IBM MaaS360 Secure Mobile Mail

控制移动设备上的企业电子邮件

关键优势

- 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
- 擦除电子邮件容器、企业配置文件或整个服务
- 提供简单直观的用户界面，不会降低员工效率
- MaaS360 无法访问机密电子邮件数据
- 不与电子邮件数据内联，不存在性能或中断风险

提供受保护的企业电子邮件访问

IBM® MaaS360® Secure Mobile Mail 提供包含电子邮件、日历和联系人的受保护办公效率应用程序，让员工可以安全地与同事协作，同时保留个人设备的移动体验。

作为 IBM® MaaS360® Productivity Suite 的基本组件，它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电子邮件和数据。借助数据流控制策略，您可以限制用户共享、附件转发以及复制和粘贴。您可以选择性地擦除丢失、被盗或受到危害的设备，以移除受保护的电子邮件容器、所有附件和配置文件。

选择合适的电子邮件保护方法

其他解决方案通过截取电子邮件流、移除附件和在单独应用程序中加载电子邮件来保护电子邮件。这通常会在本机电子邮件客户端和可能仅提供文档视图的独立应用程序之间产生脱节的用户体验。

MaaS360 Secure Mobile Mail 在 MaaS360 Productivity Suite 内无缝工作，在移动设备的一个隔离工作区内管理所有电子邮件、日历、联系人、应用程序、文档和 Web。

从邮件处理到查看、编辑和共享文档，用户能够借助一致的用户体验保持生产效率。

Robust Personal Information Manager (PIM) 应用程序

- 保护电子邮件、日历和联系人
- 提供身份验证并阻止未经授权的电子邮件访问
- 在容器内控制电子邮件和附件
- 直接在应用程序中查看附件
- 不只是查看，还在加密的 IBM® MaaS360® Content Suite 中安全地创建、编辑、保存和共享内容
- 支持常见文件类型，包括 Word、Excel、PowerPoint、文本和 PDF 格式

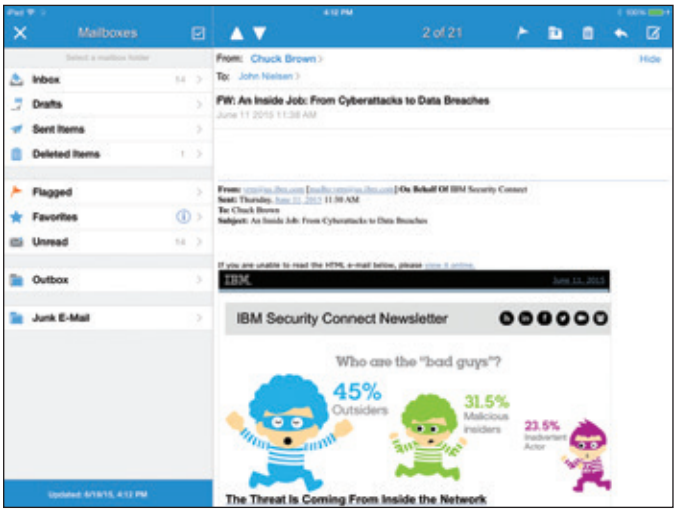

图 1： 可能在设备上显示的容器、收件箱和电子邮件示例

强大的数据丢失防范

- 控制可以在哪里复制或移动文件
- 限制转发和移动到其他应用程序
- 禁用复制、粘帖和截屏
- 不仅保护电子邮件附件，还保护电子邮件文本
- 执行设备合规检查
- 选择性地擦除容器和附件，甚至在电子邮件之外

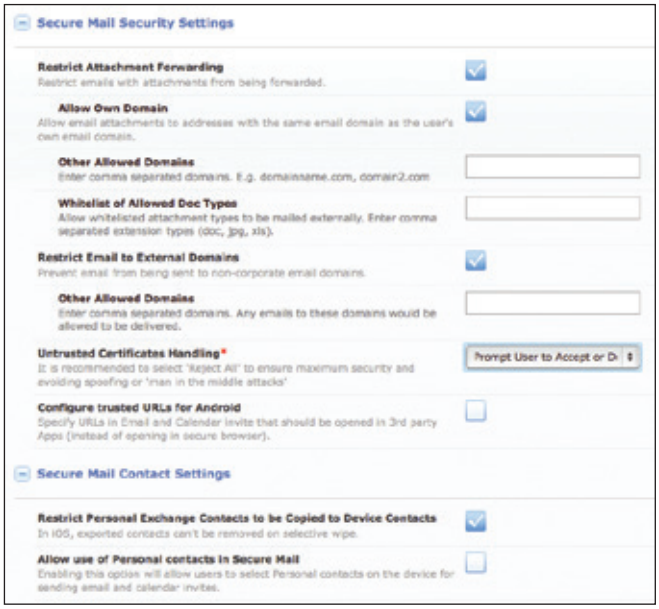

图 2： MaaS360 Secure Mobile Mail 安全设置示例

与您的基础架构轻松集成

- 基于现有的 Exchange ActiveSync 基础架构构建
- 使用 Active Directory 简化身份验证和授权
- 支持诸如 Office 365 和 Gmail 之类的云电子邮件
- 在不与电子邮件数据内联的设备级别集成强大的电子邮件安全性
- MaaS360 无法访问机密电子邮件数据
- 无额外的性能或中断风险

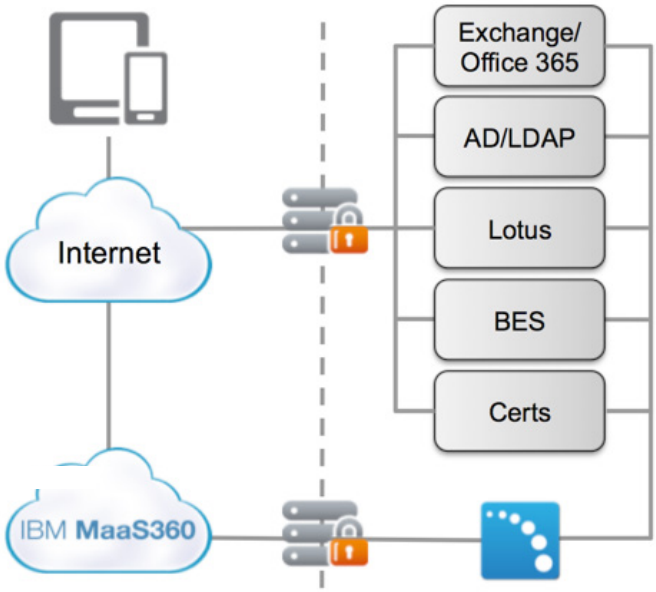

图 3： MaaS360 与 IT 系统集成的简单概览

持续的安全报警和报告

- 配置自动化的合规性实施措施
- 接收自动违规报警
- 通过自动化或人工干预迅速采取行动
- 查看安全和合规历史图形报告

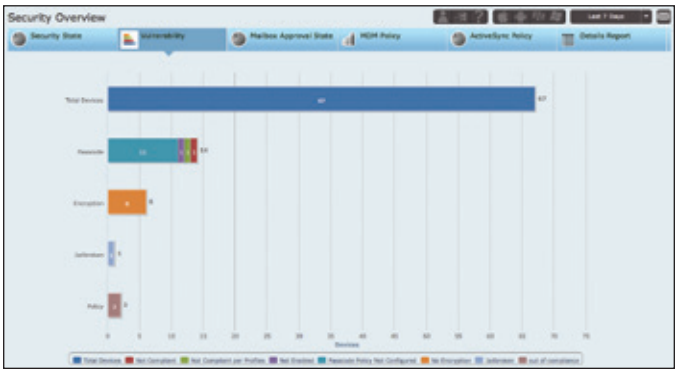

图 4： MaaS360 安全报告示例

控制企业电子邮件

电子邮件仍然是智能手机和平板电脑上的必备应用程序之一，但它可能对您组织的移动安全性和合规政策构成挑战。

MaaS360 Secure Mobile Mail 保护业务电子邮件和附件以防止企业数据泄漏，同时保持员工的移动生产效率。

关键特性

- 在容器内保护电子邮件（文本和附件）、日历和联系人
- 实现身份验证并阻止未经授权的电子邮件访问
- 在访问电子邮件前执行在线和离线合规检查
- 为 iOS 和 Android 采用符合 FIPS 140-2 的 AES-256 加密
- 直接在应用程序中查看附件
- 控制可以在哪里复制或移动文件
- 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
- 在 MaaS360 Content Suite 内工作，以存储、查看、编辑和共享内容

如要了解有关 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 Corporation
Software Group
Route 100
Somers, NY 10589

美国印制2016 年 2 月

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

WGD03062-CNZH-01