Kaspersky® Security для мобильных устройств

Многоуровневая защита и гибкий контроль мобильных устройств

Использование мобильных устройств повышает продуктивность сотрудников. В то же время обеспечение доступа к корпоративной информации в любое время из любой точки мира влечет серьезные риски, так как конфиденциальная информация находится на персональных смартфонах и планшетах сотрудников – за пределами традиционного IT-периметра защиты. Киберпреступники понимают ценность подобных данных, поэтому количество и сложность атак на мобильные устройства постоянно растут. Кроме того, мобильные устройства сотрудников часто служат для злоумышленников точкой входа в корпоративную сеть и открывают дорогу вредоносным атакам, которые могут повлечь тяжелый ущерб для компании.

Kaspersky Security для мобильных устройств сочетает передовые технологии обнаружения вредоносного ПО, глобальную облачную аналитику и технологии машинного обучения. Это позволяет успешно бороться с известными, неизвестными и передовыми киберугрозами, нацеленными на мобильные устройства.

Основные преимущества

Передовые технологии защиты от вредоносного ПО и утечек данных

За последние три года число угроз, нацеленных на мобильные устройства, преодолело отметку 17 миллионов, а количество атакованных пользователей смартфонов и планшетов увеличилось в четыре раза. Решение «Лаборатории Касперского» успешно борется с угрозами для корпоративных мобильных устройств, в том числе надежно защищает от утечки конфиденциальные данные.

Поддержка сторонних решений класса Enterprise Mobility Management (EMM)

Вы можете использовать ваше EMM-решения для развертывания и настройки Kaspersky Endpoint Security для Android, что позволяет совместить средства защиты с текущими бизнес-процессами.

Централизованное управление

Kaspersky Security для мобильных устройств позволяет управлять мобильными устройствами из той же консоли, которая используется для управления остальными рабочими местами: 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.

Управление мобильными устройствами

Решение содержит средства управления мобильными устройствами (MDM), которые, в частности, позволяют работать с аутентификационными сертификатами и определять параметры доступа к корпоративным принтерам и сетям Wi-Fi. Гибкие настройки регистрации устройств упрощают использование устройств Android и iOS и управление ими.

Возможности

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 Samsung Internet Browser и браузерах на основе Chrome.

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 несанкционированной перепрошивки

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

Интеграция со сторонними EMM-системами

Если ваша организация использует решение класса EMM для настройки мобильных устройств, вам все равно необходимо защищать файлы и приложения от вредоносного ПО, а также противодействовать фишингу и утечке данных. Благодаря интеграции решения со сторонними EMM-системами (VMware AirWatch, MobileIron, SOTI и др.) вы можете развернуть Kaspersky Endpoint Security для Android и настроить параметры защиты из вашей EMM-консоли.

Анти-Вор

Средства удаленной защиты защищают 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. Интеграция с Google Firebase Cloud Messaging (GCM) и Apple Push Notification Services (APNs) обеспечивает практически мгновенную передачу команд.

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.

Kaspersky Security для мобильных устройств доступно как отдельное решение, а также входит в состав:
- Kaspersky Endpoint Security Cloud
- Kaspersky Security для бизнеса (Стандартный, Расширенный, Total)

#истиннаябезопасность
#HuMachine

www.kaspersky.ru