

► KASPERSKY SECURITY ДЛЯ БИЗНЕСА

Контроль рабочих мест

Для защиты вашей компании от новейших угроз «Лаборатория Касперского» объединила мощные средства контроля рабочих мест с лучшими в своем классе технологиями защиты от вредоносных программ.

Надежная защита и эффективное применение политик безопасности

- КОНТРОЛЬ ПРОГРАММ
- ДИНАМИЧЕСКИЕ БЕЛЫЕ СПИСКИ
- ВЕБ-КОНТРОЛЬ
- КОНТРОЛЬ УСТРОЙСТВ

ИНСТРУМЕНТЫ КОНТРОЛЯ ДОСТУПНЫ
В ПРОДУКТАХ ЛИНЕЙКИ KASPERSKY
SECURITY ДЛЯ БИЗНЕСА ВСЕХ УРОВ-
НЕЙ, КРОМЕ СТАРТОВОГО

КОНТРОЛЬ ПРОГРАММ И ДИНАМИЧЕСКИЕ БЕЛЫЕ СПИСКИ

Использование технологий **контроля программ и динамических белых списков** повышает безопасность IT-инфраструктуры компании, позволяя системным администраторам задавать политики, которые разрешают, блокируют или ограничивают использование определенных программ (или категорий программ).

Эти технологии позволяют организациям легко применять политику «запрета по умолчанию». В этом случае доступ к любым программам по умолчанию блокируется, а администратор задает список приложений, которые разрешено запускать. Чтобы упростить работу администраторов и облегчить создание политик, «Лаборатория Касперского» составила собственную базу приложений и разделила их по категориям. Администратор может использовать эти категории или создать собственную локальную базу разрешенных приложений.

Модуль **Контроль активности программ** непрерывно отслеживает и контролирует поведение программ. Он определяет, разрешено ли программе выполнять запись в реестры, а также то, к каким ресурсам (например, хранилищам данных) она может получать доступ, с какими данными пользователей она может работать, а также многое другое.

«Лаборатория Касперского» ведет специальную **базу белых списков**, в которую включены программы, регулярно проверяемые на предмет безопасности. Мы единственная компания в отрасли IT-безопасности, в которой имеется специальная лаборатория, занимающаяся классификацией ПО.

ВЕБ-КОНТРОЛЬ

Существует множество веб-сайтов, содержащих неуместные на рабочем месте материалы. В связи с этим важно использовать функции Веб-Контроля.

«Лаборатория Касперского» создала и постоянно обновляет базу веб-сайтов, сгруппированных по категориям (азартные игры, сайты «для взрослых», поисковые системы и др.). Администраторы могут легко создавать и эффективно применять политики доступа к веб-страницам на основе этих категорий или настраивать их, составляя собственные списки сайтов. Доступ к вредоносным сайтам блокируется автоматически.

При настройке политик можно использовать расписание, чтобы разрешить посещение тех или иных сайтов в определенное время. А поскольку решения «Лаборатории Касперского» для веб-контроля интегрируются с существующей структурой Active Directory, эти политики легко применять в масштабе всей организации.

Благодаря инновационному подходу «Лаборатории Касперского» эта технология работает непосредственно на компьютере пользователя. Это означает, что любая задаваемая вами политика будет применяться даже тогда, когда пользователь не находится в сети.

КОНТРОЛЬ УСТРОЙСТВ

Для эффективного управления использованием съемных устройств не всегда достаточно просто отключить USB-порт. Зачастую для повышения производительности труда и безопасности пользователей необходимы более гибкие возможности контроля. Например, если для доступа к корпоративной сети пользователю необходим USB-токен, но при этом ему не разрешается пользоваться съемными USB-устройствами, то политика отключения порта будет неэффективной.

С помощью решения «Лаборатории Касперского» администратор может задавать политики, позволяющие в любое время контролировать устройства независимо от способа их подключения (не только через USB-порт). Это означает, что администратор может разрешать тем или иным устройствам выполнять подключение, запись или чтение, а также задавать период времени, в течение которого действует политика, и разрешенные типы устройств. Для обеспечения максимальной безопасности контроль устройств может осуществляться по их серийным номерам.

ПРОСТОТА УПРАВЛЕНИЯ

Для удобства управления решениями «Лаборатории Касперского» все функции контроля интегрируются с Active Directory, что упрощает создание комплексных политик. Все функции контроля рабочих мест управляются из единой консоли. Это означает, что администратор работает в рамках единого интуитивно понятного интерфейса.

КАК ПРИОБРЕСТИ

Инструменты контроля рабочего места не продаются отдельно, но доступны в следующих продуктах линейки **Kaspersky Security для бизнеса:**

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

НАБОР ДОСТУПНЫХ ФУНКЦИЙ ЗАВИСИТ ОТ ЗАЩИЩАЕМОЙ ПЛАТФОРМЫ

Подробнее: www.kaspersky.ru