



关键优势

- 一套用于查看和共享的稳健办公效率工具
 - 安全支持 BYOD
 - 区分个人数据和企业数据
 - 降低敏感数据泄露风险
 - 使用单点登录进行身份验证
 - 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
 - 针对 iOS、Android 和 Windows Phone 体验始终如一的无缝 workflow
 - 使用粒度管理控制和互动式图形报告
-

IBM MaaS360 Productivity Suite

移动容器保护企业数据

工作与娱乐分开

IBM® MaaS360® Productivity Suite 是在自带设备 (BYOD) 时代隔离和容纳工作数据的一套集成的跨平台解决方案。它帮助员工安全访问公司数据，同时保留他们智能手机和平板电脑上的移动体验。

MaaS360 Productivity Suite 应对数据丢失风险方面的关键问题。通过身份验证和授权，仅经过核准的有效用户才能访问敏感数据。借助安全容器策略控制数据流，您可以限制用户共享、附件转发以及复制粘贴。您可以选择性地擦除丢失、被盗或受损设备，以移除安全容器和其他企业应用程序、数据或配置文件。

提供双角色体验

MaaS360 Productivity Suite 提供稳健的数据丢失防护解决方案，具有始终如一的无缝 workflow。

它采用双角色途径，将用户工作所需信息放在一个受保护的位置。他们可以在他们的移动设备上通过一个专用工作空间管理他们所有的电子邮件、联系人、日历、应用程序、文档和 Web，无论谁拥有它们。

您可以实施控制来管理该安全容器，以便不影响其他设备，这样您就可以将工作和娱乐区分开来。

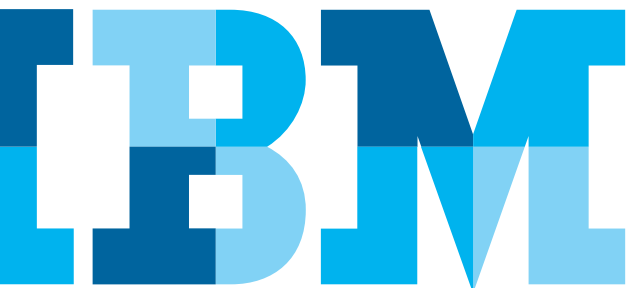




图 1: 在多个设备类型上的安全性和生产效率

借助 MaaS360 Productivity Suite 随时随地工作

MaaS360 Productivity Suite 支持 iOS、Android 和 Windows Phone，拥有营造安全且受保护的移动工作空间所需的关键移动解决方案，在员工拥有的设备上尤其如此。它兼顾速度与安全性，提供用户期望的简单轻松体验。

IBM® MaaS360® Secure Mobile Mail

支持电子邮件、日历和联系人的直观办公效率应用程序。

- 支持电子邮件、日历和联系人的稳健 PIM 应用程序
- 在容器中控制电子邮件（包括文本和附件）
- 采用符合 FIPS 140-2 的 AES-256 加密
- 支持诸如 Office 365 和 Gmail 之类的云电子邮件

- 进行身份验证以及访问电子邮件之前的在线和离线合规性检查
- 允许用户存储附件，进行修订和发送文档
- 限制转发、移动到其他应用程序、复制、粘贴和截屏
- 选择性地擦除附件，甚至在电子邮件之外



图 2: 包含 MaaS360 Secure Mobile Mail 的 MaaS360 容器

IBM® MaaS360® Mobile Application Security

具有稳健运营和安全管理移动应用程序容器，可以防止数据泄露。

- 启用所需的认证
- 执行设备合规检查
- 限制复制和粘贴，以及本地和云数据备份
- 接收近乎实时的违规警告
- 配置自动化的合规性实施措施
- 作为用于集成的易用应用程序包装器或 SDK 提供
- 应用程序级通道（非 VPN），用于受保护地访问公司数据

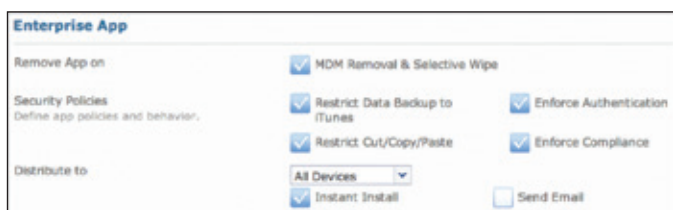


图 3：通过 MaaS360 Mobile Application Security 进行的应用程序策略选择

IBM® MaaS360® Secure Mobile Browser

旨在保护对公司内部网网站的访问并通过内容策略实施合规性的稳健 Web 浏览器。

- 在没有 VPN 的情况下安全访问公司内部网站
- 调动 SharePoint、JIRA、内部维客和原有 ERP 系统
- 使用扫描引擎和声誉数据库阻止已知恶意网站
- 按照 URL 安全性将数百万 URL 定义为 60 多个类别
- 选择 URL 类别进行允许、阻止和跟踪
- 限制 Cookie、文件下载、复制、粘贴和打印
- 向用户和管理员发送文本或 HTML 违规警告
- 查看带有审计跟踪的详细策略违反报告

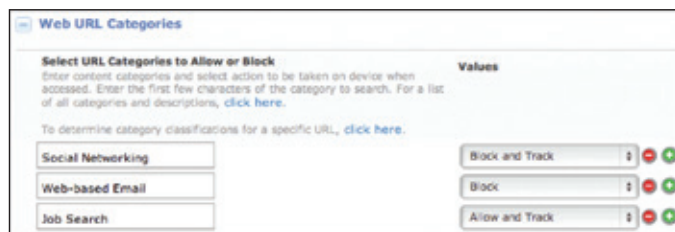


图 4：MaaS360 Secure Mobile Browser 的 Web URL 类别过滤

如要了解有关 IBM Security 防欺诈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，或者访问以下网站：ibm.com/security.



© Copyright IBM Corporation 2016

IBM Corporation Software Group
Route 100
Somers, NY 10589

美国印制
2016 年 1 月

IBM、IBM 徽标、ibm.com 和 X-Force 是 International Business Machines Corp. 在全球许多司法辖区的注册商标。BYOD360™、Cloud Extender™、Control360®、E360®、Fiberlink®、MaaS360®、MaaS360® 及设备、MaaS360 PRO™、MCM360™、MDM360™、MI360®、Mobile Context Management™、Mobile NAC®、Mobile360®、Secure Productivity Suite™、Simple. Secure. Mobility.®、Trusted Workplace™、Visibility360® 和 We do IT in the Cloud.™ 及设备是 IBM 旗下 Fiberlink Communications Corporation 的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表在以下网址的“版权与商标信息”处提供：
ibm.com/legal/copytrade.shtml

Apple、iPhone、iPad、iPod touch 和 iOS 是 Apple Inc. 在美国和其他国家/地区的注册商标或商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家/地区的商标。

本文档为初始发布日时的最新文档，IBM 可能随时对其进行更改。IBM 并未在每个开展业务的国家/地区提供所有产品/服务。

所引用的性能数据和客户示例仅供参考。实际性能结果可能会有所不同，具体取决于特定的配置和操作条件。对于与 IBM 产品和程序配合使用的其他任何产品或程序，用户应负责相关的评估与验证工作。

本文档中的信息“按原样”提供，不带任何明示或暗示的保证，包括不带任何适销性、对特定用途的适用性的保证，以及任何不侵权的保证或条件。IBM 产品根据提供这些产品时所依据协议的条款与条件进行保证。

客户负责确保遵守适用的法律和法规。IBM 不提供其服务或产品能确保客户符合所有法律或法规的法律意见、声明或保证。

关于 IBM 未来方向和意向的声明仅表示目标和目的，可能随时更改或撤销，恕不另行通知。

良好安全实践声明：IT 系统安全包括通过防范、检测和响应来自企业内部和外部的不正当访问，从而保护系统和信息。不正当访问可导致信息被更改、销毁或盗用或导致系统被破坏或滥用，包括攻击其他系统。没有任何 IT 系统或产品是完全安全的，而且在防范不正当访问方面，也没有任何单个产品或安全措施是完全有效的。IBM 系统和产品的设计旨在作为全面安全方案的组成部分，其中必然涉及其他操作程序，可能会要求其他系统、产品或服务具有最高的效率。IBM 不保证其系统和产品可免受任何一方的恶意或非法行为影响。



请回收利用