Управление мобильными устройствами

Kaspersky Secure Mobility Management

Руководитель направления решений
«Лаборатории Касперского»

Константин Никитин

ПОЛИКОМ про

Предпосылки для создания решения

Новая парадигма организации труда

Удаленная работа

Мобильные устройства
как основной бизнес-инструмент

Изменения в архитектуре ИТ / ИБ

Удаленное управление

- Размытие периметра безопасности
- Повышенное внимание к защите данных

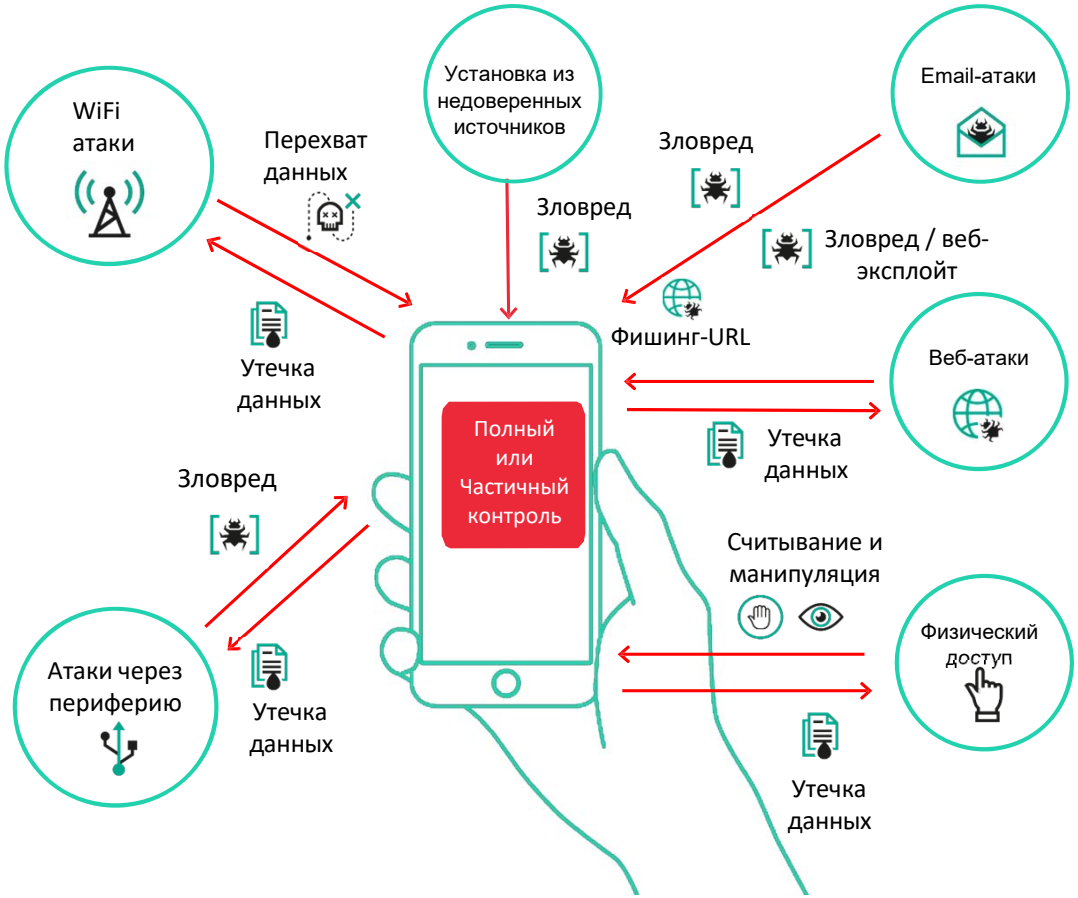
Требование локального рынка

Импортозамещение

Фокус на российское,
сертифицированное решение
класса MDM/EMM/UEM

ПОЛИКОМ про

Векторы атак и риски



Физический доступ

- Утеря
- Кража
- Временный несанкционированный доступ

Софт

- Установка (зловредных) приложений из недоверенного источника
- Эксплуатация уязвимостей
- Email и веб-атаки
- Нецелевое использование легальных средств наблюдения / управления

Периферия

- Заражение через съемные носители
- Нецелевое использование легальных средств удаленного наблюдения / управления

Сетевая атака

- Атаки через небезопасные или скомпрометированные Wi-Fi сети
- Атаки через шнур передачи данных

ПОЛИКОМ про

Модели использования устройств в компании и их связь с режимами управления

COBO
corporate owned,
business only

Владелец – компания
Не допускается его использование в личных целях сотрудником

Возможности для управления
максимальные, вплоть до превращения девайса в Kiosk с фиксированным набором доступных экранов

Технологии, позволяющие реализовать максимальный спектр для управления
Android Device Owner Mode, Supervised iOS MDM

Самый популярный подход в РФ

COPO
corporate owned,
personally enabled

Владелец – компания
Допускается его использование в личных целях сотрудником

Возможности для управления
ограниченные, в основном задача обеспечить изоляцию корпоративных данных и приложений, защиту от угроз, при этом компания сохраняет контроль над глобальными настройками

Технологии, позволяющие реализовать данную модель использования
Android Work Profile (Profile owner mode), non-supervised iOS MDM

BYOD
bring your own device

Владелец – сотрудник
Личное устройство, используемое в том числе для рабочих задач

Возможности для управления
крайне ограниченные, в основном задача обеспечить изоляцию корпоративных данных и приложений, защиту от угроз

Технологии, позволяющие реализовать данную модель использования
Android Work Profile (Profile owner mode), non- supervised iOS MDM, Security for iOS, специальные нативные приложения от UEM вендора

ПОЛИКОМ про

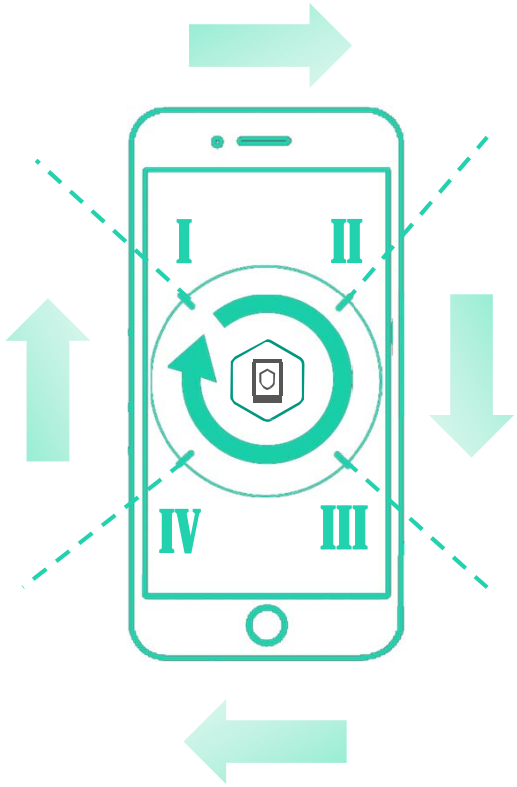
Жизненный цикл использования корпоративных мобильных устройств

Подготовка

- Развертывание сервисов поддержки мобильной платформы (серверная часть)
- Подготовка корпоративного каталога со списком доверенных приложений и портала для подключения BYOD устройств
- Подготовка и конфигурирование сценариев автоматизированного развертывания корпоративных устройств

Поддержка и выведение из обслуживания

- Обеспечение удаленной поддержки
- Аудит потерянных / украденных устройства,
- Отзыв доступа к корпоративным ресурсам
- Выборочное (для BYOD-устройств) или полное обнуление (очистка) устройства



Развертывание и конфигурация

- Загрузка сертификатов безопасности, профилей email, VPN, Wi-Fi
- Установка агентской части решения, обеспечивающей защиту устройств и функции мониторинга/контроля
- Загрузка и применение корпоративных политик безопасности и ограничений использования
- Установка и автоматизированное конфигурирование бизнес-приложений

Защита и контроль

- Отслеживание событий безопасности
- Реагирование на события уровня «инцидент», включающее вмешательство администратора
- Отслеживание и реагирование на события регуляторных политик

Kaspersky Secure Mobility Management

ПОЛИКОМ про

Соотношение с мобильной безопасностью в KESB

Kaspersky
security center

Защита конечных точек
Windows
Linux
MacOS

Защита серверов
Windows
Linux

Полная функциональность KESB

Базовое Управление
Базовое управление приложениями и системой (вкл. Windows)

Защита мобильных устройств
Антивирус
Контроли
Антифишинг

Продвинутое Управление и контроль

Поддержка режимов
Device Owner/ Kiosk и Supervised

Управление сертификатами и VPN профилями

Управление профилями приложений

Контроль соответствия

Корп. каталог приложений

Полная функциональность KSMM

ПОЛИКОМ про

Ключевые функции

Управление устройствами Android, iOS/ IPadOS и жизненным циклом Windows-устройств

Защита от угроз при помощи приложений на устройствах
KES Android и Security for iOS

Продвинутые сценарии контроля и управления для Android
режим Device Owner

Корпоративный каталог приложений
можно размещать приложения для любых платформ или ссылки

Контроль соответствия для платформ Android и iOS

Управление и работа с сертификатами и VPN
per-app VPN

ПОЛИКОМ про

Возможности Kaspersky Security for Mobile

Безопасность

- Многоступенчатая проверка признаков ВПО
- Защита от веб- угроз
- Обнаружение root привилегий

MAM

- Контроль приложений
- Выборочное удаление данных
- Централизованное управление email и доступом к VPN

Централизованное управление

- Поддержка Android и iOS
- Управление мобильными устройствами из единой консоли для ПК и серверов

MDM

- Android/iOS MDM
- Exchange ActiveSync, Samsung KNOX, Android for Work
- Совместимость со сторонними EMM решениями

Анти-вор

- Блокировка и удаление данных
- Геолокация
- Включение сигнала тревоги
- Сообщение
- Снимок с фронтальной камеры

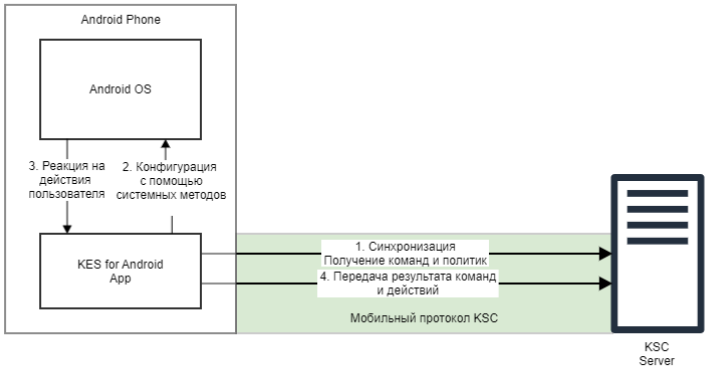
ПОЛИКОМ про

Технические способы реализации управления

С использованием агента на устройстве

Пример: KES for Android, Security for iOS

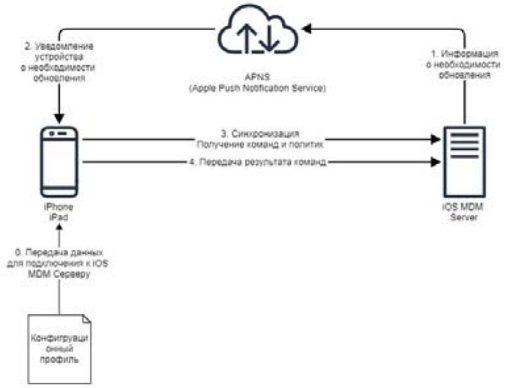
- Получение и применение политик - задача агента
- Использование системных методов для конфигурации *(Android DevicePolicyManager, Samsung KNOX API и другие)*
- Реализация функций управления на стороне агента



Без использования агента на устройстве

Пример: iOS MDM сервер и профили iOS

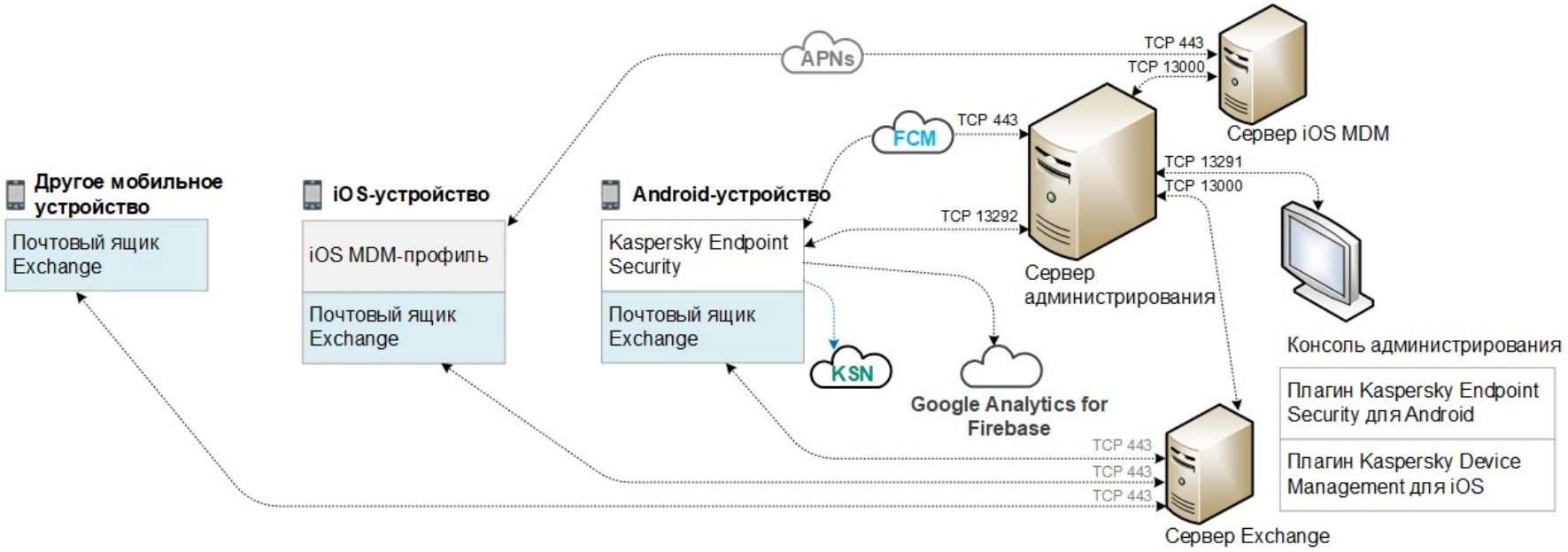
- С помощью агента управления, встроенного в ОС
- Нельзя контролировать процесс выполнения команд и применения политик
- Зависимость на инфраструктуру вендора ОС
- Набор настроек ограничен



ПОЛИКОМ про

Упрощённая схема взаимодействия компонентов

Общая архитектура решения



Kaspersky Security для мобильных устройств включает в себя компоненты:

- Мобильное приложение Kaspersky Endpoint Security для Android
- Плагин управления Kaspersky Endpoint Security для Android
- Плагин управления Kaspersky Device Management для iOS

ПОЛИКОМ про

MDM функции

Функция	Android	iOS
Аппаратные ограничения (Wi-Fi, Bluetooth, камера)	+	+
Exchange ActiveSync	+	+
Apple iOS MDM	не применимо	+
Samsung KNOX, Android for Work	+	не применимо
Ограничение на удаление приложения или профиля	+	+
Контроль соответствия политикам	+	+
Обнаружение Jailbreak/Root	+	-
Удаление корпоративных данных	+	+
Контроль приложений	+	+
Управление встроенным почтовым клиентом	+	+

ПОЛИКОМ про

Сценарии применения

Нужны спец. решения для защиты и контроля

Интегрированный продукт, все сценарии использования

Нужна безопасность данных и соответствие регуляциям

Инструменты изоляции данных и доступ при удовлетворении

Использование различных мобильных платформ

KSMM поддерживает все основные платформы

Западные вендоры ушли с рынка, нужна замена

Полноценная замена западных решений класса EMM и даже UEM

Высокий риск утери, кражи, ведет к рискам для корпоративных данных

Инструменты для удаленного стирания, вывода из эксплуатации

Мобильные устройства – мишень для соц. Инженерии

Антифишинг в том числе против SMS-атак

Динамичный жизненный цикл, частые изменения

Автоматизация жизненного цикла и удобные инструменты

Целевая аудитория – мишень для целевых атак

KSMM - часть архитектуры XDR, для противодействия APT

BYOD помогает экономить, но нужны средства контроля

KSMM предлагает полный инструментарий для безопасного BYOD

ПОЛИКОМ про

kaspersky
Platinum Partner

ПОЛИКОМ про

Руководитель направления решений
«Лаборатории Касперского»

Константин Никитин

тел: + 7 (812) 325 84 00

e-mail: KNikitin@polikom.ru