



技术透视...

2011 年 4 月 27 日

J.Gold Associates, LLC. 6 Valentine Road, Northborough, MA 01532 USA
www.jgoldassociates.com +1-508-393-5294

企业移动呈多样化发展：7 大举措助您确保移动安全

面对日新月异的企业移动形势，IT 部门在支持和连接新型小工具方面的压力陡增，致使他们无法再像以前那样轻松管理哪些用户可以使用哪些设备。这种压力往往来自企业最高管理层，他们拥有自己的个人设备，而且需要在日常工作中使用。工作模式已然发生了不可逆转的转变。

摘要：

当前，大多数企业都面临着与日俱增的形形色色的移动设备，这些设备往往会令企业面临严重风险。如果企业希望避免大规模安全故障和随之而来的后果和责任，保护这类设备必应成为工作的重中之重。企业应该采取具体、有效的保护措施，使每个用户购买的个人设备都能在保证企业安全的前提下发挥优势。

趋势

据估计，目前有 25% 的企业允许用户自由地选择和部署移动设备，预计这一比例还将继续飞快增长。但是，想要在不增加风险或成本的情况下全盘接收这些设备，对于企业来说是个艰难挑战。认清移动领域出现的一些新趋势可以为您提供更全面的了解。在未来 2-3 年内：

- IT 消费化的出现、自备设备工作以及最终用户确定策略的能力增强都将迫使企业 IT 部门彻底地改变运营方式。
- 未能通过加强可管理性、策略实施和安全评估来支持设备多样性和最终用户选择的企业 IT 部门将被淘汰。
- 企业安全和治理将难以跟上移动设备的普及速度和多样性发展。这将导致严重的数据丢失/泄露，迫使企业重新评估不断发展的“开放式”移动设备策略。
- 随着新模式的日趋成熟，企业不仅需要学习如何评估设备的特性/功能，而且还要学习如何评估设备总拥有成本 (TCO)，就像当前评估其他 IT 资产一样。

所有这些方方面面都意味着企业面临重重但并非不可逾越的挑战。如果方法有效得当，企业完全可以从容管理风险，保证运营有条不紊。本文将指导您如何实现这一目标。

移动安全的独特之处

在制定台式机和服务器策略时，很多企业将安全性视为基石。但对于移动设备来说，安全策略的定义截然不同，特别是考虑到市面上出现的形形色色的产品。部署移动安全时，企业需要全面评估三个关键漏洞。

- **创建中的数据。** 必须尽可能减少用户与应用程序的交互以及应用程序中任何可能遭到恶意软件（病毒、数据泄露、流氓应用程序）攻击的漏洞。
- **设备中存储的数据。** 必须具备保护存储在设备中的数据的能力，包括复杂的密码、强大的应用程序身份验证、板载硬件数据加密等要求。
- **传输中的数据。** 移动设备需要连接。数据传输的保护措施包括加密、VPN 等。

安全事故的代价有多大？

笔记本电脑丢失，几百万条记录泄露，这样的例子不胜枚举。现在许多移动设备都相当于内存容量，而且处理能力与几年前的笔记本电脑不相上下。毫无疑问，32GB 或 64GB 内存的设备（尤其是平板电脑这样的大尺寸设备）将包含大量的敏感数据，例如，客户记录、敏感企业数据等。大多数企业还没有有效的方法来确定设备中存储的数据类型或数据是否已破坏。据估计，每年丢失/被盗的笔记本电脑和手机分别占5%-10% 和 15%-25%。平板电脑丢失/被盗的模式预计会与之类似。一家拥有 5000 名员工的企业每年将可能丢失 500-1000 部智能手机，250-500 部平板电脑。丢失一部包含 10000 条个人身份记录的设备，公司将需要为此付出 258 万美元进行补救（据 Ponemon Institute 统计，一条记录需 258 美元的补救费）。企业级安全的价值常常被低估甚至无视。对于现有和新兴平台来说，部署企业级安全乃当务之急。

安全漏洞：您能接受多大程度的设备多样性

由于设备类型不断增加，IT 部门可以控制的设备数量减少，许多企业已暴露出“安全漏洞”。安全漏洞的程度取决于多个因素，包括

- **设备特点**，例如，加密、密码执行等
- **企业风险情况**，例如，受监管的行业、政府等
- **基础设施改造**，例如，网络和设备管理

- *用户类别*，例如，高管人员、外勤人员、管理人员
- *访问的数据类型*，例如，客户记录、财务信息

安全漏洞是动态变化的。新的流行设备并不总是将安全视为设计先决条件。每个企业都必须经常评估安全、制定相应策略，并根据需要采取补救措施。要使风险和成本最小化，补救措施必不可少。

设备之间存在差异性

对于每部设备，企业都应在使用之前评估其功能。这些设备可以按照从“不安全”（消费驱动型）到“安全”（企业加强型）的不同等级进行分类。安全等级较低的设备必须采取补救措施。许多企业认为支持 ActiveSync 就足够，但它不是首选的安全模式，也不能提供完整的企业功能。目前，大多数用户带到工作场使用的自有设备需要通过第三方产品进行加强。由于安全和设备管理双管齐下，因此大多数补充型安全产品也提供了广泛的设备管理功能，能够最大限度地提高用户工作效率、辅助 IT 部门维护设备功能和安全，并充分降低设备的总拥有成本 (TCO)。由于目前大多数企业都拥有着大量不同的移动设备，而其中许多都需要补充，因此确保对这些设备的有效保护必须是企业移动策略的一部分。

确保企业级移动安全的 7 大举措

尽管移动用户在日益增加，但目前很多企业都还没有一套成熟的移动安全策略。企业必须将移动策略作为一般企业策略的补充来制定，否则将限于始终疲于应对新设备、用户和应用程序的窘境。通过采取独立的举措评估整个企业，可以制定灵活且可持续的移动策略，从而使企业治理环境能够适应日益复杂化和多样化的移动生态系统。这些举措包括：

- *评估 IT 在移动化进程中的角色* — IT 不再按部就班地工作，而是必须保持控制。尽管预算和资源有限，对移动安全可能也缺乏专业知识，但必须适应灵活的设备选择和不断变化的全球市场。
- *确定用户类别及用户需要/诉求* — 应该按企业角色、任务和组对用户进行分类。每类用户都拥有指定的访问权限、设备策略和数据策略。高管人员的权限可以与管理员大不相同。制定明确、精细的策略是关键。

- **定义设备类型和功能/缺陷**— 设备应按操作系统、尺寸和使用情况进行分类。每类设备都应该有具体的相关策略。有些设备可能有足够的本机板载功能，但许多设备并没有。
- **为用户/设备制定和实施有效的策略**— 企业必须定义哪些用户可以使用哪些设备、什么样的数据类型可以存储于什么样的设备、谁制定了策略，以及如何实施策略。用户拥有选择权很好，但一定要权衡特定的可接受使用惯例与严格的实施。
- **了解移动“风险概况”**— 每个企业都有自己的风险概况，包括对合规性要求的评估以及企业所属的垂直行业。所有企业都面临着安全风险，因此必须设置相应的起点。
- **制定和实施“战略计划”**— 企业必须制定战略计划，确定可操作项以便为设备、平台和用户组部署所需的安全增强功能，并定义补充性安全产品要求。选择正确的安全附件对营造安全的企业环境和避免灾难很重要，同时针对快速的变化做到未雨绸缪也至关重要。
- **部署正确的补充产品**— 企业应该根据设备和应用的多样性、安全和合规要求、策略管理和实施以及设备管理和报告来选择解决方案。为了满足各种特定需求，跨平台型产品理应成为企业的首选。

想要充分满足企业的安全需求还有很多工作要做，但上述这些举措构成了构建企业级移动安全环境的基础。

总结

企业应基于整体方法而非针对独立的设备和/或用户要求实施策略。当前的设备和使用模式将不断发展/变化，因此策略的灵活性至关重要。有效的移动策略必须能够平衡安全性、可管理性和最终用户心理三者的关系，这三大因素经常会发生冲突。同时，企业应优先考虑可支持广泛的设备/平台的安全增强产品。大多数企业都需要支持多种平台、设备和尺寸，因此跨平台补救是必不可少的。最后，企业应及时制定前瞻性策略，避免陷入被动应付的“死循环”！



J. Gold Associates, LLC.
6 Valentine Road
Northborough, MA 01532 USA

电话：
+1-508-393-5294

网站：
www.jgoldassociates.com

研究、分析、战略咨询