洞察

以下是一些深入探讨 MDM 如何帮助您的企业的文章：

什么是 Kiosk 模式？锁定企业 Android

& Apple 设备指南
Kiosk 模式可将普通手机和平板电脑转变为专注的业务工具。 Cerberus Enterprise
帮助组织将设备锁定到单个应用或一小组获准应用，适用于零售 POS
、面向访客的签到和车队导航等场景，同时让这些专用设备在大规模环境下更易于保护、支持和管理。

如何选择合适的 MDM

解决方案：小型企业七点检查清单

在采购流程后期选择 MDM
时，只要比较保持务实就会更容易。此检查清单帮助小型企业按照实际部署中通常最重要的七项标准评估供应
商：安全性、 Android 和 Apple
支持、精简团队的使用便捷性、可扩展性、隐私边界、总拥有成本和日常支持能力。

打造安全且专注的数字课堂： K-12

学校 MDM 指南

学校管理的设备在以学习为中心时效果最佳。 Cerberus Enterprise 帮助 K-12 机构通过受管应用、 Kiosk 式限制、标准化的共享或借用设备设置以及远程恢复操作，让学生设备保持专注，从而减少丢失、偏离和课堂
干扰。

装备您的外勤技术人员： MDM

如何提升现场效率与安全性

外勤技术人员在现场工作时依赖移动设备查看日程、服务记录、技术参考资料、客户历史和作业更新。
Cerberus Enterprise
通过受管应用、标准化设备型号、远程支持命令和位置感知可见性，帮助这些设备保持就绪，从而改善调度协
调，同时加强现场安全。

超越地图：使用 MDM

实现更智能的车队管理和驾驶员安全

车队运营依赖移动设备进行导航、调度、消息传递、日志记录和现场执行。 Cerberus Enterprise 通过受管应用、 Kiosk
和专用设备控制、安全通信政策、远程故障排除和位置感知监督，帮助这些设备专注于已批准的工作流程，从
而减少停机时间并支持更安全的驾驶操作。

地理围栏、实时跟踪和位置地图如何改

善企业运营

Cerberus Enterprise
中的位置感知功能帮助组织从简单的设备可见性迈向更实用的运营控制。定期位置报告、实时跟踪、地理围栏切换和交互式地图可以支持物流、现场服务、医疗、零售、建筑以及其他分布式团队，帮助他们更好地了解工作发生的地点以及设备何时进入或离开重要区域。

多租户如何帮助 MSP 扩展 MDM

服务并创造新的收入来源

多租户允许 MSP、经销商和多公司组织通过单个 Cerberus Enterprise
账户管理多个企业，同时保持每个环境相互独立。此模式可减少运营摩擦、提升服务可扩展性，并通过子账户
和客户明确控制的管理支持委托访问。它还为希望将软件许可与入门、支持、合规性和托管移动服务相结合的
提供商创造更强的业务机会。

借助 MDM 解决方案提升企业运营能力

移动设备管理集中控制公司设备，简化注册、配置和维护。自动化配置和批量操作可减少手动 IT
工作，并确保所有设备上的政策保持一致。加密、合规性监控和远程擦除等安全功能可保护企业数据。总体而
言， MDM 在提高生产力的同时降低支持成本和运营复杂性。

Android Enterprise

管理中的高级安全

Android Enterprise
使用工作资料将企业应用和数据与同一设备上的个人内容隔离。这种容器化会创建独立的加密环境，由 IT 管理员独立管理。安全政策可以控制企业数据共享，而不影响个人应用。即使个人应用遭到入侵，该架构也能
保护业务数据。

Apple iPhone MDM 与自动注册
Apple 的 MDM 框架可在企业环境中集中管理 iPhone。结合 Apple Business Manager
，设备可在首次激活时自动注册并自行配置。管理员可以静默部署和配置企业应用、强制执行安全设置并监控
合规性。这种自动化可确保设备配置一致并减少设置错误。

了解移动设备管理

移动设备管理提供集中式平台，用于监控、保护和控制访问企业系统的移动设备。核心能力包括强制执行安全
政策、管理应用以及远程锁定或擦除丢失的设备。 MDM
有助于保护企业数据，同时保持设备合规性。它使各种规模的组织都能安全管理不断增长的移动办公人员。

企业设备部署模式

组织可以采用多种设备所有权模式，例如 BYOD、CYOD、COPE、COBO 和 COSU
。每种模式在成本、用户灵活性和安全控制之间有不同的平衡。 BYOD 优先考虑用户便利性，而 COBO 和 COSU 则最大化企业控制力和安全性。选择正确的模式取决于法规要求、员工需求和 IT 管理能力。

MDM、 EMM 与 UEM 对比

MDM 侧重于通过政策执行、配置控制和远程管理来管理和保护移动设备。 EMM
将范围扩展到应用和内容管理，而 UEM
则尝试管理包括笔记本电脑和台式机在内的所有端点。对于许多中小企业而言，完整的 EMM 或 UEM
套件会增加不必要的复杂性。在实践中，强大的 MDM 能力通常能满足大多数移动管理需求。

个人手机上的 MDM 与员工隐私

现代 MDM
系统使用容器化将员工自有设备上的工作数据和个人数据分开。雇主只能管理和监控工作环境，包括企业应用
和设备合规性信息。照片、消息和浏览历史等个人数据对公司仍不可访问。这种技术隔离可支持安全的 BYOD 计划，同时保护员工隐私。

MDM 投资回报与业务价值

MDM 应被视为一项战略投资，而非简单的安全支出。它通过减少设备丢失、降低 IT
支持成本和提高运营效率来产生财务回报。自动化管理还能提高员工生产力并减少停机时间。此外，更强的安

全性可降低数据泄露的风险和财务影响。

符合 HIPAA 的设备管理

医疗机构必须根据 HIPAA 安全要求保护电子患者数据。 MDM
有助于实施加密、身份验证控制、安全数据传输和详细审计日志。它还能为访问医疗系统的设备提供远程擦除
和集中式政策执行。这些控制措施可降低合规风险，同时在医疗环境中支持移动工作流程。

面向零售运营和安全的 MDM

零售组织依赖移动设备进行 POS 系统、库存管理和店内运营。 MDM 确保这些设备保持安全、更新并符合 PCI-DSS
等标准。集中管理可减少停机时间，并简化多个地点的设备部署。其结果是提高运营效率并降低支付相关安全
事件的风险。

Revision #31
Created 2026-03-12 17:08:20 UTC by Admin
Updated 2026-11-12 09:58:13 UTC by Admin