦截短信。可以将关键字的长度定义在2到10个字之间。我们不知道为何要限制字的长度。我们还发现，过滤功能还要区分大小写，而这似乎又是一个值得关注的限制。

子菜单可以显示所有被阻止的通话和短信。整体而言，反垃圾短信功能的作用还是令人满意的。默认情况下，该功能未开启。我们最初不清楚该情况，所以测试时，我们猜测该功能不起作用。如果在菜单中能显示功能的状态，将是一个进步。

### 网络管理

“网络管理”菜单汇集了与网络有关的功能。

当设备连接到一个WiFi热点，会弹出窗口，允许用户关闭无线网络，或永久允许或拒绝访问该热点。允许对已知的接入热点列表进行管理。




可以限制移动网络的使用；如果移动网络使用流量达到预定义的限制，会收到警示。*网络监控*为用户提供流量使用统计。可以根据移动和WLAN流量排序。可以分别显示各时间段内上传和下载的数据量。

### 文件加密

文件加密可以对单个文件进行加密。通过文件浏览器，可以选择多个文件，然后使用4到10个字符的密码进行加密。加密结束后，文件名结尾带有*aed，该文件无法打开。解密也要使用安博士软件。可以加密的文件类型没有任何限制，所以，图片、视频、PDF文件等都可以用这种方式进行保护。

### 更新

更新会自动进行。用户可以决定是否只通过WiFi更新或使用移动网络进行更新。因为有计划扫描，所以可以配置自动更新的时间。

### 帮助

安博士的帮助功能条理清晰。我们比较喜欢它对特定任务的逐步介绍。然而，让人颇为恼火的是，当触击“后退”按钮时，却返回到“开始屏幕”或“帮助主页面”。

### 卸载

没有卸载指南，但在“帮助功能”中提供了一步一步的指导。须先从设备管理器中删除应用程序，然后就可以从安卓应用程序管理器卸载。

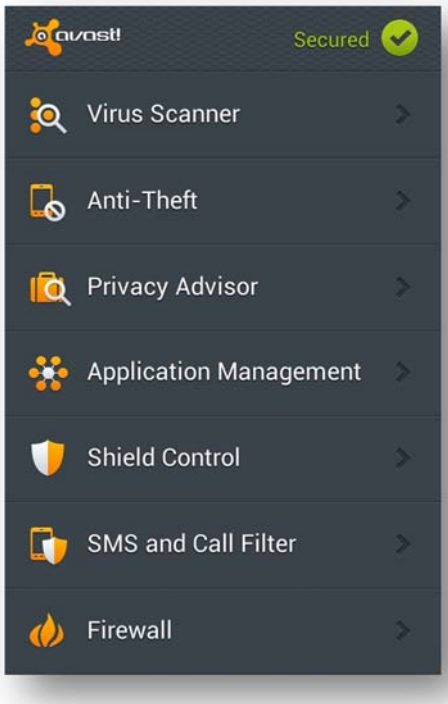
删除该程序不用密码。这可能成为一个安全隐患，因为小偷可以很容易地卸载防盗保护。

### 总结

AhnLab V3 Mobile为安卓智能手机提供了最重要的安全功能。以及传统的功能，该方案提供了创新的诸如文件加密和网络管理等功能。

## avast! Mobile Security

avast! Mobile Security 是一款为手机和平板电脑提供全面保护的免费安全产品。他的主要功能包括：防病毒、浏览器保护和防盗保护。




### 安装

我们通过谷歌商店安装了avast! Mobile Security。安装很简单，只需接受使用许可协议即可。用户可以决定是否要发匿名使用信息给厂商。

### 启动程序

程序首次启动时会显示主屏幕信息；通过该窗口展示了产品功能的广泛性。在屏幕的右上角，初始安全状态明显地显示为“过期”。但是一旦执行自动更新后，状态立即改变为“安全”。

要进入系统主菜单，很大程度上靠直觉。但通过向右滑动屏幕可以显示活动日志，但估计一些用户仍未发现。

### 病毒扫描

病毒扫描程序可以扫描所有已安装的应用程序是否感染恶意软件。用户也可以选择开启或不开启文件扫描。按住此复选框会出现一个菜单，从菜单中可以选择一个特定的文件夹进行扫描。屏幕底部的按钮可以用于配置自动扫描。可以选择扫描日期和时间。

### 防盗

防盗组件是一个需要单独安装的应用程序。他的优点是可以隐藏防盗应用程序；它与程序的其余部分集成的天衣无缝，用户可能根本没有注意到它是一个独立的程序。

安装过程简单，但相对来说要求比较全面。必须输入一个名字、朋友/家人的电话号码、和一个4-6位数的PIN码。然后必须注册avast! 帐户，如果要使用Web界面，用户需先登录。

开启防盗组件后，它会自动进入“隐藏模式”，这意味着防盗功能已经隐藏了。呼叫用作PIN码的电话号码可以取消隐藏。

一个非常刺眼的黄色符号提醒您：该配置尚未完成，并指出必须为avast!提供管理员权限。

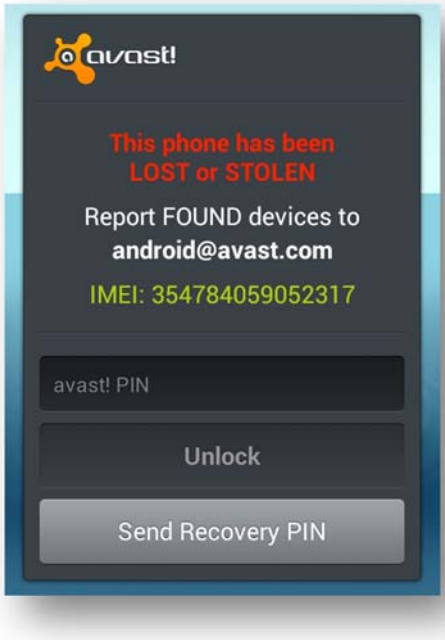
防盗组件即可以通过网络界面进行控制，也可以使用多个短信命令。除了标准的锁定、定位和擦除命令外，avast! 还有各种功能，如转发短信、通话和通话记录等。通过下列链接#TAB3 http://www.avast.com/en-gb/free-mobile-security以及点击

“通过短信控制”，可以查看可用功能的完整列表。

### 锁定

***短信指令：“〈PIN码〉LOCK“***

当收到该指令后，设备即被锁定并显示为锁屏状态。avast！要求善意捡到手机的人通知avast!该设备已被发现（可以自定义锁屏短信内容）。这需要发送手机的IMEI（国际移动设备识别码，设备的唯一识别号码）到android@avast.com。该IMEI会显示在锁定的屏幕上。此外，手机会播放音频通知“这款手机已经丢失或被盗”（只播放英文音频）。输入正确的PIN码可以为手机解锁。




在实践中，锁定功能也存在问题。当手机被锁定后，仍然可以打开安卓通知栏，向下滑动屏幕就可轻易更改设置。按住“主页”按钮会显示最近使用过的应用程序列表，个人信息也可以在此看到。avast！告诉我们，这种问题在下一版本中将予以纠正。

此外，锁屏后不能拨打紧急电话，这种情况也不妙，在一些国家也可能是不合法的。

### 警笛

***短信指令：“〈PIN码〉SIREN ON“***

此命令一发出，手机就响起与锁定手机时一样的警笛声，但并不锁定手机。因此，如果忘记了手机所放置的地方，也可以用该功能寻找。

### 定位

***短信指令：“〈PIN码〉LOCATE〈时间间隔〉“.***

此命令用来查找丢失或被盗的手机。此命令的发令人将收到一则回复短信，短信中包含带有定位坐标、移动电话服务提供商和天线杆的在线地图链接。选择参数*INTERVALL*表示定位的频率，以分钟为单位来重复进行上述定位操作。频繁返回的位置数据可以保证持续跟踪手机的位置。很显然，使用网络界面非常理想，通过界面可以清晰地显示手机的位移。

### 删除

***短信指令：„〈PIN码〉WIPE“***

avast！Mobile Security 提供两种删除功能。一个标准的删除功能，和一个在高级防盗设置中提供的彻底删除功能。这两种类型的删除功能都将测试设备重置到出厂设置，使所有的个人资料和内部存储上的所有文件都被删除。

彻底删除参数提供的数据表明，内部存储上约有1000个1MB的垃圾文件，无法恢复任何原始数据。

我们使用这两种删除方式进行了测试，只删除了诸如MP3或JPG格式的媒体文件。所有其他类型的文件（测试使用的文件类型有.exe、.dll和.txt文件）原封未动。

在测试“彻底删除”功能时我们发现，即使文件被从SD卡上删除了，但是使用免费的程序还可以恢复。

### 强行重置保护

avast！为使用rooted设备的用户提供强行重置保护。通过启用此功能，avast！安全

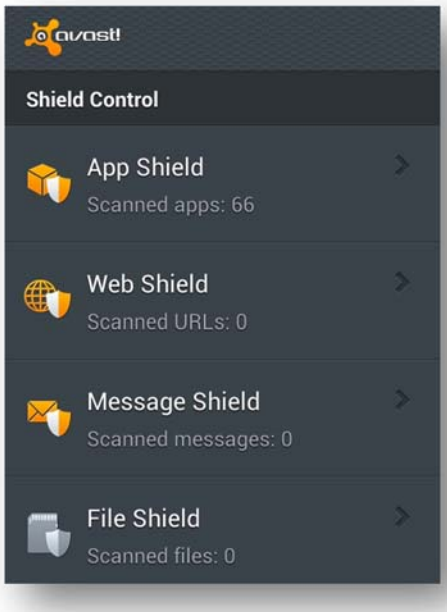
产品可以使设备重回出厂设置，且不会删除出厂设置。

### 隐私保护

“隐私顾问”可以将需要特殊权限的应用程序，如*短信处理*进行归类。它可以为用户提供设备中“有潜在的数据保护问题”的概述。点击六个类别中的任何一类，都可以显示其中的应用列表。如果用户点击一个特定的应用程序，就会显示详细的应用信息，一同出现的还有一个让程序立即停止的按钮。

### 应用程序管理

应用程序管理器分析正在运行和已安装的占用CPU、内存、存储空间和其他资源的应用，并允许用户停止那些收费应用程序。




### 实时监控

*实时监控*功能项下可以找到各种实时保护功能。具体如下：

#### *应用程序监控*

该功能可以扫描各种恶意应用程序，据配置说明介绍，在恶意程序安装或执行时都可以被监控到。

#### *网页监控*

该组件可以保护用户避免落入网络钓鱼和恶意代码的陷阱。支持默认浏览器和谷歌Chrome浏览器。

Avast还提供拼写检查，据说可以识别并纠正错误输入的网址（防止蓄意错误拼写）。然而，测试时未能发现能激活此功能的案例。

#### *短信监控*

该功能监控所有接收的钓鱼和危险网站链接短信。这项功能在我们的测试中发挥稳定。该功能也可以用于阻止未知联系人的短信。

#### *文件监控*

此功能扫描读取/写入文件时的恶意行为。测试时，此功能也发挥正常。

### 短信和通话过滤

为了阻止陌生来电和短信，avast!还提供短信和通话过滤服务。该功能允许创建要阻止的组，组中的通话和短信将被阻止，要么在特定时间阻止，要么完全阻止。

要阻止的组成员的电话号码，可以从通讯录或所有匿名呼入或短信发送者中筛选出来，实际上，.avast！使用的是黑名单原理。

### 防火墙

只有设备已经rooted，防火墙才能被开启。这是对无ROOTED的设备的操作系统的正常限制。

### 网络监控

此组件列出了所有已安装的应用程序所用的数据量。这可以根据WiFi、3G、漫游或全部使用情况逐项列出。点击其中一项应用程序，可以按日期显示数据流量（某年某月的某一天）。

### 更新

默认情况下，avast！Mobile Security将自动更新。用户可以决定是通过WiFi、3G还是漫游网络来更新。

### 帮助

除了防盗功能外，avast！不提供智能手机的任何本地帮助。需要帮助的用户需访问厂商的网站；网站提供一个完整的常见问题板块，该帮助板块涵盖了大多数的疑难问题。

### 卸载

卸载指南为用户提供卸载防盗保护的帮助。要求输入PIN码。如果通过安卓应用程序管理器卸载应用，也要输入PIN码。这意味着未经授权的用户不能卸载防盗保护功能。

### 展望

avast！宣布在未来的商业版本中，将包括某些附加功能，如应用程序和照片备份、扩展防盗功能、应用程序锁定和高级隐私扫描等。

### 许可

avast！Mobile Security是人人可用，无任何功能限制的免费安全软件。

### 总结

avast！Mobile Security提供了广泛的功能，并且免费。我们尤其欣赏它的各种配置选项和具有广泛控制功能的远程操作指令。

## 百度安全管家

百度安全管家是一款设计简洁的免费移动安全产品。主要功能包括杀毒、垃圾短信过滤和各种加速要件。

不久前，百度收购了小有名气的移动安全生产商TrustGo。这使得百度在技术层面获得了额外的提升，对自己的产品肯定也会产生一些正面的影响。


### 安装

我们毫不费力地从正规的安卓市场找到了百度安全管家并下载安装。安装过程非常简单，只需接受用户使用许可协议即可。

### 启动程序

第一次启动程序时，会出现简单而整洁的界面。点触主页面上的一些重要功能，用户可以体检并使用这些功能，以及所有其他的功能。

### 手机体检

手机体检能检查设备和性能的优化性。主页上部的体检按钮一旦启动，体检功能就开始飞速运行。首次运行后，体检报告为设备的健康程度打了91分，且“如果要使手机更健康的话”可能需要清理38个应用程序。体检还查出了几个垃圾文件。重新点击“立即优化”，这几个垃圾文件得到清理，体检终于达到100分。

再次重复运行上述过程，手机取得了95分，又出现了9个需要优化的程序。

### 手机加速

手机加速功能可以帮助您找出可能会影响手机性能的各种问题所在。测试时，报告有13个影响手机操作的问题：分别是8个后台运行的应用程序和5个“缓存”可能需要清理。点击“立即加速”，问题得到解决。清理过程结束后，程序建议执行“深度加速”。


我们发现，手机体检时获得95分，可能需要关闭12个后台应用。所以，手机体检和手机加速好像工作原理并不相关。

### 病毒扫描

百度安全管家提供“快速扫描”和“全盘扫描”。可以手动更新病毒库并向百度举报危险应用。

### 话费保镖

该功能旨在“为您守护话费安全”。该功能可以监控通话或发送短信等活动时的各种吸费应用程序，但受访问权限限制。但

愿病毒扫描时也曾经检测到这些威胁就好了。

### 骚扰拦截

垃圾短信在中国非常普遍。百度安全管家提供预防这类骚扰的功能。测试时，百度安全管家正常接收并正确地拦截了垃圾短信，并将垃圾短信与正常的短信分开。但是，应用程序确实已将垃圾短信过滤后，但在主界面的“骚扰拦截”图标下却仍然显示拦截的短信为“0”。

### 流量监控


该功能监控用户使用的数据流量。能够根据用户的签约流量进行流量计划设置。如果用户使用的流量达到限定数，百度手机管家会提醒用户关闭网络访问。流量数据可以定期与移动供应商提供的流量数据同步。

### 隐私保护

该功能列示了手机中所有已安装的可能窃取用户隐私信息的应用，以及受权限访问限制的读取通话和短信记录、读取手机位置和读取手机识别码（IMEI）。受访问权限限制的发送短信和通话记录在话费保镖功能中已经提到过，在此功能中再次出现。

### 手机备份

百度安全管家允许用户将联系人（通讯录）、通话记录和短信“备份至云端”。要使用此功能，需要先登录到“百度账户”。


### 广告扫描

百度安全管家在其启用程序中提供广告扫描模块。它能找出各种含有推送广告的应用程序。测试时，百度安全管家检测出6款这样的应用程序，其中的“pontiflex”被测出含有威胁。这一发现与病毒扫描的结论相悖，甚至在随后进行的全盘扫描的结论也是“非常安全”。用户可以通过一键点击来卸载“风险广告”。


### 安全浏览

百度安全管家为用户提供上网安全保护，“在您浏览网页时第一时间拦截恶意网站”。

### 百度纸风车

安装了百度安全管家后，测试手机的桌面右侧出现一个小小的纸风车。拖拽这个小风车到屏幕的中间释放，风车开始旋转执行手机的快速清理。

### 卸载百度安全管家

没有卸载指南。卸载百度安全产品不需要密码就能卸载。由于百度安全管家没有防盗功能，所以这种情况下，没必要卸载安全保护。

## 授权

百度安全管家是免费产品。

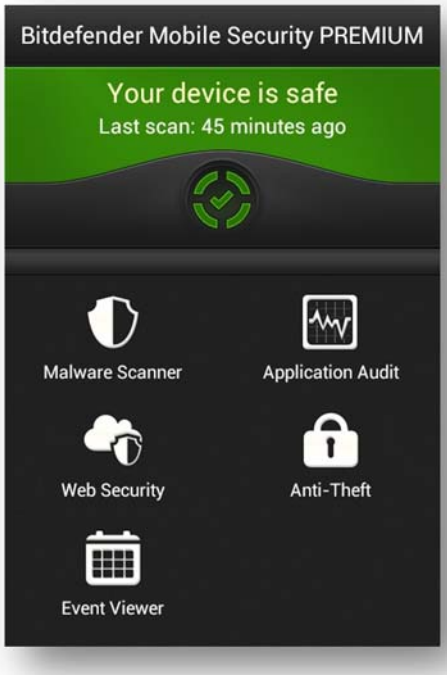
## 结论

百度安全管家是一款易用的产品，有各种重要的安全功能，如病毒扫描和垃圾短信防护。遗憾的是，缺失了重要的防盗保护功能。

病毒扫描是任何安全产品的核心功能。安全产品的任何一个模块所检测到的危险都应在这里体现。不同的模块如广告扫描模块发现的恶意广告插件，如果在病毒扫描部分能显示该警告，可能会比声称“很安全”要好的多。

## Bitdefender Mobile Security Premium

Bitdefender Mobile Security Premium提供14天的免费试用期。试用期满后，用户必须付费购买。该软件结合基于云的恶意软件扫描技术，具有上网保护和防盗保护功能。后者可以通过网络界面或短信操作。




### 安装

Bitdefender可以轻松的通过谷歌商店安装。接受使用许可协议后，用户需要为设备指定一个使用Web界面的用户名，然后登录到BitDefender帐户或指定一个谷歌帐户。这也是为了能够使用Web界面。随后显示各功能的简要概述，安装完成后，出现程序的主屏幕。

### 启动程序

安装完毕后，用户将看到一个非常醒目的通知（黄色），通知说应该运行扫描，紧接着是14天试用版本的提示（如适用）。


恶意软件扫描后，会出现3种情况：如果用户在屏幕上看到的是一个绿色的状态，表示设备是安全的；如果有需要用户注意的问题，会出现橙色或红色状态。没有提到更新状态，这是因为病毒库未保存在本地，而是保存在云端。

### 恶意软件扫描

使用该功能，用户可以为已安装的应用程序和手机内存进行恶意软件扫描。用户只有一个配置选项可用，即当手机连接到另一个设备时，是否启动自动扫描。

由于使用云进行检测，所以恶意软件扫描只在有网络连接时才工作。

### 应用程序检测

应用程序检测模块显示所有需要特殊权限的应用程序，如网络接入、读取私人信息或各种付费服务。可以通过类别过滤，来提供应用程序概述。点击其中的一个应用程序，用户可以看到有关的安卓应用程序信息页面。

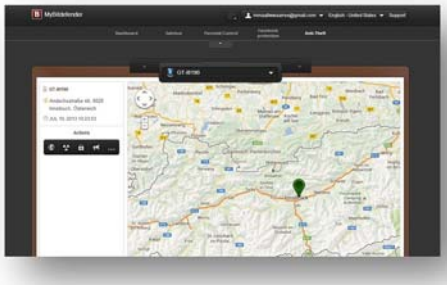
### Web安全保护

Web安全保护功能帮助用户躲过钓鱼攻击、不受信任网站和恶意软件的威胁。它支持默认的安卓浏览器和谷歌Chrome浏览器。

### 防盗

默认情况下，防盗模块未开启。可以通过时尚的Web界面进行操作[7]，允许通过多设备或短信命令进行管理。

[7] http://my.bitdefender.com



启动防盗组件会显示一个简要介绍，然后要求用户提供具有管理员权限的应用程序。必须设置一个4-8位数字的PIN码，并输入一个可信的电话号码。后者万一SIM卡被更换，可用于接收通知短信。这个电话号码也是唯一可以用来发送删除命令的号码。

有一个使用两种操作方法（网页和短信）的选项。例如，可以禁用全部Web界面或短信功能中的某些元素。任何配置更改都必须输入PIN码。


### *定位*

***短信指令：“bd-<PIN码> locate“***

设备丢失或被盗的情况下，可以使用该指令查找。指令发出后，发令手机会收到一则带有谷歌地图的回复短信，短信中显示位置信息和定位时间。如果使用Web界面，也会显示相似的地图位置信息。没有办法对设备进行持续的追踪。

### *锁定*

***短信指令：“bd-<PIN码> lock“***

这一命令可以锁定手机，防止未经授权的操作。BitDefender使用自成一体的安卓标准锁屏。它不允许显示任何标志或消息，但完全安全。你不可能避开它，但又总是能够进行紧急呼叫。

### *删除*

***短信指令：“bd-<PIN码> wipe“***

此功能可以删除用户智能手机中的所有个人数据，使第三方无法访问。一旦收到删除命令后，设备会立即恢复到出厂设置。

遗憾的是，外置SD卡上的文件却都在。

### *给我打电话*

***短信指令：“bd-<PIN码> callme”***

此功能只能通过短信操作。它会导致设备呼叫发信息人的电话号码，并激活喇叭。这种功能可以用在善意捡到手机的人身上。

### *回答*

***短信指令：“bd-<PIN码> answer“***

此功能类似于“给我打电话”。在这种情况下，先发送短信，然后用户可以呼叫丢失的手机，它会自动应答。

但测试时，这个功能罢工。电话无人接听，也没有收到任何短信回复。Bitdefender通知说，该功能不支持安卓4.1或以上版本。

### 帮助

软件没有具体的帮助功能。但是，每个功能都有自己简短但有用的文字说明。

### 卸载

未提供删除软件的卸载程序。因此，用户必须知道能删除软件的管理员的权限。这就要求输入PIN码，以防止小偷禁用安全软件。

### 许可

BitDefender Mobile Security可以免费试用14天。如果要继续使用，可以付8.99欧元购买该应用程序。

### 总结

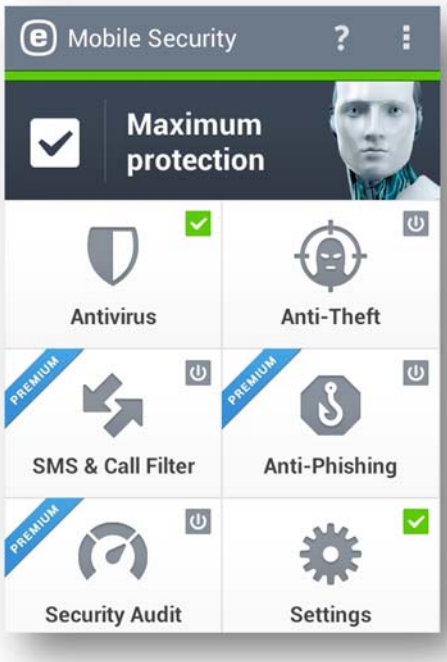
BitDefender Mobile Security为智能手机用户提供了一个易于使用的安全产品。它有全方位的防盗功能。

值得举荐的是，该软件新增了设计直观的web界面，此界面允许用户使用一个账户管理多部智能手机。

对于恶意软件扫描，我们觉得，BitDefender不应该仅依靠云端扫描，因为在没有网络连接的情况下识别恶意软件是不可能的。

## ESET Mobile Security

ESET Mobile Security是一款包含防病毒和防盗功能的安全应用程序。付费版还另外提供短信和电话过滤、反网络钓鱼和系统监控组件以及防盗功能，尤其是远程删除和SIM卡监控。




### 安装

从谷歌商店，我们安装了ESET Mobile Security。程序首次启动时，最终用户使用许可协议已被接受。通过使用复选框，用户还可以同意向ESET发送匿名使用信息。在默认情况下，该复选框选项未开启。在接下来的配置步骤中，可以关闭*ESET Live Grid*（默认情况下，它是开启的）。这是一个早期预警系统，它使用的数据，都是从参与的用户中最近刚刚收集的。最后检查使用许可，并用通知告知用户初始扫描即将开始。

### 启动程序

初始配置后，一个清晰的主屏幕呈现给用户（见上图）。屏幕中显示的是ESET产品所提供的所有单个功能组件。已开启的功能组件已用绿色的勾标注，未开启的功能全部显示为灰色的开关符号，需要注意的组件则用橙色的三角符号标注。此外，付费组件（仅适用于付费版）都用蓝条标注。付费版可以免费试用30天，还需提供电子邮件地址。

### 杀毒

防病毒功能可以对系统进行恶意软件扫描。可以对扫描进行配置，隔离列表、扫描日志和更新的详细信息都可以看到。用户可以在高级设置中更改安装软件期间配置的项目，并且当发现恶意软件时，设置默认操作。

### 防盗

防盗组件需要在首次启动时进行配置。包括输入安全密码，和一个可选的提醒短语。虽然没有限制密码长度最小值，但ESET警告用户，短密码不安全。为了防止未经授权的人卸载程序，ESET建议应为程序设一个设备管理员。接下来是短信命令通知，并可以使用不同的密码。之后，当前使用的SIM卡被注册为受信任的SIM卡，还需输入一个受信任的电话号码。我们比较欣赏的是，可以编辑手机被锁定后要显示的文字。要使用此功能的短信命令，需要密码。虽然可以使用标准的安全密码，但还是建议使用一个独立的防盗密码。

#### *SIM卡保镖*

此功能是为了防止未经授权的人更换SIM卡。如果插入一张未注册的SIM卡，手机将被锁定。测试时，该功能发挥非常好。我们可以选择输入安全密码为手机解锁，或呼叫紧急号码。我们注意到，当插入一张未注册的SIM卡后，需要密码确认，即使重新插入原来的SIM卡也一样。这里稍微有一点儿安全风险，对密码尝试没有输入次数限制，除此之外，功能设计明智且执行正常。

#### *锁定*

***短信指令：“eset lock〈密码〉”***

当收到该指令后，设备即被锁定并显示为锁屏状态。短信发送人也将收到带有IMEI和IMSI（设备识别码）的确认短信。与SIM卡保镖一样，锁屏部署同样具有很高的耐锁能力。如果用户忘记了密码，他们可以

从另一部手机发送一个重置指令，或者从自己锁屏的手机直接发送一个重置电子邮件。

*警笛*

*短信指令：“eset siren〈密码〉”*

除了额外播放差不多一分钟非常响亮的报警声以外，此命令提供的功能与“锁定功能”没有区别。

*查找*

*短信指令：“eset find〈密码〉“*

该组件功能可以查找被盗或丢失的智能手机。发送短信后，短信发送人会收到一则回复短信，内容包含一个带有手机相关位置坐标的谷歌地图链接。

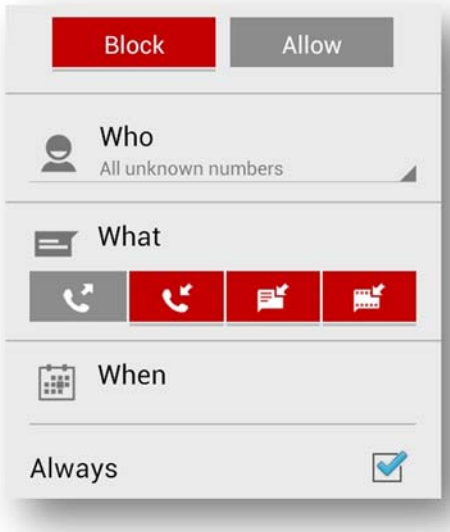
*删除*

*短信指令：“eset wipe〈密码〉“*

此功能可以删除用户智能手机中的所有个人数据，防止第三方访问。手机没有被恢复到出厂设置，这意味着防盗软件仍然在且防盗功能也将继续发挥作用。然而，日历项、浏览器历史记录、收藏夹和短信日志都未被删除。ESET告知我们说，他们计划在下一个产品版本解决这个问题。相反，内存卡删除得干干净净，而且，使用免费的程序无法从SD卡来恢复数据。

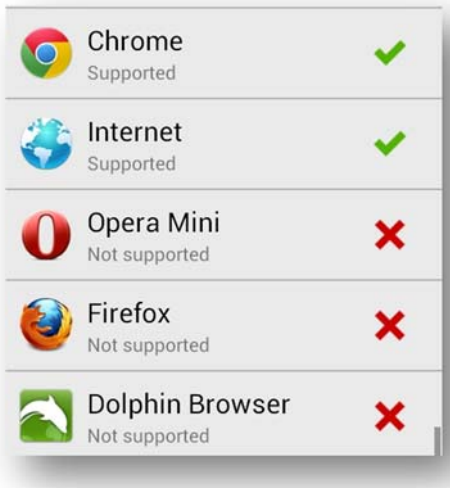
### 短信和来电过滤（付费版）

用户可以通过此功能，为通话和短信创建全面的黑名单或白名单规则。可以设置规则，来确定在指定的时间只有指定的联系人才允许通话或发短信。




### 反网络钓鱼（付费版）

此功能保护用户浏览网页时，免入钓鱼网站。ESET可以检查所安装浏览器的兼容性。虽然ESET Mobile Security声称它“集成了最常用的浏览器”，但在实践中，也意味着仅支持安卓和谷歌Chrome浏览器。并不支持Firefox、Opera和海豚浏览器。




在测试过程中，网络钓鱼防护功能与所支持的两种浏览器配合的超级好。ESET发出了一个警告页面，建议用户立即离开当前的网址。

### 安全监控（付费版）

安全监控功能提供系统设置和可能表示安全风险的程序权限信息。在测试过程中，

我们被告知，除其他事项外，“USB调试模式和来源不明的安装”设置被启用。设备监控功能包括通知，例如漫游通话和数据流量、不安全的WiFi连接和内存使用情况。

### 帮助

ESET为用户提供涵盖了所有可用功能组件的帮助文件。点击组件中的问号，用户就可以看到帮助文本的相应部分。

### 卸载

该程序可以从它自己的设置菜单卸载，或者从安卓应用程序管理器中卸载。如果防盗组件已开启，无论使用何种卸载方式，必须输入安全密码。通过程序内部菜单删除应用程序时，要求回答卸载的原因，然后只需单击可以继续卸载。

### 许可

软件的免费版本已包含大部分的功能。要使用付费版本中的自动扫描、自动更新、钓鱼防护、SIM卡锁定、删除和安全监控等功能，需要每年支付14.95欧元，从www.eset.com网站可以直接购买。这些功能可以免费试用30天。

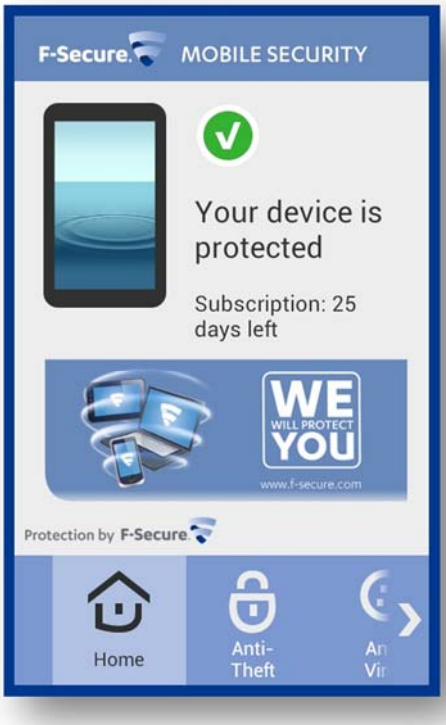
### 总结

ESET为安卓智能手机提供一套灵活的安全解决方案，其直观的界面也给我们留下了深刻的印象。ESET Mobile Security的功能也同样是经过深思熟虑而设计的。

除了删除功能漏掉了一些数据外（ESET已承诺纠正），我们也想提出一个小小的改进建议：将产品中加入一个web界面可能更圆满。

## F-Secure Mobile Security

F-Secure Mobile Security是一款提供所有重要功能的移动安全产品。除了防盗和防病毒功能外，该软件的付费版本还包括家长控制、浏览器保护和通话/短信拦截功能。




### 安装

我们从谷歌商店下载并安装了F-Secure Mobile Security。当应用程序第一次启动时，用户必须接受使用许可协议，这一过程需要网络连接。然后可以激活一个30天的试用版激活码。设置防盗保护功能需要创建一个安全密码，密码长度必须至少为5个字符，并且会检查密码的安全性。不允许使用“QQQQQ”类型的密码，但也未提供能被接受的密码类型信息。于是我们尝试使用“qqqq1”作为密码，这次被接受了。创建密码后，用户必须输入一个可信任的电话号码，当SIM卡被更换时，用于接收更换通知。最后，F-Secure开始运行初始扫描。

### 启动程序

程序的启动屏幕显示出设备受到保护的消息，紧接着显示的是试用剩余的天数。通过滑动屏幕或点击屏幕底部显示的按钮，开始进入应用程序。

### 防病毒

此组件可以保护系统免受恶意软件的侵害。最后一次更新和扫描的日期分别显示。可以启动一次完整的设备扫描，或已配置好的计划扫描；扫描频率可以设置成每天、每周或每月。
此外，云保护功能既可以完全关闭，也可以设置成只有不会产生漫游费时才运行。还有一个关闭实时保护的选项。

### 防盗

防盗组件通过向手机发送短信命令来控制，需要与密码组合使用。没有Web界面。可用的功能如下：

#### *锁定*

*短信指令：“#lock#<密码>”*

这一命令可以锁定采用安卓锁屏的手机屏幕。这一功能非常震撼，可以防止任何未经授权的访问。一旦发送命令，要开启锁定的手机就离不开锁屏PIN码了。

#### *定位*

*短信指令：“#locate#<密码>“*

此功能可以找到丢失或被盗的手机。当命令发送出去后，发令人会收到一则短信，内容包含带有手机坐标和一个指向谷歌地图的链接。

#### *报警*

*短信指令：“#alarm#<密码>#<次数>“*

除了额外发出报警声外，该命令的功能与“锁定”命令功能相同。要设定发出警报声的次数，由参数*（报警）次数*确定，如果不进行设置，报警声将不停断。如果将参数设置为“0”，报警被关闭。

#### *删除*

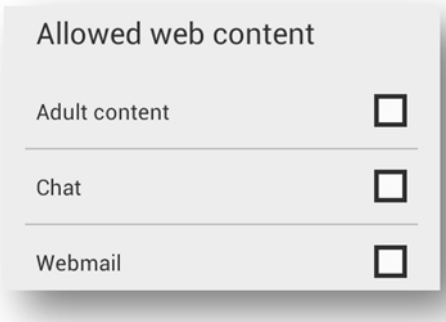
*短信指令：“#wipe#<密码>“*

删除命令会删除智能手机上保存的所有个人数据。首先，外部SD卡中的数据会被删除，设备被重置到出厂设置。测试时，除了SIM卡中的联系人未被删除外，其他所有的数据被成功删除，

删除过程眨眼间完成。使用免费工具无法恢复任何被删除的数据。

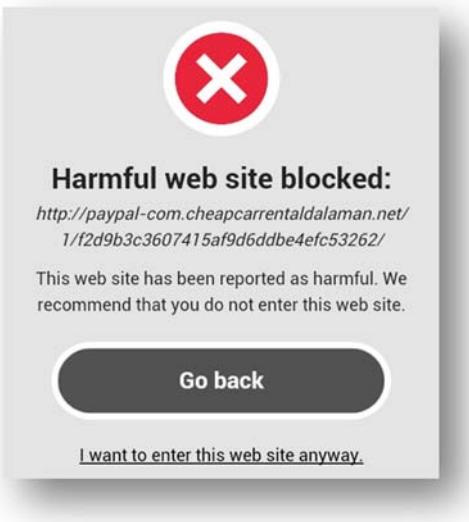
### 家长控制

这一功能可以避免儿童接触到不当的互联网内容/安装的应用程序。用户可以在*儿童*、*青少年*和*成人*内容题材间进行选择，每一种选择都有预先配置的不同的内容过滤器。每个级别还可以单独调整。例如内容方面可以阻止的有武器、赌博和非法下载。




### 安全浏览器

F-Secure的安全浏览器功能提供了一个单独的浏览器应用程序，该程序可以防止访问钓鱼网站。它阻止其他的浏览器，并只允许使用安全浏览器。如果网页被阻止，就会显示带有“返回或继续”浏览的警告消息。




如果家长控制功能已开启，F-Secure的安全浏览器功能就可以总是用于查看网址。

原则上，我们对安全浏览器功能表示赞同，但是，在用户可以选择浏览器使用的地方，全球性的网络钓鱼防护功能，或许更加实用。

### 安全联系人

此功能可以阻止来自特定电话号码的呼入和短信，这些特定电话号码可以手工输入或从联系人列表中导入。就是编辑一个简单的黑名单。如果电话号码被添加到黑名单中，该电话号码的所有呼入和呼出，以及发来的短信都将被阻止。不能只阻止来电或短信。

### 帮助

F-Secure提供在线常见问题解答。此外，每个组件都有自己简短，但内容丰富的帮助文本。

### 卸载

卸载受密码保护。在更多|关于菜单下是一个卸载向导。一旦输入密码，程序立即会被删除。该软件还可以从安卓应用程序管理器中卸载，首先必须将它从设备管理员列表中删除，这也需要输入密码。

### 许可

F-Secure允许用户免费试用程序的所有功能30天。试用期满后，需要支付7.45欧元购买6个月的使用权。

### 总结

F-Secure Mobile Security在我们的测试中表现良好。家长控制功能和简单导航给我们留下了良好的印象。安全浏览器也不错，但是如果也能支持其他浏览器将是一种完善。

## IKARUS mobile.security

IKARUS mobile.security是一款设计整齐的安卓安全智能手机应用程序。它包括诸如杀毒扫描、防盗保护和URL过滤等重要的安全功能。


### 安装

我们从谷歌商店下载并安装了IKARUS mobile.security。安装过程花费的时间相对较长，因为它包含各个组件的配置时间。

首先要接受使用许可协议。然后IKARUS运行更新，紧接着是授权期。用户可以用之前购买的激活码（可扫描二维码）来激活产品，通过谷歌商店进行内部应用程序购买，或选择30天的试用版。或者选择限制功能的免费版本。

然后需要配置保护功能。USSD保护功能最先登场。


对此，需要先确定IKARUS mobile.security为手机呼叫的标准应用程序。接下来是配置的防盗组件，用户可以打开或关闭防盗功能。如果要使用防盗功能，必须为应用程序设置一个设备管理员和锁屏管理员。用户必须确定一个密码，该密码必须至少6个字符，并且至少包含一个字母和一个数字。此后，一个用于防盗保护功能组件的短信命令的简单介绍提供给用户。在安装过程中，已配置好为用户提供上网保护的黑名单和URL过滤器功能。

安装结束后，IKARUS mobile.security建议运行初始恶意软件扫描。

### 启动程序

当程序运行时，主屏幕打开。当前的保护状态显示在屏幕上方，如果一切正常，显示的文字是“您的系统受到保护”。最后执行的恶意软件扫描时间也被显示在本窗口“杀毒”的下方。

### 杀毒

IKARUS允许用户扫描所有已安装的应用程序，或扫描整个系统。可以配置计划扫描，扫描频率可以选择每天两次、每天、每隔一天或每周。还可以显示已发现的任何感染的详细信息。

就像配置扫描频率那样，也可以对更新进行同样的配置，以便自动执行更新。当设备通过WiFi连接到互联网（为了节约流量）时，也可以将更新限制到“次”，或允许使用任何网络连接进行更新。

屏幕的底部有一个复选框，默认情况下已选中，这说明可以匿名向IKARUS实验室发送恶意软件识别数据。

### 监控

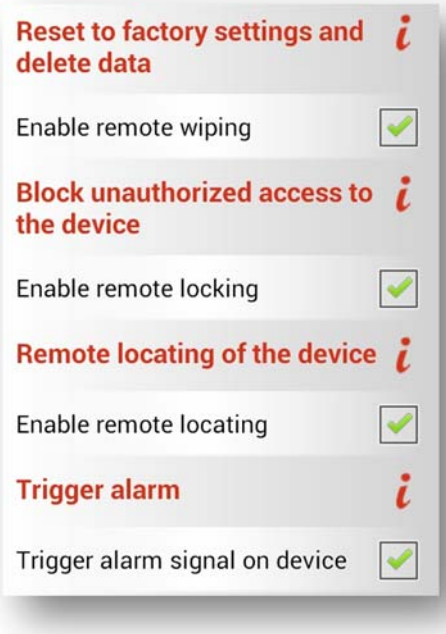
监控是IKARUS mobile.security实时保护功能的技术专用术语，它包括全新的应用程序，用于保护对文件和USSD代码的更改。每一个子功能都可以独立打开和关闭。

### URL过滤器

URL过滤器保护用户上网时避免进入危险网站。IKARUS没有说明所支持的浏览器。在我们的测试中，该保护功能与标准安卓浏览器和谷歌Chrome浏览器配合很好。

amtso.org提供的钓鱼网站测试页未被识别出来。

### 防盗保护




IKARUS列出了所有可用的防盗保护功能，每个都可以被关闭。通过短信来控制各功能，网络界面无法使用。

如果要关闭某个功能组件，必须输入密码。原则上，这样处理比较稳妥，但如果用密码将整个对话框保护起来，而不是要求取消每个复选框，那么操作起来可能更方便实用。

#### *删除*

*短信指令：„wipe:<密码>“*

此命令将删除手机中的所有个人数据，在手机丢失或被盗的情况下，可以防止被第三方访问。该功能是通过将手机重置到出厂设置来实现的。遗憾的是，测试此功能时，IKARUS mobile.security 未能删除外部SD卡中的数据。所以，IKARUS 绝对应该纠正这一失误。

#### *锁定*

*短信指令：“lock:<密码>“*

只要收到该命令，手机就会被锁屏锁定，并且发令人会收到一个确认短信回复。锁屏是安全的，且无法绕过去，但仍然可以拨打紧急电话，这一点是最佳的。如果解锁手机，也要发送一条短信。

#### *定位*

*短信指令：“locate:<密码>“*

当手机被成功定位后，发令人会收到一条短信回复，内容包含指向谷歌地图上的相应坐标的链接。

#### *报警*

*短信指令：“alarm:<密码>“*

此命令的工作原理与“锁定”相同，只是会发出响亮的汽笛声。即使手机的铃声已设置为振动，也会播放声音。

#### *SIM卡监控*

如果手机被盗并换上不同的SIM卡，该设备将被锁定，小偷将无法访问被盗手机中的数据。输入正确的密码可以为手机解锁。

### 消息黑名单

消息黑名单防止收到来自不受欢迎的发信人的短信消息。用户界面非常简单，并且只允许添加或删除电话号码。电话号码可以直接输入，或从通讯录和“最新消息”列表中导入。

我们比较喜欢它的自动应答功能，当消息被阻止后，发令人会受到一条定制的消息。

### 信息

该功能提供产品的版本信息。以及用于联系IKARUS的电子邮件地址和电话号码，还有一个可以向技术支持人员发送系统日志的功能。

### 重新启动安装程序

该功能要求输入密码。并重置初始安装时所做的设置，用户需要重新走一遍初始安装时所走的路。

### 帮助与支持

配置设备时，IKARUS提供简短但内容丰富的信息框来协助用户。然而，IKARUS网站包含许多其他产品手册，我们无法找到 IKARUS mobile.security 的产品手册。约有20个常见问题，然而内容相当肤浅。

### 卸载

IKARUS mobile.security提供了一个删除该安全产品的卸载向导。要使用卸载向导必须输入密码。屏幕上显示一个简洁的对话框，然后程序被迅速删除。

如果使用安卓应用程序管理器，删除程序则无需密码。我们认为这是一个严重的安全隐患，因为小偷可能很容易地利用此疏漏并彻底关闭防盗保护。

### 许可

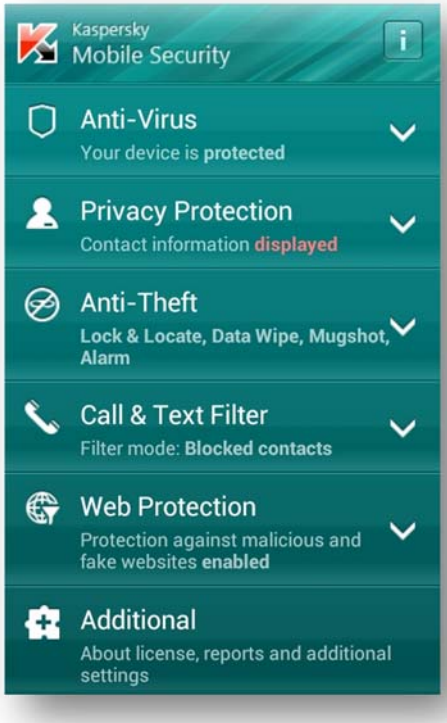
IKARUS为用户提供30天的免费试用版mobile.security产品。试用期满后，如果用户想继续使用该产品，可以从谷歌商店花19.95欧元购买一套永久版的IKARUS mobile.security，或从IKARUS官网不花钱下载一年使用期的产品。

### 总结

IKARUS mobile.security 具有移动安全产品的所有重要功能。甚至包括USSD保护和URL过滤器功能。用户界面整洁易用。然而“删除”和“卸载保护”功能有待完善。

## Kaspersky（卡巴斯基） Mobile Security

Kaspersky Mobile Security 是一款功能全面的安全应用程序。除了病毒扫描、实时病毒监控、防盗和通话/短信过滤功能外，还包括反钓鱼和隐私保护功能。




### 安装

卡巴斯基为我们提供了完整版本的APK文件和许可密钥，来运行安装程序，启动配置向导。首先，用户必须选择所在国家，并接受使用许可协议。然后，为了启用防盗功能组件，应用程序设定了系统管理员。之后，需要创建一个卡巴斯基帐户，只需提供一个电子邮件地址和密码，密码必须至少8个字符，且包含大小写字母和数字。最后，向导建议运行扫描。扫描后用户被带到应用程序启动屏幕，在此可以访问各个功能组件。

### 启动程序

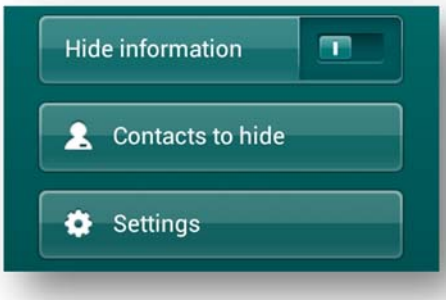
当程序启动时，出现一个精心设计的屏幕主页，在主页中，所有的功能以下拉菜单形式排列。首先映入眼帘的，是一则红色的警告信息。它告诉我们说，一个联系人都没隐藏。我们感觉这一警报多余，因为多数用户没必要隐藏所有联系人，也不隐含直接的安全风险。好在据卡巴斯基自己说，未来的版本将可以隐藏该警报。

### 防病毒

防病毒组件可以扫描手机是否感染恶意软件。用户可以手动启动扫描，或设置自动扫描的时间和频率。此外，卡巴斯基监控新应用程序的安装，如果需要的话，还可以监控文件操作。


可以设置手动扫描，以扫描整个设备、仅应用程序、或仅扫描选定的文件夹。用户可以决定是否使用*卡巴斯基安全网络*（基于云的恶意软件检测）来扫描应用程序安装。

### 隐私保护

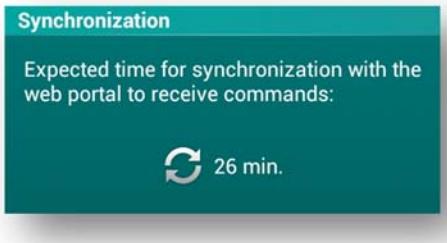



隐私保护可以隐藏与选定联系人的通讯记录。选定联系人的电话号码可以手动输入或从通讯录中导入。可以隐藏的项目包括联系人详细信息、短信记录、收到的短信和通话记录。

### 防盗

防盗功能组件防止未经授权的访问。如果手机丢失或被盗，可以协助您找回。该功

能可以通过Web界面或短信操控（卡巴斯基解释说，如果用户的设备没有网络连接时可以使用短信）。我们注意到，通过网络界面发送命令不会立即生效，只有经过同步后才开始执行命令，但每30分钟才同步一次：




我们觉得执行防盗指令时，这种延误是不能接受的。卡巴斯基告诉我们，这种失误预计很快会被纠正。

防盗功能的各项子功能如下：

### *锁定和定位*

***短信指令：“find:<密码>“***

这一命令可以锁定设备，然后确定其位置。用户首先会接到确认短信，告知设备已被成功锁定；然后会收到带有手机当前位置的通知短信，手机的位置用经度和纬度坐标的形式显示。我们认为，这种形式的位置信息很不实际，因为这些经纬度值必须手动输入到网络地图中。链接直接指向地图上的位置会更好些。

我们欣喜地注意到，可以编辑显示在锁定屏幕上的消息。锁屏本身也非常安全，无法绕过去。并且总是可以拨打紧急电话。

### *报警*

***短信指令：„alarm:<密码>“***

此命令可以锁定手机，并发出警报声。由于屏幕也同时被锁定，所以无法关闭警报声，这可能会坏了小贼的好事。

### 面部照片

该命令只能从Web界面启动。该功能可以锁定被盗的设备并使用前置的摄像头拍下小偷的面部照片，照片可以在Web界面中查看。

### *隐藏*

***短信指令：„hide:<密码>“***

发送该命令将开启隐私保护组件，从而可以隐藏通讯录中的所有联系人。

### *删除*

***短信指令：wipe:<密码>***

该命令可以删除手机中所有个人数据，但不重置设备到出厂设置。它的优点是，防盗保护功能仍然保留在手机中且处于开启状态。在测试过程中，浏览器记录、书签和短信记录都未被删除。外部SD卡上的数据被删除，但使用免费的恢复程序可以恢复已删除的数据。卡巴斯基承诺在未来的版本中改进。

### *全部重置*

***短信指令：fullreset:<密码>***

此命令会删除外部SD卡上的数据，然后将设备重置为出厂设置。虽然顺利完成，但仍有可能恢复SD卡的数据。

### 呼叫及短信过滤

该组件允许建立黑名单和白名单，然而，在同一时间只能开启一项。除了通讯录中的个别联系人外，可以对通讯录中的联系人使用任何阻止功能。还有一个过滤功能，它能过滤掉那些电话号码中包括非数字字符的短信发送号码。我们发现通话和短信过滤器功能进行了逻辑化的设计。

### Web安全保护

此功能仅适用于默认的安卓浏览器，不适用于任何其他浏览器。它提供一种文本反网络钓鱼功能组件，用它可以阻止带有钓鱼网站链接的短信。在测试过程中，这种特殊的功能未发挥作用，所用的带有钓鱼链接的短信未被阻止。然而，一旦点击链接，钓鱼网址即被卡巴斯基的Web保护功能识别并阻止。


### 帮助

卡巴斯基为用户提供全面的本地帮助服务。点击应用程序中任何对话框内的信息符号，都能打开相关的帮助页面。安装完成后，每个菜单中都有提示，这种提示非常有用。

### 卸载

使用向导可以卸载应用程序。卸载要求输入密码。当用户试图删除管理员权限，尝试手动卸载应用程序时，屏幕会被锁定。这样能防止小偷关闭防盗保护功能。

### 许可

卡巴斯基Mobile Security需要付费购买许可，10.95欧元可以使用一年。根据卡巴斯基官方网站介绍，没有试用版，卡巴斯基提供精简版的手机安全软件，可从谷歌商店下载，但其组件“有功能限制”。这种版本可以随时升级到完整版本。然而，预计许可模式不久将会发生变化。

### 总结

卡巴斯基手机安全软件提供了许多明智和成熟的功能。厂商还考虑了程序的人体工程学设计，并创建了一个直观的用户界面。

但是，产品还是存在问题。外部SD卡的数据被删除后，仍然可能恢复；从Web界面发送防盗保护命令后，执行时间延迟了差不多30分钟。

## 金山手机毒霸

金山手机毒霸是一款设计简洁的免费安全产品。它为用户提供病毒扫描、垃圾短信拦截以及其他几种非常有用的功能。


### 安装

我们毫不费力地从谷歌商店下载并安装了金山手机毒霸。最终用户使用许可已被勾选为“已阅读同意”状态。在此过程中，金山手机毒霸已提醒说有些功能需要root权限。

### 程序启动

主界面被分成上下两部分。界面下部用户只能看到“一键查杀”和“广告隐私管理”。但向右滑动屏幕后，就可以进入主菜单。

### 手机体检

启动程序后，用户可以看到窗口中部环形显示的手机体检结果。

### 杀毒扫描

首次运行金山手机毒霸将会执行深度查杀。当手机没有有效的网络连接时，金山手机毒霸建议您连接到网络以执行云扫描。

除了“一键查杀”外，病毒扫描模块不提供任何其他扫描选项。触击屏幕右上角的SD卡图标，任何人都能轻松完成SD卡扫描。

广告行为监测报告说，免费的Sudoku（数独）应用和Amazing Alex含广告插件和消耗手机流量。这两款应用还被报告可能危及隐私。如果用户同意root权限，金山手机毒霸能够修复该问题。如果不接受root权限，用户只能使用卸载按钮。

测试过程中，未给金山手机毒霸root权限，点击优化按钮后竟然取得了100分。关闭扫描选项卡，测试人员又立即重新扫描，虽然体检结果仍然是100分，但应用程序却说上述“广告行为管理“中的两个应用程序需关注。

### 系统漏洞

金山手机毒霸检测到安卓操作系统的3个漏洞，推荐立即修复：

短信欺诈漏洞
远程擦除漏洞
账号诈骗漏洞


### 广告行为管理

该功能能够报告含有广告插件的应用，也报告那些含有窃取个人隐私信息的授权应用。

在“广告”项下安装的具有广告管理有关权限的应用如“弹通知栏广告”等全部一一列示。在另一个“隐私”项下，有诸如

“访问短信记录”或“访问通话记录”等具有权限的应用。


### 应用监控日志

软件行为监控检查安装的应用、广告行为和隐私行为，并监控有潜在恶意行为的网址。根据内置的程序介绍，“恶意行为监控”能够保护手机QQ、微信、米聊、腾讯微博、新浪微博、QQ空间和安卓浏览器。

在菜单中的软件设置项，用户可以通过WIFI配置更新以及“报告毒霸使用情况”。

### 骚扰拦截

金山手机毒霸可以过滤垃圾短信或恼人的陌生来电。由于垃圾短信和不请自来的推销电话一直困扰着中国的广大手机用户。这种功能一直以来很受用户青睐，而且用户都希望参与到如举报垃圾短信和不受欢迎的推销电话的号码这一行动中来。

测试过程中，金山手机毒霸已经拦截了陌生的来电如臭名昭著的“响一声”。这种呼叫就是主叫方呼叫一声后立即挂断。很多被叫方都能在手机上看到显示有未接来电，如果立即回拨对方会播放语音销售信息或诈骗信息。

### 二维码安全扫描

金山手机毒霸有一个内置的“二维码安全扫描”功能。测试过程中，扫描仪能够扫描出大部分二维码。在下面的图片中，金山手机毒霸将香港通讯运营商PCCW的网址netvigator.com判断为“未知网址”。


### 来去电归属地显示

本功能能够显示中国的移动电话号码的地区服务提供商所在地。测试时，来自不同省市的各种号码都被正确的识别出来。

### 广告扫描

金山手机毒霸在自身的应用中提供“广告行为管理”模块。测试时，免费的“Sudoku（数独）”应用被看作是有威胁应用。这一发现与杀毒扫描功能的结果相悖，甚至在随后进行的全盘扫描的结论也是“非常安全”。用户可以通过一键点击来卸载“风险广告”，未提供其他选项。

### 卸载

没有卸载指南。默认情况下，卸载金山手机毒霸无需密码。

### 授权

金山手机毒霸是免费的移动安全产品。

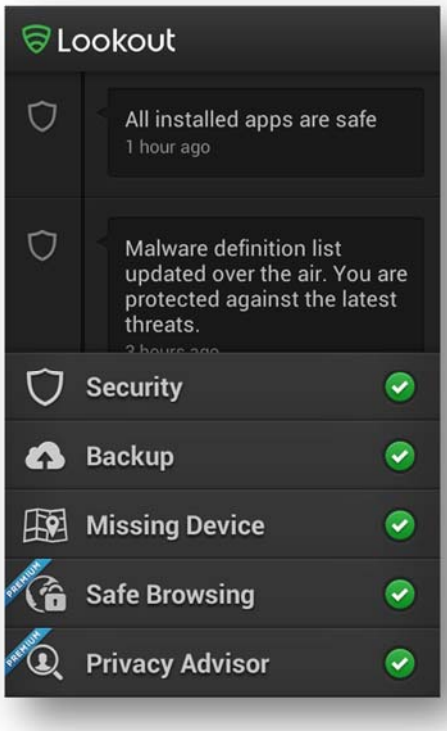
### 结论

金山手机毒霸是一款易用，并提供很多有用功能的免费产品。然而，它不具备防盗功能。

再有，如果安全程序的任何模块检测到的威胁都在杀毒项下和手机体检项下有显示应该会更好。

## Lookout PREMIUM

Lookout 付费版为用户提供了诸如防病毒、反垃圾短信、上网保护和防盗保护等现代的安全防护功能。备份让产品功能更圆满。




### 安装

我们从谷歌商店下载并安装了Lookout付费版。安装完成后，用户可以免费试用两周Lookout的高级功能。试用期满后，可以购买许可，否则程序将自动降级到免费版本。

对于程序的功能范围有一个简要的指南。之后，用户需要创建一个Lookout帐户（或使用现有账户登录）。随后产品就配置好了。用户可以决定是否开启隐私保护、备份和安全浏览功能，程序建议开启所有功能。完成这一步后，设置就完成了。

### 启动程序

当程序启动时，设计清晰的主屏幕打开了。上半部分显示活动日志，下半部分提供程序功能使用接口。立即执行了一次恶意软件扫描，其他所有显示绿勾标记（对号）的功能，表明一切正常

### 安全

Lookout的安全组件用于保护用户抵御恶意软件。在此菜单下，有一个启动扫描的按钮和记录了之前操作的日志。屏幕顶端的一则信息表明实时保护功能已开启。

在“设置”中，可以配置自动扫描。可以按每天或每周设置扫描间隔，也可以设置优先扫描时间。按需扫描只扫描已安装的应用程序，而不是所有文件。Lookout告诉我们，实时保护可以监控设备上所有文件的更改，因此，为了省电，扫描仅限于已安装的应用程序。

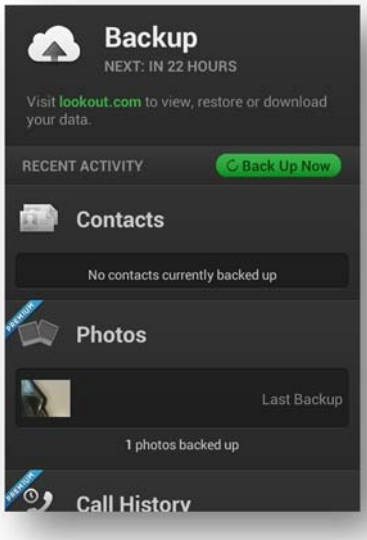
### 备份

备份功能将联系人、图片和通话记录都保存到Lookout服务器，据此，图片和通话记录也只能通过付费版保存。第一次备份后，数据可通过Web界面查看并下载。[8]

可以每天或每周自动运行备份。虽然功能的出发点很好，也合情合理，但我们还是发现了问题：不能选择用于备份的网络连接类型（例如WiFi）照了许多照片的人会产生大量的数据流量，费用可能相当可观，尤其是假如用户正在国外旅游。

不过值得一提的是，备份可以通过Web界面执行。如果用户的手机丢失或被盗，至少可以保存自己的数据。

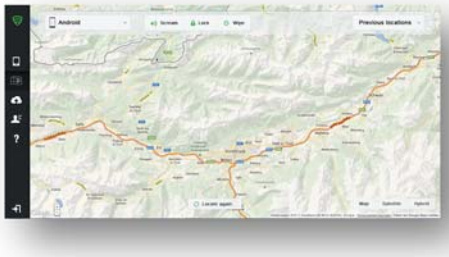
[8] http://lookout.com




应该引起注意的是，仅手机上保存的联系人得到备份。并未备份谷歌帐户中的联系人或SIM卡上保存的联系人。Lookout未使用户意识到这一点。

### 丢失设备保护

这是Lookout的防盗保护功能组件。它通过Web界面控制，没有短信命令。同名的菜单显示出一个带有设备当前位置的地图。用户籍此可轻松的测试定位功能。



在菜单的下面，有一个“开启更好的保护”按钮。点击该按钮，用户可以为Lookout确定一个设备管理员。在设置菜单，可以取消更改。

屏幕底部，有简要的防盗保护功能介绍。

#### *警报*

此功能可以从菜单直接测试，当然，也可从Web界面正常运行。该功能会引发嘹亮的警笛声，并且红蓝警灯交替闪烁。由于不是安全功能，所以手机并未被锁定，但可以用于查找忘记放在哪里的手机。

#### *定位*

如果手机丢失或被盗，可通过此命令找回。用户只需登录到Web界面，就能够迅速找到手机所在的位置，并显示在谷歌地图上。

#### *信号弹*

信号弹是电池耗尽前，查找手机的一项非常巧妙的功能。可以在Web界面中发现手机的位置。

### Lockcam

设备被锁定后，会用到Lockcam。如果密码错误三次，Lookout的前置摄像头会拍下使用者的头像，并将照片通过电子邮件发送给机主。

#### *锁定*

该功能允许用户远程锁定自己丢失或被盗的手机，以预防未经授权的操作。此功能只在付费版可用。要锁定设备，用户登录到web界面，点击“Lock”；在此可以定义手机解锁密码。可以显示一条消息，甚至可以显示联系人的详细信息，以供善意拾到手机的人使用。

锁定的屏幕无法绕过去，但可以拨打紧急电话。

#### *删除*

此功能仅供付费用户使用。如果删除命令发出，设备将被重置为出厂设置。如果程序具有设备管理员权限，Lookout（如同所有的安卓应用程序）只能删除外部SD卡中的数据。我们发现，在安装过程中或在程序启动时，程序都不提示用户分配管理员权限。

在测试过程中，Lookout删除了SD卡中的所有数据，然而，使用普通的免费工具可以恢复这些数据。

### 安全浏览

付费版安全浏览功能，可以在用户使用默认安卓浏览器和谷歌Chrome上网时提供安全保护。在设置中可以关闭安全浏览功能。也可以看到关于扫描的站点数的统计信息。

### 隐私保护

隐私保护也是一个付费功能，可以发现那些可能对用户的隐私构成威胁的应用程序所有安装的应用都根据各自的访问权限排列。隐私内容包括定位服务、访问联系人或短信。点击组，显示所有具有相关权限的应用程序。点击其中一项应用程序，显示所有其他权限和详细信息。

### 帮助

Lookout提供了一个全面的在线常见问题服务，要使用此服务当然必须有有效的网络连接。

### 卸载

没有提供卸载向导。如果应用程序已经设定设备管理员，Lookout建议，删除产品前必须关闭。卸载应用程序不需要密码，这会使小偷轻易绕过防盗保护。

### 许可

Lookout提供削减了功能的免费版本。每月支付2.26欧元或一年22.66欧元可以购买付费版，包括安全浏览、隐私保护、删除、锁定、恢复数据到新设备上，再加上通话记录和照片备份功能。

### 总结

Lookout提供成熟的安全产品，他因提供如Lockcam和全面的备份功能而更显出众。其他的保护功能也让我们难忘。但是，还有一些改进的空间，如为用户提供整个SD卡的按需扫描或添加卸载保护等。

## 360手机卫士

360手机卫士是一款具有广泛功能的免费移动安全解决方案，并且可以添加更多功能。自从首次对360进行测试后，360手机卫士已经又有了进一步的完善。


厂商已经发布了英文版的移动安全产品，据厂商自己的介绍，英文版产品与中文版不同。

### 安装

安装文件从谷歌商店下载并安装。也可以从厂商的官网直接下载。

### 程序启动

首次启动程序后，用户使用许可已被告知“继续使用即代表您已阅读并同意…（包括同意360申请root权限）”

### 手机体检

手机体检出现在程序首页的主要位置。它能扫描可能消耗资源的设备的应用。该功能还能检测出文件系统中的垃圾文件。


### 手机杀毒

滑动手机杀毒按钮进入病毒查杀菜单。360手机卫士提供全盘扫描或快速扫描。点击“手机杀毒”界面右上角的“设置”可以开启或关闭：自动更新病毒库、自动联网云查杀和安装监控。

### 防盗

默认情况下，该组件已处于开启状态，用户需要输入一个6-12位数的密码，和一个当SIM卡被更换后，用于接受通知的可信任的电话号码。

要使用防盗功能，360手机卫士用户必须发送短信到丢失或被盗的手机。

大多数安全软件厂商，不论界面使用何种语言，都是用英文短信命令。而360手机卫士使用的是用拉丁字母组成的汉语拼音命令：定位（weizhi位置），报警（jingbao警报），锁定（suoding锁定），防盗（fangdao）删除（shanchu 删除）。

#### *防盗*

**短信命令：“fangdao#密码”**

该命令发出后，可以定位和锁定失窃的手机，同时响起防空警报样的刺耳响声。

SIM卡监控

通过该功能可以向用户指定的信任号码发送一则短信，通知您SIM卡已被更换。短信内容可以在设置过程中定义。

#### *定位*

**短信命令：“weizhi#密码”**

该命令可以定位手机。发送该命令的手机随后会收到一则带有位置信息的短信，并配有360地图服务提供的已标注了手机具体位置的信息。

### *警报*

**短信命令：“jingbao#密码”**

使用该命令，手机会发出刺耳的防空警报声，但手机并未被锁定。警报声一直会持续几分钟。

### *锁定*

**短信命令“suoding#密码”**

该功能可以锁定手机防止未经授权的访问。然后，只需输入正确的密码即可解除锁定。如果两次输错密码，应用程序会照下嫌疑人的头像，照片会被发送到fd.shouji.360.cn，且在开启防盗保护功能时，所配置的信任联系人手机会收到一个可以查看该照片的链接。

### *删除*

**短信命令：“shanchu#密码”**

该功能本来是用于删除隐私，包括短信记录、通讯录、通话记录、和所有个人文件。设备未被重置到出厂设置，也就是说防盗保护功能可以继续发挥作用。测试此项功能时，手机中保存的通讯录和短信记录都被完全删除。但通话记录仍然保留完好，可是360手机卫士却通过短信亲自确认删除成功。此外，手机中保存的照片和SD卡中的图片都已删除。

谷歌账户原封未动。虽然应用程序的文本未要求删除谷歌账户，但我们认为还是有必要删除谷歌账户。

### *密码*

**“短信命令：“mima#（自选并）注册的电话号码”**

使用该命令可以更改安全密码。

### 隐私保护

360手机卫士提供多种方式来保护手机用户的隐私。

### 密码保护

用户可以为360手机卫士程序设定密码，如果未输入密码，都无法打开保护程序。

隐私空间

使用隐私保镖功能，用户可以为与具体电话号码的短信记录，选定的照片、视频和其他文件设定特殊保护。基本的保护诸如应用程序密码保护（程序锁）和隐藏指定号码的短信记录等都无一例外的具备。如果要保护照片、视频、音频和其他文件，必须安装附加程序。当卸载此应用后，加密的照片、视频等都将被删除。用户也会收到适当的通知。

隐私保护密码是一种默认的手势。这种密码可以切换到一种由1到12个字符组成的文本密码。我们尝试设置简单的“1”作为保护密码，居然被接受了。

如果用户添加如某些照片到隐私保险箱中，那么这些照片只能在保险箱的私人相册中看到，通过常规的图片库无法看到。该功能需要安装360保险箱。

在“密码本”中，用户可以备忘自己的用户名和各种上网服务密码。要使用“密码本”功能，需要用至少6位数字或字母配置不同的密码。

### 骚扰电话和垃圾短信

360手机卫士已集成了防止用户被骚扰电话和垃圾短信打扰的功能，即常用的黑名单和白名单。用户可以向360举报垃圾短信和呼入的电话号码。如果有未知的电话号码第一次呼入，用户可以将该号码标记为“广告推销”或“快递服务”，这样可以为所有360用户提高对来电号码的准确识别率。

测试期间，大多数接收到的垃圾短信和呼入电话被正确归类。


## 省电管理

360省电王也是一个需要单独安装的附加应用。该功能是为了让用户来控制手机的电量消耗。

## 软件管理

360手机卫士还可以管理软件更新和软件卸载和安装包等。还可以将应用从内部存储搬家到SD卡或反之亦然，有详细的系统概述。

## 通讯录备份

使用该功能可以备份并存储通讯录、所有短信（包括受密码保护的）以及360手机卫士设置。用户必须注册一个账户或使用已有账户才能备份。用户名就是手机号码。备份日志可以恢复或删除。备份数据可以保存在SD卡中。

## 数据流量管理

360手机卫士的流量管理可以显示每天或每月的数据流量。此外，可以输入签约移动服务商提供的月度数据流量限额，已用的流量在通知菜单显示。通过发送短信给中国移动服务提供商，可以查询已用的流量。短信发送间隔时间可以配置。每月流量限额可以手工输入。


## 安全二维码

360手机卫士提供安全二维码扫描，程序自称可以扫描出URL是否是恶意网址。

应用工具

在此菜单项下，360手机卫士提供诸如文件管理和系统测试等功能。

也可以直接检查手机号码所属的地区服务提供商。测试时，使用的不同省份的号码都被正确识别出来。

在旅游旺季，中国的火车票仍然很难获得，360手机卫士现在还能帮用户买火车票。

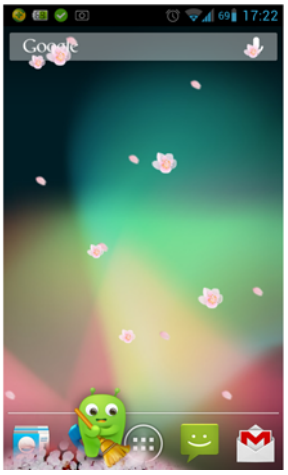
菜单最后一项有益于中国用户的功能是，可以查询预订飞机票、预订酒店的电话号码，以及银行、保险公司和电话服务商的特服号码。

## 360优化大师

360优化大师是另外一项需要单独安装的附加应用。使用人性化设计的“一键优化”，可以轻松完成“内存清理、垃圾文件清理”，隐私痕迹清理如浏览器使用记录、Gmail搜索记录，剪贴板使用记录可以单独或与其他各项一起处理。

### 安卓小机器人

测试期间，一个绿色的安卓小卡通人一直驻留在测试使用的手机屏幕上。这个小卡通人时不时的变成红色，并强烈建议进行系统清理。因为根据它的经验，太多的资源被占用。拖拽红脸的小人到屏幕的低端，让它拿着扫帚使劲儿地清扫，同时屏幕上开始撒下花雨。过了一会儿，程序报告说进程结束，一定数量的内存已释放。可以一遍又一遍地重复此操作，总是有内存被释放。但最新版的360手机卫士对此已改进。




### 卸载

没有卸载指南。默认情况下，卸载360手机卫士不需要密码。这对于防盗组件来讲，可能会产生问题。因为偷盗手机者可能会先卸载手机保护程序。最新版本中可以设置卸载密码。

### 授权

360手机卫士是免费产品。

### 结论

360手机卫士又新增了不少功能。有些需要单独安装。除了安全组件外，它还提供优化工具和国内日常生活帮助。目前360手机卫士还在程序中加入了有趣儿的元素，如内置的游戏以及还可以自行拍摄照片设为呼叫方的显示状态，当其他手机中也安装了360手机卫士的用户呼叫您时，该图片会显示给对方。

除了通话记录外，远程擦除功能删除了所有的程序自己声称的将要删除的隐私信息。另外，该功能对谷歌账户视若无睹。

360手机卫士提供许多清理和优化功能，但某些功能可以不断地重复操作，且始终声称可以源源不断地释放内

## Quick Heal Total Security

Quick Heal Total Security 是一款拥有广泛功能的配套产品。除了传统的防盗保护功能外，软件还提供诸如网络监控和备份功能。这些功能给我们留下了深刻的印象。

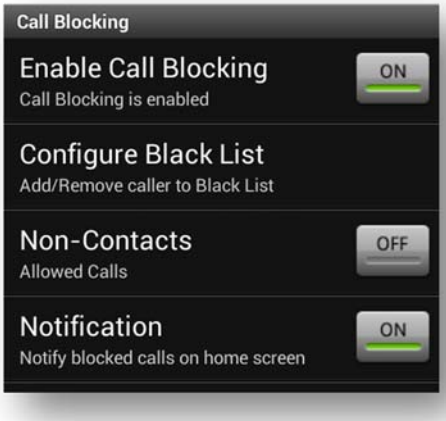

### 安装

我们从厂商的官网下载并安装了Quick Heal Total Security。接受使用许可协议后，用户需激活产品。通过输入已有的激活码，或输入新购的激活码，就可以激活产品；也可以选择有时间限制的产品免费试用。

然后防盗保护组件就配置完毕。密码必须是6到20个字符。需要注册两个问题的答案，以供忘记密码需要重设时使用；当然，用户应该选择只有自己知道答案的问题。随后，还要输入一个受信任的电话号码，如果SIM卡被更换，用于接收通知。我们高兴的看到，可以关闭卸载保护。

### 呼叫限制

此功能防止用户被不受欢迎的呼叫打扰。此功能采用黑名单工作原理。被加入黑名单的电话号码将被限制呼叫。用户也可以选择阻止所有不在通讯录上的电话号码。




如果呼叫被阻止，用户可以选择是否被通知。总的来说，该功能非常简单且容易配置，测试时，表现非常好。

### 短信过滤

短信过滤可以阻止垃圾短信，类似于呼叫限制。但是，此功能的配置选项更全面。事实上，我们都被第一个选项搞糊涂了。可以开启“短信扫描”，但是如何扫描却没有进一步的说明。我们猜测可能是通过扫描短信中的恶意链接进行过滤。然而，测试时，我们无法触发这一过滤机制。

Quick Heal 还提供第二种保护机制，就是对垃圾短信过滤。它可以阻止来自组联系人（群发）、非联系人和带有非数字号码文字发送人的短信。此外，还可以创建黑名单和白名单，以及单独添加的短信发送号码。还有一个黑名单关键字列表-任何含有这些关键字的短信都将被阻止。总体而言，我们认为短信过滤功能发挥了其所应发挥的作用，但缺少最简单的呼叫限制配置方法。

### 防盗

要配置该功能，需输入安装过程中设置的密码。那么，用户就可以进行广泛的配置选择。下面介绍的各种防盗功能都通过短信指令控制，没有Web界面。

### *定位*

***短信指令：“TRACE〈密码〉”***

收到指令后，发令人会收到一则带有指向Quick Heal网站链接的回复短信，链接中可以查看谷歌地图服务提供的位置图。图中显示了该设备的位置。

### *锁定*

***短信指令：“BLOCK〈密码〉”***

收到此命令的手机，会被设计精致的屏幕锁锁定。屏幕上可以显示由用户事先编辑好的消息。锁定的屏幕非常安全，并且无法绕过去，但允许进行紧急呼叫，也可以被受信任的电话呼叫（在安装过程中指定的电话号码）。

### *SIM卡锁定*

如果SIM卡被更换，使用该指令可以锁定设备。可以打开或关闭此功能。SIM卡如果被更换，用户可以决定是否发送短信通知到受信任的手机。我们很高兴地看到，可以将多个SIM卡注册为受信任的SIM卡，所以，使用多个SIM卡的用户可以随意更换而不必浪费更多时间。

### *删除*

***短信指令：“WIPE〈密码〉”***

此功能可以删除智能手机中的个人数据，防止未经授权的访问。设备未被重置到出厂设置，优点就是防盗功能仍然在并能发挥作用。测试时，Quick Heal未能删除浏览器记录或书签。使用免费工具可以恢复外部SD卡上的数据。厂商告诉我们，其最新的产品版本含有安全删除方法，可以防止删除的数据被恢复。

### 病毒防护

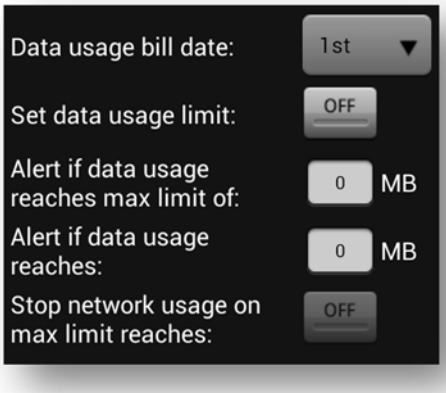
此功能可以为设备进行恶意软件扫描。如果检测到恶意软件，可以配置采取默认的操作，可以选择：修复、删除或跳过。这种配置同样适用于实时保护功能。如果发生误报，用户可以自行定义应用或文件是安全的。

### 性能监控

性能监控可以显示当前使用的资源，如电池的剩余使用时间、CPU使用率和内存使用情况。已安装的应用程序及其所占用的内存也被显示。美中不足的是，该列表只能按字母顺序排列，如果要找到耗费资源的应用程序，用户必须一篇一篇的滚动整个列表进行查找。

### 网络监控

网络监控可以测量通过2G、3G和WiFi连接所用的数据流量。用户可以设置每月的流量限额，如果超过流量限额，可以关闭网络连接。还可以进行另一种设置，当流量达到一定量时提醒用户。一个独立的视图，显示了所有已产生流量的的应用程序，以及对应所使用的流量。




### 备份

备份组件可以备份联系人、日历和短信记录。这些都被保存在Quick Heal的服务器中。如果用户丢失手机中的任何数据，只需点击“恢复”按钮就可还原数据。还可以设置自动备份，它可以根据定义的时间间隔备份（可以选择每日或每月）。


备份的数据可以恢复到不同的设备中。如果设备丢失，所有的数据可以传输到新的设备中。

### Web安全保护

Web安全功能组件能防止用户误入钓鱼站点和推送恶意软件的网站。Quick Heal还提供家长控制功能，家长可以通过此功能进行设置，从而阻止儿童进入某些类别的网站。我们注意到，该功能仅支持标准的安卓浏览器，而不支持谷歌Chrome浏览器。可以将受信任的站点添加到白名单中，也就是说，这些站点将永远不会被阻止。默认情况下，更改家长控制功能的设置不需要密码（虽然可以开启密码保护）。

### 帮助

有问题的用户可以使用帮助文件。帮助文件排列清晰，内容易懂。还有一个常见问题解答，但问题数量有限，只有约20个问题。

### 卸载

通过菜单>帮助>停止快捷菜单先关闭许可，然后可以自动卸载该产品。必须输入密码才可卸载，如果通过安卓应用程序管理器也可以卸载。因此，小偷没有机会通过卸载应用程序而绕过防盗保护。

### 许可

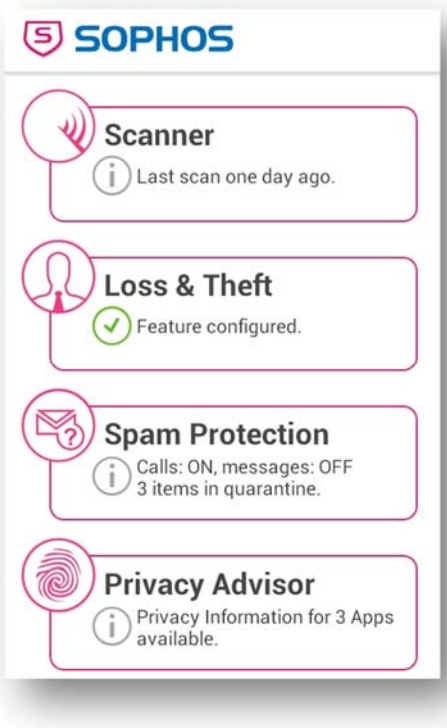
Quick Heal Total Security可以花10.76欧元从谷歌商店购买，使用有效期为一年。用户可以免费试用程序的大部分功能30天。

### 总结

Quick Heal Total Security给人的印象是，一个具备了用户想要使用的所有功能的安全产品。但是，我们确实发现，在界面方面还有不直观的地方，或许是需要 Quick Heal能够完善的。

## Sophos Security and Antivirus

Sophos Security and Antivirus 是一款具有了所有重要功能的现代安全产品，可以免费使用。




### 安装

我们从谷歌商店下载并安装了Sophos Security and Antivirus。安装完成后，用户只需接受使用许可协议，就能显示应用程序的开始页面。运行初始恶意软件扫描。

### 恶意软件扫描

此功能可以为手机进行恶意软件扫描。在设置中，用户可以决定扫描时是否使用云功能；漫游时可以关闭，或设置为，仅在有Wifi连接时使用。当发现恶意软件时，用户可以选择忽略、删除或显示更多信息。也可以开启或关闭“识别可能不受欢迎的应用程序”。此外，计划扫描可设置为每六个小时和每3天执行一次。Sophos还提供实时监控保护功能，它可以实时检查新安装的应用程序和对文件所做的更改。

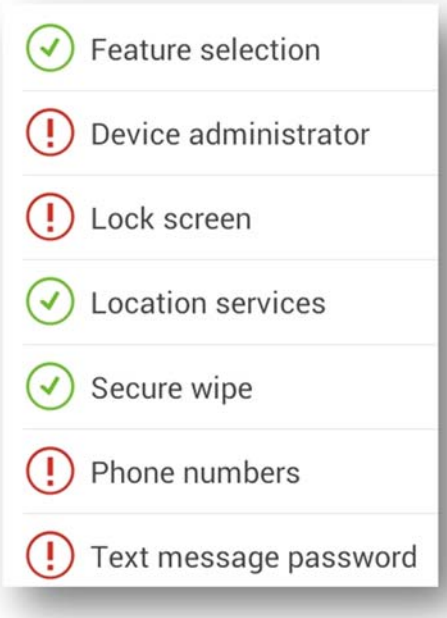
### Web安全保护

设置中有点儿不太好找的功能是Web安全保护功能。此功能可以预防用户上网时避免进入危险网站。警告等级有标准、最高、从不。在我们的测试中，该功能表现非常出色。

### 遗失和防盗保护

如果手机丢失，此功能可以发出警报声、锁定设备、定位、或删除数据。此功能只能通过短信控制，没有Web界面。短信只能从事先已确定的可信任的手机号码发送。发送的指令需包含密码。从其他手机发送的命令，即使包含了正确的密码也无效。

我们比较欣赏防盗功能屏幕上显示的概述，概述中可以一目了然已开启的功能组件，以及仍然需要进行配置的功能组件。



### *锁定*

***短信指令：Lock〈密码〉***

此命令可以锁定当前使用安卓设置的手机。一个带有锁定消息的图标也会出现。锁屏本身非常安全，无法绕过去。当锁定命令执行完毕，发令人会收到一则回复短信。

### *报警*

***短信指令：Alarm〈密码〉***

此命令也可以锁定屏幕，就像“锁定功能”的指令一样。不同的是，此功能将播放报警声，这对小偷来说可是非常倒胃口的事情。

### *定位*

***短信指令：Locate〈密码〉***

收到命令后，设备将尝试使用GPS和WiFi来搜索设备的位置。当定位后，发令人将收到一则回复短信，短信内容包含设备的大体坐标和谷歌地图上的位置链接；随后会收到另一个带有更精确坐标的短信。

### 电量不足提醒

如果开启该功能，电池电量不足手机也会被定位；详细信息将被发送到可信任的手机号码。

### *解锁*

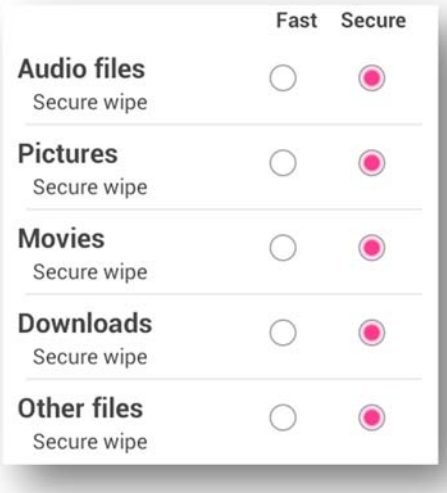
***短信指令：Unlock〈密码〉***

要使用此命令，需要为设备定义一个新的随机选择的密码。发令人会收到一个包含新密码的短信。

### *删除*

***短信指令：Wipe〈密码〉***

此功能使用起来比较麻烦。用户可以为不同类型的文件定义不同的删除类型。除了简单的删除外，文件可以用垃圾文件覆盖（安全删除）。这意味着，这一进程将需要更长的时间。测试过程中，安全擦除功能发挥了预期的作用；使用我们常用的方法无法恢复SD卡上被删除的文件。




### *SIM卡更改*

如果SIM卡被替换，带有IMEI和IMSI码的短信会发送到所有受信任的电话号码。设备也将被安卓屏幕锁锁定。

### 垃圾短信防护

垃圾短信防护功能，可以防止用户被不想要的电话或短信打扰。每个子功能组件即可以完全开启也可以完全关闭，如只用呼叫限制或只用阻止短信。但对于特定的联系人，则无法分开使用，即要么全部阻止呼叫和短信，要么全不阻止。通过一个直观的菜单，可将号码加入到黑、白名单中。如果不小心将一个号码添加到了两个名单中，则白名单使用优先。

还可以选择阻止匿名通话和短信，以及任何未记入通讯录中的号码。

如果开启文本拦截功能，Sophos可以阻止带有恶意URL的短信。测试中，该功能运行良好，但我们注意到，短信拦截功能未开启时，也能阻止带有恶意链接的短信，我们奇怪为何该功能被想象为关闭了。
被阻止的短信可在隔离区中找到，在隔离区，可以查看、恢复或删除这些短信。

### 隐私保护

隐私保护功能显示了可能对用户隐私构成风险的应用程序。Sophos将应用按风险等

级归类（高、中和低），并在列表中用红、黄和白色标注。用户可以根据以下类别进行过滤：吸费应用、访问个人信息或访问互联网。

### 安全指导

安全指导功能使用户意识到手机的任何设置可能导致的安全风险。Sophos检查六种不同设置，如屏幕锁或设备加密是否开启。点击任一条目都会显示其信息，和一个直接进入相应的安卓设置页面的按钮。


### 应用程序保护

这一组件可以使用四个字符的密码完成应用程序的密码保护。设置后，会出现一条警告，提醒用户“使用‘任务管理器’可以绕过‘应用程序保护’”。但Sophos提供了另一形式的解决方案，就是安装Sophos Security and Antivirus Guard可确保安全产品不会被中断。

配置参数*宽限期*可以定义使用应用程序被重新锁定前使用的时长。默认设置是两分钟。

Sophos采用密码保护其自身和安卓配置，该项不可关闭。同一密码还可以保护附加的应用程序。

### 帮助

Sophos以信息框的方式为每一功能组件提供了全面的帮助。信息确实足够丰富，但还是希望看到卸载操作的更多帮助。

### 卸载

没有提供卸载向导。但在安全指导功能中有一条消息说，卸载“安全指导”前，程序必需从设备管理器中删除。一旦此操作完成，应用程序就可以用安卓应用管理器卸载。

无论是删除设备的管理员权限，还是随后删除该程序都不需要密码。但这样的话，小偷可以很容易地解除防盗保护。

### 许可

Sophos Security and Antivirus是免费产品，且对个人使用没有任何限制。

### 总结

Sophos Security & Antivirus 提供了现代安全产品的全部功能，而且免费。该应用程序给人的印象是成熟且考虑全面。我们注意到，Sophos Security & Antivirus的功能与去年测试的版本相比，已经有显著的扩展。

## 腾讯手机管家

腾讯手机管家是一款具有广泛功能和众多可添加附件的免费安全解决方案。与之前的版本相比，给程序已经进行了重要更新。


### 安装和程序启动

安装文件从谷歌商店下载。

首次运行时，腾讯手机管家的许可及服务协议已被接受。安装后，“手机体检”自动执行。手机第一次运行体检得分68分，最多100分。

腾讯手机管家报告说，内存使用了72%，垃圾文件8.9MB. 点击带有体检健康分值的圆圈可以执行优化.

### 健康优化

腾讯手机管家提供各种优化工具,见下图:


### 流量监控

腾讯手机管家可以显示每天和每月的数据流量.每月的流量限制根据用户与签约移动服务商的套餐协议,可以输入,这样当前可用的流量可以以百分比的形式显示出来.如果有可用网络连接,流量数据可以与服务商同步.也可以通过短信校对.

### 空间清理

使用此功能，腾讯手机管家可以扫描手机中的垃圾文件不常用软件、多余安装包、和音视频文件。后两项需要“手动清理”。


### 进程管理

此功能允许用户关闭运行的程序。测试过程中，建议手机关闭29个运行程序。用户不想用的进程可以被挪到一受保护的列表中。

### 电池健康

电池健康是一个需要单独安装的应用。该程序旨在通过控制手机电量的消耗，延长电池的使用时间。包括诸如关闭CPU内核，仅在程序被授予Root权限时访问等功能。

电池的充电周期概况也有显示；目的在于提醒用户及时充电，从而增加电池的使用寿命。

### 安全保护

在此项下，腾讯手机管家列示了所有可用的安全功能，如：

骚扰电话和垃圾短信

腾讯集成了很多功能来防止用户受到陌生电话和短信的骚扰。除了常用的黑名单和白名单功能，软件还允许用户向腾讯举报垃圾短信。测试期间，该功能成功地处理了多条中文垃圾短信。

首次接到未知电话后，可以标注未知的电话号码为推销或快递服务。这样，用户可以帮助增加电话被阻止的精确度。

### 隐私保护

腾讯手机关机提供大量的隐私保护功能，如：

### 隐私空间

要配置此功能，需要定义一个图形密码。该密码可以隐藏来自特定电话号码的短信、照片、视频和其他文件。如果用户添加如照片到隐藏的项目中，那么这些照片只能在带有“隐私保护”工具的相册中看到，常规的图片库则不再可以看到。隐私工具自身也可以隐藏在程序菜单中。

### 软件权限扫描

已安装的应用根据与隐私有关的权限排列。此功能可以找出构成隐私风险的，可能窃取个人信息的应用程序。

### 病毒查杀

点击“病毒查杀”为用户带来的是病毒查杀项。在此版本中，腾讯只提供一个扫描按钮。在本部分的设置项，用户可以选择“智能扫描”、“快速扫描”、和“全面扫描”，以及手动更新病毒库。“快速扫描”不扫描恶意文件。


### 防盗保护

默认情况下，此组件未开启。开启此组件，需要用户配置一个密码和一个可信任的手机号码，该号码用于在SIM卡被更换时接收通知。密码必须16位数字。

防盗保护功能由短信控制。与大多数手机安全产品一样，腾讯手机管家也使用英文短信命令。

删除

短信指令： “#QQDeleteALL#密码”

该命令可以删除手机中的个人数据。手机未被重置到出厂设置，好处就是防盗保护软件还处于开启状态。删除功能删除了内存的联系人、短信和照片。而SD卡中的通话记录和照片原封未动。删除开始和结束都有短信确认。

测试设备中的谷歌账户密码未被删除。这可能会是一个隐患，因为窃贼可能在谷歌商店中购物并产生费用。

锁定

短信指令： “#QQLock#密码”

此功能可以锁定手机，防止未经授权的访问。要想为手机解锁，必须输入之前设置的密码。锁定短信发出后，手机被成功锁定。

测试后，手机被远程锁定，但还是可以访问最近使用过的应用程序。这可能存在隐私风险，因为个人数据可能会被显示。

定位

短信指令： “#QQLocate#密码”

通过发送此命令，用户可以确定遗失手机的位置。机主将收到另外一则回复短信，

短信中含有位置和有关腾讯地图服务提供的相关链接。
恢复密码
短信指令：“#QQPin#注册的紧急联系人号码
此功能可以重置密码。在防盗保护功能注册的手机中发挥良好。

### SIM卡监控

如果SIM卡被更换，该功能会发送短信到注册的紧急号码上。

### 程序管理

程序管理的功能包括：下载软件、更新软件、安装软件和卸载软件。


应用程序可通过腾讯自己的安卓应用商店下载。它允许用户浏览设计精致的商店并安装应用（在安卓设置中必须启用“从外部资源安装”）。

其他功能包括更新和卸载已安装应用。安装文件的管理功能对于安装之前已下载且仍在设备中的APK文件有益。安装文件根据下载来源列示，如从腾讯下载或从“其他来源”下载。

### 其他实用工具：

点击程序界面右上角的四个方块儿，用户可以使用各种实用工具，如扣费扫描。除了使用已安全的工具外，还可以添加诸如截屏工具、或IP电话拨号等功能。多数工具在之前的版本已经熟知。
手机扣费扫描正确识别出三种短信支付的确认短信。

### 腾讯小火箭

安装了腾讯手机管家后，测试设备的屏幕上显示一个小圆环，很明显地显示出腾讯检测出的测试设备已占用的内存数。拖拽这个小圈到屏幕的底部，会发射出一枚腾讯小火箭，射落飞碟，关闭进程并释放内存。

### 卸载

没有卸载向导。默认情况下，卸载产品不需要密码。这可能对防盗组件不利，因为小偷可能卸载该保护。

### 许可

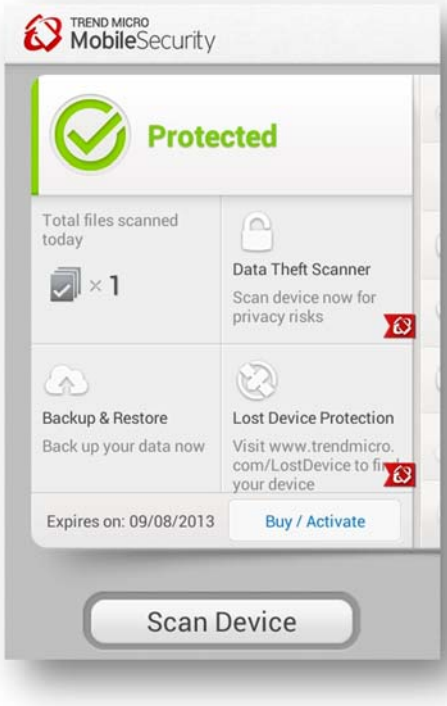
腾讯手机管家免费。

### 结论

腾讯手机管家已经对产品进行了升级，使一些关键功能更容易访问。我们比较喜欢其产品功能的广泛性。
然而，防盗保护功能需要一些巩固，尤其是删除功能，它无法删除SD卡上的照片和谷歌账户密码。锁定功能也需要一些改进。

## Trend Micro Mobile Security

Trend Micro Mobile Security 提供诸如防盗保护和防病毒等重要的功能，同时还有安全上网和家长控制功能。




### 安装

我们从谷歌商店下载并安装了Trend Micro Mobile Security。接受使用许可协议后，启动屏幕就立即出现。

### 启动程序

显示给用户的是一个简短的程序介绍和程序界面，如向右滑动屏幕可以打开扩展功能的控制。出现的消息框提示用户应注册一个Trend Micro账号，或使用已有账号登录。

在开始屏幕上出现的是恶意软件扫描、数据防盗扫描、备份和防盗按钮。静态的“扫描设备”按钮非常醒目，因为它一直显示在主屏幕下方。

### 病毒扫描程序

点击”病毒扫描“按钮，会打开适当的页面。还有一个立即扫描设备按钮，加上一个各种配置选项，如是否使用云扫描或扫描SD卡。可以立即和/或自动执行更新。后者的时间间隔可以设置为每天、每周或每月。也可以将应用程序设置为，只有设备通过WiFi连接到网络时才更新。作为一种选择，每次更新后可以运行扫描。日志中记录了扫描和更新事件。

### 数据防盗

此功能可以检查设备中安装的可能与盗窃隐私数据有关的应用程序。Trend Micro还为此功能提供实时扫描，它可以检查新安装的应用程序是否对隐私信息构成威胁。

此功能在其操作中表现并不积极主动。如脸谱（Facebook）应用程序，由于其中的很多权限对隐私信息构成极大的风险，但并未被报告出来。

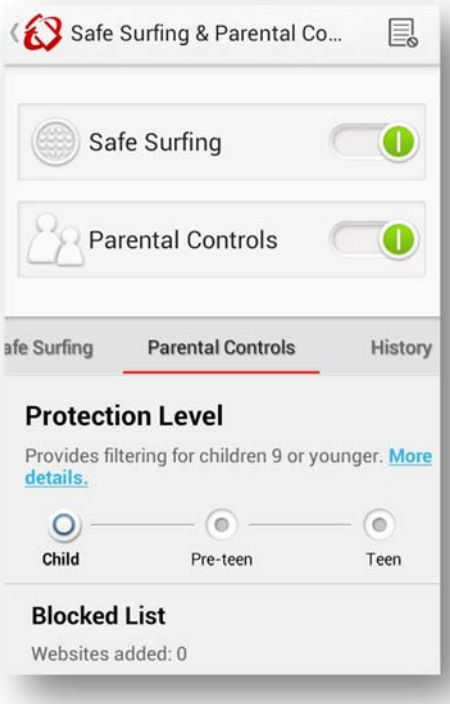
### 安全上网和家长控制

此功能合并了两项与网络有关的保护功能。安全上网可以为用户上网时提供安全保障，在此，可以选择高、中或低安全等级。如果设置高安全等级，那么稍微可能有点儿风险的网站就会被阻止，而设置低安全等级，又会有漏网的，且忽视了对未成年人存在的威胁。

家长控制功能需要设置一个至少8个字符的密码。然后，就可以为孩子们设置一个适当的上网保护了。这可以根据不同年龄段的孩子进行设置，可以分别通过黑名单或白名单来阻止或允许具体的网站。

卸载保护可以防止儿童或青少年卸载应用程序。我们认为，卸载保护不应仅仅限于防止孩子使用，如果对全局性的卸载进行限制可能更合理。

测试该功能时，表现不够充分。虽然设备管理员功能被删除后电话被阻止，但当设备重新启动后，约60秒左右又可以完全访问。此时，无需密码就可以轻松卸载应用。对此，Trend Micro说，在下一版本中将被完善。




“安全上网和家长控制功能”中的日志记录了所有被阻止的网站；包括被定义为危险的网站和不适合儿童的网站。

### 呼叫和短信限制

该功能可以阻止不必要的电话和短信。可以拦截电话和短信，并可以分别配置。对于每种通信类型，可以设置使用黑名单或白名单，以及对于被拦截的项目可以采取的操作。例如，如果拦截的是短信，可以定义为自动回复。

对于短信拦截，可以创建一个关键字列表；任何含有这些词语的短信都将被拦截。

“呼叫和短信限制”功能也有日志记录，从日志中可以查看被阻止的呼叫和短信。

### 设备丢失保护

设备丢失保护是趋势科技的防盗保护组件之一。它能提供诸如定位、锁定和删除等功能。它通过Web界面控制，没有短信命令。

在我们的测试中，在能够发送任何命令（如锁定）前，由于系统试图找到手机，所以发生明显的延迟。

这一点完全有可能，因为电话所在的方位需要能够连接到移动网络，但太慢就不好解释了。在这种情况下，意义就不大了。例如只能在手机位置固定时，才能发送锁定命令。

更改“丢失设备保护”中的任何设置都需要输入密码，这使小偷不能简单地关闭防盗保护。

#### *定位*

定位功能可以在谷歌地图上显示丢失或被盗手机的位置。Web界面打开后，自动执行此项操作。

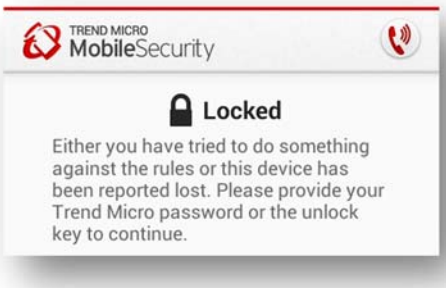
#### *SIM卡监控*

此功能可以在SIM卡被拔出或更换时，锁定设备。测试SIM卡监控功能，着实花了很长时间。一旦设备被重新启动，该功能生效前，我们通常能够使用设备约60秒。

#### *锁定*

使用此命令可以锁定设备，防止第三方未经授权的操作。然后，输入正确的密码才可以解锁。

当手机被锁定后，仍然可以进行紧急呼叫，可以重新要求一个新的密码（通过电子邮件发送）。




然而，还是能打开安卓通知栏，进行设置更改并查看消息。此外，按住主页按钮，可以显示最近使用的应用程式列表，这可

能构成隐私威胁。对此，Trend Micro说，这些错误在下一版本中将被改正。

### *警笛*

此命令会触发响亮的报警声；设备不会被锁定，所以，可以使用该命令寻找放错地方的手机。

### *删除*

趋势科技提供两种不同的删除方法。“部分远程删除”可以删除设备中的个人数据，而“完整远程删除”则重置设备到出厂设置。

在测试该项功能时，虽然使用流行的免费数据恢复工具能够恢复SD卡中被删除的数据，但删除功能总体发挥良好。

### 备份和恢复，扫描Facebook

虽然这些功能都可以在趋势科技移动安全软件的菜单中找到，但实际上这是两个独立的应用程序。点击任一项目，用户都会被带到谷歌商店，在那里可以安装此功能。

### 帮助

趋势科技向用户提供全面的帮助功能，提供了大量的有用信息。此外，每个组件都可以看到信息框，通过项目的配置来帮助用户。

### 卸载

可以从设备管理器列表中删除该应用程序，然而设备随后将立即被锁定。如果重新启动手机，一段时间内锁定不会被开启，这样，小偷就不能卸载防盗保护/家长控制功能。

### 许可

趋势科技移动安全软件的基本版本是免费的。具有安全上网、家长控制、定位、锁定、删除、SIM卡监控和卸载保护功能的高级版，则必须购买许可。定价19.95欧元，有效期为一年。高级版可以免费试用30天。

### 总结

趋势科技提供了一个具有广泛功能的安卓安全解决方案。其中家长控制功能给我们留下了深刻的印象。防盗保护包括了所有预期的现代安全特点，但仍然有一定的改善空间。

## Webroot SecureAnywhere

Webroot SecureAnywhere 是一款利弊兼顾的免费安全产品。对于需求广泛的用户，可购买收费版本；它提供更全面的配套功能。


### 安装

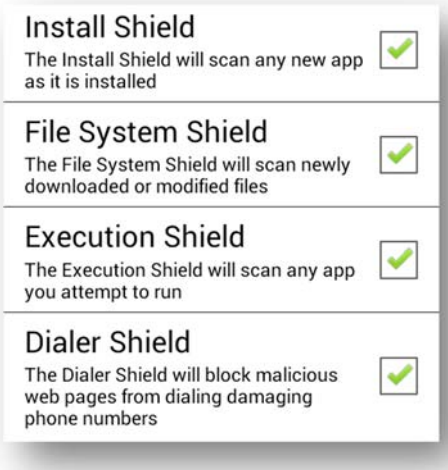
从谷歌商店下载并安装SecureAnywhere。接受使用许可协议后，用户必需注册一个新的Webroot账号，或用现有账号登录。密码至少需六个字符，以设备管理员身份注册应用程序后，安装过程结束。

### 启动程序

程序初次启动时，出现一条黄色的警告信息，提示我们尚未开启安卓屏幕锁。修改此项后，警告变成绿色，提示设备已被保护，并自动运行病毒扫描。

### 防病毒

该防病毒功能组件帮助用户抵御恶意软件。“防毒盾”设置提供4项不同的实时保护功能，但需要被开启：安装实时监控、文件系统实时监控、应用程序执行实时监控、和拨号实时监控。




此外，还提供自动扫描恶意软件，可以设置为每小时、每天或每周扫描。自动更新时间间隔也可以采用此种方式设置，也可手动运行更新。测试时，产品不能识别EICAR恶意软件测试文件。

在进行电量消耗测试时，安装了SecureAnywhere后，电量消耗提高到6%，大部分都是因为“执行防病毒实时监控”。开发者可能需要在此多下功夫。

### 安全浏览

此功能为用户上网时提供安全保护。如果某个网站被软件阻止，如果用户感觉是被错误拦截，可以将其归类到安全站点。那么将来就可以浏览该站点。测试过程中，只有使用安卓标准浏览器才能阻止钓鱼站点；厂商解释说，在即将发布的3.4版本会支持谷歌Chrome。

### 设备丢失保护

防盗保护组件可以通过短信或网络界面操控。后者经过精心设计且直观易用，并允许管理多个设备。每一个设备上的保护状态和例如恶意软件记录都可以看到。

如果用户通过此界面定位设备，不需要进一步的指令来执行定位，手机的位置就可以完全确定。


### *警报*

***短信指令：“scream <密码>”***

此指令会触发刺耳的警报声，而不锁定设备。因此，也适用于帮助查找不知放在哪里的手机，不仅仅当做安全功能使用。警报声一旦响起就没法停止；用户只能耐心的等待两分钟，直到响声自己停下来。

### *锁定*

***短信指令：“lock <密码>”***

使用此命令可以锁定设备，防止第三方未经授权的操作。在后台运行安全且无法绕过的安卓锁屏程序。不过，Webroot自己的锁屏功能可以交互重叠使用。可以显示一条消息（该消息可以在网络界面自定义，用于善意拾到手机的人）。

### *删除*

***短信指令：“Wipe <密码>”***

此功能仅适用于付费版。收到该指令后，设备即会被锁定；个人信息将被删除，且设备会被重置到出厂设置。测试过程中，外部SD卡上的文件未被删除。Webroot说，他们正在考虑在未来的版本中引入SD卡删除功能。

### *定位*

***短信指令：“Locate <密码>”***

使用该命令可以找到丢失或被盗的手机。如果从网络界面发送命令，手机的位置将会通过谷歌地图服务显示在地图上。位置被确定的同时，未收到其他回复的命令。如果处理位置信息需要这么长的时间，应该引起关注。Webroot通知我们说，在稍后的版本可能会启用命令查询功能。

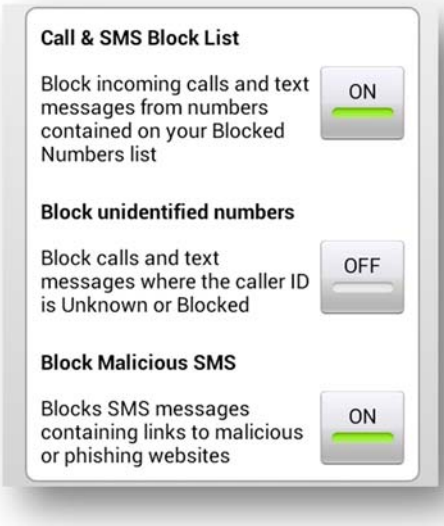
如果发送短信命令，将会收到回复。回复短信中包含谷歌地图中的有关位置链接。

### *SIM卡监控*

此功能也只在付费版可用。如果拔出注册的SIM卡，手机将被锁定。这样，小偷就不能用自己的SIM卡使用该设备。

### 呼叫和短信过滤

此功能可以防止收到不必要的电话和短信，使用的是黑名单原理。用户可以将已知的电话号码添加到黑名单中，这意味着他们所进行的呼叫或发送的短信都会被过滤拦截。也可以阻止匿名电话，即阻止不显示呼叫人号码的来电。此外，Webroot还提供一种防止短信中带有恶意网站链接的功能。该功能在测试过程中表现非常好。



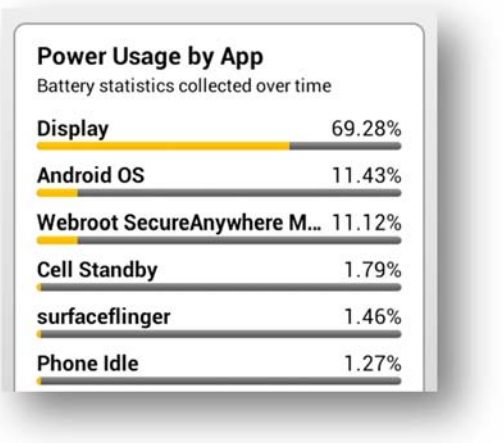

被阻止的短信和电话都清晰地显示在一个列表中。列表不仅显示被阻止的日期，还有短信的内容，以及被阻止的原因。

### 应用程序监控

该功能可以检查安装的应用程序对隐私是否构成威胁。例如风险可能是应用程序可以访问手机中的信息或手机位置。消耗电池较高的应用程序也在列。

### 电池监控

电池监控提供有关电池的详细信息。充电状态和温度、电量消耗大的应用程序都被显示出来。该功能以条形图的形式形象地显示在屏幕上（请注意，Webroot产品本身的电池消耗相对较高，可能是由于我们在测试其各项功能的原因）：




### 网络监控

网络监控显示应用程序使用的网络。所使用的协议、本地和远程IP地址和端口，以及状态都有显示。点击其中一个项目，执行远程IP地址查询，并显示出如ISP和大致位置的详细信息。

### 帮助

Webroot为用户提供了全面的在线帮助功能，这当然需要一个有效的互联网连接。帮助服务的范围和内容都很充分。应用程序本身就是每个菜单条目的迷你文本，这非常有用。

### 卸载

使用程序提供的卸载向导，只需单击一下就可以进行卸载。在免费版本中，则无需密码。小偷很容易解除防盗保护功能。而如果使用付费版本，卸载前，需要先输入密码才能执行卸载。

### 许可

Webroot SecureAnywhere可以免费使用，在缩减版本中没有功能限制。要使用包含卸载保护、SIM卡监控和各种应用程序监控的付费版，可以支付15.75欧元购买，有效期为一年。

### 总结

Webroot SecureAnywhere在我们的测试中表现良好。即使是免费版本，也能提供可靠的防盗和各种过滤器功能。卸载保护、SIM卡监控和应用程序监控使付费版更具吸引力。然而，防盗保护功能的某些设计还有待改进，网络钓鱼的扩展保护功能值得保留。

## 结论

对于一些用户来说，智能手机已经成为个人电脑的替代品。还有一些用户使用智能手机保存个人和专业信息，这都可能引起盗贼的极大兴趣。网络钓鱼是一种潜在的攻击形式，通过对钓鱼网站的访问可能影响用户的任何设备。在各种网上商店应用中，尤其是谷歌商店，保存的信用卡详细信息，无论是通过恶意软件还是通过未经授权的访问，都可能产生高额的消费。这种风险同样存在于手机合同中。

攻击的可能性很大，尤其是开放的如安卓这样的操作系统，给无害应用程序的开发人员提供了广泛的机会。遗憾的是，恶意软件的程序员也同样在滥用这样的机会。

我们认为，手机安全软件可以帮助广大用户杜绝大多数此类威胁，而不应该被当作是可有可无的。尽管如此，许多用户宁愿身处险境也不采用这种保护措施，我们很难理解。市面上有那么多的安全软件，其中不乏免费产品，都能帮助提供较高的安全保证（为什么不用）。通过此次测试，对关于安全产品会影响手机性能或电池使用时间的不恰当说法，我们在很大程度上给予了反驳。

| **Feature List Android Mobile Security (as of August 2013)** | FREE | FREE | COMMERCIAL | FREE | COMMERCIAL | FREE | COMMERCIAL | COMMERCIAL | COMMERCIAL | COMMERCIAL | FREE | FREE | COMMERCIAL | FREE | COMMERCIAL | FREE | FREE | COMMERCIAL | COMMERCIAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Product name: | AhnLab V3 Mobile | avast! Free Mobile Security | avast! Premium Mobile Security | Baidu Security Guard | Bitdefender Mobile Security | ESET Mobile Security | | F-Secure Mobile Security | IKARUS mobile.security | Kaspersky Mobile Security | Kingsoft Mobile Security | Lookout | Lookout Premium | Qihoo 360 MobileSafe | Quick Heal Total Security | Sophos Mobile Security | Tencent Mobile Security Manager | Trend Micro Mobile Security Personal Edition for Android | Webroot Security & Antivirus |
| Supported OS versions: | Android 2.0 and higher | Android 2.1 and higher | | Android 2.2 and higher | Android 2.2 and higher | Android 2.2 and higher | | Android 2.2 and higher | Android 2.2 and higher | Android 2.2 and higher | Android 2.2 and higher | Android 2.1 and higher | | Android 2.2 and higher | Android 2.1 and higher | Android 2.3 and higher | Android 2.1 and higher | Android 2.2 and higher | Android 2.2 and higher |
| Supported Program languages: | English, Korean | Belarusian, Russian, Catalan, Czech, German, English, Spanish, French, Italian, Hungarian, Dutch, Polish, Portuguese, Turkish, Vietnamese, Chinese, Japanese, Korean | | Chinese | English, French, German, Italian, Spanish, Romanian, Polish, Portuguese | English, Polish, Danish, Finnish, Norwegian, Japanese, Russian, Hungarian, Spanish, German, Portuguese, Dutch, French, Romanian, Turkish, Swedish, Chinese, Italian, French, Korean, Czech, Hebrew, Slovak, Vietnamese, Arabic, Bulgarian, Thai | | English, Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Tagalog, Thai, Turkish | German, English, Italian, Spanish, French, Chinese, Russian | English, Russian, French, German, Spanish, Italian, Portuguese | Chinese | English, French, Spanish, German, Japanese, Polish, Portuguese, Russian, Korean, Chinese | | Chinese, English | English | English, German, French, Japanese, Italian, Chinese | Chinese | English, Japanese, Chinese, Korean, Vietnamese, French, German, Italian, Spanish, Dutch, Russian, Portuguese, Turkish | English, Japanese, Chinese, Dutch, German, French, Italian, Korean, Portuguese, Spanish, Turkish, Russian |
| Anti-Spam Features | | | | | | | | | | | | | | | | | | | |
| Whitelist/Blacklist SMS | ● | ● | ● | ● | | | ● | ● | ● | ● | ● | | | ● | ● | ● | ● | ● | ● |
| Whitelist/Blacklist calls | ● | ● | ● | ● | | | ● | ● | | ● | ● | | | ● | ● | ● | ● | ● | ● |
| General blocking of known/unknown contacts and hidden numbers | ● | ● | ● | | | | ● | | | ● | ● | | | ● | ● | ● | ● | ● | ● |
| Whitelist/Blacklist MMS | | ● | ● | | | | ● | ● | | | ● | | | ● | | ● | ● | | ● |
| Block known SMS/MMS spam | | | | ● | | | | | | | ● | | | ● | ● | ● | ● | ● | ● |
| Block known call spam | | | | ● | | | | | | | ● | | | ● | | ● | ● | ● | |
| White- and Blacklisting with wildcards | | ● | ● | | | | | | | ● | | | | ● | | ● | ● | | |
| Parental Control | | | | | | | | | | | | | | | | | | | |
| Lock apps | | | ● | | | | | ● | | | | | | ● | | ● | ● | | |
| Block Phone calls, email, SMS/MMS, Web-Browsing, apps between specified hours | | ● | ● | | | | ● | | | | | | | | | | | | |
| Make the device call you back so you can hear what's happening around it | | ● | ● | | ● | | | | | | | | | | | | | | |
| Authentication | | | | | | | | | | | | | | | | | | | |
| Lock Screen with Password protection | | | ● | | ● | ● | ● | ● | ● | ● | | | ● | ● | | | ● | ● | ● |
| Password policy: Strength, length, etc. | | | | | ● | ● | ● | ● | ● | ● | | | | | | | | ● | ● |
| Maximum number of failed attempts and/or grace period | | | ● | | | | | ● | ● | | | | ● | | | | ● | | |
| Access control | | | ● | | | ● | ● | ● | ● | ● | | | | | | | | | |
| Anti-Malware | | | | | | | | | | | | | | | | | | | |
| On Demand Scan (Full system scan) | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Automatic Update | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Real Time File protection | | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Prevent access to harmful (e.g. phishing) web sites | | ● | ● | ● | ● | | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● |
| Scheduled Scan | ● | ● | ● | ● | | | ● | ● | ● | ● | | ● | ● | | | ● | ● | ● | ● |
| Application Audit / Security info about installed apps | | ● | ● | ● | ● | | ● | | | | ● | | ● | ● | | ● | ● | ● | ● |
| On Demand Scan (scan of specified folders, SD card) | | ● | ● | ● | ● | | | | ● | ● | ● | | | | | ● | ● | | |
| USSD Blocking | | ● | ● | | | ● | ● | | ● | ● | ● | ● | ● | | | ● | ● | | |
| Cloud Scanning (requires cloud connection) | | | | ● | ● | | | ● | | ● | ● | | | ● | | ● | ● | ● | ● |
| SMS/MMS Scanner | | ● | ● | ● | | | | | | ● | ● | | | | ● | ● | ● | | ● |
| Different Update profiles | ● | ● | ● | | | | | ● | ● | | ● | | | ● | | | ● | | |
| Central Managed updates | | | | | | | | ● | ● | | ● | | | ● | | | ● | | ● |
| Own roaming update profile | | ● | ● | | | | | ● | ● | | ● | | | ● | | ● | ● | | |
| Network protection | ● | ● | ● | ● | | | | | ● | ● | ● | | | ● | | | ● | | |
| Quarantine | | | | | | ● | ● | | | ● | | | | | ● | ● | | | ● |
| Anti-Theft | | | | | | | | | | | | | | | | | | | |
| Remote localization (GPS) | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● |
| Remote localization (Network) | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | |
| Remote Wipe and Remote Lock | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | | ● | ● | ● | ● | ● | ● | ● |
| Remote alarm | | ● | ● | | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● |
| SMS for controlling Anti-Theft components | ● | ● | ● | | ● | ● | ● | ● | ● | ● | | | | ● | ● | ● | ● | | ● |
| Webinterface for controlling Anti-Theft components | | ● | ● | | ● | | | ● | | ● | | ● | ● | ● | ● | | ● | | ● |
| Possibility to make emergency calls while locked | | | | | ● | ● | ● | ● | ● | ● | | | ● | | ● | ● | | ● | ● |
| Lock phone on SIM change | ● | ● | ● | | | | ● | ● | ● | ● | | | | | ● | | ● | ● | ● |
| Report thief's phone number | ● | ● | ● | | ● | ● | ● | ● | | ● | | | | ● | ● | ● | ● | | |
| Remote unlock | | ● | ● | | | | | ● | | | | | ● | ● | ● | ● | | | ● |
| Track location (automatic locating in timewindow) | | ● | ● | | | | | | | | | ● | ● | ● | ● | | ● | | ● |
| Remote configuration | | ● | ● | | | | | ● | | | | ● | ● | | ● | | ● | | ● |
| Lock Contacts, SMS/MMS | | ● | ● | | | | | | ● | | | | | ● | | ● | ● | | |
| Remote updates | | ● | ● | | | | | | | | | ● | ● | | ● | | ● | | ● |
| Possibility to receive calls while locked | ● | | | | | ● | ● | ● | | | | | | | ● | ● | | | ● |
| Report thief's location at SIM change | ● | ● | ● | | | | | | | ● | | | | | | | ● | | |
| Lock Images/Files | | ● | ● | | | | | | | | | | | ● | | ● | ● | | |
| Backup | | | | | | | | | | | | | | | | | | | |
| Backup (online / memory card) | | ● | ● | ● | | | | ● | | | | ● | ● | ● | ● | | ● | ● | ● |
| Backup of contacts | | ● | ● | ● | | | | ● | | | | ● | ● | ● | ● | | ● | ● | |
| Backup Call History | | ● | ● | ● | | | | | | | | ● | ● | ● | | | ● | ● | |
| Scheduled data backup | | ● | ● | | | | | | | | | ● | ● | | ● | | ● | ● | |
| Backup of SMS/MMS and user data | | ● | ● | ● | | | | | | | | | | ● | ● | | ● | ● | |
| Backup Pictures/Multimedia | | | ● | | | | | ● | | | | | ● | | | | ● | ● | ● |
| Support | | | | | | | | | | | | | | | | | | | |
| Email support | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● |
| User Forum | | ● | ● | ● | ● | ● | ● | ● | | ● | ● | | | ● | ● | ● | ● | ● | ● |
| Online Help | | ● | ● | | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● | ● | ● | ● |
| Phone Support | | | | ● | ● | ● | ● | ● | ● | ● | ● | | | ● | ● | | ● | ● | ● |
| Online Help (special URL designed for browsing with the phone) | | ● | ● | | | ● | ● | | ● | ● | ● | ● | ● | | | ● | ● | ● | ● |
| User manual | ● | ● | ● | | ● | ● | ● | ● | | ● | ● | | | ● | ● | | ● | | ● |
| Online Chat | | ● | ● | | ● | | | ● | | ● | ● | | | ● | ● | | ● | ● | ● |
| Supported languages (of support) | English, Korean | English, German, Czech, Polish, Russian, French, Chinese, Japanese, Turkish, Spanish, Portuguese, Arabic | | Chinese | English, German, Romanian, Italian, French, Portuguese, Spanish | All | | English, Finnish, French, Dutch, Danish, German, Chinese, Italian, Norwegian, Polish, Swedish | German, English | English, Russian, French, German, Spanish, Polish, Japanese | Chinese | English, French, Spanish, German, Japanese, Polish, Portuguese, Russian, Korean, Chinese | | Chinese | English, Hindi, Marathi, Tamil, Telugu, Malyalam | English, German, French, Japanese, Italian, Chinese | Chinese | English, Japanese, Chinese, Korean, Vietnamese, French, German, Italian, Spanish, Dutch, Russian, Portuguese, Turkish | All |
| Additional features | | | | | | | | | | | | | | | | | | | |
| Password protection for settings | | ● | ● | | ● | ● | ● | ● | ● | ● | | ● | ● | | ● | ● | ● | ● | |
| No SIM activation | | ● | ● | | ● | ● | ● | ● | | ● | | ● | ● | ● | ● | ● | ● | ● | |
| Statistics | | ● | ● | ● | ● | ● | ● | ● | ● | ● | | | ● | | | ● | ● | | ● |
| Account (not device) based licensing - same license for multiple devices if same owner | | ● | ● | | ● | ● | ● | ● | ● | | | ● | ● | | ● | | ● | | ● |
| PW protection of uninstallation | | ● | ● | | ● | ● | ● | ● | ● | ● | | | | | ● | ● | | ● | ● |
| Central Management | | ● | ● | | ● | | | ● | | | | ● | ● | | | ● | | | ● |
| Data network usage monitor | ● | ● | ● | ● | | | | | | | | | | ● | ● | | ● | | |
| Battery Monitor | | | | | | | | | | | | | | ● | ● | ● | ● | | ● |
| Updates thru PC | | | | ● | | | | ● | | | ● | | | ● | | | ● | | ● |
| Offline activation | | ● | ● | | | | | | | | | | | ● | ● | ● | ● | | |
| Task Killer | | | | ● | | | | | | | | | | ● | ● | | ● | | |
| Several trusted SIM cards | | ● | ● | | | | ● | | | | | | | | ● | | | | |
| Local wipe | | | | | | | | | | ● | | | | | ● | | ● | | |
| Storage Monitor | | | | | | | ● | | | | | | | | | | ● | | |
| Price (may vary) | | | | | | | | | | | | | | | | | | | |
| Price 1 phone / 1 year (USD/EUR) | FREE | FREE | USD 15 / 10 EUR | FREE | USD 10 / 8 EUR | FREE | USD 15 / 10 EUR | USD 20 / 15 EUR | USD 12 / 9 EUR | USD 15 / 10 EUR | FREE | FREE | USD 30 / 23 EUR | FREE | USD 12 / 10 EUR | FREE | FREE | USD 30 / 25 EUR | USD 20 / 26 EUR |
| Price 4 phones / 2 years (USD/EUR) | FREE | FREE | USD 120 / 80 EUR | FREE | USD 80 / 60 EUR | FREE | USD 120 / 80 EUR | USD 160 / 120 EUR | USD 68 / 62 EUR | USD 120 / 80 EUR | FREE | FREE | USD 90 / 68 EUR | FREE | USD 95 / 80 EUR | FREE | FREE | USD 200 / 180 EUR | USD 160 / 120 EUR |

## 版权及免责声明



更多关于AV - Comparatives及测试方法，请访问我们的网站。

AV-Comparatives e.V. (2013年8月)