MaaS360®
by Fiberlink, an IBM company

移动数据安全性

寻找平衡

移动数据安全性：寻找平衡

目录

了解自己的目标 4

选择适合自己的方法 5

根据优先级做出选择 6

三思而后行 7

MaaS360®
by Fiberlink, an IBM company

在保护公司机密数据规避安全风险，以及高效、简单的用户体验之间找到平衡。

移动数据安全性：寻找平衡

*数据泄露防护(DLP)*和*容器*逐渐成为与移动管理有关对话的焦点。过去几年，人们在提供适用于移动设备的管理和安全工具及解决方案方面取得了长足进步；这些工具和解决方案既适用于企业拥有的设备，也适用于员工的自有设备。

尽管这些解决方案可以满足为设备提供安全保护的需求，但是它们却一直未能满足一些在笔记本电脑和分布式网络部署中常见的更复杂的安全需求。特别是缺少笔记本电脑管理解决方案中常用的全方位DLP控制。

小心谨慎的您肯定想通过更多更强大的安全控制功能为移动设备管理(MDM)解决方案作补充，从而防止有人无意或恶意将敏感数据泄露给未经授权的第三方。

了解自己的目标

在研究技术时，您会发现种类繁多的方法。这些方法各有优势和缺陷，而您的首要任务是了解自己的目标。在制定目标和方法配置文件时，您需要在让公司机密数据规避安全风险，以及提供高效、简单的用户体验之间找到平衡。请务必考虑以下事项：

阻止内部人员 – 如果获得授权的用户有意复制数据，那么验证码策略和设备加密将无法阻止他们。而DLP则可以解决这一问题。贵组织可能已投入了大量资金，来控制用户从笔记本电脑和台式机的硬件及软件中移出机密数据。如果是这样的话，请寻找可以将DLP扩展到移动设备部署的方法。组织内对各类设备的策略和目标应该保持一致。

阻止外部人员 – MDM供应商们表现突出，为我们提供了可以保护移动设备上的数据的工具。如果您实施了验证码和加密而且可以清除设备数据，即表示您掌握了90%的决胜权。但是，在实现持续可靠地应用和验证这些控制方面仍然存在很多重大挑战，特别是在版本众多的Android平台上。如果不能为所有设备提供程度合理的安全保护，这种分散性就会提高设备的多样性程度。

广泛灵活的BYOD计划支持 – 在选择自己的方法和策略时，设备多样性是需要考虑的重要因素。毕竟自带设备(BYOD)并不等同于*自带经过IT批准的设备*，而且后者在一定程度上违反了BYOD计划的精神。尽管设备证书程序和流程可以提供某类基础，但完全公开的BYOD计划仍然需要某些技术方面的帮助，才能维持最低标准的数据安全保护。

公私双系统 – 从现在开始，我们不再单纯讨论安全问题，而改为讨论支持灵活的BYOD计划的功能和动力。有些组织并不需要强大的DLP控制，或者没有这方面的策略。他们只希望可以单独存储用户的个人数据，同时仍然可以控制公司数据。如果要实现这类想法，公私双系统解决方案可能就是贵组织的恰当之选。从根本上讨论，公私双系统是管理两个独立的用户环境的机制，它在移动设备上实现了“工作”和“个人”数据及体验的分离。

公私双系统是管理两个独立的用户环境的机制，它在移动设备上实现了“工作”和“个人”数据及体验的分离。

其他因素 – 与其他任何事情一样，推出解决方案也要付出很多代价。您需要考虑它的扩展性、如何使其适应弹性需求以及成本预算。您需要重点考虑用户体验，确保用户愿意接受并采用您提供的工具或解决方案。现在不是IT垄断的黄金时代，用户拥有自己的选择权。

选择适合自己的方法

既然您已经将自己的目标量化，那么我们来看看可用的方法吧。

容器 –“容器”似乎是最常用来描述以下解决方案的词语：提供单独的办公应用程序和数据区的解决方案。“沙盒”也是个高频词。人们可能也会使用“公私双系统”来说明这类解决方案，但公私双系统更应被视作目标，而非解决方案（也就是说，实施容器解决方案来实现公私双系统的目标）。

这种方法提供某些活动会在其中发生的完全独立的“沙盒”区，而且这一区域中的数据移动操作只能在沙盒内执行。因为用户要在此沙盒中开展所有工作，所以他们无法使用本地电子邮件客户端，而必须改用容器内部的软件提供的电子邮件、日历和通讯录功能。这可能会让用户产生不满情绪，但实施得当的话，这种方法也可以为用户带来顺畅的体验。该解决方案在帮助组织实现其数据安全目标方面具有重要价值，帮助您的用户群了解这一点很重要。

分离 – 该解决方案会拦截电子邮件流、分离出相关内容（即附件、文字等），从而可以让用户在单独的应用程序中查看和/或操控这类内容，实现对数据流的控制。使用电子邮件时，如果用户需要访问的内容并未从电子邮件流中移除（分离），那么他们就可以通过本地客户端访问这些内容。已删除的内容可能会存储在执行“分离”操作的服务器上，也可能存储在移动终端上，以便仅在安全的应用程序中打开这些内容。

分离解决方案可能会导致用户体验不连贯。用户可能会收到不含文字内容或附件的电子邮件（很多解决方案都不会出于这种原因分离文字内容），而且必须打开其他应用程序才能安全地访问文字内容和附件。

如果贵组织重点要阻止已经授权的用户传播移动设备中的机密数据，那么容器、虚拟化或电子邮件附件分离解决方案都非常有效。

虚拟化 – 具体而言，此处提到的虚拟化是一项技术，该技术通过一种软件（称为“虚拟机监控程序”）在移动设备上的软件中（而非在远程服务器上）实施“虚拟机”。通过这种解决方案，企业可以全面控制并管理虚拟设备。所有的公司应用程序和数据均会存储在移动设备上的虚拟机内，而且虚拟设备和实体设备之间的数据移动会受到严密控制。这基本与PC和笔记本电脑的Virtual Desktop Infrastructure (VDI)相同，同时也带来了很多相同的部署和管理方面的挑战。

当设备硬件和软件，以至深入到网络连接和硬件层面的所有功能均可实现虚拟化并受到控制，该技术就提供一定保证的成效。例如，当SIM在网络之间移动时，用户就可以对其进行虚拟化并以虚拟方式对其进行更改（电讯服务供应商可能会不喜欢这种虚拟化）。实际上，在移动设备支持在硬件中进行虚拟化之前，大规模运用虚拟化是难以实现的（尤其是在iOS设备上），这与PC上的Intel VT和AMD-V类似。

以上选项都不适合 – 尘埃落定之后，这可能就是很多公司面临的结果。如果您不从事健康保健或金融服务，不受PCI或HIPAA监管要求，或者在您还没确定您的特定移动安全需求，就实施了相应的设备和应用程序管理策略，由此产生的额外费用和复杂工作对用户和IT部门来讲并不划算。

根据优先级做出选择

现在，我们来根据您的优先级规划一下吧。

优先级 – 内部威胁：如果贵组织重点要阻止未经授权的用户传播移动设备中的机密数据，那么容器、虚拟化或电子邮件附件分离解决方案都非常有效。它们都可以为文字内容和附件提供安全保护，但却会在使用过程中提供完全不同的体验（如上所述）。（如果选择使用分离解决方案，请务必选择文字内容和附件均可分离的产品。）如果无法承受电子邮件中的数据泄露带来的后果，或在这一方面缺乏灵活的应对方案，那么容器解决方案可能就是比较适合您的选择，因为它可以提供更好的用户体验，而且配置和管理起来较为简单。理论上虚拟化非常合适应对内部威胁，但却面临着实施和管理方面的挑战。

优先级 – 外部威胁：如果您采用可靠的方法让那些在自己的授意下的设备连接至电子邮件系统，那么您就不用担心外部威胁的问题了。如果您使用MDM解决方案（您已经拥有该解决方案了吧？）将连接限制于仅限支持验证码策略和加密、而且可以远程清除数据的设备，那么数据泄露和失窃或丢失的设备造成的损害即使无法避免，也微乎其微了。如果您最大的威胁来自外部，那么您就可以省下一笔费用，而且也无需实施复杂的DLP解决方案了。只有堵塞其他漏洞后，堵塞移动数据漏洞才会起作用。

优先级 – BYOD计划支持：实施BYOD计划时，一项保险的措施是：设置设备认证流程，并创建获准设备的列表，这些获准设备可以提供基本的安全保护。如果您已经实施了BYOD计划，那么您会立即意识到，各个Android版本的重要安全功能支持级别存在巨大差异。在理想状态下，BYOD就是要达成上述目的，容纳各种各样的设备。

MaaS360®
by Fiberlink, an IBM company

容器解决方案可以在不安全的设备上提供安全区域，供用户存储公司数据，该解决方案是对未经认证或不符合条件的用户自带设备进行升级的备选方案。

容器解决方案可以在不安全的设备上提供安全区域，供用户存储公司数据，该解决方案是对未经认证或不符合条件的用户自带设备进行升级的备选方案。分离解决方案也可以产生类似的效果，但前提是这类解决方案支持并已配置为可以分离电子邮件文字内容和附件，并为这些内容提供安全保护。由于支持运行虚拟机监控程序的设备数量有限，因此虚拟化无法为大范围的BYOD设备配置文件提供支持。

优先级 – 公私双系统：容器或附件分离解决方案另一个吸引人的优势则不只与安全问题有关。随着企业中消费类设备的激增，公司数据与个人数据混合已成定局，无论我们付出多大努力，可能都无法避免这种状况。在这些设备中以柔和的方法处理公司数据也是上述两种解决方案的主要优势。

您可以在用户设备丢失、被盗或他们离职后，告诉他们全面清除设备数据，但您并非只有这一种选择，您还可以让他们使用容器或分离解决方案。这样一来，用户便可以放心地只清除公司数据，而不用担心会影响他们放在设备上的个人数据。容器方法对实现这一目标最有效，而且在“软硬兼施”的方法中，容器可能是其中最柔和的方法。设备会将用户引导至“工作”系统，而且用户非常乐意接受这种安排，因为他们知道IT人员不会弄乱他们的个人内容了。

相比之下，分离方法在实现公私双系统目标方面就没有那么有效了，因为本地电子邮件客户端仍会用于个人和公司活动，这就导致工作数据和个人数据无法完全分离。

虚拟化在这一方面也有很大潜力，但受到设备支持的极大限制，因此目前还无法成为BYOD的实用备选方案。

三思而后行

总的来说，您需要三思而后行。了解自己的目标、用户和可用的技术，以及这些因素对您的环境和用户的影响。最重要的是，在供应商推销之前先了解相关信息。在与供应商互动，并试用他们的解决方案时，请选择可以适应快速变化的移动产业，而且可以经常重新评估您的目标的解决方案。

了解详情
要详细了解我们的技术和服务，请访问www.maaS360.com。
1787 Sentry Parkway West, Building 18, Suite 200 | Blue Bell, PA 19422
电话 215.664.1600 | **传真** 215.664.1601 | sales@fiberlink.com

WP_201304_0046