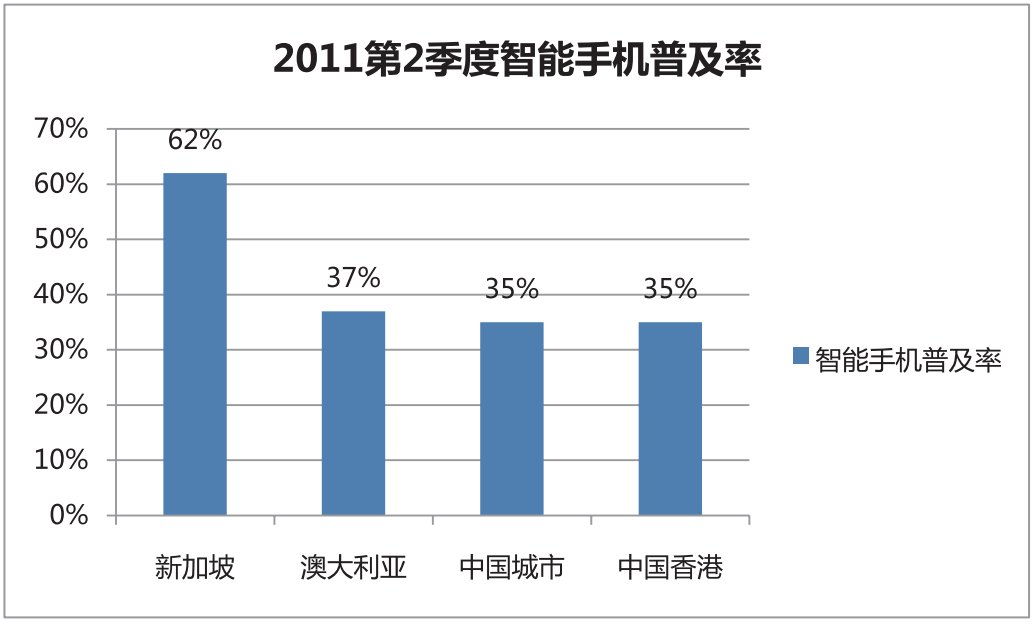
目　　录

一、摘要

伴随着智能终端性能的提升和价格的回落，智能型终端的普及率越来越高，谷歌和益普索市场研究集团（IPSOS Group，简称IPSOS）最新联合进行的一项研究发现，亚太地区作为一个整体拥有全球最高的移动电话普及率。通过3万份调查报告显示，4个亚太市场的智能手机普及率（31%）更高。它们是：新加坡（62%）、澳大利亚（37%）、中国香港（35%）和中国城市地区（35%）。



智能终端的普及和3G/WIFI网络的不断完善，也带动了移动互联网的蓬勃发展。第28次《中国互联网络发展状况统计报告》显示截至2011年6月底，手机网民规模达到3.18亿,在总体网民中占比达到65.5%。中国手机网民数量早已超越美国跃居世界第一。

一方面，移动互联网的快速发展，让各类手机应用如雨后春笋般出现，更好的满足了用户需求。此外，手机电子商务、手机支付、LBS、联系人云备份、手机预定机票酒店等商务应用的不断成熟，也极大的方便了用户生活。另一方面，手机上网应用在方便了用户生活的同时，还让手机从简单的通话工具变为了“贴身秘书”。而移动终端的各类安全问题也层出不穷，比如，病毒、恶意扣费、骚扰电话、手机系统垃圾、程序偷偷联网、手机支付安全隐患、隐私泄漏等等各类问题困扰着手机用户。

但同时，由于越来越多的安全厂商在移动安全领域进行了较大的投入，腾讯也提出“浸泡式安全解决方案”，让手机用户无处不安全，从而极大地降低了用户在移动终端安全方面的风险。与此同时，用户在移动生活、移动娱乐、移动商务、移动学习等需求呈现爆炸式增长，导致手机安装的应用越来越多，更好的优化手机各项性能指标，让其更好的发挥价值就变得非常必要。这个时候，让手机更加健康变得和手机基础安全一样重要。

打一个形象的比喻，当前手机用户对安全的需求正如同人对食物的需求一样，在满足了吃饱吃好的同时，已经跃升到吃的是否健康。基于此，腾讯移动终端安全架构(Mobile Terminals Assurance Architecture, 以下简称MTAA）将进行全面的升级，由原来“浸泡式安全解决方案”，升级为“移动设备健康管理解决方案”。

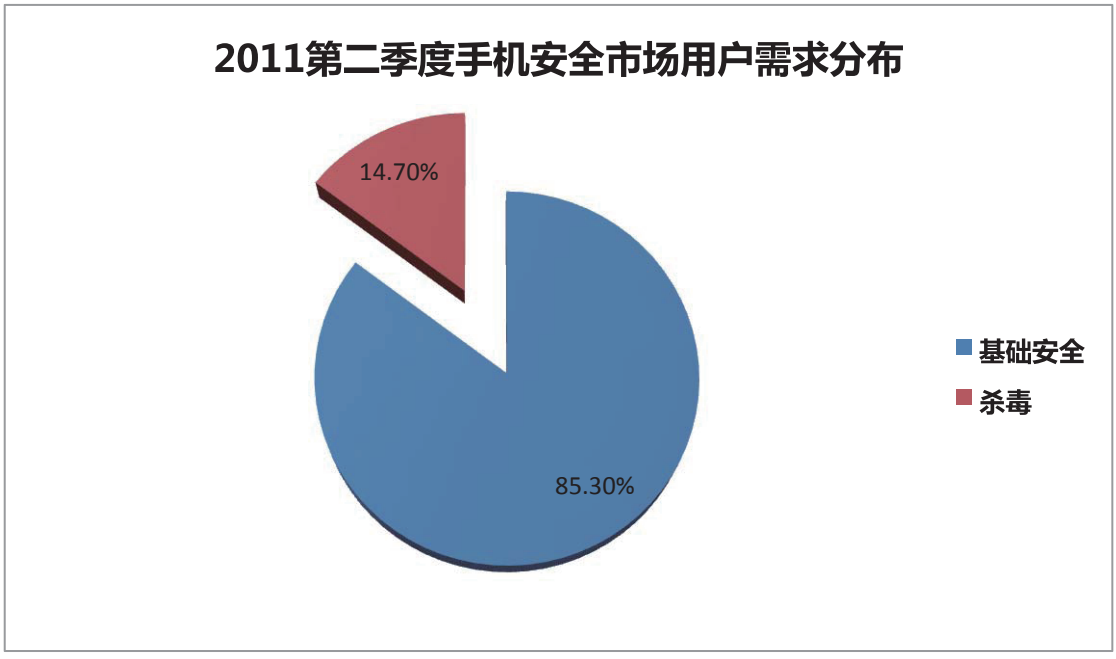
二、手机安全行业现状与用户需求分析

2.1 手机安全行业现状

艾媒咨询(iimedia research)研究数据显示，截至 2011 年 3 月，手机病毒数已达到上千个，预计 2011 年全年手机病毒总数将超过两千，同比增长 51.7%。 手机病毒数量正以极快的速度增长，尤其是 Android 系统， Android 几乎成了手机病毒“重灾区”。腾讯移动安全实验室也率先截获了多个手机病毒，比如，伪 Google 框架病毒、伪卡巴杀毒病毒、饥渴吸费魔病毒等，通过对这些病毒的研究分析发现，这些手机病毒多采用伪装成工具或者游戏软件的方式诱骗用户下载安装，以达到恶意吸费、取用户隐私的目的。而且病毒产业链完善，可以通过云端控制进行远程控制，轻松变换扣费号码，制造病毒变种。

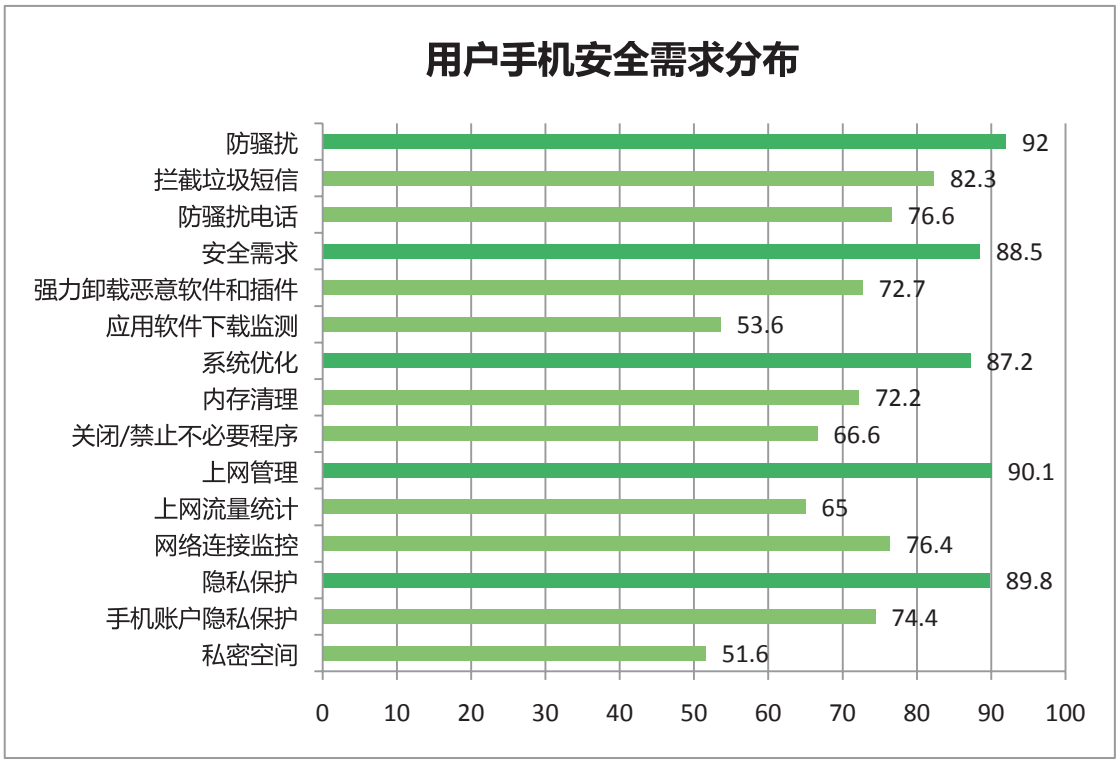
但是据 EnfoDesk 易观智库近期发布的《2011 年第 2 季度中国手机安全市场季度监测》研究显示：2011 年第 2 季度中国手机安全市场仍然保持快速增长势头，累计帐户数已经达到 1.29 亿， 环比增长 8 %。2011 第 2 季度中国手机安全市场基础安全需求帐户数新增 946

万，市占率已增至 85.3%，在杀毒类应用方面其份额再次下降，达 14.7%。这也充分说明了，用户对手机查毒、杀毒等被动式防护需求已经趋于稳定。



与此同时，有调查显示，当前手机上网应用主要集中在浏览网页和新闻、手机聊天、看空间、看微博和博客、听音乐和看小说、玩游戏等，未来手机应用的增长点将出现在搜索信息、看股票、GPS 导航、收发电子邮件、网购和支付、酒店机票预定等更加商务性质的应用。这也意味着手机安全的重点也将不仅包括查毒、杀毒、防骚扰和欺诈等被动式基础防护，还需要更加智能化的帮助用户管理和优化手机性能，做手机用户的“贴身管家”。

2.2 用户手机安全需求分布



如上图所示，当前用户对手机安全的基础需求，包括防骚扰、安全需求、上网管理等，很多手机安全软件都已经具备这些基础安全功能。而随着智能机的普及，手机上网各类商务、办公、娱乐应用的增加，产生了新的需求，比如，系统优化、隐私保护等，这些更高级的手机健康管理需求迫切需要满足。

三、腾讯提出 MTAA 升级：从浸泡式安全向移动设备健康管理升级

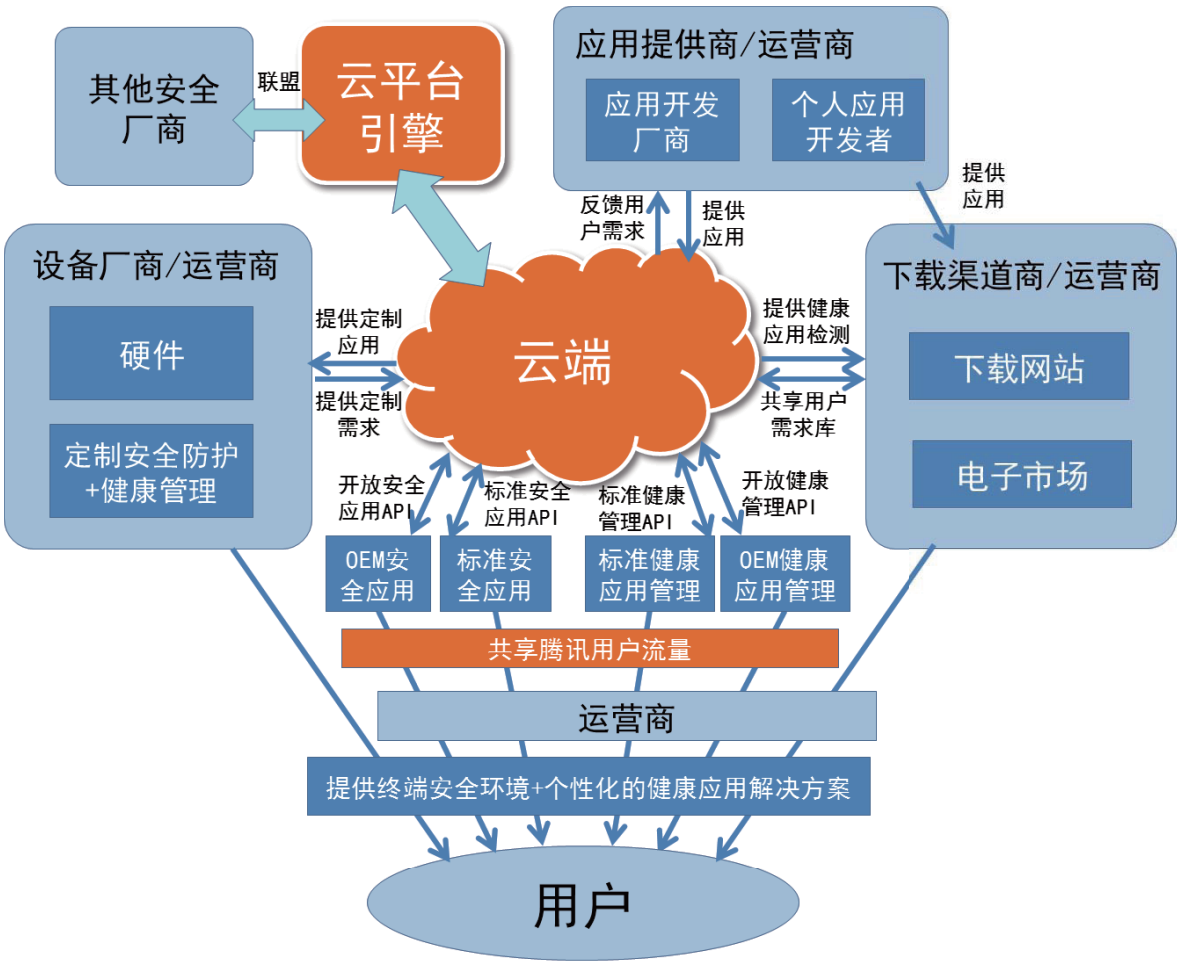
3.1 目标：推动移动互联网产业链的健康发展

由浸泡式的移动设备解决方案，升级为“移动设备健康管理解决方案”。

基于MTAA开放平台，通过联合产业联盟，与运营商和广大手机厂商、软件厂商协同合作，共同为用户提供一站式移动设备健康管理解决方案，使用户最大化地发挥移动设备的性能与功能，实现更便捷、更强大的移动生活、移动娱乐、移动商务、移动学习等应用，推动整个移动互联网产业链的健康发展。

3.2 升级后的MTAA体系架构

升级后的 MTAA 体系架构图：

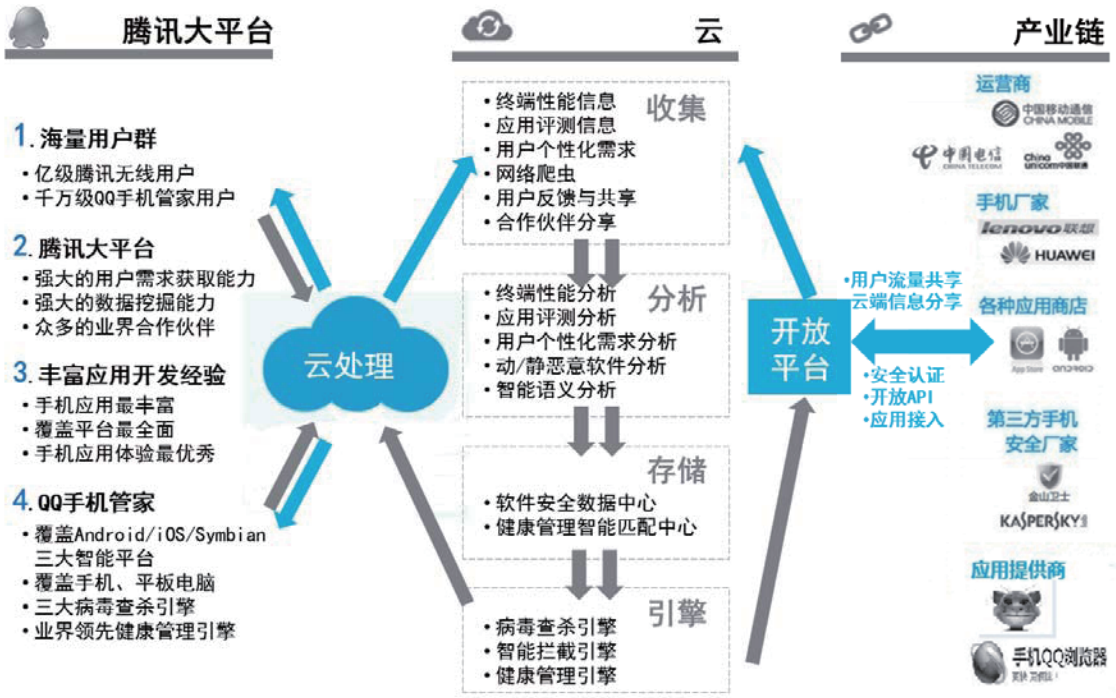


移动设备安全，升级为移动设备健康管理，为用户的移动设备提供个性化的健康管理解决方案。

新框架是在原架构的基础上，增加了用户的个性健康应用需求的相关内容，具体表现在增加了健康应用管理的标准 API 与开放 API ,以及健康管理中的用户需求与用户个性化信息的共享库，合作伙伴可以针对个性化的用户需求，提供更好的应用软件、应用下载方式、应用管理方式 。

3.2.1 MTAA 云端与云平台引擎

云端与云平台引擎体系图：



解释：云端与云平台引擎，是MTAA核心技术与提供对外开放合作的核心，由原来以安全为重点的云端，现升级为安全防护+健康管理。

1、移动终端安全解决方案

MTAA的移动终端安全解决方案，是一个深入到多个智能手机操作平台的系统层面、获得高权限的，并与云端一起，共同构成四大防御体系的解决方案。

（1）面向多平台系统层面的高权限解决方案：

至今应用最广的智能操作平台包括Android、iOS、Symbian，移动安全解决方案在系统层面优先考虑这三大智能平台。

1）Android平台深层次安全解决方案

MTAA与众多知名厂商达成深度合作，在多款手机中取得最高root权限，能够在系统底层通过实时监控应用程序的行为，例如API调用，实现主动式防御引擎，对终端实现高度融合与

深层次的保护。

通过先进的监控技术：

监控应用程序的Activity以及对各种数据的读取，比如短信，联系人，通话记录等，同时也可以监控某个应用程序的开启，实现应用锁功能。

监控应用程序对phone, sms, phoneinfo 等服务的访问，实现拨打来去电话，短信收发，获取手机唯一码，地理位置等信息的保护。

监控应用程序对input服务的访问，在用户输入账号和密码时，提供实时保护。

2）Symbian平台深层次安全解决方案

MTAA直接从Nokia取得最核心和最高级的权限，通过赋予的最高权限，可以紧密地在手机的内核形成有效的保护，让手机系统最核心的部分可以免受病毒的侵扰。

MTAA可实现专业而且强悍的系统防护功能：

深入内核，形成系统保护层，让系统文件无法被破坏。

专业查杀病毒，对手机系统里的文件了如指掌，病毒无所遁形，并且使用先进的杀毒技术，粉碎病毒各种自我保护机制，使得病毒被彻底清除。

有效的对手机资源的访问监控。

(2)“云到端”的解决方案

为了弥补终端本身的处理速度、容量等的限制，MTAA解决方案还着重开发具有强大运算能力的云端平台。

云端平台实现了强大的病毒与木马云端实时检测功能，能应对普通手机终端、合作伙伴服务器、其他下载类的应用程序（如浏览器、下载器）的软件安全性检测请求。

终端与云端的结合解决方案：

MTAA围绕着用户使用手机的整个流程、不同的使用习惯，对不同级别的安全事件进行分布式处理。当系统开始启动，安全软件即进驻系统底层，对系统软件、内存驻留软件进行扫描。在手机使用过程中，对系统软件与应用软件的运行进行安全监控，主要包括对各种敏感操作调用过程进行监控，如发现超出安全许可的敏感操作，立即进行主动式的防御，如：防隐私信息的扫描（通讯录、短信、彩信、照片、视频、位置信息、文件文档、收藏夹、上网记录、cookies等）、防某指定程序的扫描（部分机型）、防按键捕捉，防帐号密码捕捉，防私自信息交换（短信、彩信）、防私自无线数据交换（联网、蓝牙、红外等）。用户下载软件时，能实时通过云端检测正在下载软件的安全性，防止下载高风险软件。在用户安装新软件时，对软件进行安全性扫描，防止安装高风险软件。

(3)五大防御体系：防病毒、防骚扰、保隐私、网络防御、保险防范

1）防病毒：

基于MTAA在Symbian、Android平台构建的移动安全软件具备强大病毒查杀能力。具体包含：

多引擎查杀：QQ手机管家查杀病毒引擎+卡巴斯基查杀病毒引擎+云查杀病毒引擎

高性能的本地查杀引擎——QQ手机管家查杀病毒引擎、卡巴斯基查杀病毒引擎，在无需联网的情况下，可以快速的对本地已安装软件和即将安装软件进行病毒查杀，第一时间保护手机的安全。

精准的云查杀引擎：在用户允许的前提下，终端会联网将本地的软件信息及行为特征上传到云端服务器，服务器根据所上传的信息进行精准的病毒扫描，将最终精确的查杀结果返回给终端。

病毒特征库云更新及病毒预警技术

可以以最快的速度将最新的病毒特征库进行更新，从而能全面及时的保障用户手机的安全。基于“防杀结合，预防为主”的理念，系统会在截获病毒后第一时间推送病毒预警，让用户防患于未然。

联网行为监控

用户可以清晰的观察到手机上安装的每个软件的联网行为，出现异常时可以及时进行处理。

强力卸载

某些病毒简单的使用系统无法卸载，这时强力卸载可以帮助用户清理手机，保障手机远离病毒。

安全软件管理

基于“以防为主”的理念，MTAA提供了安全、可靠、完善的软件管理渠道，全部软件都经过全面病毒检测，确保安全。可以满足用户大部分场景的应用使用需要，保证用户能放心的安装使用。

全网数据监控拦截技术

通过对全网数据的抓取和与合作伙伴的资源合作，可以达到最全面数据监控，能第一时间发现病毒，并进行预警。

自动化检测技术

采用智能的动静态检测、用户行为模拟、软件行为模型分析等技术，对软件进行自动化检测，从而发现病毒木马。

2）防骚扰：

商家广告、诈骗、钓鱼、色情等信息被推送到手机终端，甚至还有深夜陌生人电话响一声的骚扰，这些都严重影响用户的正常生活。基于时刻为用户着想，为客户实现最大价值的理念，MTAA为用户建立骚扰防护的安全盾。 鉴于手机的最大骚扰来源于电话和短信，MTAA实现了一整套针对电话与短信的安全解决方案。

防电话骚扰：通过用户设置的黑白名单可以实现对黑名单号码拨打电话的时候提示各种语音信息，包括空号、关机、不在服务区、停机等，还通过本机智能判断+云平台信息共享，智能拦截“响一声”的吸费电话。

短信拦截：通过用户自定义的黑白名单或模式外，还依靠智能语义分析技术，实现了智能度业界领先的短信智能拦截平台。智能拦截能实现关键字语义分析，对内嵌电话号码、广告号码、客服号码、银行帐号、网址等进行智能分析拦截。

3）保隐私：

隐私问题是所有安全类问题中最备受关注的。

MTAA构架的“隐私保护”的解决方案是基于高权限用户模式下，结合手机操作系统本身的框架特点，通过先进技术，可截获系统的大部分调用，如发送短信、拨打电话、读取数据库、获取IMEI号等，来实现终端层面颗粒度极细、力度极强的解决方案。

隐私安全问题，具体到手机平台，主要是指用户电话号码、短彩信记录、通话记录、联系人、帐号密码、地理位置、浏览器书签、手机唯一码等私密信息的保护问题。

针对一般的智能手机，可以建立一个隐私数据保护模块，把用户的隐私数据保存在一个加密的数据模块中，为用户提供一个隐私数据的保护空间。在隐私空间里，保存着用户的所有隐私信息，如收发的短信、通话记录等。其本质思想，就是通过创建另外一个数据源，把用户

认为隐私的数据从系统数据抽离出来，并通过数据加密技术进行二级保护。

而针对已经破解的智能手机，除了可以实现上述隐私数据保护功能之外，还可以实现主动防御式的隐私保护，并形成功能上的互补。一般来说，一个应用的权限，是在安装的时候就已经提示给用户的。但用户往往会忽略掉这个权限提示列表，而直接安装应用。针对这种情况，主动防御系统可以阻断某个应用的隐私数据访问（如读取系统短信、系统联系人等），并询问用户是否允许操作。同时，主动防御系统也会根据用户的选择，进行智能分析学习，更好的保护用户的隐私。

4）网络防御：

目前无线互联网高速发展，智能手机上网的安全隐患也日益突出。一些恶意软件偷偷联网产生大量流量资费，甚至收集用户隐私信息，给用户造成损失。MTAA上网监控功能能够实现：

实时流量监控。由于是直接读取系统信息文件，因此流量统计更加精确，当本月使用的流量接近用户设置的限额时，会弹出提示让用户关闭网络连接。

采用先进的IPTABLE防火墙技术实现联网黑白名单功能，用户可以自由设置信任的程序列表，非信任程序则无法联网，从而可针对特定的程序的联网行为进行监控，除了避免产生不必要的流量外，还可以控制恶意程序联网带来的高风险。

根据手机的状态智能调整监控行为，从而达到最佳用户体验和省电目的。通常用户使用蜂窝制式（如3G）通道上网才会产生流量资费，因此当手机处于网络关闭状态（包括休眠状态）或者在WIFI环境下将关闭上网监控，节约用户的电池使用成本。

网站访问监控与提示：通过云平台进行恶意网址的监测，以及本地平台对网页的恶意代码的监控，达到网站访问监控与提示，使用户上网时远离恶意网站与钓鱼类网站，为用户打造一个安全、无忧的上网环境。

5）保险防范：

随着智能机的普及，用户在各种移动终端保存的重要数据越来越多，如果没有预先做好保险防范，一旦手机丢失、被盗，或因某些原因造成手机损坏，都会造成数据丢失，追悔莫及。MTAA 通过主动备份与远程备份方式来实现数据的保险防范。

A．面向多平台的安全云备份

实现功能：联系人、短信、通话记录、书签、文件等多种数据的备份和恢复，并具备扩展数据源的能力，使用户能在多终端实现多种数据的备份；支持 3 种数据传输方向，适应用户的不同使用场景；支持 QQ 面板，WEB，WAP 等方式管理终端备份的资料，方便用户维护各种资料。

对外开放接口：完全支持 OMA 标准，服务器可以与支持 SyncML 标准的厂家无缝对接，并具备良好的兼容性；引擎独立封装，可以方便给其它产品提供同步功能。

B．手机防盗：

防盗功能可以帮助丢失手机的用户，可能通过远程指令获取手机地理位置信息，尽可能帮助失主找回手机；通过远程指令对原手机各种私隐数据进行备份，锁定手机并且删除失主个人隐私，最大程度保护失主个人信息的安全。

2、健康管理解决方案

用户在移动终端的需求已不仅仅局限于安全方面，在健康管理方面的需求日益突出，MTAA 根据用户的需求与移动终端的特点，特别针对性地研发出移动设备的健康管理解决方案。

（1）面向多平台不同硬件层面的针对性的解决方案

Android、iOS、Symbian 平台的硬件要求与性能表现各有特点，MTAA 深入到硬件层面进行健康管理方案。

MTAA 针对不同操作系统，不同的硬件规格，分别进行深入多样、丰富的应用评测，为最佳应用组合推荐奠定坚实的基础。

众多的厂商加入到 Android 的阵营 ,推出的终端由低配普及到高端高性能 ,跨度较大；iOS 平台硬件性能比较聚焦，只推出了 iPhone 与 iPad 的系列产品，硬件相对高端，并形成一定梯度的特征表现 , 软件与硬件的匹配主要体现在屏幕上的差别 , 其次才是性能上的差别。

相对于 Android 与 iOS，Symbian 平台是硬件相对较低，但能耗也相对较低的平台，但智能机的主流机型也相对较为集中 , 性能表现存在一定梯度上特征表现 , 存量用户是一个非常庞大的用户群，相对主流的手机应用还是会兼顾到 Symbian 的热门机型。

（2）“云到端”的解决方案

同样，为了弥补终端的处理速度、容量等限制，MTAA 的健康管理解决方案同样采用云端与终端结合的解决方案。

其中轻量级的硬件健康管理、系统优化管理、操作便捷管理功能 ,可以放在终端侧完成。

而庞大的健康管理的智能库保存在云端 , 由云端实现智能匹配的运算 , 并把结果反馈到终端，云端与终端互补实现应用健康的管理。

（3）四大健康管理体系：硬件健康管理、系统优化管理、操作便捷管理、应用适配管理

1）硬件健康管理：

移动设备的硬件都是电子器件，正确的使用方式可以延长寿命、提高性能、降低能耗，MTAA除了关心移动设备的软件应用外，还关心硬件的使用健康问题。

A.电池健康管理：

智能充电保护：通过对锂电池物理性能的研究，科学地设置各种监测点，为每个电池建立健康档案，，最大化地延长电池的寿命。

省电节能管理：智能分析用户使用场景，在不影响用户使用手机的情况下，全面分析WiFi、移动网络、蓝牙的使用情况，若耗电大项处于长期开启但没连接使用状态，可智能控制其开启、等待、关闭，还可以由用户自定义设置关闭闲置运行程序，最大限度地降低手机耗电量。

B.CPU低损超频

超频或许对CPU的使用有一定损害，但也是一种提高速度的办法，MTAA为一些低频的CPU用户提供了CPU低损超频方案，在一定条件下超频，根据CPU的使用率来动态调节频率减少CPU损害。

2）系统优化管理：

智能化的移动设备就像 PC 一样，同样存在着垃圾文件、启动变慢、运行变慢、ROM 空间不足等系统“亚健康”问题，MTAA 采用一整套的解决方案来帮助用户进行优化，使用系统运行得更健康。

A．垃圾清理：随着终端软件的种类繁多，用户安装的软件也随之增加，每个软件或多或少都会产生一些垃圾文件（包括配置文件、缓冲文件、残留文件等）。这些文件日积月累 ,会严重影响手机运行速度及存储空间 ,造成 CPU 及存储资源的大量浪费，甚至影响到手机的响应速度及使用手机软件的体验。MTAA 开发高速的智能分析扫描引擎，有效地分析出系统垃圾，并一键清除。

B．手机加速：

开机优化：提供建议给用户禁止不必要的程序开机启动；

运行变慢：由用户手动结束，或智能动态分析结束一些暂时不用的服务、进程，释放内存、节省 CPU 资源，加速系统运行速度。

C．程序智能清理：MTAA 能实现根据移动设备上的软件的使用频率，引导用户进行卸载一些没有使用过的软件。

3）便捷方式设置：

目前手机操作和PC操作系统一样，都是非中国原生的操作系统，虽然国内很多公司对这些系统进行过各种各样的改造，就目前用户调研的数据发现70%以上用户对手机操作存在疑问或者感觉繁杂，认为还有很多不够人性化的地方。MTAA关心更人性化的便捷操作：

A.网络设置

网络设置包括GPRS、EDGE、3G等移动网络数据服务开启与关闭，APN设置，Wap、Net的切换等，这些MTAA都提供便捷的配置、开关与切换。

B.通讯辅助

由于国内运营商的特色，用户存在多种多样的通话拨号方式，例如有IP拨号，需要不同运营商使用不同的IP号码，而且号码过长，造成打电话时输入繁琐，还有分不同SIM卡在不同时间段优惠方式不同等，MTAA智能化解决这些繁杂的操作，给通讯一个便捷帮助。

C.文件管理

部分手机平台还不提供文件管理系统，需要用连接电脑或安装各种应用等操作去实现，MTAA可以对文件进行分类，例如搜索管理最常用的应用安装包等管理。

4）应用适配管理：

“最适合用户需要与硬件性能的应用，才是最好的”，MTAA为用户提供最适合的应用适合方案：

A．应用+需求双匹配：MTAA通过不断地细化用户的需求，为不同的用户需求匹配应

用方案，务求给到用户最适合的应用组合。这就有点像，根据不同人的体质与口味需求，提供不同的营养套餐，使用户得到健康的体魄。

B．官方包保障：MTAA与各大软件开发商与开发者均有深厚的合作关系，能向用户提供安全的官方包下载。

3、标准应用：QQ 手机管家

在云端与云平台引擎的基础上，腾讯打造自己的标准应用，向最终用户直接提供的服务，也为第三方厂商提供开发的范例，同时允许第三方厂商在这些标准应用上直接嫁接自己的应用。

标准应用QQ手机管家，具有“安全防护”与“健康管理”两个标准模块的功能：

（1）安全防护标准应用：

1、一键体检：快速全面了解手机状况，一键修复；

2、病毒查杀：本地查杀引擎加上联网云查杀，快速准确扫除病毒；

3、骚扰拦截：轻松智能拦截垃圾短信，屏蔽各种骚扰电话；

4、扣费扫描：全盘扫描、实时拦截恶意扣费信息，防止恶意软件吸费；

5、上网管理：联网防火墙预防程序偷偷联网，实时监控网络流量；

6、手机防盗：在用户手机丢失后进行定位，并保护用户隐私。

（2）健康管理标准应用：

1、同步助手：一键备份手机联系人，云端备份手机通讯录；

2、软件管理：一站式安全绿色软件下载，安装包安全扫描和管理；

3、私密空间：对重要联系人短信、通话加密，保护你的隐私；

4、系统优化：一键释放系统内存，清理系统垃圾，优化开机速度，给手机提速；

5、常用工具：来去电归属地显示，便捷查询归属地，查询常用号码、IP 拨号、便捷网络设置。

3.2.2 应用接入开放平台

MTAA围绕着用户使用安全应用与健康应用，通过标准应用与开放API向用户提供安全应用与个性化的健康应用推荐。

MTAA为应用开发商与个人开发者提供产品管理平台、产品展示平台，除了能分享腾讯大平台的亿万级用户流量外，还可以分享通过MTAA的开放API的合作伙伴的流量。

除了单向的提供下载外，MTAA还注重用户的信息反馈，在标准API与开放API上，都有相应的用户反馈、用户调研、用户下载与使用偏好等的各种运营信息可以与合作伙伴进行分享，力求帮助各应用开发商与个人开发者，开发出能满足用户需求的多样化的健康应用。

3.2.3 开放 API 接口

1、供 OEM 应用开发：

腾讯云引擎为所有移动应用，提供统一的安全类功能，如应用程序监视、加载/释放、控制、调度等，也提供健康管理类功能，如移动终端体检、电量管理、任务与进程管理、启动管理、软件评测、终端性能、用户喜好分类、健康应用组合推荐方案等；并且能通过开放API提供给合作伙伴进行安全引擎的调用 ,合作伙伴不需要自己开发安全与健康管理引擎，就能轻而易举地开发出专业的安全与健康管理类OEM应用。

2、提供软件安全检测合作：

与电子市场、论坛、下载网站进行软件认证合作：电子市场、论坛、下载网站通过接口把软件传输到MTAA云查杀平台，云查杀平台对这些软件进行多方位的安全检测，并给出可靠的软件安全结论。

技术实现：合作伙伴通过接口把软件传送到MTAA的云检测平台，云检测平台经过静态、动态、人工三重检测，确保结果的可靠性，并把结果反馈给合作伙伴，力求让合

作伙伴能向用户提供安全的软件下载。

3、提供云查杀合作

与有下载功能的软件进行云查杀合作：包括浏览器类、搜索下载类，使这些软件的用户在下载的过程中就能知道下载文件的安全性。

4、提供健康应用推荐接口：

为有应用下载功能的其他WEB网站、WAP网站、电子市场客户端提供健康应用推荐接口，此接口为个性化的终端提供个性化喜好的健康应用推荐，从而使各下载网站/电子市场能根据用户的喜好类别选择提供更精准的个性化的下载推荐，提升用户的下载转化率与增强用户的使用体验。

3.2.4 厂商/运营商定制应用

各大移动终端设备厂商/运营商都随着用户需求的提升，而有安全性与健康管理的应用预装到终端上的需求。MTAA 拥有多年的与各大移动终端厂商的预装合作经验，同时也在开发预留了厂商、运营商的安全防御、健康管理的个性化需求，按需定制移动终端设备的安全防护环境、健康管理环境。

3.3 MTAA 体系升级前后对比

MTAA 架构在升级前，主要着重在安全防护上，满足用户在移动设备上的安全需求，满足上下游企业在围绕个性化的用户的移动设备的安全需求上提供合作；升级后， 除了安全防护上延续原来的服务与合作模式 ,还能满足用户升级后的移动设备上的健康管理的需求，同时，也提供给上下游企业相应的移动设备的健康管理的接口与合作模式，与上下游企业一起，为最大化发挥移动设备的性能来达到更好的移动生活、移动娱乐、移动商务、移动学习等方面的健康管理需求，而共同打造更丰富的产品、服务、应用。

第四章：MTAA 升级之后对产业链的影响

4.1 腾讯移动安全实验室

腾讯移动安全实验室是基于MTAA的策略 ,为腾讯无线安全产品的开发与技术实现提供测试、验证的平台，并向业界以及合作伙伴提供和分享面向应用的最佳实践，是一个开放、增值、孵化产业链生态的坚实平台。

更多信息请关注“腾讯移动安全实验室”的微博。

4.2 MTAA战略合作模式

针对不同行业、产业链的不同角色、合作伙伴与终端用户的具体需求，MTAA具有不同的策略与合作侧重点：

1、相关机构/组织

中国互联网协会、国家计算机病毒应急处理中心、计算机病毒防止产品检测中心、中国反网络病毒联盟、中国软件评测中心等机构与组织，一向重视移动终端的安全与健康，MTAA同样利用自己的优势资源，与相关的机构与组织共同合作，根据不同的组织与机构需要，采用定制化的分享资源、分享技术、合作产品等合作模式，为中国的移动互联网网络安全、移动终端安全出自己的一分力量，助力发展健康的产业生态。

2、移动运营商

在信息产业链的上游 ,移动运营商既是移动网络的建设者 ,也是移动应用规则的制定者。移动运营商在硬件、通道、终端各个层面都存在着非常直接内在的安全需求。特别是在手机终端应用领域，由于直接面向终端消费者，关系到客户关系的运营维护，运营商更

是高度关注。包括手机号码、手机通话、短信等隐私信息的安全；代收费安全；移动商务电子支付安全内容等等遍及各个细节。目前垃圾信息对用户的持续不断的骚扰、诈骗信息的日益泛滥、吸费电话的持续轰炸等等都给用户带来了直接或间接的经济损失或威胁。因此，运营商手机安全领域的安全需求尤为突出。

腾讯移动安全实验室MTAA的解决方案专门针对运营商关注的上述问题，提供从终端到云端的全方位安全解决方案，为手机用户切实防范潜在安全威胁，从根本上防止产生经济损失。还包括其它方面，如针对扣费病毒木马的主动扫描防御、针对手机运用中各种帐户与密码的保护、对应用程序的访问以及权限控制、对各种私隐信息的主动保护，对垃圾短信、诈骗短信、吸费电话的智能拦截，等等，所有这些，都致力为运营商提供终端安全的全面支撑，并协助营造健康的网络通道与健康标杆应用。

3、金融机构

与金融领域的大型银行进行战略合作，帮助银行、证券等金融机构进行与用户资金交付相关的支付平台的信息安全建设，以及完善支付平台各项功能，提供移动终端设备的交易安全环境的保障，协助完善健康的无线领域的金融支撑。

4、移动终端厂商

与国内外知名移动终端厂商如：诺基亚，中兴，华为，酷派，金立，联想，天语，康佳，海尔等进行战略合作，在其推出的智能平台手机中全面预置QQ手机管家，为用户提供安全的手机应用环境，并通过移动安全实验室作为技术支撑，共同提升整个产业链的价值合作，支持健康的终端发展。

5、下游厂商

MTAA还覆盖与产业链的下游厂商合作。包括，电子市场、论坛、下载网站、手机专卖店、手机卖场等，提供安全认证、云查杀等合作；提供用户喜好类别与健康软件匹配的各种推荐组合参考，创造健康的合作共赢局面。

6、应用开发厂商/开发者

与优秀的移动终端应用开发者、个人开发者合作提供软件接入合作，共享亿万级的用户流量，并提供多种市场数据分享与建议，力求为更多的开发商/开发者提供更精确的用户信息，使其能开发更多的满足多样化的用户需求的产品、服务、应用，鼓励健康的创新开发。

4.3 MTAA升级让移动互联网产业链绿色健康

MTAA的升级，首先提出了手机健康管理的理念，并围绕着手机健康管理升级MTAA构架与开放平台，进一步使产业链由原来的手机安全防护转移到更着重用户手机的健康管理，在关注手机安全基础性需求的同时，也开始关注手机健康体检、系统优化、流量监控、联系人云备份、软件管理等各类手机健康管理。

因此，MTAA升级之后，手机安全市场将催生更多新的更细分市场，这将引起从上游运营商、移动终端生产厂商，到下游的电子市场、下载网站都将自己的产品和服务往满足更为安全健康和个性化的用户需求上转变。这就意味整个移动互联网产业链都变得绿色、健康起来，从而推动移动互联网健康快速的向前发展。

术语列表

LBS：基于位置的服务(Location Based Service)，它是通过电信移动运营商的无线电通讯网络获取移动终端用户的位置信息，为用户提供相应服务的一种增值业务。

MTAA：腾讯终端安全架构（Mobile Terminals Assurance Architecture）。

Android： Android 是 Google 开发的基于 Linux 平台的开源手机操作系统。

API：应用程序编程接口(Application Programming Interface)。

Root：Root是Linux系统中唯一的超级用户，具有系统中所有的权限，如启动或停止一个进程，删除或增加用户，增加或者禁用硬件等等。

Hook技术：计算机术语，一般是指对正在运行中的函数地址进行重定向，达到截获函数调用的目的。

Inject技术：计算机术语，一般是指对一个正在运行中的进程注入片段，并通过修改进程运行地址，达到运行被注入代码的目的。

Pm指令：Android平台上提供的一个命令，可以直接用安装包进行操作，如删除，安装等。

Activity服务：Android平台上的一个本地服务，负责各个APP的数据读写、服务开关、界面跳转等功能。

Sms服务：Android平台上的短信服务。

Phoneinfo服务：Android平台上的话机信息服务。

Input服务：Android平台上的输入法服务。

Cookies：指某些网站为了辨别用户身份、进行session跟踪而储存在用户本地终端上的数

据。

IMEI码：是国际移动设备身份码(International Mobile Equipment Identity)的英文缩写，是由15位数字组成的"电子串号"，是每台手机在全世界的唯一标识码。

IPTABLE技术：指静态防火墙技术，对进出计算机的数据包进行过滤的技术。

Symbian：Symbian 操作系统是 Symbian 公司为手机而设计的操作系统，诺基亚原主流手机机型主要采用此系统。

iOS :是由苹果公司为 iPhone 开发的操作系统。它主要是给 iPhone、iPod touch 以及 iPad 使用。

OMA :开放移动联盟(Open Mobile Architecture),它的宗旨是寻求一种与系统无关的、开放的，使各种应用和业务能够在全球范围内的各种终端上实现互联互通的标准。

SyncML：平台无关的信息同步标准协议集(Synchronization Markup Language)，分为 SyncML 数据传输协议（ SyncML-DS ）和 SyncML 设备管理协议(SyncML-DM)。

VCard：电子名片的文件格式标准，vCard 可包含的信息有：姓名、地址信息、电话号码、URL，logo，相片等。