KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

СТАНДАРТНЫЙ

Средства для обеспечения безопасности мобильных сотрудников, эффективное применение политик IT-безопасности и защита от вредоносных программ.

Решение «Лаборатории Касперского» уровня СТАНДАРТНЫЙ включает в себя средства для управления мобильными устройствами и защиты их от вредоносных программ. Средства контроля корпоративных ПК (контроль использования веб-ресурсов, устройств и программ) помогут вашей организации эффективно применять политики, обеспечивающие безопасность важнейших элементов IT-инфраструктуры.

Возможности защиты и управления, которые необходимы именно вам.

«Лаборатория Касперского» предусмотрела множество функций и возможностей на каждом уровне защиты. При этом наши технологии достаточно просты в использовании для предприятий любого масштаба.

Какой уровень подходит вам?

- СТАРТОВЫЙ
- **СТАНДАРТНЫЙ**
- РАСШИРЕННЫЙ
- TOTAL

ДОСТУПНЫЕ ФУНКЦИИ:

- ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО
- СЕТЕВОЙ ЭКРАН
- ИНТЕГРАЦИЯ С «ОБЛАКОМ» KSN
- КОНТРОЛЬ ПРОГРАММ
- ДИНАМИЧЕСКИЕ БЕЛЫЕ СПИСКИ
- ВЕБ-КОНТРОЛЬ
- КОНТРОЛЬ УСТРОЙСТВ
- ЗАЩИТА СЕРВЕРОВ WINDOWS
- УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ (ПЛАНШЕТАМИ И СМАРТФОНАМИ)
- ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

ОСНОВНЫЕ ВОЗМОЖНОСТИ

НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Технологии антивирусной проверки «Лаборатории Касперского» работают на разных уровнях операционной системы, эффективно удаляя вредоносное ПО. Облачная сеть безопасности Kaspersky Security Network (KSN) защищает пользователей от новых угроз в режиме реального времени.

ГИБКИЕ СРЕДСТВА КОНТРОЛЯ

Облачная база опасных и легитимных программ и веб-сайтов помогает администратору создавать и применять политики доступа к программам и веб-страницам. При этом гибкие средства контроля позволяют гарантировать, что к компьютерам в сети будут подключены только разрешенные устройства.

БЕЗОПАСНОСТЬ СМАРТФОНОВ И ПЛАНШЕТОВ

Защита на основе программных агентов доступна для устройств под управлением Android™, BlackBerry®, Symbian и Windows® Mobile. С помощью средства управления мобильными устройствами (Mobile Device Management) политики и приложения легко устанавливаются по беспроводным каналам связи на мобильные устройства, в том числе на устройства под управлением iOS.

ПОИСК УЯЗВИМОСТЕЙ

Проверка операционной системы и используемых программ на наличие уязвимостей. Используя полученную информацию администратор может принять меры по их устранению.

ЗАЩИТА РАБОЧИХ МЕСТ

СИГНАТУРНЫЙ МЕТОД
Традиционный метод обнаружения вредоносного программного обеспечения, основанный на использовании сигнатур.

ПРОАКТИВНАЯ ЗАЩИТА
Защита от угроз, для которых еще не созданы сигнатуры.

ЗАЩИТА ИЗ «ОБЛАКА»
Облачная сеть безопасности Kaspersky Security Network (KSN) позволяет реагировать на новые угрозы намного быстрее, чем традиционные методы защиты. Время реакции KSN на появление нового вредоносного ПО может составлять всего 0,02 секунды!

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ И ПЕРСОНАЛЬНЫЙ СЕТЕВОЙ ЭКРАН
Предустановленные правила для сотен наиболее распространенных приложений позволяют сократить затраты времени на настройку сетевого экрана.

КОНТРОЛЬ РАБОЧИХ МЕСТ

КОНТРОЛЬ ПРОГРАММ
Позволяет системным администраторам задавать политики, которые разрешают, блокируют или ограничивают использование определенных программ (или категорий программ).

ВЕБ-КОНТРОЛЬ
Обеспечивает контроль использования веб-ресурсов независимо от того, находится пользователь в пределах корпоративной сети или нет.

КОНТРОЛЬ УСТРОЙСТВ
Позволяет администратору создавать и применять (в том числе по расписанию) политики работы с данными на съемных носителях и других периферийных устройствах, подключаемых через USB или любой другой интерфейс.

ДИНАМИЧЕСКИЕ БЕЛЫЕ СПИСКИ
Репутационная проверка файлов в режиме реального времени по базе Kaspersky Security Network (KSN), гарантирует, что доверенные приложения не содержат вредоносного кода.

ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПО
Защита в режиме реального времени возможна благодаря сочетанию сигнатурных, проактивных и облачных технологий. Безопасный браузер, защита от спама и технология Sandbox для безопасного запуска программ повышают уровень защиты.

УДАЛЕННАЯ УСТАНОВКА ПО
Возможность предварительной настройки и дальнейшей централизованной установки программ на мобильные устройства с помощью SMS, электронной почты или ПК.

ЗАЩИТА ЦЕННЫХ ДАННЫХ
Функции поиска, удаленной блокировки устройства и стирания данных на нем, а также SIM-Контроль служат для предотвращения несанкционированного доступа к корпоративным данным при утере или краже мобильного устройства.

КОНТРОЛЬ ПРИЛОЖЕНИЙ НА МОБИЛЬНЫХ УСТРОЙСТВАХ
Позволяет осуществлять мониторинг приложений на корпоративных мобильных устройствах в соответствии с групповыми политиками безопасности.

ЗАЩИТА ЛИЧНЫХ УСТРОЙСТВ СОТРУДНИКОВ
В вашей компании приветствуется работа на личных устройствах? Корпоративные данные и приложения могут быть помещены в изолированные зашифрованные контейнеры, «прозрачные» для пользователя. Данные в таком контейнере можно удалить независимо от других данных, хранящихся на устройстве.

УНИКАЛЬНАЯ ПЛАТФОРМА ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Единая консоль управления
Администратор может наблюдать за состоянием защиты всех физических, виртуальных и мобильных устройств, а также управлять их безопасностью с помощью единой консоли администрирования.

Единая платформа для обеспечения безопасности
Все используемые в продуктах «Лаборатории Касперского» ключевые технологии, функциональные компоненты и модули разрабатываются внутри компании на собственной технологической базе. Благодаря этому растет эффективность, снижается нагрузка на систему и повышается стабильность работы приложений.

Единая лицензия
Вы не получаете несколько отдельных решений в рамках одной покупки — вы приобретаете единое комплексное решение, которое вы можете гибко настраивать в соответствии со своими бизнес-целями.

НАБОР ДОСТУПНЫХ ФУНКЦИЙ ЗАВИСИТ ОТ ЗАЩИЩАЕМОЙ ПЛАТФОРМЫ
Подробнее: **www.kaspersky.ru**

KESB-S/Version 0.1/Sept12/Global

KASPERSKY lab