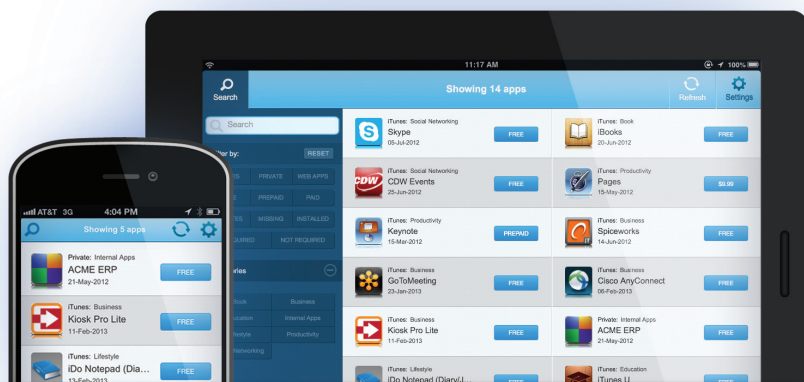




MaaS360®移动应用程序管理

从云端简单部署、管理和保护移动应用程序



实现应用程序安全访问

借助智能手机和平板电脑，不断地改变企业提高了生产力、增加了效率并且提升了客户满意度。但是，移动设备在不断普及，我们不能任其发展，而不管敏感企业数据的安全性，特别是在当前的BYOD时代。

我们需要做的不再只是控制电子邮件和管理设备。移动应用程序正在释放移动设备的真正潜力。

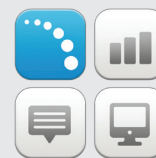
但是，由于欠佳的数据存储做法、恶意软件、未经授权的访问、缺乏加密以及同步数据泄露，移动应用程序渐渐成为公司安全漏洞的来源。

“到2017年，25%的企业将拥有企业应用程序商店，用于管理PC和移动设备上公司认可的应用程序。”

— Gartner¹

员工在智能手机和平板电脑上可以选择安装和使用的移动应用程序有一百多万种。

企业必须能够分配、管理和保护个人和公司所有设备上对企业业务至关重要的移动应用程序。



企业移动应用程序容器

MaaS360提供简单易用的企业应用程序目录和全面的应用程序安全和操作生命周期管理，简化了移动应用程序管理。

企业应用程序目录

针对iOS和Android设备的直观、可定制企业应用程序目录。

移动应用程序生命周期管理

用于分配、更新、管理和保护公共和企业移动应用程序的平台。

MaaS360 Mobile Application Security

一个具有全面安全管理功能，面向企业应用程序的移动应用程序容器，

移动应用程序合规和实施

安全策略以规范应用程序的白名单、黑名单和必需名单。用于提醒管理员、阻止电子邮件、限制网络资源以及执行远程擦除的自动执行规则。

MaaS360应用程序云

在全球性优化的应用程序分配网络上托管和分配企业移动应用程序的选项。

批量购买方案

支持批量为员工提供应用程序许可。

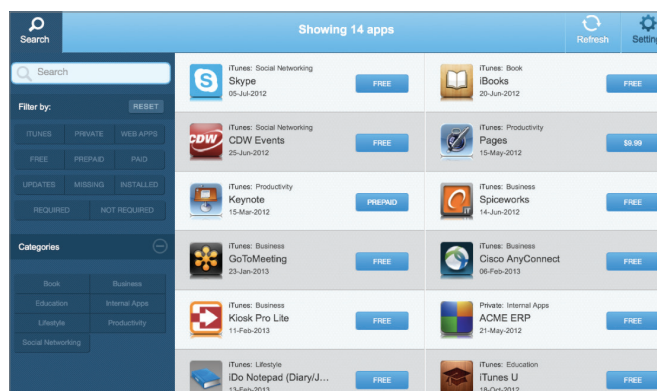
主要优势










- 通过全部集装箱化保护企业应用程序
- 提高员工效率和满意度
- 通过基于网络的控制台集中管理移动应用程序
- 使用精确的管理控制和交互式图形报告
- 降低敏感数据泄露的风险
- 强制执行基于设备的访问控制并且遵守政策法规
- 选择性擦除应用程序目录和托管应用程序
- 为BYOD提供安全支持
- 减少网络负载并且提高应用程序性能和可扩展性

¹ “Gartner声明，到2017年，25%的企业将拥有企业应用程序商店，” Gartner Group, 2013年2月12日

企业应用程序目录

- 提供针对iOS和Android设备的直观、可定制企业应用程序目录
- 提供出色的用户体验
- 允许用户立即查看可用应用程序、安装应用程序并且收到关于更新应用程序的提醒
- 分配精选的公共和企业应用程序
- 使用基于网络的安全控制台来管理和分配应用程序



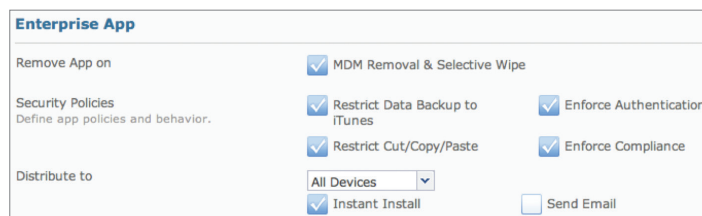
App	Name	Type	Category	Device Type	VPP Codes	Installs
	Skype	Apple	Social Networking	Tablet, Smartphone		1
	Cisco WebEx Meetings	Android	Business	Smartphone		1
	Salesforce Mobile	Android	Business	Smartphone		1
	iBooks	Apple	Book	Tablet, Smartphone		1
	iTunes U	Apple	Education	Tablet, Smartphone		0
	AnyConnect ICS+	Android	Business	Smartphone		0
	ACME ERP	Apple	Internal Apps	Tablet, Smartphone		0
	CDW Events	Apple	Social Networking	Tablet, Smartphone		0
	LinkedIn	Android	Social	Smartphone		0

移动应用程序生命周期管理

- 利用移动应用程序管理工作流的最佳实践
- 分配应用程序并且跟踪所有用户、用户组或单个设备的应用程序安装情况
- 发布应用程序更新
- 参考实时应用程序清单报告
- 与公共应用程序店（例如Apple App Store和Google Play）相集成，实现无缝工作流

MaaS360移动应用程序安全性

- 使用简单的应用程序包装器或软件开发工具包(SDK)
- 在用户访问应用程序之前先对其进行身份验证
- 执行设备合规性检查
- 限制复制和粘贴，限制本地和云端数据备份
- 接收关于违规行为的实时提醒
- 针对公司数据安全访问的应用程序级隧道，无需设备VPN



移动应用程序合规和实施

- 划分白名单、黑名单以及设置所需应用程序
- 限制设备上的本机应用程序（例如YouTube）
- 限制对遭破解或初始化设备的访问
- 配置合规性自动实施操作
- 通过自动或手动干预采取即时措施，以阻止电子邮件访问、限制网络资源（例如，无VPN）以及执行远程擦除
- 查看安全性和合规性历史记录的数据报告

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



本文档中提及或引用的所有品牌及其产品均为其各自持有人的商标或注册商标，同样应予以注意。