



技术白皮书

SecureIT Mobile 企业版

企业移动三大支柱:

安全、隐私和自由

Rob McCammon

产品管理副总裁

Open Kernel Labs, Inc.

2011年2月

内容

简介	3
企业移动三大支柱	3
谁应该阅读这份白皮书	3
企业移动	4
移动趋势 — 2011年	4
挑战	5
现有方案的缺陷	7
SecureIT Mobile 企业版介绍	8
背景	8
方案架构	9
安全企业移动	10
结论	12
即将在手机和平板电脑上实现	12

简介

该白皮书介绍了移动计算中一种重要的新兴模式——企业移动。白皮书集中探讨了移动/无线和决定企业移动的企业IT之间的融合趋势，以及满足这一形式安全实践要求的途径。

企业移动三大支柱

有效的企业移动需要三大支柱：安全、隐私及自由。该白皮书探讨了支撑这些支柱所遇到的挑战，以及OK Labs的新产品，SecureIT Mobile企业版如何能够满足以下实际需求：

- 安全部署企业应用和安全接入企业数据服务
- 保护用户隐私以及隔离员工与企业资产
- 使用所有设备功能的自由，包括安装应用和自由浏览网页

该白皮书提出了一种重塑现有企业移动实践的方案，该方案巩固并加强了这三大支柱，且基于移动虚拟化而构造。

谁应该阅读这份白皮书

该白皮书旨在帮助以下企业和个人理解企业移动的定义及推出将会遇到的挑战：

- 企业：首席信息官（CIO），首席安全官和IT主管
- 移动运营商：方案设计师和企业细分市场专家
- 设备OEM厂商：产品经理和系统软件设计师
- 芯片方案提供商：产品经理和系统软件设计师

企业移动

“企业移动”这个词逐渐占据了商业和技术报道的头条，究其原因主要是移动/无线生态系统正努力为以下两个交叉的现象营造有利环境：

- 与日俱增的移动劳动力
- 无处不在的移动设备和运行在这些设备上的应用

企业移动的条件究竟是什么？让我们来看看Forrester Research给出的定义：

企业在任意地点保持联络和控制资产的能力。支持企业移动的技术包括无线网络、移动应用、中间件、设备、安全和管理软件。

这个定义不仅准确，还留有丰富的想象空间——包括联系什么人、联系这些人的原因以及因为什么原因而控制哪方面的资产？此外，这个定义还提出了更深层面的问题——企业移动与传统企业连接有什么不同？对于这些问题，我们可以从以下趋势中找到一些答案：

移动趋势 — 2011年

移动劳动力：当今许多员工都在公司总部以外的区域办公——这一移动员工的群体数量超过了十亿，相当于全球劳动力人口的三分之一（Forrester数据）。这些人员同样需要访问公司数据、建立文档、通过公司邮件进行交流，以及利用智能手机和平板电脑远程访问公司应用，这些都是他们在办公桌前所要进行的日常工作。

企业IT的消费化趋势：在十年间或者更长的时间内，企业员工享受到了在办公环境和工作往返途中公司提供办公设备的便利，包括移动电话、笔记本电脑和其他设备。现在，公司和员工都愿意利用员工自己的设备——40%的公司已经实现了这一目标（Juniper Networks数据）。用自己的设备工作（BYOD）不仅节省了购买和维护成本，还可以让员工选择和使用符合自己生活方式和工作习惯的智能手机和平板电脑。

开放移动操作系统（OSes）：当今越来越多的智能手机和平板电脑开始部署开放及开源操作系统（OSes）——包括Android、Linux等。在加速开发和鼓励创新的同时，当今构建于社区的平台逐渐主宰了移动领域。

应用市场：2010年是移动应用年，开发商们为iPhone、Android和其它平台打造了成千上万的应用，智能手机和平板电脑所有者们也相应地进行了数十亿次的下载。然而不幸的是，这些市场提供的应用在质量和安全性能方面参差不齐。因此，首席信息官（CIO）难免会担心员工喜爱的游戏、应用和社交媒体客户端会直接导入病毒、间谍软件和其它威胁。

云计算的应用：就企业和SMB而言，IT部门越来越倾向于将数据中心虚拟化，因为这些数据中心往往会占据整个地下室甚至是整座建筑。将企业应用和数据过渡到云的过程与企业移动紧密相连——访问分散的财产同样也可以分散进行。

挑战

以上趋势反应了一个令人振奋、日益凸显的现实。然而，这些趋势——主要是企业移动的趋势——也为企业IT带来了新的挑战和顾虑。

移动设备配置和管理

从企业IT的角度来说，智能手机、平板电脑以及其它移动/无线设备对配置和管理所带来的挑战是我们熟悉的笔记本电脑和台式电脑不会有的：

- 部署路径——许多移动设备必须通过运营商渠道来配置——而不是直接通过企业IT人员进行编程。
- 部署机制——在移动设备上安装软件和实现服务通常涉及“空中”交易，而不是磁盘安装或本地配置——许多移动设备甚至没有用户能够看到的文件系统。
- 设备管理——移动设备管理（MDM）通常属于要么全有要么全无的状态：IT人员或管理整个设备，或退一步完全让运营商或用户全权负责。MDM软件在不断变革，以为IT人员提供更为精细的控制。然而，因为他们很难或者无法控制工厂安装（预装）的软件，移动和桌面管理功能之间还是存在一大片空白。

安全

在过去十年中，企业IT已经解决了桌面系统的安全性。现在，移动设备是公认的企业安全链中最薄弱的环节

手机、平板电脑和其它无线设备是公认的企业安全链中最薄弱的环节。尽管桌面系统的安全性也还存有诸多变数，但是企业IT已经能够应对这个环境，而且拥有优越的工具和程序来保护运行Windows和其它桌面操作系统（OSes）的PC、工作站和笔记本电脑。

然而，保障移动设备的安全性使IT专家们想起了十年前应对桌面系统的情景。现存的威胁已经不容忽视——在过去12个月中，移动软件遭受的威胁上升了250% (Juniper Networks数据)。

恶意软件和其它攻击

随着移动设备变得更为强大和复杂，这些设备也成为世界黑暗势力更大、更具诱惑的“攻击界面”。危险的内容和从应用商店下载的程序、基于网络的攻击和无线网络的破坏等更增加了移动设备的复杂性。因此针对移动设备软件的威胁包括：

- 下载应用中的病毒和间谍软件
- 系统和用户软件中的零时差攻击
- Android等开放平台的操作系统（OS）级别攻击
- 防病毒软件和MDM软件自身面临的威胁

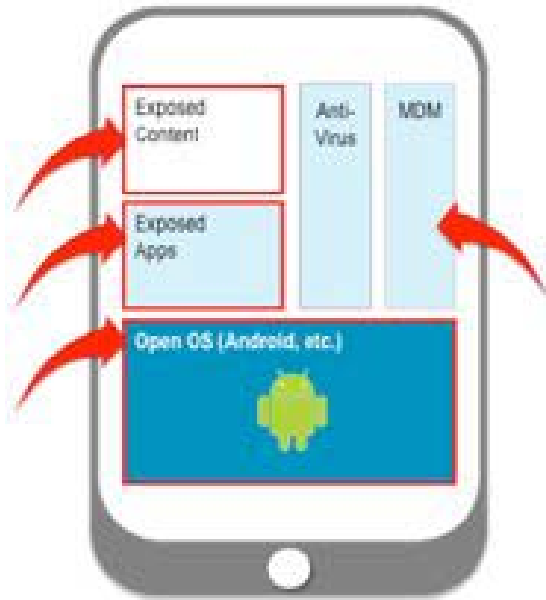


图 1: 移动软件面临的威胁.

安全访问

企业移动的价值体现在提供访问业务数据和程序的通道，提高员工的工作效率。利用移动设备危险渠道打开关键业务数据库和应用的可能性，是抑制企业移动发展的关键因素之一。这个渠道的威胁来源于设备自身，并祸及本地数据、应用和浏览程序。此外，这些威胁还会殃及数据中心和云上的企业资产。

隔离资产

内部主要安全威胁之一是个人和企业资产掺杂在一起。这些资产包括各种类型的应用和数据，比如个人财务与企业的财务信息，私人邮件与公司邮件，家电与企业工厂运营与自动化。

隐私和功能性

如果必须携带功能受限的设备，且个人生活受到影响，用户将只能继续携带两部设备：一部用于工作，另一部用于个人生活。

对企业移动的大部分讨论都以公司管理优势为起点和终点，涉及的话题包括如何提高员工工作效率和降低主要设备和操作成本。如果公司真的希望最大化自己的移动投资回报（ROI），就必须考虑移动工作者的需求和习惯。公司如果忽视员工的爱好，企业自身发展也会受到威胁。如果必须携带功能受限的设备，且个人生活受到影响，用户将只能继续携带两部设备：一部用于工作，另一部用于个人生活。

锁定设备

企业移动安全的一个捷径是采用完全锁定的设备，即该设备只能用于访问企业数据。在过去，这意味着公司提供一部电话；在今天，在携带个人设备（BYOD）这个概念出现以后，完全锁定的设备就意味着限制员工使用自己的设备，以减少以上提到的安全威胁。

员工隐私

在企业移动应用中一个经常被忽视的因素是企业安全的反面——员工隐私。如果为了在一部设备上保护企业数据，而向企业审查系统暴露私人用户信息和应用，那么用户也不会使用这一设备。

应用选择

用户在智能手机和数据计划方面投入的主要动力是可以访问有趣的应用和服务，这些应用和服务包括游戏、生活方面应用及视频。如果将这些用户喜爱的应用和服务列入黑名单并阻止使用，打击了用户投入的积极性，那么企业的移动制度也不会获得成功。

现有方案的缺陷

当今的企业移动涉及终端安全、防病毒（AV）软件和移动设备管理（MDM）软件套件，它们存放在设备中，以及数据中心和云的网关服务器中。这些技术很有必要且很强大，但却满足不了关键需求。尤其是MDM和安全性有赖于智能手机底层OS和软件栈的完整性，而这恰恰是最易受攻击的部分。

防病毒软件

与网页相关联的桌面计算是恶意软件的攻击目标。在过去十年中，全球每年因为恶意软件造成的损失高达150亿美元(Computer Economics数据)。随着智能手机和平板电脑的兴起，移动恶意软件也开始蠢蠢欲动，妄图步其后尘。同时，智能手机遭受攻击的比例可能是Windows PC的两倍(SANS Institute数据)。

在桌面系统中，因为出现新的恶意软件和攻击界面，防病毒软件销售商和平台及应用供应商也在不断提供更新和补丁。对于IT团队来说，最好的实践经验就是及时评估和应用这些补救措施。另一方面，对于移动设备软件来说，要跟上恶意软件不断演进的步伐则更加困难。现在的移动平台更多（Android有多个部署版本，iPhone, Linux, RIM OS, Symbian, WindowsMobile/Phone等），并且应用也日益增加（截至2011年1月末统计的数据，针对Android平台的应用就有20万种）。

对补救措施的支持问题同样重要——移动软件更新速度有待改进。虽然对于设备OEM厂商和运营商来说，移动软件现在能够达到供给平衡，但就其更新速度而言，还远远落后于桌面系统。这一频率上的差距是由最初的预装部署、推出和安装固件无线（FOTA）更新以及终端用户忽视软件维护造成的。此外，防病毒（和移动设备管理）方案自身也容易遭受侵袭和攻击，并成为被感染目标。

移动设备管理(MDM)

集成移动设备管理软件填补了许多企业移动方面的空白，涉及应用配置、安全策略执行、设备定位、支援、清扫和其他管理功能。由于MDM趋向于横向的综合方案，因此同一家厂商的方案是最好的选择。然而，这一趋势在简化购买支持过程的同时，也会导致集成的方案泛泛肤浅，忽略针对所有功能的顶尖性能集成。

MDM软件通常涉及底层固件、系统软件和应用中间件组件。就MDM自身而言，该系统至少在部分程度上是依赖移动操作系统（OS）集成和移动网络的完整性。因此，如果其中一个遭受攻击，也会严重影响到MDM软件。

SecureIT Mobile企业版介绍

为了迎接企业移动的挑战和填补现有方案的空白，OK Labs公司推出了SecureIT Mobile企业版。通过基于OK Labs公司内核移动虚拟平台OKL4 Microvisor，SecureIT Mobile企业版重塑企业移动性。此外，该产品完善和巩固了MDM、防病毒和其他移动技术，并且实现了安全、隐私和功能的完美组合。

作为一款软件和服务方案，SecureIT Mobile企业版可以帮助企业与个人应用平行部署和管理企业应用及服务。利用OKL4安全HyperCells（虚拟机），SecureIT Mobile企业版将关键业务应用与个人应用、服务和数据隔离开来。

通过在一部物理设备上同时支持开放个人域和可靠企业域，SecureIT Mobile企业版满足了个人和企业的双向需求。

背景

SecureIT Mobile企业版源自安全和认证的系统。2010年, OK Labs公司针对国家防御、紧急救援和公共安全发布了SecureIT Mobile 政府版。利用SecureIT Mobile政府版, OK Labs公司帮助OEM厂商、集成商、政府承包商和政府部门使用COTS移动硬件, 构建了类似奥巴马黑莓¹的设备, 并且价格只相当于传统定制系统成本的几分之一。

基于SecureIT Mobile企业版, OK Labs公司为企业移动带来了军用级安全性。

¹ <http://techcrunch.com/2009/01/23/up-close-with-the-obamaberry/>

方案架构

移动虚拟化

SecureIT Mobile企业版基于成熟且广泛部署²的OKL4移动虚拟化平台架构。此外，该产品采用了片上存贮管理和ARM等现代微处理器的特殊执行功能，其核心和数据中心虚拟化一样，都是纯硬件管理程序。

坚固的隔离系统

该产品是一款虚拟化企业移动方案，实现了可信（企业）及非可信（个人）操作域之间的坚固隔离。

公司信息和个人数据应用被安排在了不同的OKL4安全HyperCells里，这些区域之间相互隔离，并且在独有的一个或更多移动操作系统（OSes）环境中运行。

安全基础

开发商在开发移动设备和移动软件时，需要最大的灵活性设计原型、开发和测试平台及应用程序。在可以“松绑”和实地部署设备和应用时，设备OEM厂商、集成商和运营商必须退后一步，再次确保整个软件栈的安全，包括操作系统（OS）、设备驱动、网络、中间件和应用程序——这就意味着数千万条源代码。鉴于安全挑战如此庞大，移动设备遭受日增攻击威胁的原因也就显而易见了。

相比较而言，SecureIT Mobile企业版基于底层安全性，以及专为OKL4 Microvisor开发的小巧、可信的计算基础。

基于微核的架构

OKL4 Microvisor以成熟高性能的微核技术为基础。微核确保了为小巧可信计算基础而设计的特权模式下运行的编码数量最少。简单一流的架构涵盖了精细的访问控制机制，这一机制在设计过程中（而不是事后）就确保了OKL4的安全，并为开发商和集成商提供了简易安全的机制，实现跨域共享资源，包括设备驱动和CODEC。

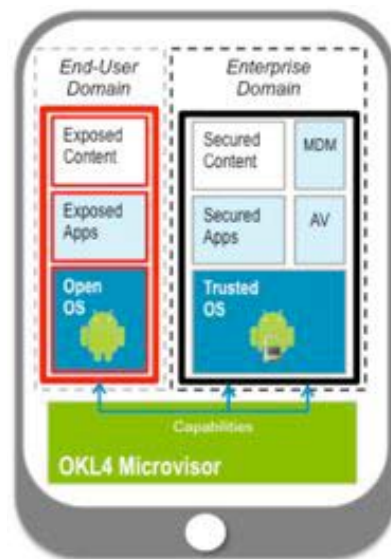


图 2: SecureIT Mobile企业版软件架构

² 手机上的部署至今已超过了11亿

安全企业移动

通过隔离和保护，SecureIT Mobile企业版为企业安全策略提供了“坚固的”支持：

- 敏感文件和数据库
- 本地及远程应用及服务器
- 语音和文本通信（例如SMS）
- 防病毒和防恶意软件的软件
- MDM和其他用于远程控制和管理的代理

让我们来了解一下提供这种保护的意义：

保护本地和上游数据

通过隔离用户和企业域，SecureIT Mobile企业版使本地和远程企业数据免遭攻击。就设备层面而言，SecureIT Mobile企业版为业务着急数据提供安全保障。

SecureIT Mobile企业版还保护了上游数据和基础设施。“Golden Master”软件涵盖了与公司数据实现交互的所有组件和服务，并且部署于企业域之中。该软件不会遭受来自用户域的恶意软件和攻击的威胁（图2）。即使移动用户下载和安装了包含病毒、间谍软件和其他危险的应用，恶意软件还是无法进入企业域，上行到存放企业数据、服务和MDM方案的服务器和网关。

为保护者提供保护

之前在这份白皮书里，我们注意到在帮助保护移动设备、防病毒、MDM及其他安全的同时，管理和远程控制软件自身也容易遭受攻击（图1）。通过在可信企业域里部署“保护器”，我们可以将其与用户下载软件中的威胁隔离。基于这一安全定位，防病毒软件可以扫描企业域和用户域。同样，MDM也可以选择性的管理一个或两个空间内的应用和内容。

为了实现更高的安全性，SecureIT Mobile 企业版支持在专用虚拟机上部署防病毒、MDM 及其他重要软件。基于微核的 OKL4 提供了应用程序接口，开发商利用 OKL4 轻量级执行环境，为安置现在的独立软件和推动与未来其他个人和企业软件的重新部署，包括不同的操作系统和应用。

完善移动设备管理

SecureIT Mobile企业版为MDM软件提供了增强的基础，完善——有时甚至是超越了——MDM功能。让我们来看看MDM的主要功能，以及SecureIT Mobile如何使这些功能更加安全和完善：

数据跟踪：SecureIT Mobile为资产跟踪软件和设备标识数据提供了一个安全的执行环境。定位软件运行可以远离下载间谍软件和其他攻击的探测系统。移动用户需要的定位信息（GPS数据、定位服务等）也可以在企业域和用户域上实现安全有选择性的共享。

备份：在企业域里，关键业务数据、应用和配置数据可以安全地备份到数据中心或云存储空间，并且完全不受用户域操作的影响。

设备清扫/还原：万一设备丢失、被盗或用户部署状态变更，MDM软件可以完全清除（和还原）企业域中的数据和应用。同时，还可以保证用户的个人软件和数据不受影响，设备基本可以还原到他们投入业务应用之前的状态和操作。

FOTA：无线下载固件是众多移动设备中的功能，然而，很多时候这一功能都没有得到充分利用。在通常情况下，配置和管理软件运行于移动操作系统“下层”，通过限制FOTA的可见性和访问驻留在操作系统上软件的精度，这些软件可以帮助升级和操作系统自身运行。有了SecureIT Mobile企业版，FOTA代理软件可以驻留在特定虚拟机上，可以更容易管理和更新其他虚拟机内容，无需要消耗资源的补丁和补充。

的确，移动虚拟化还实现了新版本的无线虚拟化（VOTA）。其不仅将虚拟化引入了移动设备，还利用这一关键技术升级固件、系统软件和应用程序。

故障修复与诊断：基于在多虚拟机上的实践能力，基于OKL4的SecureIT Mobile企业版成为了诊断软件的最佳环境。软件探测可以与企业应用平行部署或占用特定虚拟机。

针对操作系统和应用程序的升级：SecureIT Mobile 企业版可以帮助执行和协调软件升级机制。系统软件 and 关键业务应用的升级可以在企业域中进行，不会影响用户域中应用的运行，反之亦然。既然每个域都由独一无二的虚拟机负责，那么每个域都可以在不互相影响的前提下重新启动。

结论

本白皮书阐述了OK Labs公司的SecureIT Mobile企业版如何支持企业移动三大支柱 —— 安全、隐私和自由 —— 在移动虚拟化的帮助下。此外, 该白皮书还从企业管理、企业IT和移动办公等多个方面分析了企业移动面临的挑战, 也为这一宝贵的体系进行新的可行性研究。

采用SecureIT Mobile 企业版之前:

- 企业安全和管理软件限制了提高用户工作效率的设备功能
- 员工排斥公司设备, 支持更个性化更灵活的个人设备
- 携带个人设备 (BYOD) 不是发展方向, 并且企业移动的投资回报 (ROI) 也会频频让人失望。

采用SecureIT Mobile 企业版之后:

- 员工携带个人设备工作, 会很乐意让公司安装企业移动方案, 因为不会泄露隐私和影响设备功能。
- 满足企业安全和管理需求
- 企业对工作效率的提高感到满意之后, 允许员工使用他们喜欢的软件和服务

如果您的组织正在考虑实施企业移动, SecureIT Mobile企业版可以通过以下方式, 为您提供方便开展和提升投资回报 (ROI) 的突出优势:

- 确保用户隐私及充分使用设备功能的自由, 提高了企业移动的使用率和投资回报 (ROI)
- 防止恶意软件和其他攻击通过手机, 或上游的云和数据中心到达企业应用和数据
- “为保护者提供保护”, 防止恶意软件影响防病毒系统和MDM软件
- 确保高价值设备和软件功能可用, 帮助员工提高工作效率
- 为安全策略框架提供OKL4功能, 针对域间资源共享和应用程序接口(APIs)提供精细控制

即将在手机和平板电脑上实现

OK Labs公司正与移动设备OEM厂商、集成商、移动/无线运营商和其他生态系统成员紧密配合, 加速实现SecureIT Mobile企业版的独特价值和功能。让OK Labs公司携手您和您的供应链伙伴, 寻找贵企业通向企业移动的捷径。

详情请登录 <http://www.ok-labs.com/>, 或通过电话+1-312-924-1445 和邮箱 info@ok-labs.com 联系我们。