

Kaspersky Endpoint Security 8 for Smartphone

Kaspersky Endpoint Security 8 for Smartphone обеспечивает безопасность корпоративных данных в случае потери или кражи смартфона, несанкционированного доступа к устройству или заражения телефона мобильными вирусами.

Многие компании сегодня заинтересованы в том, чтобы их сотрудники имели доступ к различным данным и ИТ-сервисам не только в офисе, но и за его пределами. Наиболее эффективным решением этой задачи является использование смартфона. Звонки, сообщения, электронная почта, доступ к корпоративным сетевым ресурсам и интернету – и все это с помощью одного устройства. В то же время смартфон может стать добычей злоумышленников, а это в свою очередь может привести к утечке корпоративных данных. Маленькое устройство легко потерять. К тому же большинство смартфонов не защищены по умолчанию от мобильных вредоносных программ.

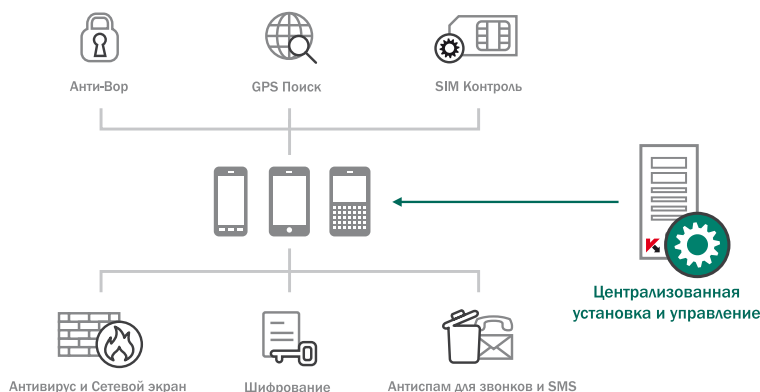
По сравнению с ПК и ноутбуками смартфоны гораздо чаще теряют и крадут. Множество мобильных устройств ежегодно остается на столиках ресторанов и кафе, в такси и салонах самолетов. Владельцы смартфонов также становятся жертвами карманных воров. При этом теряется не только устройство – теряются данные. В чужие руки могут попасть корпоративные почтовые сообщения, личные данные клиентов компании, финансовая и аналитическая информация, не говоря уже о персональных данных пользователя, его контактах, паролях и т.д.

Кроме того, в большинстве случаев мобильные устройства не защищены от вредоносного и мошеннического ПО. Поскольку масштаб этой проблемы еще не так велик, как в среде ПК, она зачастую игнорируется. Это может привести к плачевным последствиям, поскольку все основные операционные системы для смартфонов в той или иной степени подвержены риску заражения. Вредоносное ПО способно в скрытом режиме отсылать SMS на платные номера, тем самым воруя деньги с мобильного счета владельца устройства, или незаметно отсылать на сто ронние серверы личные данные пользователя в мошеннических целях.

Что может произойти с незащищенным смартфоном:

- Утечка корпоративных данных в случае потери или кражи устройства
- Несанкционированный доступ к данным, хранящимся на смартфоне
- Заражение телефона вредоносной или мошеннической программой

Kaspersky Endpoint Security 8 for Smartphone разработан с целью предотвращения всех этих угроз. Он позволяет удаленно управлять устройством (даже если оно потеряно или украдено), защищает пользователя от вредоносных и мошеннических программ, шифрует выбранные папки и файлы и т.д.



О КОМПАНИИ

«Лаборатория Касперского» – один из ведущих мировых производителей антивирусного ПО для домашних пользователей и предприятий любого масштаба. Продукты компании обеспечивают комплексную защиту от всех типов интернет-угроз: вредоносных и шпионских программ, спама и хакерских атак. В настоящее время решения «Лаборатории Касперского» защищают более 300 миллионов пользователей по всему миру, а технологии компании интегрированы в продукты и услуги более 100 ведущих производителей компьютерного, сетевого, телекоммуникационного оборудования и программного обеспечения.

ПРЕИМУЩЕСТВА РЕШЕНИЯ

- Комплексная **защита** для мобильных устройств
- Простая **установка** на удаленные смартфоны с помощью Kaspersky Administration Kit или сторонних систем управления мобильными устройствами
- Широкие возможности **управления** настройками и политиками с помощью Kaspersky Administration Kit, Sybase Afaria или Microsoft® System Center Mobile Device Manager
- **Поддержка** наиболее **популярных смартфонов** Nokia®, Android™, BlackBerry® и устройств на базе Windows® Mobile

Как Kaspersky Endpoint Security 8 for Smartphone защищает пользователей смартфонов?

- **Анти-Вор.** Удаленное блокирование телефона, очистка его памяти и определение местонахождения по GPS в случае, если устройство потеряно или украдено.
- **SIM Контроль.** Если в украденном устройстве сменили SIM-карту, оно автоматически блокируется и сообщает законному владельцу новый номер телефона.
- **Шифрование.** Наиболее важные файлы, папки и карты памяти могут быть зашифрованы, а доступ к ним будет предоставляться по паролю.
- **Антивирус.** Защита от вредоносных программ в режиме реального времени, сканирование телефона по требованию и по расписанию, автоматическое обновление антивирусных баз.
- **Антиспам для звонков и SMS.** Легкий способ заблокировать нежелательные звонки и сообщения, отвлекающие от дел.
- **Личные Контакты.** Одним нажатием клавиши можно скрыть важные контакты и историю общения с ними.

Развертывание

Kaspersky Endpoint Security 8 for Smartphone может быть легко и быстро установлен на смартфоны сотрудников компании, находящихся в любом уголке мира. Установка может быть незаметной для пользователя и не требовать от него никаких действий.

Продукт может быть установлен и управляться с помощью:

- Microsoft® System Center Mobile Device Manager
- Sybase Afaria
- Kaspersky Administration Kit

Управление

С помощью средств управления Kaspersky Endpoint Security 8 for Smartphone ИТ-специалисты компании могут осуществлять полный контроль над продуктом, установленным на удаленных устройствах. При этом администратор может определить, какие возможности продукта будут доступны (или недоступны) пользователям, какие настройки пользователь сможет менять самостоятельно, а какие нет, а также настроить расписание антивирусных обновлений, сканирования телефона и т.д. К различным группам пользователей могут быть применены различные политики. Обновления и передача политик удаленным устройствам осуществляются по любым доступным беспроводным каналам связи: GPRS, EDGE, Wi-Fi и т.д.

Администратор может настроить:

- **Антивирус:** какие типы файлов следует проверять, какие действия выполнять при обнаружении вредоносной программы (удалять ее, помещать в карантин, запрашивать действие у пользователя), как часто следует обновлять антивирусные базы
- **Анти-Вор:** какие компоненты должны быть включены (Блокирование, Удаление данных, GPS Поиск, SIM Контроль), какие адреса электронной почты и телефоны должны использоваться для оповещения владельца в случае неприятностей, а также детальные настройки каждого из компонентов
- **Шифрование:** какие файлы, папки и карты памяти должны быть зашифрованы
- **Антиспам для звонков и SMS или Личные Контакты**
- периодичность, с которой продукт должен устанавливать связь с сервером администрирования

В соответствии с политикой безопасности компании можно запретить или разрешить сотрудникам изменять эти настройки самостоятельно.

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Поддерживаемые платформы

- Android™ 1.5 - 2.3
- Symbian S60 9.1 - 9.4, Symbian^3 (только для смартфонов Nokia®)
- BlackBerry® 4.5 - 6.0
- Windows Mobile® 5.0 - 6.5

Поддерживаемые средства управления

- Kaspersky Administration Kit 8.0 (версия 8.0.2121 и выше)
- Microsoft® System Center Mobile Device Manager 2008 SP1
- Sybase Afaria 6.5

Подробная информация на сайте:

www.kaspersky.ru

Kaspersky Endpoint Security 8 for Smartphone можно приобрести в составе продуктов линейки Kaspersky Open Space Security. Для выбора подходящего продукта обратитесь в отдел продаж ближайшего к вам партнера компании (подробнее см. на сайте www.kaspersky.ru).