Kaspersky Secure Mobility Management

Оглавление

Проблематика

Предпосылки создания продукта

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

Аналитика рынка

- Мобильный парк смартфонов (Android + iOS) в B2B / B2G – 19-26 млн устройств
- Используют MDM/EMM/UEM ~10%, преимущественный сценарий – COBO (устройство принадлежит компании, исп. только для бизнеса)
- До «великого исхода» в основном обслуживались западными вендорами

Модели использования устройств в компании и их связь с режимами управления

COBO (corporate owned, business only)

Владелец – компания

Не допускает 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

COPE (corporate owned, personally enabled)

Владелец – компания

Допускается 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

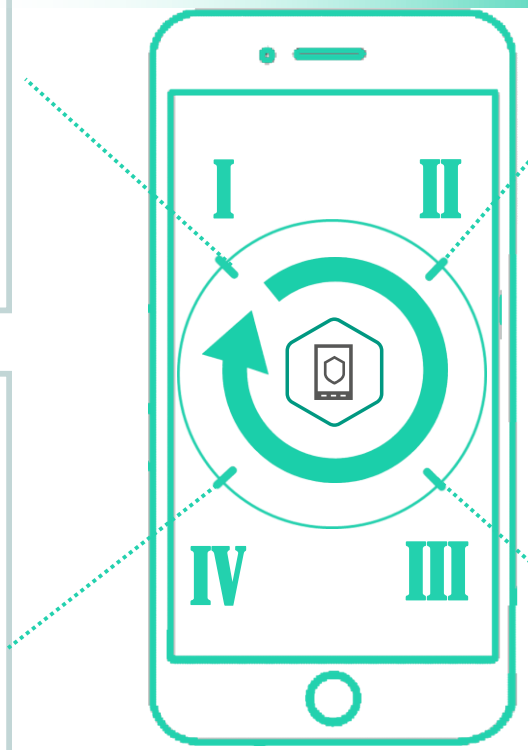
Жизненный цикл использования корпоративных мобильных устройств

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

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



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

Защита и контроль

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

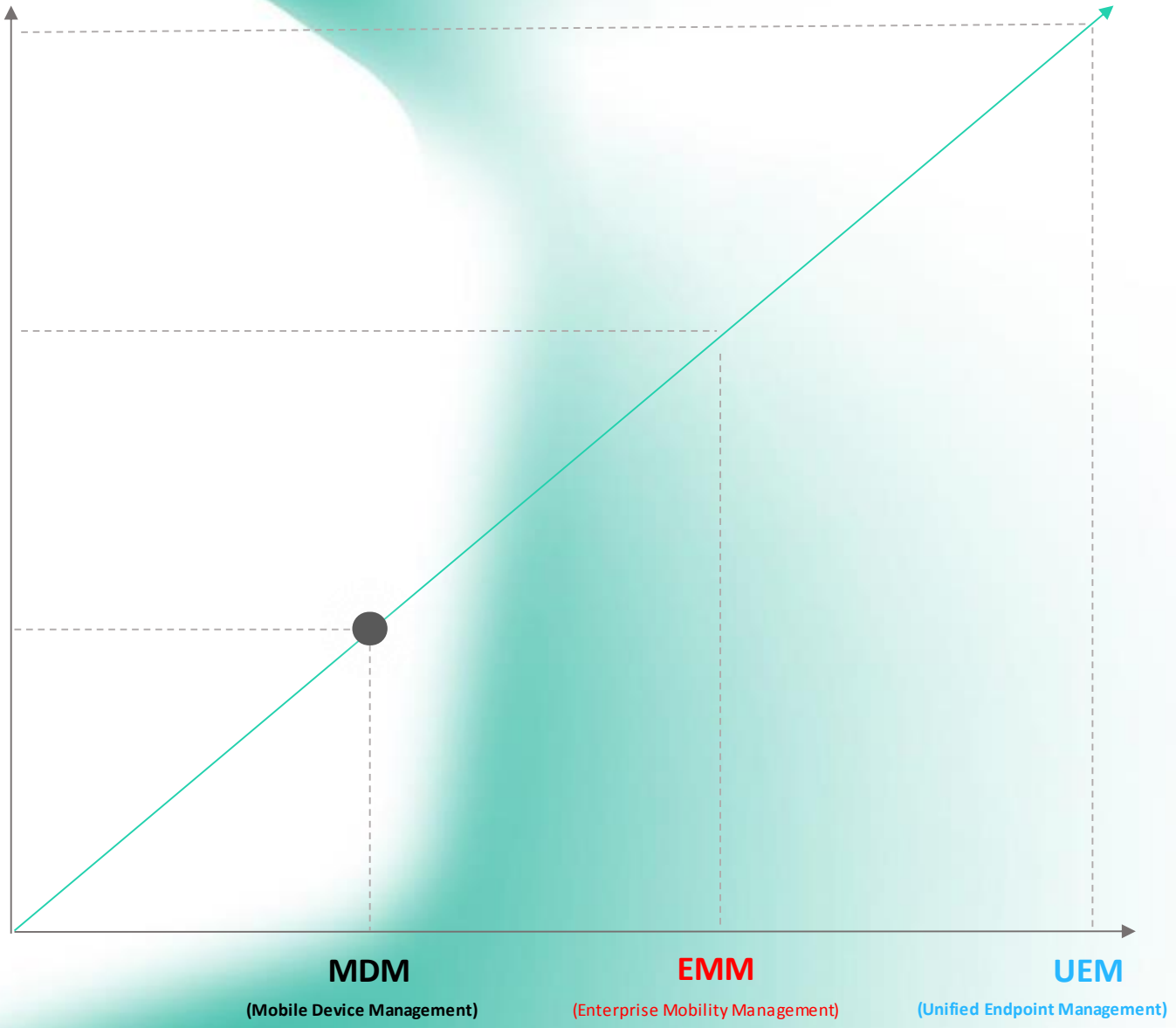
Kaspersky Secure Mobility Management

Позиционирование

MDM vs EMM vs UEM?

Позиционирование на рынке решений по управлению мобильными устройствами

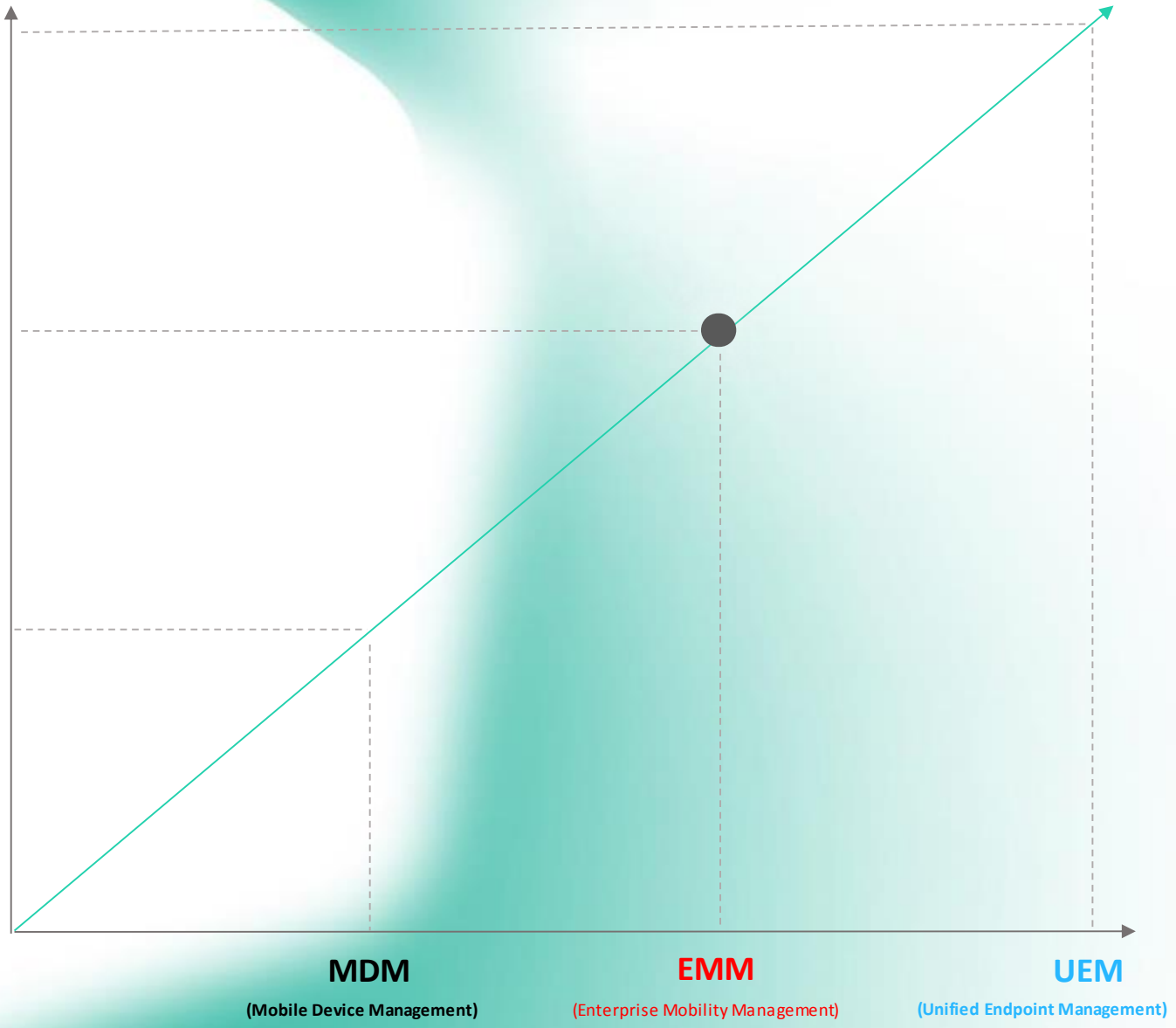
- Сбор отчетов и отслеживание местоположения
- Затирание информации и блокировка устройства
- Инициализация мобильных устройств
- Управление сторонним ПО
- Применение политик



Позиционирование на рынке решений по управлению мобильными устройствами

- Контроль соответствия устройства требованиям ИБ
- Обеспечение безопасности данных
- Поддержка контейнеризации
- Поддержка BYOD и COSU

- Сбор отчетов и отслеживание местоположения
- Затирание информации и блокировка устройства
- Инициализация мобильных устройств
- Управление сторонним ПО
- Применение политик



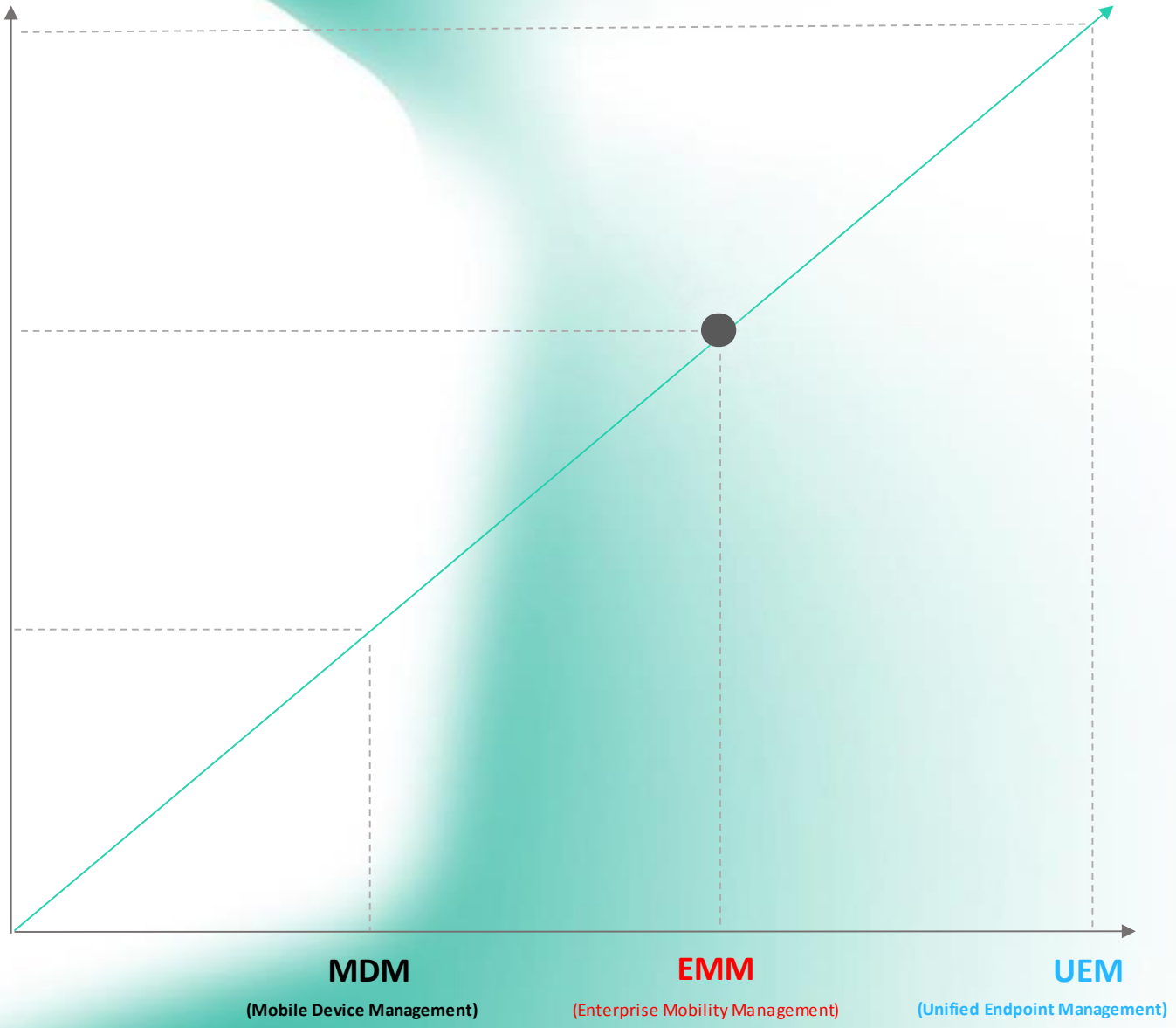
Позиционирование на рынке решений по управлению мобильными устройствами

Kaspersky Security Mobility Management

Больше чем просто EMM?...

- Контроль соответствия устройства требованиям ИБ
- Обеспечение безопасности данных
- Поддержка контейнеризации
- Поддержка BYOD и COSU

- Сбор отчетов и отслеживание местоположения
- Затирание информации и блокировка устройства
- Инициализация мобильных устройств
- Управление сторонним ПО
- Применение политик

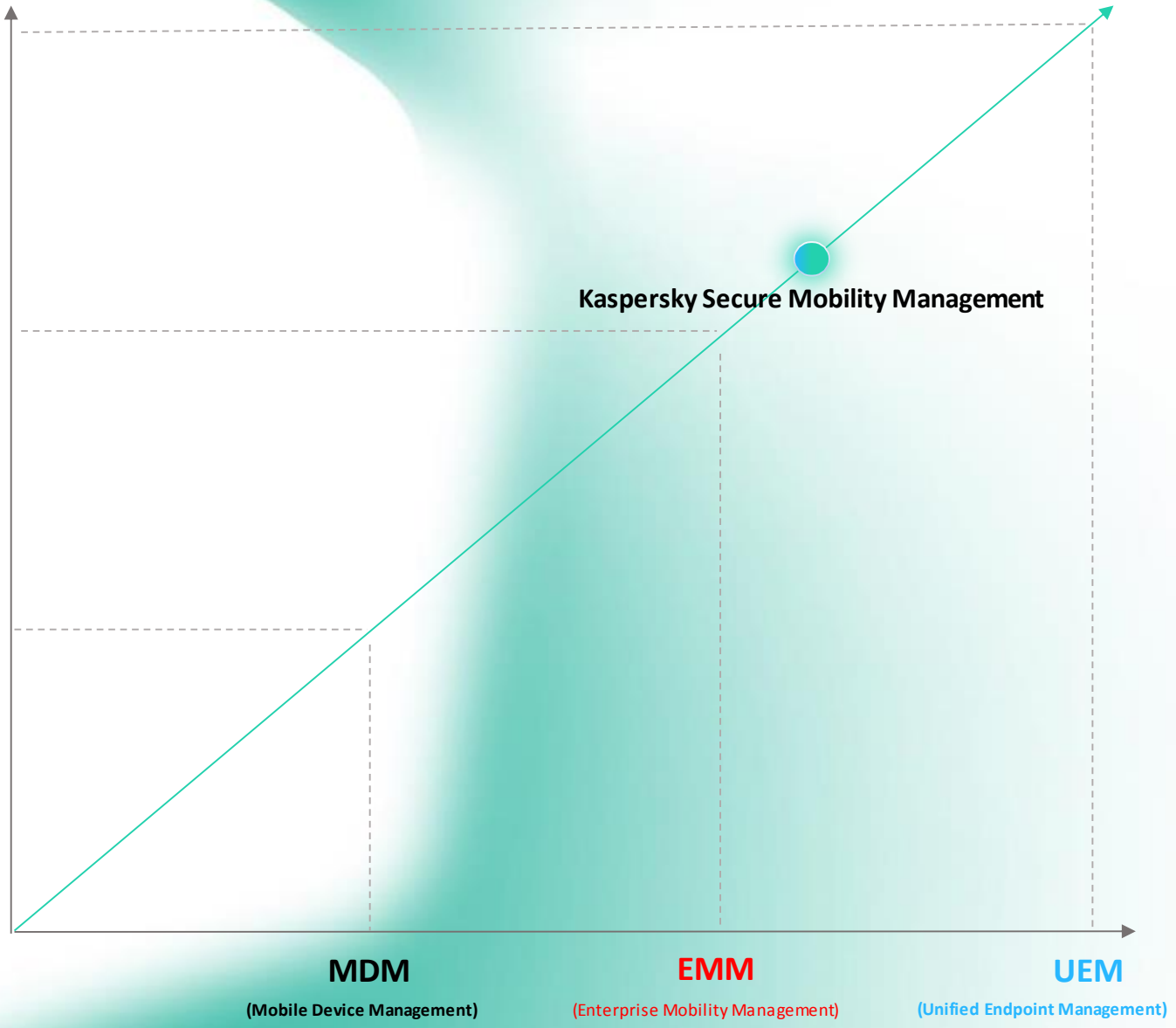


Позиционирование на рынке решений по управлению мобильными устройствами

- Управление и контроль инфраструктуры рабочих станций и мобильных устройств из единой консоли Сервера Администрирования Kaspersky Security Center

- Контроль соответствия устройства требованиям ИБ
- Обеспечение безопасности данных
- Поддержка контейнеризации
- Поддержка BYOD и COSU

- Сбор отчетов и отслеживание местоположения
- Затирание информации и блокировка устройства
- Инициализация мобильных устройств
- Управление сторонним ПО
- Применение политик

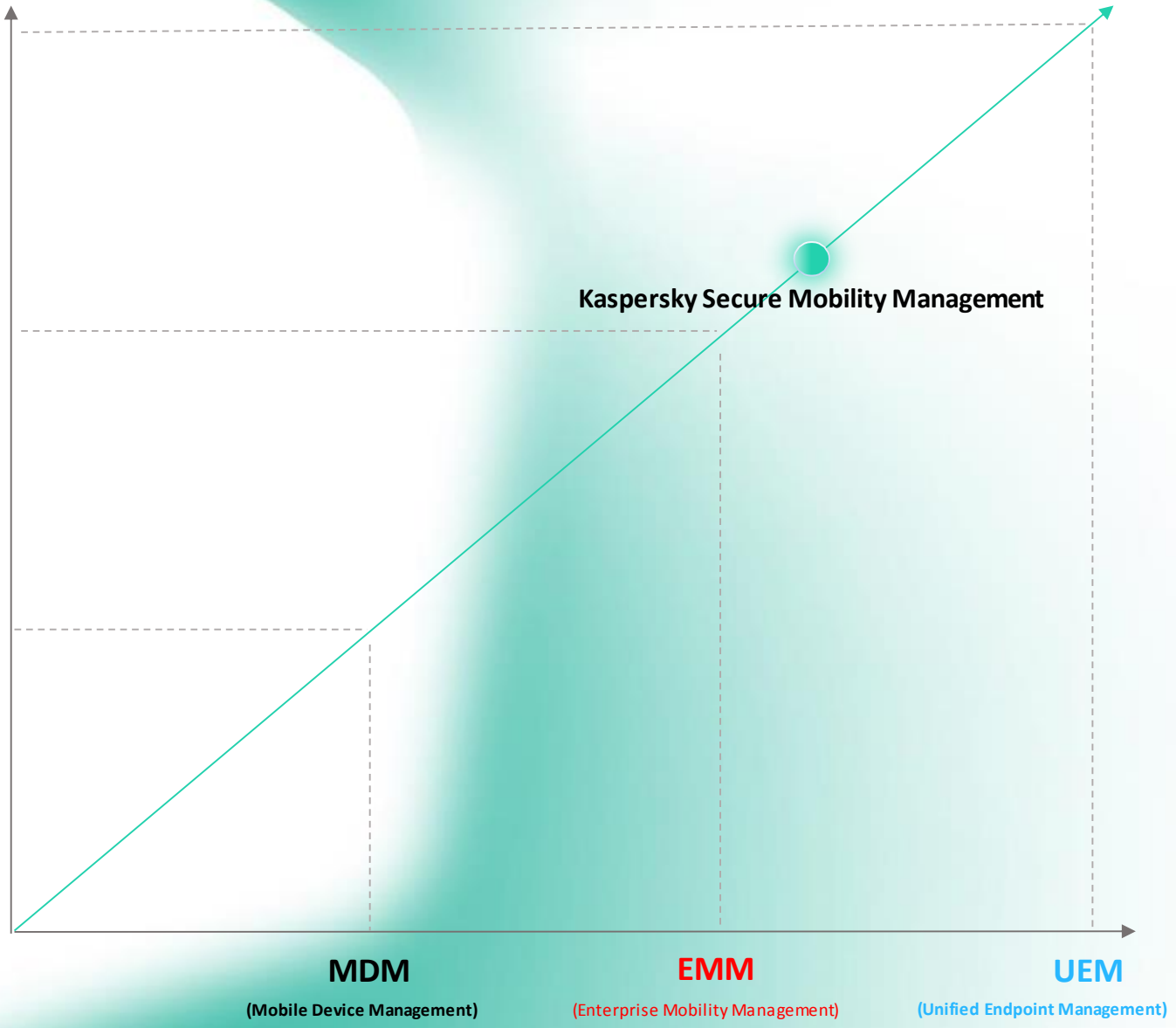


Позиционирование на рынке решений по управлению мобильными устройствами

- Управление и контроль инфраструктуры рабочих станций и мобильных устройств из единой консоли Сервера Администрирования Kaspersky Security Center

- Контроль соответствия устройства требованиям ИБ
- Обеспечение безопасности данных
- Поддержка контейнеризации
- Поддержка BYOD и COSU

- Сбор отчетов и отслеживание местоположения
- Затирание информации и блокировка устройства
- Инициализация мобильных устройств
- Управление сторонним ПО
- Применение политик



Что представляет из себя новый продукт?

Класс решения: продукт полностью соответствует классу Enterprise Mobility Management и частично соответствует классу Unified Endpoint Management (согласно определению Gartner)

Публичное позиционирование: продукт позиционируется как Unified Endpoint Management решение

Ключевые функции:

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

Корпоративный каталог приложений (можно размещать приложения для любых платформ или ссылки)

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

Контроль соответствия для платформ Android и iOS

Продвинутые сценарии контроля и управления для Android (режим Device Owner)

Управление и работа с сертификатами и VPN (per-app VPN)

Полная поддержка режима supervised для iOS и возможностей в нем

Функционал Kaspersky Systems Management

Управление обновлениями программного обеспечения при постоянном отслеживании потенциальных уязвимостей – одна из самых важныхn и ресурсоемких задач IT-департамента.

Контроль устройств и ПО

- Централизованное управление доступом пользователей и устройств к корпоративным данным
- Мониторинг новых приложений и устройств в инфраструктуре
- Инвентаризация программного и аппаратного обеспечения

Безопасность инфраструктуры

- Загрузка, тестирование и распространение исправлений и обновлений;
- Интеграция со сторонними SIEM – системами (Syslog);
- Выявление и приоритизация уязвимостей;
- Составление отчетов по уязвимостям.

Управление рабочими станциями

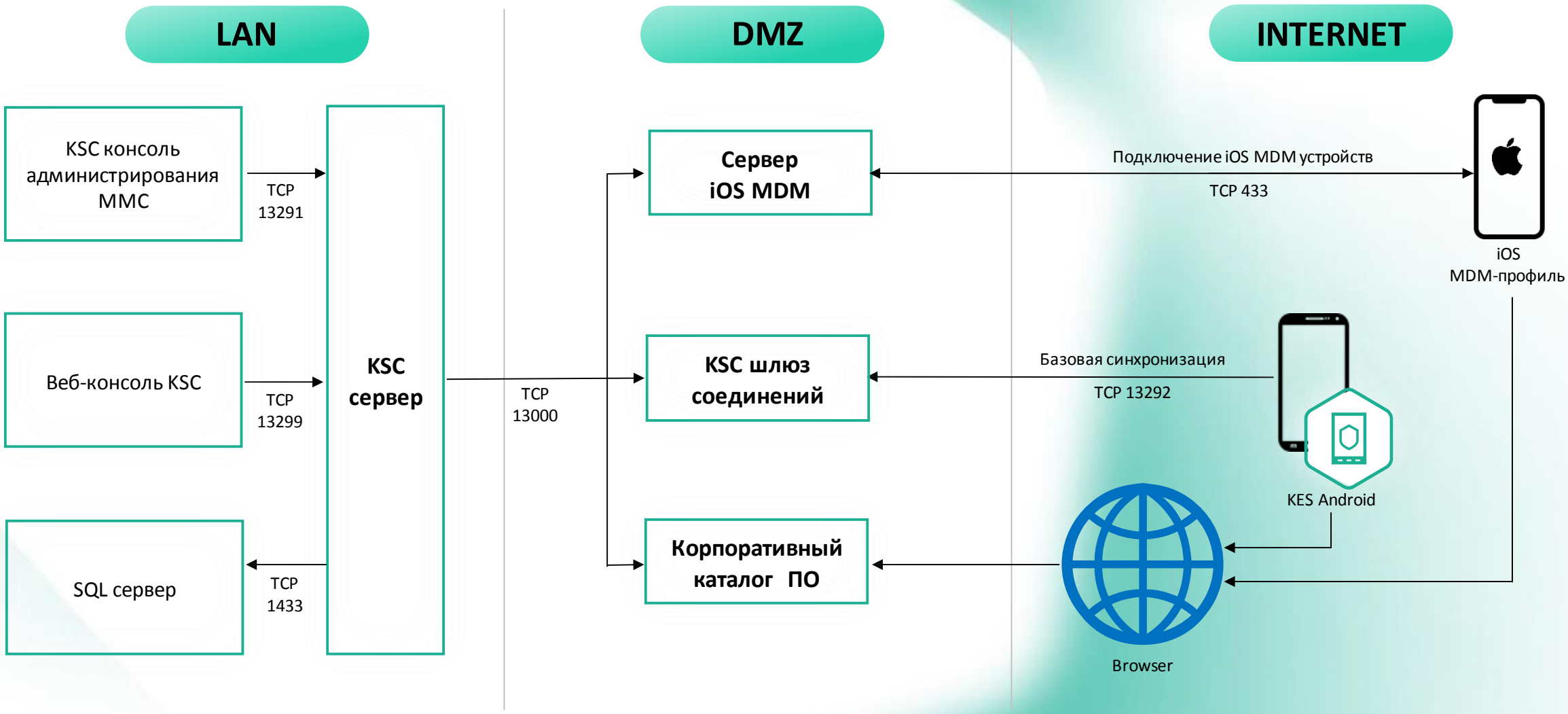
- Удаленное подключение к PC (просмотр / перехват управления);
- Установка сторонних программ и управление лицензиями;
- Установка обновлений Центра обновления Windows;
- Синхронизация с Windows Update;
- Развертывание образов ОС.

Как новое решение соотносится с MDM и мобильной безопасностью в KESB

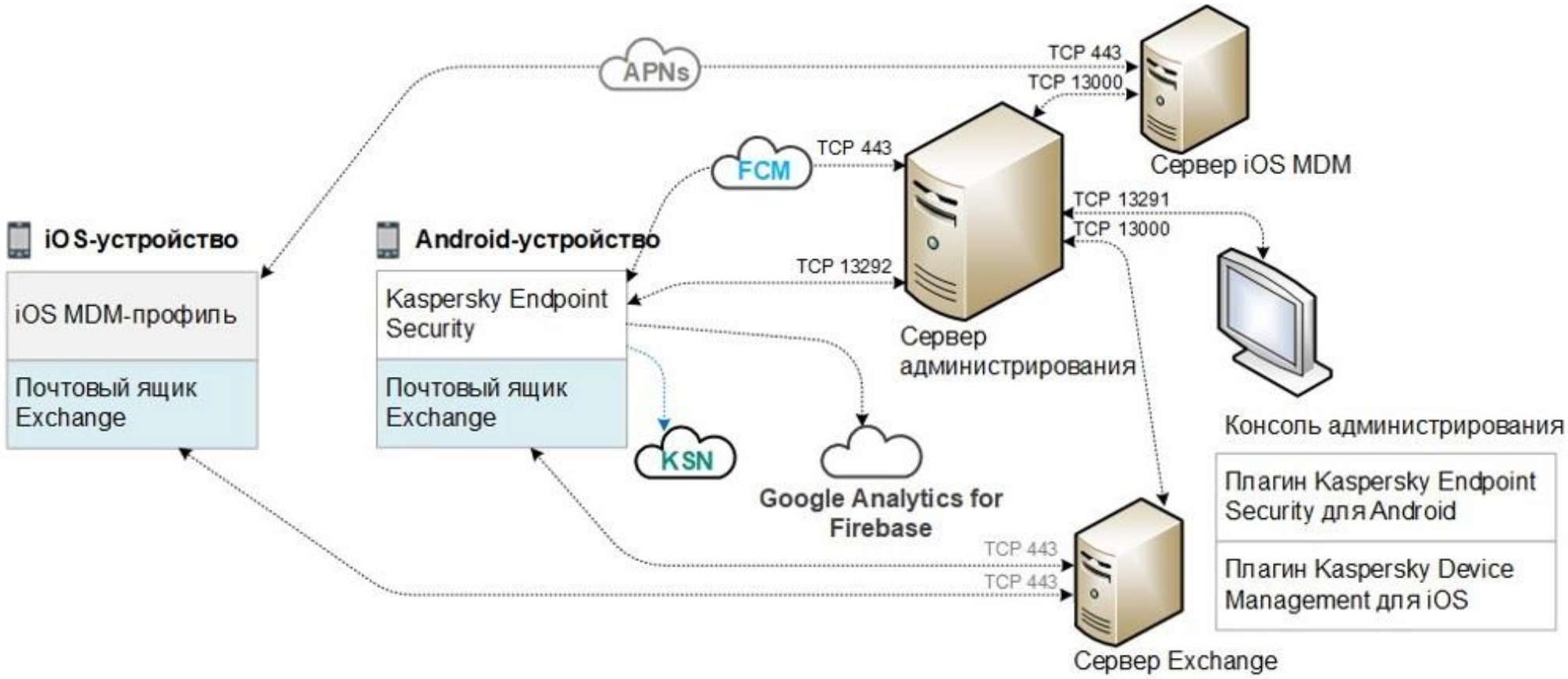
Полная функциональность KESB

Полная функциональность KSMM

Принципиальная схема взаимодействия компонентов Kaspersky Secure Mobily Management



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

Упрощённая схема взаимодействия компонентов

Kaspersky
Security Center

MDM и MTD для
устройств на Android и iOS

Нативный транспорт Apple Push
Notification Service

MDM профиль

Синхронизация с настраиваемым интервалом
средствами Kaspersky mobile protocol

KES для Android

Для Android возможна синхронизация через FCM

Защита мобильных устройств

Контроль приложений

- Поиск вредоносного ПО
- Репутация и категоризация ПО
- Белые/чёрные списки ПО
- Эффективная работа в офлайн режиме

Безопасность сети

- Проверка URL на malware и phishing
- Доставка сертификатов для VPN доступа

Kaspersky Security Network

Контроль уязвимостей

- Обнаружение Root
- Контроль применения политик безопасности, с возможностью блокировки доступа

Совместимость с большинством устройств

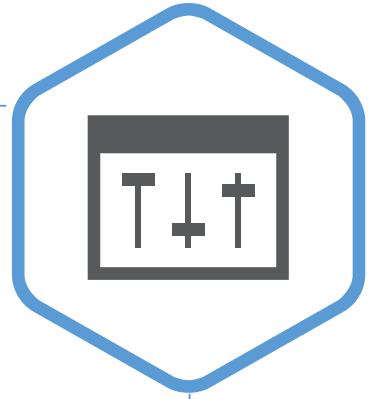
- Оперативная поддержка новых версий ОС
- Возможность установки минуя Google Play

Основные модули

Модуль	Android
Защита от мобильного ВПО	
Сигнатурный анализ	+
Kaspersky Security Network	+
Защита от веб-угроз	+
Обновление баз	+
Веб-контроль	
Анти-фишинг	+
Категорирование веб-ресурсов	+
Анти-вор	
Блокировка и удаление данных	+
Геолокация	+
Снимок с фронтальной камеры	+
Сигнал тревоги	+
Определение root устройств	+

Mobile Device Management

Kaspersky Security Center



Apple MDM

- Управление через iOS MDM профили
- Все базовые функции Apple MDM

Samsung KNOX

- Поддержка KNOX-контейнеров
- Поддержка Samsung устройств начиная с Android 5.0

KES для Android

- Большой список возможностей через единое приложение
- Поддержка Android for Work
- Работа с 3rd party EMM платформами

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	+	+

Технические способы реализации управления мобильными устройствами

Управление с помощью агентского ПО

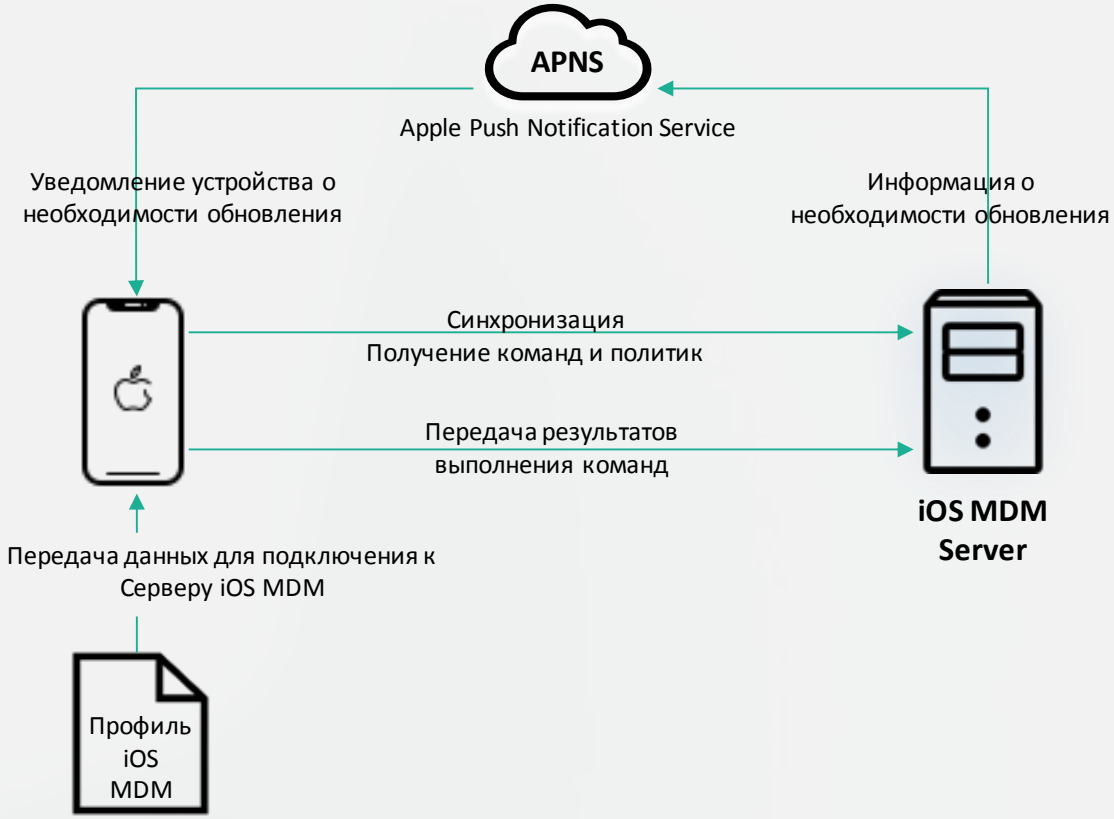
- Реализация агентом Kaspersky функций управления и защиты мобильного устройством
- Использование системных методов для конфигурации Android Device Policy Manager
  Samsung KNOX API и др.

Агентское ПО Kaspersky:

- Kaspersky Endpoint Security for Android
- Kasperksy Security for iOS

Безагентное управление

- С помощью Агента управления, встроенного в ОС
- Доставка конфигурации через инфраструктуру вендора ОС



Лицензирование

Ключевые сценарии

Kaspersky Secure Mobility Management

Kaspersky Secure Mobility Management лицензируется по схеме “per device” – т.е. одна лицензия позволяет использование всех функций защиты и управления, доступных для конкретной поддерживаемой платформы на одном устройстве

Все клиенты, переходящие с конкурентного решения (вкл. импортозамещение)

Существующий клиент KESB: покупка в момент обновления

Существующий клиент KESB, покупка до истечения их терма

Новый клиент, без миграции с конкурентов

План развития на 2023 год

kaspersky

План выпуска новых версий

Сделано | **В разработке**

I кв. 2023 New

Version 1

Android

Поддержка Device Owner режима

Улучшенные настройки требований к паролю на устройстве

Дополнительные настройки для Samsung KNOX

Новые вожможности по настройке Wi-Fi

Новые опции для удаления всех данных на потерянном или украденном Android-устройстве

Добавление Web-Clips на рабочий стол

iOS MDM

Контроль соответствия устройства требованиям для iOS

Продвинутые сценарии управления установленными приложениями

Новые команды - сбросить пароль, настроить обновление ОС и Bluetooth

Новые возможности по настройке Wi-Fi - IKEv2, Safari domains

Новая опция для настройки принудительного использования пароля на устройстве

Новые опции для управления функциями операционной системы на устройствах в режиме supervised

Корпоративный каталог приложений, первый релиз

II кв. 2023 New

Version 2

Android

Новые опции в режиме Device Owner

Поддержка отслеживания смены SIM-карты

Режим списка запрещенных сайтов в Web Control

Обработка необходимости выдачи дополнительных разрешений в режиме Profile Owner на устройствах с MIUI (Xiaomi)

iOS MDM

Расширение возможностей контроля соответствия

Поддержка режима "Пропажа"

Поддержка Activation Lock

Поддержка режима отдельного VPN для каждого приложения

Принятие соглашений в консоли управления

III кв. 2023 New

Version 3

Android

Поддержка Android 14

Новые возможности в режиме Profile Owner

Новые опции в режиме Device Owner

Сценарии автоматизации управления сертификатами и пользователями

AppConfig конструктор в консоли

Снижение минимального периода синхронизации, без использования Push-сервисов

Huawei MDM базовая поддержка

iOS MDM

Поддержка iOS and iPadOS 17

Сценарии автоматизации управления сертификатам и

Поддержка отслеживания смены SIM-карты

Поддержка режим киоска

Управление обоями рабочего стола

IV кв. 2023 New

Version 4

Android

Улучшения в сценариях лицензирования

Сбор информации об установленных приложениях и удобное представление в консоли

Новые опции для удаления данных на устройстве

Дополнительная защита от Factory Reset

Управление разрешениями для установленных приложений

Отправка push-нотификаций

Специальные политики для роуминга

Применение политик в зависимости от гео-позиции девайса

Расширение возможностей контроля соответствия

iOS MDM

Улучшения в сценариях лицензирования

Сценарии автоматизации для списка пользователей

Отправка push-нотификаций

Поддержка определения местоположения

ЗАПРОСИТЬ ДЕМОНСТРАЦИЮ

kaspersky АКТИВИРУЙ БУДУЩЕЕ