IBM软件

利用IBM安全解决方案保护移动企业

凭借久经考验的企业移动计划安全保护经验，实现可见性和可控性

要 点

- 通过企业级安全性应对所有移动风险
- 保护设备，保护对企业资源的访问，实现安全的移动应用程序
- 支持移动员工、合作伙伴和客户提高响应速度和生产力
- 通过可见性和自适应的移动安全方法提高企业对移动环境和数据安全性的信心

技术的采用总是始于企业内部，然后才逐渐普及到消费者市场。但移动技术的出现颠覆了这种模式。已采用移动计算的所有类型、各种规模的企业都看到了它的潜力，移动计算不仅能提供消费者喜爱的通信方式，还能提高生产力和响应速度，并加强创新。到2015年，预计将有约40%的企业设备是移动设备。[1]

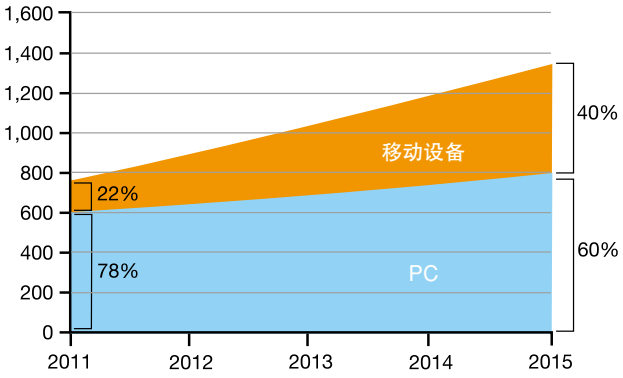
然而，移动技术的采用并非毫无缺点，当今组织最担心的方面莫过于如何管理和降低与移动交互相关的风险。事实表明，为移动设备提供安全性与为企业的其他方面提供安全性截然不同。这是因为移动设备本身与众不同，它们的共享更频繁、使用的地点更多、担当的角色更多，并且技术差异更大。半数的移动应用程序要传输个人详细信息或设备信息。[2]因此，到2013年，恶意应用程序和社会工程所造成的威胁预计将翻番。[2]

为了应对这些挑战，IBM开发了覆盖各IT领域(人员、数据、应用程序和基础架构)的移动安全解决方案产品组合。IBM的各种功能强调自适应的安全方法，可降低成本，因此是安全的，并且与当今的业务环境保持协调一致。对于设计移动服务、将数据和工作负载部署到移动设备，或者使用的信息来自基于移动技术的服务的组织而言，IBM解决方案能满足控制运营风险以及坚守安全性优先事宜等关键需求。

随着移动技术的采用日益增多，移动安全威胁也会增加

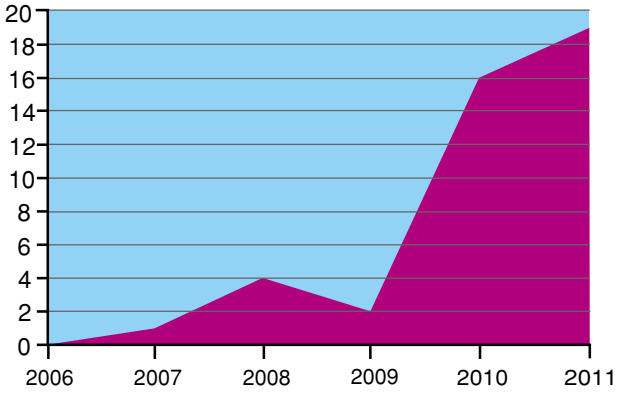
预测得出了值得关注的结果：到2014年，企业中的智能手机数量将达到10亿部，移动员工的数量将达到12亿人。到2015年，大型企业的智能手机用户群将增至原有的三倍。[2]到2014年，85%的大型企业将使用消费者拥有(而非企业专用)的设备。[2]半数的组织计划在12个月内部署自己的移动应用程序。[2]但移动技术的高速采用也伴随着巨大的威胁。维护业务敏捷性以及支持不断变化的员工行为的需求不仅会促使移动设备的使用持续增长，还要求组织设法降低与移动性相关的运营风险。

各类企业设备的增长[1]



移动操作系统的利用情况[3]

2006年-2011年



虽然企业在PC和Internet时代已经积累了丰富的安全经验，但移动技术不但带来了全新的挑战，也使原有挑战发生了演进。稳居威胁列表第一位的就是丢失和被窃的设备，而恶意应用程序、社会工程、恶意软件、身份窃取、数据被窃、恶意网站和拒绝服务也在不断复杂化，并且数量也在不断增加。

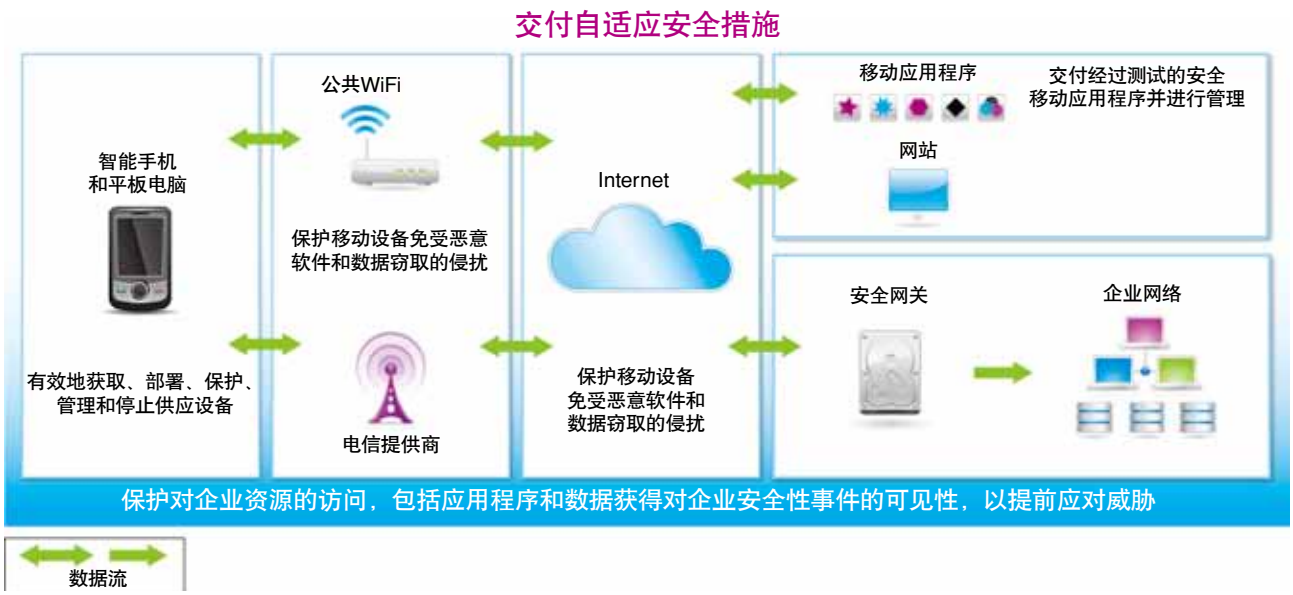
与此同时，平台和应用程序的多样性、企业可见性和可控性的整体缺失，以及证实法规合规性的复杂度日益走高也让IT更难为移动计划提供支持。大多数移动平台最初的设计并未提供全方位的安全性，随着移动设备数量的爆炸式增长，黑客专门针对此类设备开发新技术或发起攻击的动机也变得更强烈了。

因此，组织必须具备必要的工具和流程，以应对专门利用移动技术相关漏洞的威胁，其中包括：

- 允许访问业务或个人帐户的凭据
- 各类敏感数据，例如机密的业务或个人信息
- 设备通信服务
- 可能成为访问其他企业资源的跳板的移动设备本身

跟踪数据的流动

未受保护的终端设备犹如将敏感信息的大门大敞而开。组织需要保护这些设备上的数据，无论此类数据是静止的，还是通过未受保护的网络和基础架构动态传输的。制定企业移动战略时，必须将数据保护作为首要目标。因此，必须设计切实有效的移动环境安全性，跟踪数据的流动，并保护数据免受未经授权的访问干扰。自适应安全措施的设计应包含策略管理和安全智能，以指导整体的计划和各种功能的制定工作，从而在整个移动生命周期内保护数据。



企业内采用的设备多种多样，如果组织采用了“自带设备”(BYOD)策略，这种情况会更加明显，因此首先必须具备综合全面、跨平台的设备和应用程序管理与保护能力。对企业资产的安全访问应包括安全连接，以及管理身份、访问和授权的能力。对移动应用程序执行漏洞测试，以支持组织与客户、员工和业务合作伙伴之间的信任关系。拥有对完整数据流的可见性，这在保证移动安全计划领先于不断增加的威胁方面尤为重要。

在移动世界中，让安全模型适应用户(而不是要求用户遵循各种强制的要求)的能力比在传统IT环境中要更为重要。让安全性适应用户的另一个原因在于，攻击更倾向于针对个人、部门或组织，而不是那种综合性的大规模攻击。必须牢记，考虑移动设备和移动访问时，用户行为会有着明显的差异，因此要更加注重不会影响用户体验。如果安全模型能适应用户的移动环境(例如，位置、所访问的内容类型、具体访问时间或风险概况)，而且能保证对用户体验的影响最低，必将有助于确保满足安全性策略的要求，并且最终有助于保护企业数据的安全。

IBM产品组合确保实现业务驱动型移动安全

IBM以完善的IBM安全性框架作为参考，采用全面的方法来满足移动安全要求。IBM移动安全解决方案能帮助客户应对移动设备管理、访问管理、应用程序安全和安全智能方面的挑战。这些解决方案不仅能提供专注于移动技术的功能，还能扩展和补充现有的IT安全基础架构、策略和过程。IBM解决方案旨在帮助组织在不断变化的移动安全环境中变被动为主动，强调集成化、端到端的安全模型以及整个企业范围内的可见性，并且致力于促进主动式的响应。

人员: 简化身份和访问管理

移动设备逐渐成为许多用户最喜爱的设备，因此避免移动用户的未经授权访问已经成为所有组织的当务之急。然而，要控制移动访问，同时承担与控制传统访问基础架构相同的许多目标，就必然面临着一些特定的挑战。

IBM Security Access Manager for Mobile能对移动用户及其设备执行身份验证和授权，保护对企业资源的访问。这种基础架构适用于所有类型的用户，也能满足移动访问控制所特有的部分要求。IBM Security Access Manager for Mobile提供了可靠的会话管理功能，能防止中间人攻击，也能提供利用多种身份验证和授权模式验证用户和设备的灵活性。它还能集成IBM Worklight，交付无缝的用户和应用程序安全性。

IBM Security Access Manager for Mobile的上下文感知身份验证和授权功能正在开发之中。届时，组织能充分利用移动设备提供的上下文信息来计算风险概况并采用合适的控制措施。

数据: 保护敏感信息的安全

保护敏感数据和降低未授权访问的风险是任何移动安全计划的核心。IBM Endpoint Manager for Mobile为移动设备提供了数据安全性。它将强制要求设备配置符合企业安全策略，利用平台工具来实施数据加密。这种解决方案提供了远程设备锁定以及全部数据和选定数据擦除功能，还提供了可交付防恶意软件解决方案的基础架构。它还能强制要求使用虚拟专用网络来保护敏感数据的通信。

IBM Worklight提供了加密应用程序数据所必不可少的设施和工具，为开发人员提供了应用程序级别的数据安全性。

另外，基于订阅的IBM Hosted Mobile Device Security Management是一种全套式的软件即服务(SaaS)解决方案，通过防恶意软件、防窃取、锁定与擦除特性(所有特性均通过云交付)提供了数据安全性和策略合规性保障。

应用程序: 为移动部署的Web应用程序筑起坚固的防线

不良的编码实践和人为错误，再加上黑客相对较易发现和利用这些漏洞的现状，可能导致应用程序安全性成为企业安全计划中最薄弱的环节。预计企业移动应用程序的数量将显著增加，而安全性必须跟上这种步伐。

IBM Worklight的安全特性支持组织有效地开发、交付和运行安全的HTML5、混合和本机移动应用程序，并提供了直接更新和应用程序验证功能。IBM Security AppScan®能通过开发过程中的静态分析，检测移动Web应用程序、混合移动应用程序的Web元素以及Android应用程序中的漏洞。IBM WebSphere® DataPower®消息保护和XML防火墙功能可保证消息内容的完整性，并保护应用程序编程接口的调用。

基础架构: 保护移动终端和连接

移动终端可以随身携带，因此比传统的固定设备更容易被攻击、丢失、受到感染或入侵。因此，移动设备的管理应从设备的采购和注册开始，一直到通过虚拟专用网络提供安全通信，再到密码和配置的合规性。

IBM Lotus® Mobile Connect支持移动设备安全地连接到后端系统，而IBM Endpoint Manager for Mobile Devices可收集和提供具体设备信息，以评估合规性。IBM Endpoint Manager还可用于识别被入侵的移动设备(包括“越狱”或者“root”过的设备)，并限制此类设备连接到企业网络。

安全智能: 对各种活动和威胁的可见性

每天，对设备、应用程序和访问进行的攻击数量和复杂程度都在迅速增加，因此组织比以往更要注重获得事件和环境的可见性。全方位的可见性能够在他人利用漏洞之前识别这些漏洞，或者在攻击产生效果之前识别攻击。

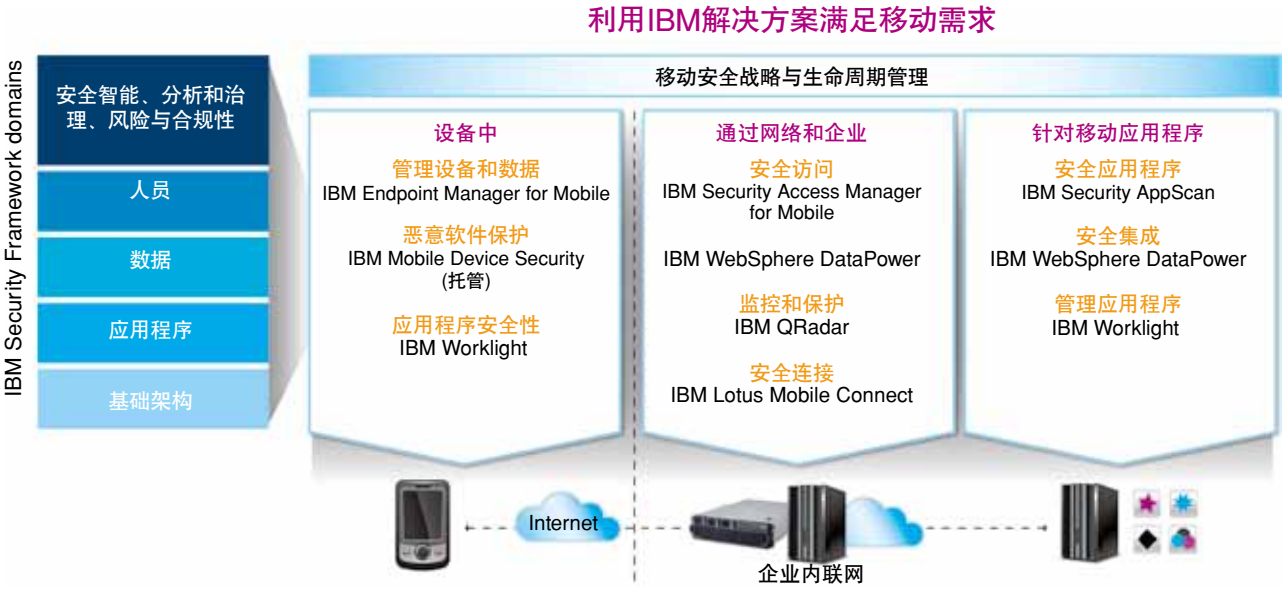
IBM QRadar提供了统一收集、聚合和分析架构，促进了IBM Worklight提供的安全日志、IBM Endpoint Manager for Mobile Devices和IBM Access Manager for Mobile提供的安全事件、IBM Security AppScan for Mobile提供的漏洞数据以及配置文件和网络流量遥测数据的应用。IBM QRadar还包含了取证功能，支持安全调查与审计。

移动企业安全性路线图

无论一种移动安全解决方案的功能有多么强大，如果无法有效地部署或无法轻松地管理它，其价值也会大打折扣。组织需要谨慎评估解决方案的初始部署和长期管理给企业带来的整体风险和必需的工作量。为了帮助企业制定切实有效的移动企业战略和路线图，IBM可以提供一系列全面的专业安全服务，不但可以直接提供给企业，还可通过地方业务合作伙伴提供给企业。

依托于自身的技术领先地位以及与全球各行各业、各种规模组织的合作经历，IBM采用了基于风险的方法，通过以下步骤保护移动企业:

- 保护移动设备:
  - 捕获具体的设备信息并识别不合规的设备；检测“越狱”或“root”过的设备
  - 实施各种安全最佳实践并采取校正措施，包括更新、拒绝访问或删除访问权限、虚拟专用网络配置和交付防恶意软件解决方案
  - 在设备丢失、被窃或淘汰时，远程定位、锁定设备并执行选择性的擦除操作
  - 充分利用单一基础架构提供对广泛企业终端的控制，包括智能手机、平板电脑、台式机、笔记本电脑和服务器
- 保护对企业资源的访问:
  - 为移动用户及其设备部署上下文感知的身份验证和授权
  - 支持适合移动技术的开放标准，例如OAuth
  - 实施强大的会话管理与保护
  - 扩展为保护从任意终端进行访问而采用的基础架构，增加了满足移动计算特有需求的能力
- 交付安全的移动应用程序:
  - 为开发人员提供安全特性支持，包括数据加密、直接更新和应用程序验证
  - 在开发、测试和运行时执行漏洞评估，降低部署不安全应用程序的风险
  - 利用安全的渠道向企业移动用户交付移动应用程序
  - 为移动应用程序提供安全的运行时环境，支持集中化管理与应用程序锁定
- 实现可见性，交付自适应的安全措施:
  - 生成合规性报告
  - 评估安全策略实施一致性
  - 主动响应新兴威胁，适应不断变化的用户行为



IBM成功案例: 欧洲银行交付安全的移动网上银行

考虑到扩展银行应用程序的安全访问以覆盖移动客户，同时加强员工通过移动设备执行安全交易的能力这两个目标，该银行将目标设定为流行的Google Android和Apple iOS平台，并计划在未来支持基于Microsoft Windows Mobile的设备。这家银行利用IBM Security Access Manager for Mobile对请求进行身份验证，利用IBM Worklight平台支持后端服务，通过数据加密和即时的应用程序更新保护了与客户之间的信任关系。

为何选择IBM?

借助IBM解决方案，组织即可支持移动员工，支持与合作伙伴之间的移动协作，并培养客户关系。组织能够在降低风险的同时开辟新的收入渠道。还能确保为移动环境实现有效的安全性，提供移动设备管理、移动身份和访问管理、网络和数据保护以及移动应用程序安全性等功能。

行业领先的IBM X-FORCE®研发团队凭借自身的专业经验指定了可靠、超前的安全方法。该团队提供的报告记录了影响Internet安全性的威胁的所有方面，同时还维护着一个综合全面的威胁和漏洞数据库，为IBM产品提供的超前保护提供可靠的支持。除此之外，该团队还会发布各种警告和建议，提供如何利用IBM产品和服务针对最新的威胁进行保护的信息。

更多信息

如需了解有关IBM移动安全解决方案的更多信息，请联系您的IBM代表或IBM业务合作伙伴，或者访问：**ibm.com**/mobile-security

此外，IBM Global Financing可帮助您以最经济高效的战略性方式获得您的业务所需的软件功能。我们将与信用合格的客户展开合作，定制一个财务解决方案来满足您的业务和发展目标，实现有效的现金管理，以及改善您的总体拥有成本。IBM Global Financing是您进行关键IT投资和向前推进您业务的最智慧选择。有关更多信息，请访问：**ibm.com**/financing

IBM Corporation
Software Group
Route
Somers, NY 10589

在中国印刷
2013年6月

1 IBM预测。
2 Blackstone，“IBM企业移动性”，2011年9月12日。
3 IBM X-FORCE，“IBM X-FORCE 2011趋势和风险报告”，2012年3月。

WGS03003-CNZH-00