IBM Security
思维领导力白皮书

调动公司内容和应用程序

为企业提供简单且受保护的移动协作

IBM

新时代的移动战略

问：您是否制定了强大的移动战略？

答：移动战略？您说的是我们的员工可以在自己的移动设备上访问电子邮件吗？我们当然有了。

给出这种答案的不止您一个。许多公司仍把电子邮件作为“应用程序之选”，让员工可以在办公室之外进行沟通。短短几年前，这还算得上一项巨大的进步。但是真实的情况却是，在办公室之外查收回复电子邮件这样的“工作”与消除障碍、推动事务进展以及维持表面状况并不完全是一回事。在当今世界，移动协作中蕴含着巨大的潜力，它可以释放真正的生产力并能够近乎实时地推动实际工作，但很多公司只是触及了一些皮毛而已，并未真正接纳、规划和部署稳健的移动战略，以简单且受保护的方式访问业务资源，从而充分利用移动性的力量。

在本文档中，我们将讨论如何对笔记本电脑、台式机及其他端点设备进行持续监控。

本白皮书将带您了解如何：

- 在没有设备 VPN 的情况下以受保护的移动方式访问公司数据
- 调动 SharePoint、Windows File Share 和您的所有内部网站点
- 使用强大的安全策略和 DLP 控制保护敏感的公司数据
- 在无需更改网络或防火墙安全配置的情况下提供移动访问
- 使用户能够随时通过其个人设备进行协作

继续阅读，深入了解如何让员工访问防火墙之后的资源，同时通过授权、加密和容器化策略保护数据。

简单安全的访问

下面是一项简单的挑战：建造一座绝对安全的房子用来保护您的所有无价之宝。您会怎么做？您可能会建造一座无窗无门的房子 — 没有进口也没有出口。它可能会很安全，但不利于实际生活。或者您也可能会装上窗户和门，并配上顶级的锁和安全系统加以保护，这样既有了安全性又方便进出，还能欢迎访客，呼吸到新鲜的空气，且不用担心自己珍贵的物品会丢失。

您的移动战略可能就像一座没有窗户或门的房子。或者是像一座有窗户和门却从不上锁的房子。您肩负着保护公司资源的责任，同时又要让用户使用这些资源，以提高生产力。从客户联系人名单到患者数据，从财务信息到人力资源文件，再从公司应用程序到董事会会议记录，您的用户需要访问的信息每天都在增长，禁止访问这条路已经走不通了。您需要一些窗户和门，需要一种安全的系统，确保只有得到允许的人才能进入。

如果用户将个人智能手机或平板电脑用于工作并将销售联系人下载到设备上，会怎么样？如果他们将专有财务报告通过电子邮件发送到家庭电子邮件地址，以便在晚上等孩子们入睡之后继续工作，会怎么样？供应商呢？您想分享内容和应用程序以便高效协作，但是项目结束之后该如何处理呢？

这些场景每天都在发生。人们罔顾公司信息安全，想方设法获取自己所需的信息，除非您有更安全、可靠且简单的方法让他们得到自己需要的信息。

内容方面的考量

企业内容存储在公司网络中诸如 Windows 文件共享、SharePoint、内部网站和网络应用程序这样的地方。人们与同事、合作伙伴及客户紧密合作以完成工作所需的信息都封锁在内部驱动器、数据商店、知识库、内部维客、ERP、SCM、HRM、CRM 以及其他管理系统或流程中。

所以现在的问题是，您如何利用它们来满足现代移动员工从并不属于您的设备上多次访问资源的需求?

在您保护存放信息的数据和内部网络、文件共享及其他系统时，您可能要考虑一下移动战略中的以下几点。有些看似显而易见，但还是值得在此一提。

1. 用户必须通过推送或提取方式按需访问内容
2. 每位用户都必须根据上下文和身份仅访问所需内容
3. 数据必须可以不时跨设备更新同步
4. 用户的数据访问流程必须简单方便
5. 安全性维护成本不能过于高昂，尽管这是一项大投资
6. 安全性维护对于 IT 而言不能过于耗时
7. 动态数据必须加密并妥善保护
8. 未经授权，数据不得离开组织
9. 应用程序中创建和存储的数据必须有安全保障
10. 因为个人设备并非归组织所有，您可以控制的方面会受到限制

联邦网络安全立法最重要的目的之一在于，必须使防御者像攻击者一样快速采取行动保护系统。

当前技术

让我们一起了解一下当今所用技术，以及确保安全性和生产力过程中无法避免的一些问题。

电子邮件

电子邮件是为了开展协作而选择的一种应用程序，但用于开展协作的工具有很多，它只是其中一种。

它并非专为协作而设计的。电子邮件支持一对一或者一对多的沟通，但不能实现多对多的互动，而您的用户需要这样的互动实现真正的高效。这样会在本应一起工作的团体之间形成孤岛。

电子邮件发送的信息很容易过时 — 人们得到一张电子表格并继续处理，并未意识到它已被更新的内容所取代。

最大的问题在于，数据可以被剪切、粘贴并转发到您不希望它出现的地方。

VPN

利用 VPN 登录是穿越防火墙的常见选择。

不幸的是，强行要求用户登录才能访问，会降低用户体验。假如有两个选择摆在眼前：一个是较难访问的新鲜内容，一个是旧电子邮件附件中附带的易于获得的过时内容，人们可能会愿意选择途径更简单的那个。

VPN 需要按设备许可，因此成本会随着时间不断增加。此外，也有证据显示，使用设备 VPN 会更快耗尽设备的电量。

因为移动设备使用无线技术进行连接，因此您需要加密。但是，还要面对漫游时的访问问题。通常来看，当用户在接入点之间漫游时，需要更高级别加密技术的解决方案有可能发生中断。幸运的是，这一问题已经有了解决方案。

桌面虚拟化

有些应用程序可让您在移动设备上显示桌面。所有可从桌面访问的项目也可从智能手机或平板电脑上访问。但是通常都会成本高昂，且用户体验不尽如人意。这种方法下的可用性和性能在很大程度上取决于网络连接。另外，屏幕尺寸和分辨率也是另外一个不容忽视的问题，在屏幕和工作空间更小的智能手机上时尤其如此。针对桌面环境进行优化的应用程序可以在移动设备上通过桌面虚拟化进行访问，但是并不意味着它们一定有用。

IT 必须考虑的另外一个因素是，服务器和网络资源必须能够同时支持接入网络的众多设备。

第三方文件共享

您可通过第三方文件共享将资源保存在云端。一个很大的问题在于，您会失去控制。内容可以发送给任何人，可以被任何人访问，并且您可能还会遇到版本控制问题。

此外还会出现用户体验问题。用户并不希望为了访问所需的内容而必须了解新的软件，而您则必须算上他们学习它所用的时间。

第三方文件共享代价也很高：添加用户就需要添加许可，此外您可能无法使用当前投资，例如应用程序和内容商店等。

第三方及定制应用程序

如果您选择第三方开发人员为您开发应用程序，则会受制于供应商。数据泄露防护 (DLP) 可能不会内置到应用程序中。

您可以尝试开发自己的应用程序，但这样就需要员工来支持它，也需要员工执行因为新设备类型、操作系统更新等带来的更改。

许多安全专家、高级政府网络安全官员以及国会领导人，都在不断进行敦促，要求更加重视持续监控、自动化监控工具以及对政府信息技术系统所受攻击的快速应对。

策略的重要性

如果您打算允许用户在自己的个人设备上访问公司资源，则需要制定策略，规定如何访问和使用数据。

您可以要求用户在访问重要数据之前输入密码。

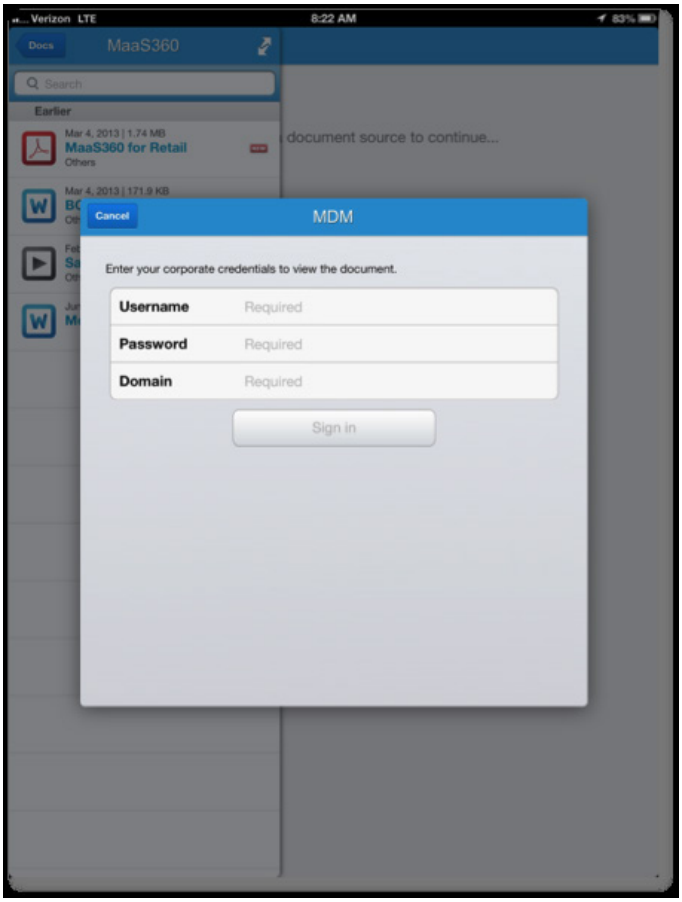

图 1：一项验证请求

您还可以限制从文档中复制粘贴文本。

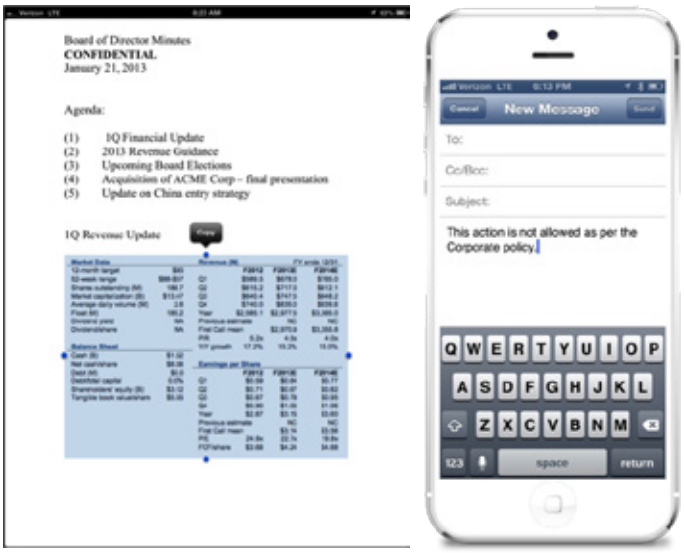

图 2：复制粘贴限制等数据泄露防护控制

IBM® MaaS360® Productivity Suite

MaaS360 Productivity Suite 有助于克服当前技术带来的挑战，并以多种方式提供安全访问并保护数据远离风险：

1. IBM® MaaS360® Secure Mobile Mail
2. IBM® MaaS360® Mobile Application Security
3. IBM® MaaS360® Secure Mobile Browser

MaaS360 使用容器实现双重角色 — 公司特定的数据、应用程序和内容都保存在设备上的受保护区域中。您自己决定受保护区域实施的控制，以便邮件、联系信息、日历、应用程序（和应用程序数据）、文档以及网页访问得到保护。

图 3：MaaS360 Productivity Suite 和 MaaS360 Content Suite

MaaS360 Productivity Suite 运用角色策略在所有用户设备上指定安全性。这些策略都在 MaaS360 门户中创建，并通过无线技术部署到注册的设备上，因此 IT 不必直接接触设备。

若设备未能遵守相关要求，或者项目结束，供应商离开，您只需远程移除容器，所有数据和应用程序就会消失得无影无踪。

容器具有内置的安全功能。它符合 FIPS 140-2 要求，采用 AES-256 加密技术。您可以要求用户在访问时输入密码。如果设备已遭破解或获得根权限，或者设备没有在指定的时间内签入，您也可以使用这些策略设置彻底移除容器。

您还可以防止从容器中移除、复制或打印文件，并防止将文件导入容器。

IBM® MaaS360® Content Suite

MaaS360 Content Suite 提供加密的容器和生产力工具，以在移动设备上分发、查看、创建、编辑并共享文档，赋予组织必需的控制权，同时让员工能够访问所需的资源：

1. IBM® MaaS360® Mobile Content Management
2. IBM® MaaS360® Mobile Document Editor
3. IBM® MaaS360® Mobile Document Sync

MaaS360 Mobile Content Management 为内容协作提供移动文档容器，借助一系列强大的生命周期管理功能分发、更新和管理文档并确保文档安全无虞。IT 管理员可以实施验证、复制/粘贴和只限查看限制。用户可以访问公司分发的内容和文件库，例如 SharePoint、Box 和 Google Drive。

MaaS360 Mobile Document Editor 可以防止公司数据泄露，同时允许用户创建、编辑并保存数据。用户可随时通过移动设备上的 Word、Excel、PowerPoint 和文本文件开展协作。

MaaS360 Mobile Document Sync 使用户能够在受管移动设备上同步内容，在不发生中断的情况下继续创建或编辑文件。IT 可以针对内容实施各种策略，例如限制复制/粘贴，禁止在非受管应用程序中打开或共享内容。这些控制措施可以应用于所有文档、一组文档或单个文档，提供保护珍贵公司数据所需的灵活性。

受保护的内容共享使用案例不胜枚举，几乎在任何组织中都是如此，无论销售部、营销部、运营部还是财务部：

- 就在客户会议开始之前，方便地查看和共享销售演示最后一刻的变动
- 登机之前研究电子表格中的最新财务数据

- 在咖啡馆与同事讨论，集思广益，分享营销信息
- 向董事会分发季度财务文档，并设置成会后过期
- 与销售团队近乎实时地共享产品资料，他们就不必忙着寻找最新数据表或竞争性信息
- 确保零售店的平板电脑拥有最新产品和库存信息

IBM® MaaS360® Gateway Suite

MaaS360 Gateway Suite 是让这一切成真的重要组件。它让您通过移动设备安全无缝地访问公司内容和内部网站，从而保护动态数据：

- 以简单受保护的方式移动访问数据，无需设备 VPN；不必在每次需要信息的时候登录 VPN
- 调用 SharePoint、Windows File Shares、内部网站和网络应用程序
- 使用强大的安全策略和 DLP 控制保护数据
- 无需更改网络或防火墙安全设置

图 4：MaaS360 Gateway 中的数据流

您可以配置策略选项，从而管理 MaaS360 Productivity Suite 与您用户设备的交互方式。例如，您可以指定公司维客的 URL、缺陷跟踪系统等，或者是通过 MaaS360 Gateway 访问的公司文件夹，它们会在 MaaS360 Secure Mobile Browser 中显示为书签。您也可以指定访问这些位置是否需要验证。

当用户在自己的设备上访问数据容器时，MaaS360 Gateway 可确定用户可以访问哪些公司资源。

先试用后购买

MaaS360 的试用快捷简单 — 您为满足自己需求配置 MaaS360 的时间也会花得其所。一旦您认为 MaaS360 就是适合自己组织的解决方案时，就可从试用环境转变为真实环境！

要免费试用 MaaS360，请单击此处. 您可以立即开始试用 — 无需复杂的设置流程，也不需要更改基础架构。立即试用 MaaS360！

图 5：MaaS360 产品

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资讯，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

IBM Corporation
Software Group
Route 100
Somers, NY 10589

美国印制 2016 年 3 月

请回收利用

WGW03111-CNZH-01