KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Многоуровневая защита, управление и контроль мобильных рабочих мест

Мобильные устройства все чаще служат мишенью для атак киберпреступников. В то же время, политика использования личных устройств в рабочих целях (Bring Your Own Device, BYOD) расширяет диапазон устройств в составе корпоративной сети, что создает IT-администраторам дополнительные сложности в управлении и контроле IT-инфраструктуры.

Kaspersky Security для мобильных устройств обеспечивает безопасность устройства независимо от его местонахождения. Решение защищает от постоянно развивающегося вредоносного ПО для мобильных устройств и позволяет осуществлять мониторинг и контроль смартфонов и планшетов в вашей корпоративной сети из единого центра и с минимальным влиянием на работу пользователей.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Надежная защита от вредоносного ПО
- Защита от спама и фишинговых ссылок
- Веб-Контроль
- Контроль программ
- Выявление попыток рутинга/джейлбрейкинга
- Контейнеризация
- Анти-Вор
- Управление мобильными устройствами
- Портал самообслуживания
- Централизованное управление
- Веб-консоль

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ:

- Android™
- iOS®
- Windows® Phone

Основные возможности

ПЕРЕДОВАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО И БЕЗОПАСНОСТЬ ДАННЫХ

В одном только 2014 году «Лаборатория Касперского» зафиксировала почти 1,4 млн. вредоносных атак на мобильные устройства. Kaspersky Security для мобильных устройств сочетает защиту от вредоносного ПО с другими технологиями безопасности, что позволяет обеспечить многоуровневую защиту данных, хранящихся на мобильных устройствах, от известных и новых угроз.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (MDM)

Интеграция со всеми основными платформами для управления мобильными устройствами позволяет осуществлять развертывание и контроль удаленно (Over-the-Air, OTA), что значительно облегчает защиту и управление устройствами на базе Android, iOS и Windows Phone.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ ПРИЛОЖЕНИЯМИ (MAM)

Изолированные контейнеры для приложений и возможность выборочной очистки памяти устройства позволяют разделить корпоративную и личную информацию, хранящуюся на устройстве сотрудника. Сочетание функционала шифрования и защиты от вредоносного ПО в составе Kaspersky Security для мобильных устройств дает возможность обеспечить проактивную защиту мобильного устройства, а не просто изолировать устройство и хранящиеся на нем данные.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Возможность управлять мобильными устройствами на базе различных платформ через ту же единую консоль, которая служит для управления защитой остальных рабочих мест, значительно упрощает выполнение задач мониторинга и контроля без применения дополнительных усилий или технологий.

Функции защиты и управления мобильными устройствами

НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Сигнатурная, проактивная и облачная (с помощью Kaspersky Security Network) защита от известных и новых вредоносных программ для мобильных устройств. Проверка по требованию и по расписанию в сочетании с автоматическими обновлениями обеспечивают дополнительный уровень безопасности.

ЗАЩИТА ОТ СПАМА И ФИШИНГОВЫХ ССЫЛОК

Мощные технологии блокирования спама и фишинговых ссылок защищают устройство и хранящиеся на нем данные от фишинговых атак и помогают фильтровать нежелательные звонки и сообщения.

АНТИ-ВОР

В случае утери или кражи устройства возможна удаленная активация таких функций компонента Анти-Вор, как удаление данных, блокировка устройства, определение его местонахождения, оповещение о новом телефонном номере устройства в случае замены в нем SIM-карты, тайное фото несанкционированных пользователей и сирена (включение на устройстве звукового сигнала). В зависимости от ситуации, функционал компонента Анти-Вор может применяться очень гибко. Интеграция с Google Cloud Messaging (GCM) позволяет активировать функции практически мгновенно, что обеспечивает быструю реакцию и повышает уровень безопасности. Кроме того, пользователь может самостоятельно активировать нужные функции через Портал самообслуживания, без вмешательства IT-администратора.

ВЕБ-КОНТРОЛЬ И БЕЗОПАСНЫЙ БРАУЗЕР

Данные технологии работают в режиме реального времени и при поддержке Kaspersky Security Network блокируют доступ к вредоносным и нежелательным веб-сайтам. Безопасный браузер использует постоянно обновляемую репутационную базу интернет-ресурсов, что гарантирует мобильным пользователям безопасное посещение веб-сайтов.

КОНТРОЛЬ ПРОГРАММ

Интегрированный с Kaspersky Security Network, Контроль программ допускает использование только разрешенных программ, блокируя запуск нелицензионного или нежелательного ПО. Выполнение некоторых функций на устройстве можно ограничить за счет обязательной установки определенных приложений. Также можно применить политику, требующую от пользователя повторной авторизации в том случае, если приложение не использовалась в течение заданного периода времени. Это позволяет обеспечить безопасность данных, даже если устройство, на котором работало приложение, было утеряно или украдено.

ВЫЯВЛЕНИЕ ПОПЫТОК РУТИНГА/ ДЖЕЙЛБРЕЙКИНГА

Автоматическое выявление и уведомление администратора о попытках рутинга или джелбрейкинга может сопровождаться автоматической блокировкой доступа к контейнерам, выборочной или полной очисткой памяти устройства.

КОНТЕЙНЕРИЗАЦИЯ

Контейнеризация позволяет разделить личные и корпоративные данные, поместив приложения в специальные контейнеры. Для защиты конфиденциальной информации могут применяться дополнительные меры, такие как шифрование. Выборочная очистка памяти устройства дает возможность удалить с него корпоративную информацию, хранящуюся в контейнерах, не затрагивая личные данные пользователя – например, если сотрудник покидает компанию.

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Поддержка Microsoft® Exchange ActiveSync®, Apple MDM и Samsung KNOX™ 2.0 позволяет применять широкий спектр политик – через единый интерфейс, независимо от защищаемой платформы. Например, администраторы могут задать обязательное шифрование и использование паролей, ограничить использование камеры, применять политики к отдельным пользователям или группам пользователей, управлять настройками APN/VPN и т.д.

ПОРТАЛ САМООБСЛУЖИВАНИЯ

Портал самообслуживания дает пользователям мобильных устройств возможность самостоятельно выполнять некоторые задачи – например, подключить к корпоративной сети новое устройство и автоматически установить на него необходимые сертификаты без участия администратора. В случае утери сотрудником мобильного устройства портал также предоставляет пользователю доступ к основным функциям компонента Анти-Вор.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Все мобильные устройства управляются централизованно с помощью той же самой единой консоли, которая служит для управления защитой всех остальных рабочих мест в составе корпоративной сети. Веб-консоль позволяет администраторам контролировать и управлять устройствами удаленно с любого компьютера.

КАК ПРИОБРЕСТИ

Решение Kaspersky Security для мобильных устройств доступно в составе следующих продуктов линейки Kaspersky Security для бизнеса:

- Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ
- Kaspersky Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Total Security для бизнеса

Кроме того, Kaspersky Security для мобильных устройств можно приобрести отдельно. Чтобы выбрать нужный вам продукт, проконсультируйтесь с партнером «Лаборатории Касперского». Контактная информация и адреса партнеров представлены на нашем сайте в разделе http://www.kaspersky.ru/find_partner_office

ПОДРОБНЕЕ:
www.kaspersky.ru/security-mobile

KASPERSKY lab