Аналитика

Вот несколько статей о том, как MDM может помочь вашему бизнесу:

Что такое режим киоска? Руководство по ограничению устройств Android & Apple для бизнеса

Режим киоска превращает обычные телефоны и планшеты в специализированные бизнес-инструменты. Cerberus Enterprise помогает организациям закреплять устройства за одним приложением или небольшим утверждённым набором приложений для таких сценариев, как розничные POS-терминалы, регистрация гостей и навигация автопарка, сохраняя при этом такие специализированные устройства более простыми в защите, поддержке и управлении в масштабе.

Как выбрать подходящее решение MDM: контрольный список из 7 пунктов для малого

бизнеса

Выбирать MDM на позднем этапе покупки проще, когда сравнение остаётся практичным. Этот контрольный список помогает малому бизнесу оценивать поставщиков по семи критериям, которые обычно важнее всего в реальных внедрениях: безопасность, поддержка Android и Apple, простота использования для небольших команд, масштабируемость, границы конфиденциальности, совокупная стоимость владения и повседневная поддержка.

Создание безопасного и сосредоточенного цифрового класса: руководство по MDM для школ K-12

Устройства, управляемые школой, работают лучше всего, когда остаются сосредоточенными на обучении. Cerberus Enterprise помогает организациям K-12 сохранять сосредоточенность ученических устройств на учёбе с помощью управляемых приложений, ограничений в стиле киоска, стандартизированных настроек общих или выдаваемых устройств и удалённых действий по восстановлению, которые снижают потери, отклонения и нарушения в классе.

Оснащение выездных специалистов: как MDM повышает эффективность и

безопасность на месте

Выездные специалисты зависят от мобильных устройств при работе на месте: расписание, заметки об обслуживании, технические справочники, история клиента и обновления по заданиям. Cerberus Enterprise помогает поддерживать эти устройства в готовности с помощью управляемых приложений, стандартизированных моделей устройств, команд удалённой поддержки и видимости с учётом местоположения, что улучшает координацию диспетчеризации и укрепляет безопасность в поле.

За пределами карты: использование MDM для более разумного управления автопарком и безопасности водителей

Работа автопарка зависит от мобильных устройств для навигации, диспетчеризации, обмена сообщениями, ведения журналов и выполнения задач на местах. Cerberus Enterprise помогает удерживать эти устройства в рамках утверждённых рабочих процессов с помощью управляемых приложений, элементов управления киоска и выделенных устройств, политик безопасной связи, удалённого устранения неполадок и наблюдения с учётом местоположения, что снижает простои и способствует более безопасному вождению.

Как геозоны, отслеживание в реальном времени и карты местоположения улучшают работу организации

Функции с учётом местоположения в Cerberus Enterprise помогают организациям перейти от простой видимости устройств к более практичному операционному контролю. Периодическая передача местоположения, отслеживание в реальном времени, переходы геозон и интерактивные карты могут поддерживать логистику, выездное обслуживание, здравоохранение, розничную торговлю, строительство и другие распределённые команды, которым нужно лучше понимать, где идёт работа и когда устройства входят в важные зоны или покидают их.

Как мультитенантность помогает MSP масштабировать услуги MDM и создавать новые потоки доходов

Мультитенантность позволяет MSP, реселлерам и многокомпанийным организациям управлять несколькими организациями из одного аккаунта Cerberus Enterprise, сохраняя раздельность каждой среды. Эта модель снижает операционные трения, повышает масштабируемость услуг и поддерживает делегированный доступ через субаккаунты и явное администрирование под контролем клиента. Она также создаёт более широкие

деловые возможности для провайдеров, которые хотят объединить лицензирование ПО с адаптацией, поддержкой, соответствием требованиям и услугами управляемой мобильности.

Повышение операционной эффективности организации с помощью решений MDM

Mobile Device Management централизует управление корпоративными устройствами, упрощая регистрацию, настройку и обслуживание. Автоматизированная подготовка и массовые операции сокращают ручную работу ИТ и обеспечивают единообразие политик на всех устройствах. Функции безопасности, такие как шифрование, мониторинг соответствия требованиям и удалённая очистка, защищают корпоративные данные. В целом MDM повышает производительность, снижая затраты на поддержку и операционную сложность.

Расширенная безопасность в управлении Android Enterprise

Android Enterprise использует рабочий профиль для изоляции корпоративных приложений и данных от личного содержимого на одном устройстве. Эта контейнеризация создаёт отдельные зашифрованные среды, управляемые ИТ-администраторами независимо. Политики безопасности могут контролировать обмен корпоративными данными, не затрагивая личные приложения. Архитектура защищает деловые данные даже при компрометации личных приложений.

MDM для Apple iPhone и автоматическая регистрация

Платформа MDM от Apple обеспечивает централизованное управление iPhone в корпоративных средах. В сочетании с Apple Business Manager устройства могут автоматически регистрироваться и настраиваться при первом включении. Администраторы могут незаметно развёртывать и настраивать корпоративные приложения, применять параметры безопасности и отслеживать соответствие требованиям. Эта автоматизация обеспечивает единообразную настройку устройств и снижает число ошибок при настройке.

Понимание Mobile Device Management

Mobile Device Management предоставляет централизованную платформу для мониторинга, защиты и контроля мобильных устройств, обращающихся к корпоративным системам. Основные возможности включают применение политик безопасности, управление приложениями и удалённую блокировку или очистку потерянных устройств. MDM помогает защищать корпоративные данные, поддерживая соответствие устройств требованиям. Это позволяет организациям любого размера безопасно управлять растущей мобильной рабочей силой.

Модели развёртывания корпоративных устройств

Организации могут применять различные модели владения устройствами, такие как BYOD, CYOD, COPE, COBO и COSU. Каждая модель по-разному уравновешивает затраты, гибкость пользователей и контроль безопасности. BYOD отдаёт приоритет удобству пользователя, тогда как COBO и COSU максимально повышают корпоративный контроль и безопасность.

Выбор правильной модели зависит от нормативных требований, потребностей персонала и возможностей ИТ-управления.

MDM, EMM и UEM: в чём разница

MDM сосредоточен на управлении мобильными устройствами и их защите посредством применения политик, контроля конфигурации и удалённого управления. EMM расширяет эту сферу, включая управление приложениями и контентом, а UEM пытается управлять всеми конечными точками, включая ноутбуки и настольные компьютеры. Для многих компаний малого и среднего бизнеса полноценные пакеты EMM или UEM добавляют ненужную сложность. На практике надёжные возможности MDM часто покрывают большинство потребностей мобильного управления.

MDM на личных телефонах и конфиденциальность сотрудников

Современные системы MDM используют контейнеризацию для разделения рабочих и личных данных на устройствах, принадлежащих сотрудникам. Работодатели могут управлять только рабочей средой и отслеживать её, включая корпоративные приложения и сведения о соответствии устройства требованиям. Личные данные, такие как фотографии, сообщения и история просмотров, остаются недоступными для компании. Такое техническое разделение позволяет безопасно внедрять программы BYOD, сохраняя конфиденциальность сотрудников.

ROI от MDM и бизнес-ценность

MDM следует оценивать как стратегическую инвестицию, а не как простую статью расходов на безопасность. Он приносит финансовую отдачу за счёт сокращения потерь устройств, снижения затрат на ИТ-поддержку и повышения операционной эффективности.

Автоматизированное управление также повышает производительность сотрудников и сокращает простои. Кроме того, более надёжная защита снижает риск и финансовые последствия утечек данных.

Управление устройствами в соответствии с HIPAA

Организации здравоохранения обязаны защищать электронные данные пациентов в соответствии с требованиями безопасности HIPAA. MDM помогает обеспечивать шифрование, контроль аутентификации, безопасную передачу данных и подробные журналы аудита. Он также позволяет выполнять удалённую очистку и централизованно применять политики для устройств, обращающихся к медицинским системам. Эти меры снижают риски несоответствия, одновременно обеспечивая мобильные рабочие процессы в медицинских учреждениях.

MDM для розничных операций и безопасности

Розничные организации полагаются на мобильные устройства для POS-систем, управления запасами и операций в магазине. MDM обеспечивает безопасность, актуальность и соответствие этих устройств стандартам, таким как PCI-DSS. Централизованное управление сокращает простои и упрощает развёртывание устройств в нескольких точках. В результате повышается операционная эффективность и снижается риск инцидентов безопасности, связанных с платежами.

Revision #31
Created 2026-03-12 17:07:43 UTC by Admin
Updated 2026-11-12 09:57:34 UTC by Admin