KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

РАСШИРЕННЫЙ

В линейке решений «Лаборатории Касперского» эффективно сочетаются технологии обеспечения безопасности и инструменты управления IT-инфраструктурой.

Решение «Лаборатории Касперского» уровня РАСШИРЕННЫЙ предоставляет возможности защиты и управления, необходимые вашей организации для внедрения политик IT-безопасности, защиты от вредоносного программного обеспечения и потери данных, а также для повышения производительности корпоративной IT-инфраструктуры.

Возможности защиты и управления, которые необходимы именно вам.

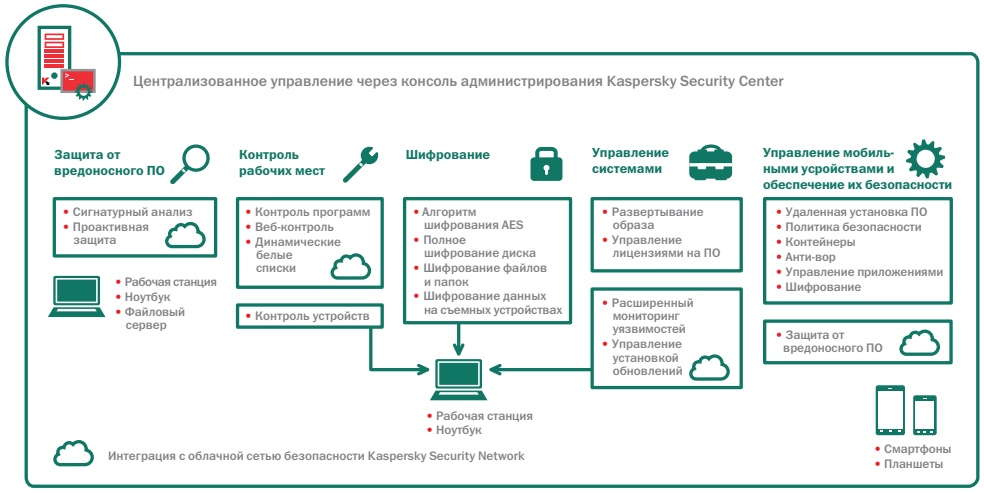
«Лаборатория Касперского» предусмотрела множество функций и возможностей на каждом уровне защиты. При этом наши технологии достаточно просты в использовании для предприятий любого масштаба.

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 ФАЙЛОВЫХ СЕРВЕРОВ
- УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ
- ЗАЩИТА МОБИЛЬНЫХ УСТРОЙСТВ (ПЛАНШЕТОВ И СМАРТФОНОВ)
- ШИФРОВАНИЕ
- ИНСТРУМЕНТЫ СИСТЕМНОГО АДМИНИСТРИРОВАНИЯ
- МОНИТОРИНГ УЯЗВИМОСТЕЙ
- УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ



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.

ШИФРОВАНИЕ И ЗАЩИТА ДАННЫХ

ПОЛНОЕ ИЛИ ВЫБОРОЧНОЕ ШИФРОВАНИЕ ДАННЫХ
Чтобы защитить ценные корпоративные данные в случае кражи или утери устройства, на котором они хранятся, можно использовать как полное шифрование диска, так и шифрование отдельных файлов и папок – с помощью алгоритма Advanced Encryption Standard (AES).

ШИФРОВАНИЕ ДАННЫХ НА СЪЕМНЫХ НОСИТЕЛЯХ
Политики шифрования данных на съемных носителях позволяют повысить уровень безопасности.

БЕЗОПАСНОЕ СОВМЕСТНОЕ ПОЛЬЗОВАНИЕ ДАННЫМИ
Пользователи могут легко создавать зашифрованные самораспаковывающиеся контейнеры, чтобы обеспечить защиту данных, передаваемых на съемных носителях, по электронной почте, через локальную сеть или интернет.

НЕЗАМЕТНОСТЬ ДЛЯ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ
Наши технологии шифрования работают незаметно для пользователей и не снижают производительность системы.

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 РАБОЧИХ МЕСТ

НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО
Доказавшие свою эффективность методы обнаружения вредоносного ПО: сочетание сигнатурных, проактивных и облачных технологий.

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!

ИНСТРУМЕНТЫ СИСТЕМНОГО АДМИНИСТРИРОВАНИЯ

УПРАВЛЕНИЕ УСТАНОВКОЙ ИСПРАВЛЕНИЙ
Расширенный мониторинг уязвимостей в сочетании с автоматическим распределением исправлений (патчей).

РАЗВЕРТЫВАНИЕ ОБРАЗОВ ОПЕРАЦИОННЫХ СИСТЕМ И ПРОГРАММ
Простой централизованный процесс создания, хранения и развертывания образов системы. Идеально подходит для миграции на Microsoft® Windows® 8.

УДАЛЕННАЯ УСТАНОВКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ
Централизованная установка программного обеспечения на клиентские компьютеры, в том числе в филиалах организации.

КОНТРОЛЬ ДОСТУПА В СЕТЬ (NAC)
Возможность создать политику для подключающихся к корпоративной сети «гостей». Гостевые устройства (в том числе мобильные) автоматически распознаются и перенаправляются на корпоративный портал, где пользователи вводят выданные им идентификационные пароли и получают доступ к разрешенным вами ресурсам.

УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ, УЧЕТ ОБОРУДОВАНИЯ И ПО
Сводные отчеты об аппаратном и программном обеспечении помогают контролировать статус лицензий на ПО.

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.

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

KESB-ADV/Version 0.2/Oct12/Global

KASPERSKY lab