Kaspersky® Security для мобильных устройств

Гибкий контроль и надежная защита мобильных устройств

Возможности

- Защита от вредоносного ПО
- Анти-Фишинг и Анти-Спам
- Защита от интернет-угроз
- Контроль приложений
- Обнаружение попыток несанкционированной перепрошивки
- Контейнеризация приложений
- Анти-Вор
- Портал самообслуживания
- Централизованное управление
- Веб-консоль

Поддерживаемые платформы:

- Android™
- iOS®
- Windows 10 Mobile®

Преимущества мобильных устройств для бизнеса очевидны: они повышают продуктивность работы сотрудников, позволяя получить доступ к информации отовсюду и в любое удобное время. В то же время мобильные устройства, используемые в рабочих целях (BYOD), представляют большую опасность для безопасности компании.

Kaspersky Security для мобильных устройств – это решение классов Mobile Threat Defense (MTD) и Mobile Threat Management (MTM), которое обеспечивает безопасное использование смартфонов и планшетов в рабочих целях.

Основные возможности

Передовая защита мобильных устройств

Количество угроз для мобильных устройств растет огромными темпами. Уже в первой половине 2017 года число вирусов-шифровальщиков для мобильных ОС превысило общее число угроз для мобильных угроз, зафиксированное в 2016 году. Kaspersky Security для мобильных устройств сочетает защиту от вредоносного ПО с анализом угроз на основе облачных технологий и возможностями машинного обучения. Это позволяет успешно бороться с известными, новыми и сложными угрозами.

Управление мобильными устройствами (MDM)

В решении доступны групповые политики для Android, iOS и Windows Phone, позволяющие создавать или активировать правила использования паролей, шифрования, Bluetooth и камеры. С помощью консоли управления можно получать отчеты об устройстве и установленных приложениях.

Управление мобильными приложениями (MAM)

Контроль приложений для Android и iOS позволяет определить, какие приложения могут быть установлены, а также дает возможность создавать «белые» и «черные» списки для этих приложений.

Гибкое развертывание

Гибкие возможности развертывания поддерживают сценарии BYOD и COPE (корпоративное устройство для персонального использования) – для сред BYOD приложение устанавливается из Google Play или AppStore, а для сред COPE можно использовать портал самообслуживания или же установить приложение с необходимыми настройками силами администратора. Другими словами, компаниям не нужно менять стратегию обеспечения кибербезопасности мобильных устройств.

Централизованное управление

Kaspersky Security для мобильных устройств позволяет управлять мобильными устройствами из той же консоли, которая используется для остальных рабочих мест: Kaspersky Security Center или Kaspersky Endpoint Security Cloud. Просмотр данных на устройствах, создание и администрирование политик, отправка команд на устройства и составление отчетов — все это доступно из единой, простой в использовании консоли управления.

Возможности защиты и администрирования

Многоуровневая защита от вредоносного ПО

Сочетание проактивных облачных методов обнаружения и анализа с традиционными технологиями обеспечивает защиту от известных, новых и комплексных угроз. Проверки по требованию и по расписанию и автоматические обновления повышают эффективность защиты.

Защита от фишинга и спама

Мощные технологии борьбы с фишингом и спамом защищают устройства и данные на них от фишинговых атак и помогают отфильтровывать нежелательные звонки и текстовые сообщения.

Защита от интернет-угроз

Сеть Kaspersky Security Network (KSN), данные которой обновляются в режиме реального времени, служит основой для надежной и безопасной технологии веб-фильтрации. На устройствах под управлением Android веб-фильтрация доступна в браузере Chrome™, а для платформ iOS и Windows 10 Mobile доступен безопасный браузер «Лаборатории Касперского».

Контроль приложений

Контроль приложений позволяет разрешить использование только приложений, одобренных администратором. Пользуясь Контролем приложений, администраторы могут получать данные об установленном ПО и устанавливать нужные приложения. Интеграция с KSN упрощает создание черных и белых списков и управление ими.

Обнаружение попыток несанкционированной перепрошивки

Решение обнаруживает перепрошитые устройства и оповещает администратора, который может заблокировать эти устройства или выполнить на них выборочную очистку.

Контейнеризация приложений

Технология контейнеризации приложений позволяет разделять корпоративные и личные данные и применять дополнительные политики (такие как шифрование) для защиты конфиденциальных данных. Если сотрудник решит покинуть компанию, данные в контейнерах можно будет удалить, а личную информацию – оставить.

Анти-Вор

Средства удаленной защиты оберегают корпоративную информацию, даже если устройство похищено или утеряно. Доступны средства определения местонахождения и блокирования устройства, выборочной или полной очистки, отслеживания SIM-карты, создания тайного фото и активации тревожного сигнала.

Управление мобильными устройствами (MDM)

Благодаря поддержке Microsoft® Exchange ActiveSync®, iOS MDM и Samsung KNOX™ возможно создание единых или раздельных политик для каждой платформы (например, обязательное шифрование, обязательное применение пароля, правила использования камеры и настройки APN/VPN). Сервисы Android for Work позволяют создавать корпоративные профили, а также управлять бизнес-приложениями и устройствами.

Портал самообслуживания

Портал позволяет передать повседневные задачи управления безопасностью и регистрацию одобренных устройств сотрудникам. При подключении к сети нового устройства все требуемые сертификаты могут доставляться автоматически через портал. В случае потери устройства сотрудник может сам выполнить все необходимые действия для защиты информации.

www.kaspersky.ru

#ИстиннаяБезопасность

Как приобрести

Kaspersky Security для мобильных устройств продается отдельно, а также входит в состав следующих решений:

- Kaspersky Endpoint Security для бизнеса Cloud;
- Kaspersky Endpoint Security для бизнеса Стандартный;
- Kaspersky Endpoint Security для бизнеса Расширенный;
- Kaspersky Total Security для бизнеса.

Узнайте, как приобрести продукты и решения «Лаборатории Касперского»: www.kaspersky.ru/how-to-buy