IBM Security
思维领导力白皮书

满足 Android 用户需求

Android 以甜品命名的更新能否提高设备和数据安全以胜任企业工作?

IBM

Android 准备进军企业市场。您的企业准备好使用 Android 了吗?

简介

Android 长期以来一直统治着消费市场。如今，Google 和设备制造商在安全方面取得了最新进展，加上领先的 EMM 解决方案提供商支持 Android，使得它在企业市场的影响力不断扩大。为了帮助确保安全性并遵守行业标准和政府法规，企业需要找到一种方法，来保护和管理各种可用设备、版本以及世界上最受欢迎的移动操作系统的各种特性。

这种情况并不是一款解决方案就能满足的。IT 需要检查设备及应用程序环境，然后确定哪些安全和管理功能在定制的企业移动战略中至关重要。MaaS360®提供实现 EMM 的灵活方式，通过像它这样的平台，企业可以利用本地设备和操作系统控件、数据容器化和基于云端的可扩展性，从而自信地接受 Android。

尽管公司目前允许员工使用他们自己喜欢的或行业特定设备，但 IT 必须解决保护企业数据和提供标准化管理时遇到的切实问题。

Android 几乎无处不在：有利有弊

Android 拥有全球 84% 的移动设备市场份额，[1]为全球 190 多个国家/地区的数亿台移动设备（工作和玩耍）提供支持。它在任何移动平台都拥有最大的客户群，并且仍在继续增长。市面上具有各种各样的 Android 设备，这意味着它们通常能够出色地满足企业拥有的设备程序。举例来说，许多现场员工需要坚固耐用的 Android 设备，以便经得起灰尘、电击、震动、雨水、湿气、太阳辐射、海拔高度和极端温度。其他人则希望 Android 设备具有数据捕获功能，能够完美进行库存控制和仓库操作。

这种增长带来了一些意想不到的后果，同时也为 IT 带来了一些重要考量。尽管公司目前允许员工使用他们自己喜欢的或行业特定设备，但 IT 必须解决保护企业数据和提供标准化管理时遇到的切实问题。

尽管它是全球最受欢迎的移动平台，但安全记录也并不稳定；[2] 不过，Android 最近推出了名字甜美的版本 4.0 (Ice Cream Sandwich, Jelly Bean and KitKat)、5.0 (Lollipop) 和 6.0 (Marshmallow)，帮助弥补了过去最大的安全漏洞。在操作系统端，Android 4.0 支持加密，采用全新的密钥链框架进行认证管理，并且可以防范诸如内存利用等复杂的攻击。Android 5.0 会为用户自动开启许多关键的安全功能，包括锁屏、设备加密和设备管理器（有助于查找或远程擦除丢失的设备）。Google 还为安全增强 Linux (SELinux) 规定了强制模式，其实质是限制应用程序和用户的权限，从而防止系统上的安全漏洞。为了帮助在企业环境中启用 BYOD，Android 5.0 中新增受管配置流程，可以在设备上创建受保护的工作配置文件。在启动器中，应用程序与工作角标一起显示，以表明该应用程序及其数据由 IT 管理员在工作配置文件内进行管理。

个人及工作配置文件的通知显示在统一的视图中。每个配置文件的数据彼此独立，即使两个配置文件使用同一应用程序时也是如此。

Android 5.0 还为手机和平板电脑提供访客模式，让您可以固定（或锁定）应用程序，从而使用户无法访问设备的其他部分。这也是一个绝妙的方法，可以使零售网点展示的设备以信息亭模式使用应用程序。

Android for Work

显而易见，Google 一直在倾听企业的心声，了解企业的需求。在准备发布 Android for Work 时，Google 为 IT 提供了容器化和企业就绪安全控制等选项。通过全新的企业管理平台，Android for Work 允许 IT：

- 在 Android 智能手机上区分工作数据和个人数据
- 轻松管理和分配免费和付费的 Google Play 应用程序

Android for Work 将自动集成到 Lollipop，并且可以在任何运行 Android 4.0 以上版本的设备中用作应用程序。

制造商：内置的安全和 EMM 集成

许多顶级的 Android 设备制造商，包括三星、HTC、LG 和亚马逊，也在其最新设备上实施了企业级保护。由于内置功能，如 SD 卡远程擦除和文件加密、企业级 WLAN 安全、VPN 访问以及同时在单一设备上支持公开和加密信息的能力，许多 Android 设备更适合企业使用。

- Samsung KNOX 提供受保护的容器，您可以用以管理、维护和保护企业情报。
- HTCpro 认证的设备提供政府级别的数据加密，以及 VPN 和其他高级安全功能。
- Amazon Fire 设备具备加密功能、VPN、单点登录和证书注册功能。
- LG 支持 GATE 的移动设备提供先进的安全可管理性，支持增强的 Microsoft Exchange ActiveSync、数据加密和 VPN。

这四家及其他 Android 设备制造商不仅启用了关键安全功能，而且与行业领先的企业移动性管理 (EMM) 解决方案提供商结成了合作关系。EMM 集成和 API 使企业能够通过单一门户体验强大的管理和安全功能。

最佳实践与功能

鉴于 Android 版本 4 和版本 5 广泛采用安全增强功能，IT 应该强制规定所有设备都要运行 Android 4.0 或更高版本，并且都要进行密码保护。这将大大减少碎片化和没加密造成的“传统 Android 风险”。当 Android 的灵活性让企业（和用户）满意于某些最佳“合用”设备时，它也带来了风险，需要 IT 保护企业数据并实施安全措施来防范根权限获取和移动恶意软件。

高风险的根权限获取：企业之大忌

用户可通过访问 Android 设备的 UNIX 核心“获得根权限”，这样他们便可以安装包括恶意软件在内的几乎任何应用程序，并破坏应用级控制。被“获得根权限”的设备会使企业网络面临受该设备上同一恶意软件感染的风险，并且覆盖数据丢失保护。

数据丢失：业务就在您的口袋中

还记得过去的美好时光吗？主力台式机想受到威胁都难！而现在，当数据在设备间迁移时，极易受到攻击。具有可移动 SD 卡和 USB 连接的设备很容易丢失数据，即使数据经过加密也是如此。在不安全的 Wi-Fi 区域传输数据同样具有风险，而且企业数据丢失或泄露会招致巨额罚款，并且失去客户的信任和忠诚。

移动恶意软件：无论是意外还是蓄意为之，都非常危险

在《移动应用安全现状》报告中，[3]Arxan Technologies, Inc. 声称，97% 的顶级付费 Android 应用程序和 80% 广受欢迎的免费 Android 应用程序都被黑客攻击过。由于 Android 用户能够安装任何应用商店中的任何应用程序（并不仅限于 Google Play），所以包含恶意软件或与恶意软件相连的社会工程的应用程序，比例要远远高于任何其他移动操作系统的应用程序。Arxan 发现，即使越来越多的公司走向以应用为中心的创新，越来越多的员工开始利用移动技术，“破解版”移动应用程序仍然随处可见。

即便是 Google Play 商店中被认为无害的应用程序，都有可能破坏您的网络和您的品牌，造成潜在的收入损失、关键数据遭到未经授权的访问、知识产权 (IP) 被盗、欺诈和改变的用户体验。举例来说，如果您的孩子拿您的设备下载了流行游戏 Temple Run，其代码就会访问您的根文件系统、下载缓存，甚至访问设备中所插 SD 卡。它还会通过设备上的麦克风记录音频权利并跟踪您的位置。有了 IBM® MaaS360® App Risk Management 产品，您可以查看所有这些（有点令人震惊）关于 Temple Run 的应用安全详细信息。

要防止这样的漏洞，IT 需要知晓安装了哪些软件，检测移动恶意软件和获得根权限的设备，执行某一级别的黑名单以及根据需要执行合规规则。

如何在 Android 环境下实现 EMM

无论设备是属于公司还是员工，许多 IT 部门都正管理多种设备类型和无数应用程序，并且可能不止一种操作系统。

实现 EMM 的最佳实践：定制以适应您的精确环境和安全策略。

IT 应该针对不同类别的用户、部门、地理位置、设备和应用程序规划移动性管理投资规模，并且运用最能满足这些使用案例需求的技术方法。举例来说，销售人员需要访问客户联系信息和产品数据，而人力资源 (HR) 则需要访问更加敏感的数据，此类信息一旦发生泄漏，可能需要承担合规责任。EMM 既非一劳永逸，也非一视同仁。

MaaS360 有助于满足 Android 用户需求

作为一名技术预览合作伙伴，IBM 与 Google 及三星这样的制造商紧密合作，帮助确保客户充分利用 Android 体验。MaaS360 可直接与 Samsung KNOX 和 Android for Work 相集成。利用 MaaS360，您可以跨多个平台管理各种设备并获得天衣无缝的稳定体验。

通过利用 Google、设备制造商和 MaaS360 提供的功能，IT 可以访问各种移动安全选项以及统一的平台，并从中构建、管理和扩展分层式安全程序。凭借 MaaS360，您可以只部署所需内容，选择有助于保护您的移动世界的个体解决方案，以及您环境中所需要的特定控件。

MaaS360	您可以用它做什么
IBM® MaaS360® Mobile Device Management 您需要的设备生命周期功能	• 根据需要控制访问和隔离特定的设备或 Android OS 版本 • 利用增强的密码、地理围墙规则和情境管理保护传输中的数据 • 检测并限制被获得根权限的设备 • 远程查找、锁定和擦除被盗或丢失的设备
IBM® MaaS360® Mobile Application Management 如何实现智能移动企业	• 通过容器化保护企业应用程序 • 利用基于 Web 的控制台集中管理移动应用程序 • 黑名单、白名单并设置必需的应用程序以停止数据泄露和网络攻击
IBM® MaaS360® Productivity Suite 个人层面的世界级保护	• 区分个人数据和企业数据 • 设置用户层面的角色策略 • 能够进行在线和离线合规性检查 • 擦除套件容器、应用程序容器、企业配置文件或整个服务
IBM® MaaS360® Content Suite 有控制地协作	• 集中管理文档分配，或者以受保护的方式访问现有企业文件商店，例如 SharePoint、Windows File Share、IBM Connections、Box、Google Drive、CMIS 源及其他 • 确保用户在 Android 设备上的加密容器中安全查看、创建、编辑并保存文档 • 跨不同设备类型同步内容，其中包括 iOS、Android 和 Windows 设备
IBM® MaaS360® Gateway Suite 保护入口通道	• 提供受保护的公司数据移动访问，无需设备 VPN • 调动 SharePoint、Windows File Share 和您的内部网站点 • 使用接入企业系统的应用程序内 VPN 通道

MaaS360	您可以用它做什么
IBM® MaaS360® Mobile Threat Management 将攻击扼杀在摇篮之中	• 利用不断更新的数据库提供的恶意软件签名检测应用程序 • 利用近乎实时的合规规则引擎自动执行修复 • 发现试图屏蔽被获得根权限的设备的检测的隐藏者
MasS360 App Risk Management 有助于从应用程序中消除高风险业务	• 通过深入的自动化分析找出数百代码漏洞和高风险的应用程序行为 • 先设计并测试应用程序规则，然后再向业务部门、地理位置或工作组进行部署 • 针对用户设备和企业应用程序商店实施应用程序安全策略

Android 现已正式准备进军企业市场，因此，请与我们联系以详细了解 MaaS360 如何让企业做好使用 Android 的准备。既保护公司数据，又能让用户在自己的设备上无缝访问工作信息。充分利用统一的策略、威胁管理、应用程序分配、设备管理以及标准框架，在不同的 Android 设备上获得一致的体验。如要立即体验 IBM MaaS360 的 30 天免费试用，请转至：**ibm.com**/maas360

IBM MaaS360 简介

IBM MaaS360 是一款企业级移动性管理平台，让人们的工作方式更高效，同时实现数据保护。数以千计的组织信赖 MaaS360，将它作为实施移动性计划的基础。MaaS360 可为用户、设备、应用程序和内容提供具有强大安全控制的全面管理，从而支持所有移动部署。如需了解有关 IBM MaaS360 的更多信息，并开始 30 天的免费试用，请访问：www.ibm.com/maas360

IBM Security 简介

IBM 的安全平台提供安全情报，帮助组织为员工、数据、应用程序和基础架构提供全方位保护。IBM 提供下列解决方案：身份和访问管理、安全信息和事件管理、数据库安全、应用程序开发、风险管理、端点管理、新一代入侵防御等。IBM 是全球最广泛的安全研发和交付组织之一。如需更多信息，请访问www.ibm.com/security

1 “Worldwide Smartphone Shipments Edge Past 300 Million Units in the Second Quarter; Android and iOS Devices Account for 96% of the Global Market, According to IDC”，IDC Worldwide Mobile Phone Tracker，2014 年 8 月 14 日（付费专区），http://www.businesswire.com/news/home/20140814005599/en/Worldwide-Smartphone-Shipments-Edge-300-Million-Units

2 同上，2014 年。

3 “State of Mobile App Security（研究），Apps Under Attack，卷 3（之前的标题是：State of Security in the App Economy)”，2014 年 11 月 17 日，Arxan Technologies, Inc., https://www.arxan.com/wp-content/uploads/assets1/pdf/State_of_Mobile_App_Security_2014_final.pdf

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印制 2016 年 3 月

WGW03108-CNZH-01