Kaspersky Endpoint Security 8 для Windows

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Осенью 2011 года «Лаборатория Касперского» представила новое корпоративное решение - Kaspersky Endpoint Security 8 для Windows, пришедшее на смену Антивирусу Касперского 6 R2 для Windows Workstation.

Новый продукт «Лаборатории Касперского», на мой взгляд, является уже не столько антивирусом, сколько именно решением по обеспечению безопасности оконечных устройств (серверов и рабочих станций). Т.е. в данном случае антивирусная защита обеспечивается в том числе, наряду с другими функциями безопасности. Насколько это правильно? На мой взгляд – безусловно. Так как, увы, многие руководители, особенно в сфере малого бизнеса, думают, что купив антивирусное решение, они полностью обеспечивают свою безопасность.

Что изменилось в продукте? В нем появились пять коренных улучшений. Давайте перечислим их, а потом попробуем разобраться в них подробнее:

1. **Усиленная защита**:
   1.1. **Улучшенная проактивная защита** — компонент System Watcher, выполняющий мониторинг активности запущенных программ. Теперь модуль проактивной защиты является обновляемым — он регулярно получает новые шаблоны для детектирования активности вредоносных программ, а также включает в себя механизм отката вредоносных действий.
   1.2. **Новая система шаблонов поведения вредоносных программ (**pattern-based similarity, **PBS)**, повышающая уровень детектирования угроз и, что также немаловажно, позволяющая заметно сократить размер обновлений.
2. **Интеграция с «облаком» Kaspersky Security Network**
3. **Контроль рабочих станций:**
   3.1. **Веб-контроль** для мониторинга интернет-активности пользователя, фильтруя посещаемые интернет-ресурсы по категории, содержимому и типу данных.
   3.2. **Контроль устройств** позволяет предотвратить случайную или злонамеренную утечку данных и защититься от атак вредоносного программного обеспечения.
   3.3. **Контроль запуска приложений** позволяет разрешать или запрещать выполнение приложений согласно внутренним корпоративным стандартам, а также включает в себя возможность инвентаризации программного обеспечения.
4. **Контроль приложений и белые списки**
5. **Оптимизированная система управления**

Давайте остановимся немного подробнее на некоторых из этих улучшений.

Усиленная защита

Как уже было написано выше, усиленная защита в KES для Windows обеспечивается с помощью нескольких компонентов. Рассмотрим их подробнее.

System Watcher

Данный компонент отслеживает активность запущенных приложений. Он доступен как в составе персональных продуктов (KAV, KIS, Crystal) так и в составе корпоративных (начиная с KES для Windows) и позволяет в режиме реального времени анализировать действия всех установленных на ПК программ. Например, изменился системный реест, загрузочный сектор или просто файл (или произошло что-то другое) все это записывается в специальную базу данных. В результате появляется возможность восстановить систему до ее оригинального состояния. Процесс восстановления при этом называется «откатом». Откатить можно многое: создание, удаление, изменение файлов, загрузочного сектора, системного реестра и т.д.

Вместе с тем стоит учесть, что в состав System Watcher входит набор шаблонов (Behavior Stream Signatures, BSS) – моделей вредоносного поведения, по которым можно вычислить неизвестное вредоносное программное обеспечение. Во-вторых, System Watcher обменивается информацией с другими компонентами антивирусного ПО и, запоминая цепочки событий, формирует целостную картину поведения и следы каждой отдельной программы и групп программ. Это значительно повышает точность обнаружения вредоносного ПО.

Следует также учесть, что System Watcher отслеживает действия программ не только в текущей сессии, а на протяжении всего жизненного цикла программы.

Вместе с тем следует учесть, что System Watcher интегрирован с облаком Kaspersky Security Network (подробнее о работе KSN см. ниже).

Интеграция с облаком Kaspersky Security Network

Для начала необходимо рассмотреть, а что же такое технология Kaspersky Security Network (KSN)?

Kaspersky Security Network

KSN – облачная технология, реализованная в последних версиях продуктов «Лаборатории Касперского» для домашних и корпоративных пользователей. KSN обеспечивает быструю реакцию на появление вредоносных программ, позволяет детектировать и блокировать ранее неизвестные угрозы, выявлять и вносить в черный список их источники в Интернет.

Корпоративным пользователям Kaspersky Security Network предлагает дополнительные возможности, такие как расширенный контроль программ и белые списки приложений. Kaspersky Security Network совмещает постоянный мониторинг и централизованный анализ актуальных угроз и оперативную подготовку и применение защитных мер.

Основные принципы работы KSN

В состав KSN входят несколько подсистем:

- Постоянный географически распределенный глобальный мониторинг актуальных угроз на ПК пользователей
- Мгновенная доставка собранной информации на серверы «Лаборатории Касперского»
- Анализ полученной информации

- Разработка и применение мер по защите от новых угроз

Поступающая в KSN информация о попытках заражения автоматически передается экспертам «Лаборатории Касперского». Кроме того собирается информация о подозрительных файлах, загруженных и исполняемых на ПК пользователей, независимо от источника получения таких файлов. Пользователи корпоративных решений не участвуют в формировании базы данных KSN.

Вердикт о безопасности программы выносится на основании цифровой подписи, удостоверяющей ее происхождение и гарантирующей ее целостность, а также ряда других признаков. Такая программа включается в список доверенных приложений.

Если по окончании проверки программа признается вредоносной, данные о ней поступают в UDS (Urgent Detection System). Данная информация становится доступной пользователям KSN еще до создания соответствующей сигнатуры. Таким образом, клиенты «Лаборатории Касперского» получают оперативную информацию о новых и неизвестных угрозах спустя считанные минуты после начала кибератаки, в то время как традиционные антивирусные базы, как правило, обновляются раз в несколько часов.

Схема работы Kaspersky Security Network

Данная схема описывает основные принципы взаимодействия KSN с компьютерами пользователей продуктов «Лаборатории Касперского», которое происходит в 4 этапа:

1. Информация о запускаемых или загружаемых приложениях и посещаемых веб-страницах (URL) отправляется в KSN с компьютеров, на которых установлены последние версии продуктов «Лаборатории Касперского» для домашних и корпоративных пользователей:
    a. информация о заражениях, либо атаках на пользователя;
    b. информация о подозрительной активности исполняемых файлов на компьютере пользователя.
2. Информация о файлах и URL проверяются и, в случае признания их вредоносными, добавляются в базу Urgent Detection System. Легитимные файлы вносятся в белые списки (Whitelisting). **Следует учесть, что сами файлы не пересылаются!**
3. Эксперты «Лаборатории Касперского» анализируют подозрительные файлы, определяют степень их опасности и добавляют описание в базу сигнатур.
4. Информация о вновь обнаруженных вредоносных и легитимных файлах и URL становится доступна всем пользователям продуктов «Лаборатории Касперского» (не только пользователям Kaspersky Security Network).

По завершении анализа новой вредоносной программы создается ее сигнатура, которая включается в антивирусные базы, регулярно обновляемые на компьютерах пользователей.

Белые списки – не единственная технология в рамках KSN, позволяющая пользователю принять решение о том, стоит ли запускать ту или иную программу. В KSN также используется технология Wisdom of the Crowd (WoC), предоставляющая информацию о степени популярности программы и ее репутации среди пользователей KSN.

Помимо этого, последние версии продуктов «Лаборатории Касперского» позволяют получать данные Глобальных рейтингов безопасности (GSR) непосредственно из «облака». Рейтинг (GSR)

каждой программы рассчитывается с помощью специального алгоритма и широкого набора репутационных данных.

При использовании KSN мы можем получить следующую информацию:

- Заключение «облачной системы» о том, можно ли доверять приложению.
- Примерную оценку количества пользователей, которые запускали это приложение.
- Примерную дату появления информации о файле в Kaspersky Security Network.
- Статистику использования файла пользователями KSN в различных странах.
- Основные данные о файле: название, имя разработчика, версия, размер файла.

Что дает проверка репутации?

- Проверка репутации в Kaspersky Security Network дает следующий эффект: сотни тысяч пользователей по всему миру либо рекомендуют вам программу, либо советуют держаться от нее подальше. Важно понимать, что эта рекомендация, как и совет ваших друзей в реальной жизни не является истиной в последней инстанции.
- Запрос репутации позволяет вам самостоятельно оценить ту или иную программу, которую вы только что скачали из сети. **Следует учесть, что это не самый распространенный сценарий применительно к корпоративной среде, где ответственным за установку приложений является администратор.**

Расширенная облачная защита для корпоративных клиентов

Корпоративные компьютеры, работающие под управлением Windows, используют Kaspersky Security Network для оценки репутации файлов и URL и на основании полученной информации блокируют доступ к вредоносному контенту или ограничивают действия подозрительного ПО.

Функциональность Kaspersky Security Network в корпоративных продуктах расширена. Во-первых, облачные технологии (данные из Kaspersky Security Network) используются для создания белых списков приложений. Известные легитимные приложения автоматически распределяются по категориям (игры, коммерческое ПО и т.д.). Используя эти категории, системный администратор может быстро настроить и применить правила для определенных типов программ в соответствии с корпоративной политикой безопасности. При формировании белых списков приложений наряду с информацией, получаемой от пользователей, используются данные, предоставляемые более чем 200 ведущими производителями ПО.

Инструмент для централизованного управления Kaspersky Security Center дает возможность тонкой настройки взаимодействия с Kaspersky Security Network для защиты узлов корпоративной сети. Администратор может активировать или отключить облачную защиту в различных модулях Kaspersky Endpoint Security 8 для Windows. Также есть возможность отключить передачу данных в Kaspersky Security Network, если этого требует корпоративная политика безопасности. В целях снижения нагрузки на каналы передачи данных в корпоративной сети может быть установлен внутренний прокси-сервер Kaspersky Security Network (рис.1).

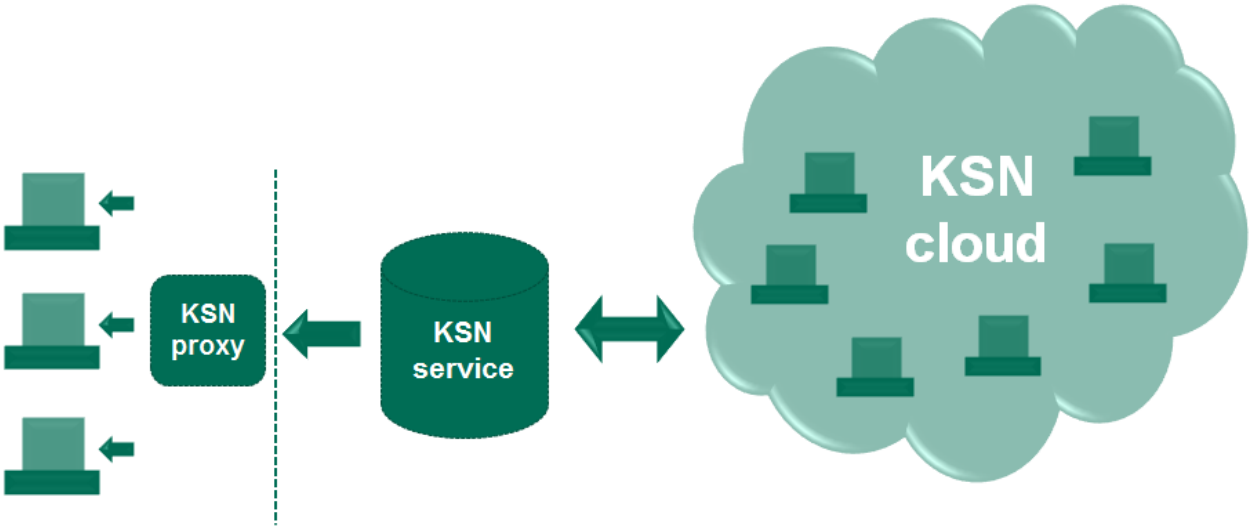

Рисунок 1 Применение KSN в организации

База белых списков

- Перед применением политик безопасности проводится учет программного обеспечения, в ходе которого автоматически собирается полная информация о программах, используемых в корпоративной сети
- Облачная репутационная база «Лаборатории Касперского» содержит информацию о более чем 3 млрд. файлов и постоянно пополняется
- Динамическая база белых списков содержит более 300 миллионов уникальных чистых файлов. Ежедневно в нее добавляется 1 млн новых файлов
- Осуществляется постоянный мониторинг статуса программ, уже входящих в белые списки, что позволяет обеспечить более высокую скорость реакции на изменение их статуса по сравнению с решениями других вендоров. Это возможно благодаря тому, что вся технологическая инфраструктура и экспертные ресурсы, необходимые для анализа ПО, сосредоточены в одной компании
- Информация о продуктах, готовящихся к выходу, поступает от 200 компаний-производителей ПО, таких как HP, Mozilla, Cisco, Adobe, Intel и Asus, что позволяет свести к минимуму количество ложных срабатываний

Контроль рабочих станций

Веб-контроль

Служит для мониторинга интернет-активности пользователя, фильтруя посещаемые интернет-ресурсы по категории, содержимому и типу данных (рис.2). Эта функция обеспечивает возможность применения гибких правил и расписания доступа к ресурсам.

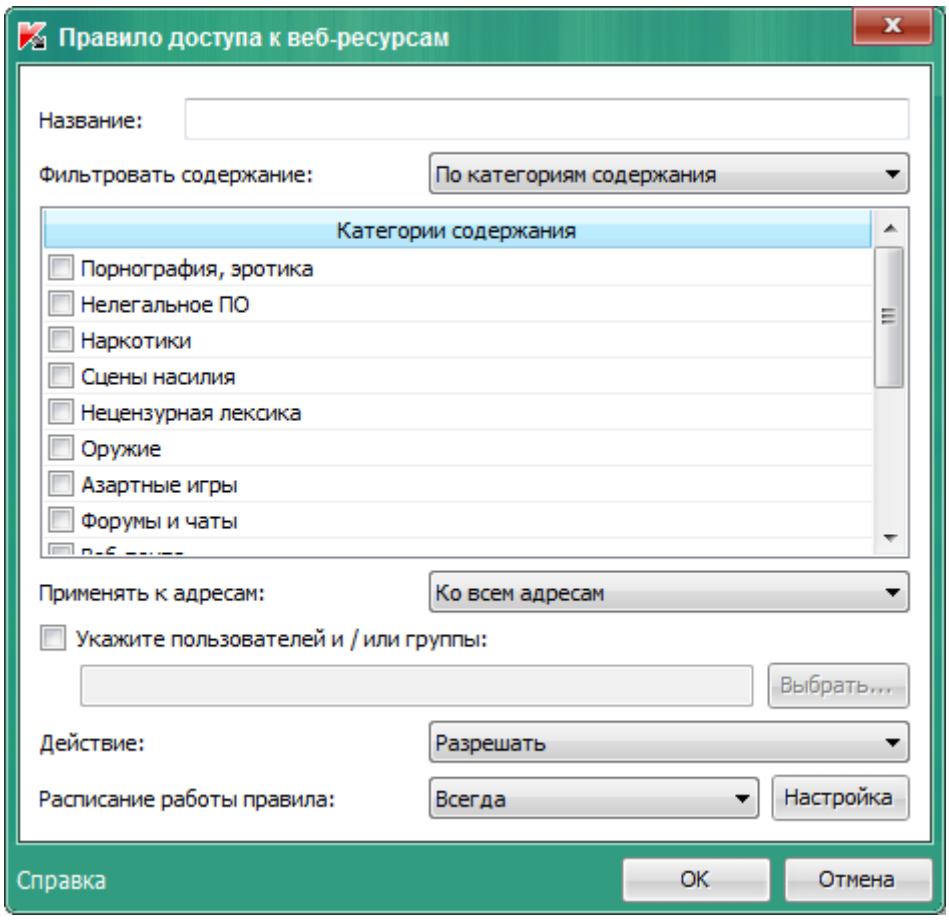

Рисунок 2 Правила доступа к веб-ресурсам по типам ресурсов

Кроме того, вы можете указать временные ограничения для ваших пользователей (рис.3).

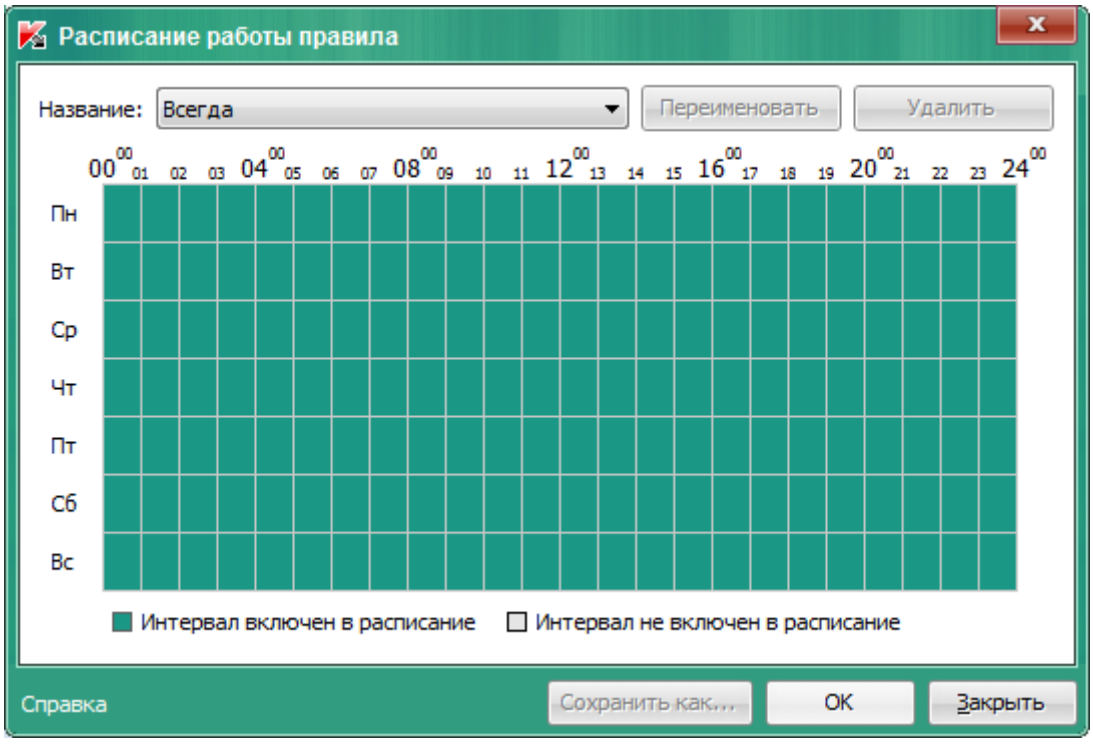

Рисунок 3 Расписание работы правила

Контроль устройств

Контроль устройств позволяет:

- Контролировать устройства по типу, шине
- Создавать белый список категорий (в том числе по серийным номерам)
- Создавать возможность доступа по чтению (записи)
- Проводить инвентаризацию оборудования
- Совместимо с Active Directory

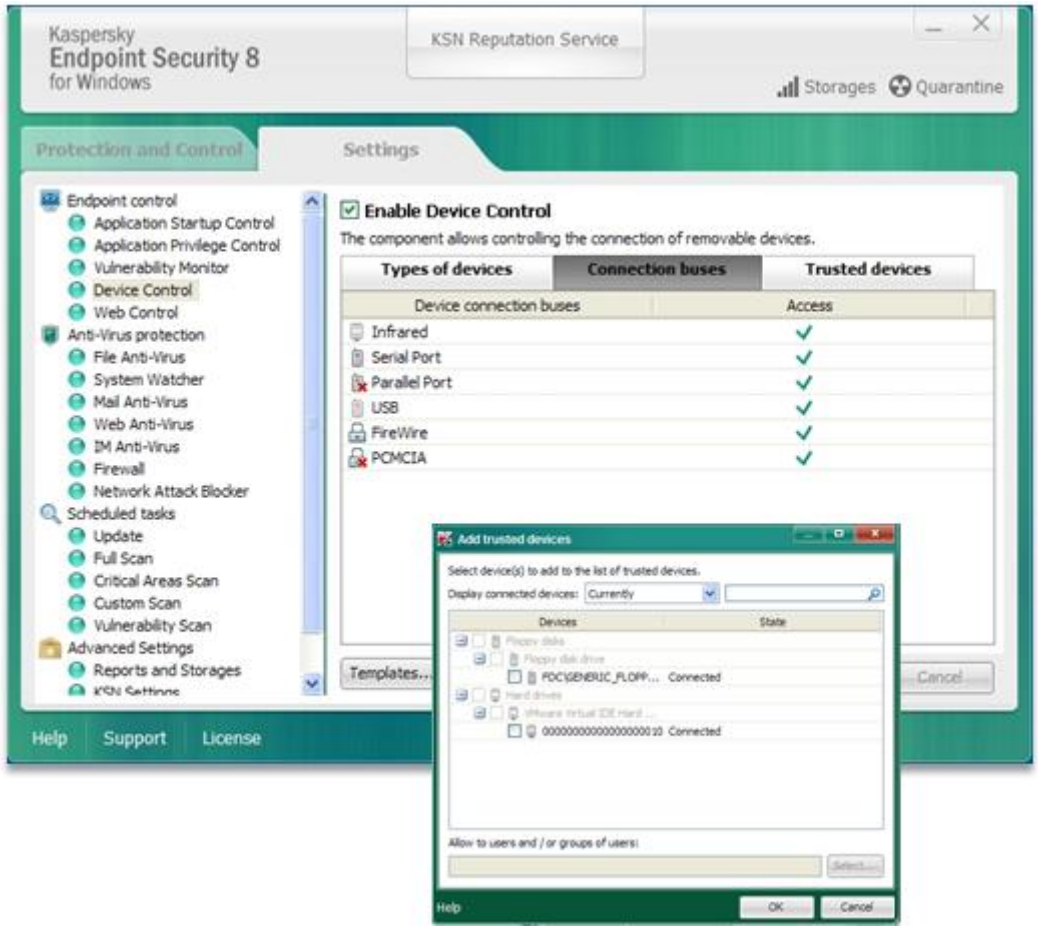

Рисунок 4 Контроль устройств

Контроль запуска приложений

Позволяет разрешать или запрещать выполнение приложений согласно внутренним корпоративным стандартам, а также включает в себя возможность инвентаризации программного обеспечения.

В том числе вы можете разрешать (запрещать) запуск приложений по «KL-категориям».

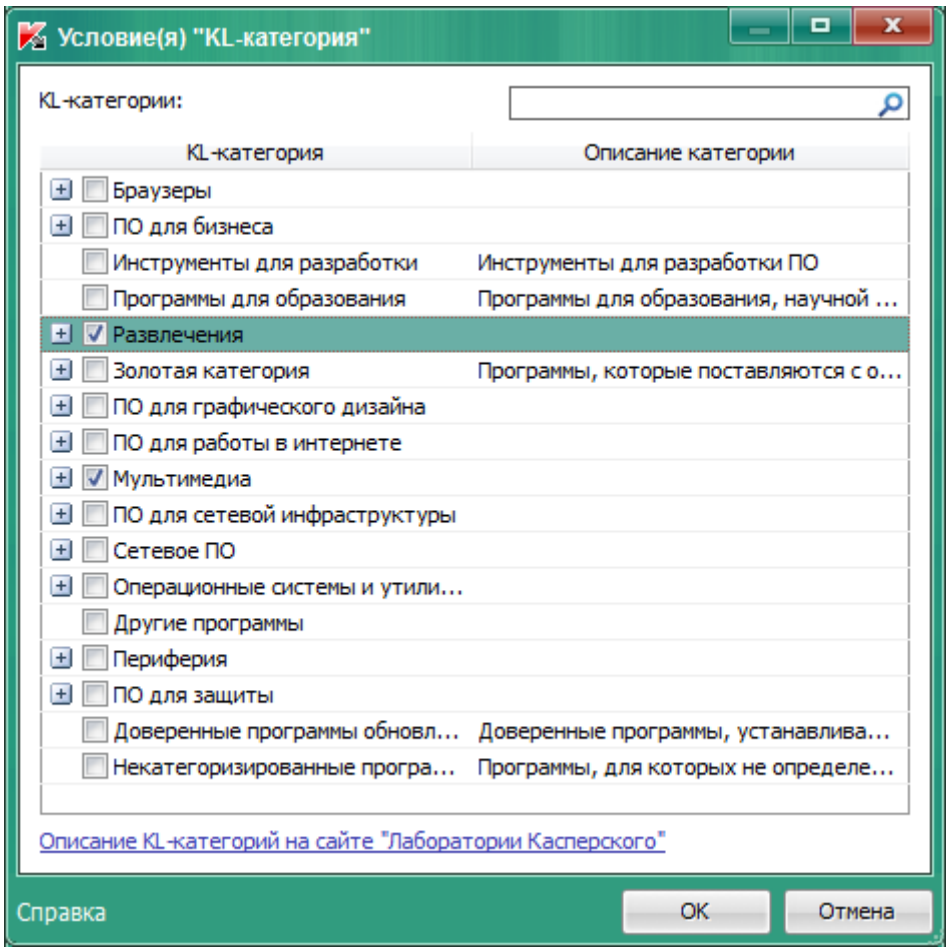

Рисунок 5 Условие для запрета запуска по KL-категориям

Следует учесть, что запуск правил возможен не только в режиме «Вкл/Выкл», т.е. разрешение(запрет), но и в режиме «Тест». При этом запуск приложений не будет запрещен, однако об этом будет сделана запись в отчете.

Контроль приложений и белые списки

Локально администрируемые и основанные на облачной защите «whitelisting» правила запуска приложений вместе с контролем привилегий приложения основываются на мониторинге уязвимостей и репутации приложений и образуют эффективную защиту от APT атак (рис. 6).

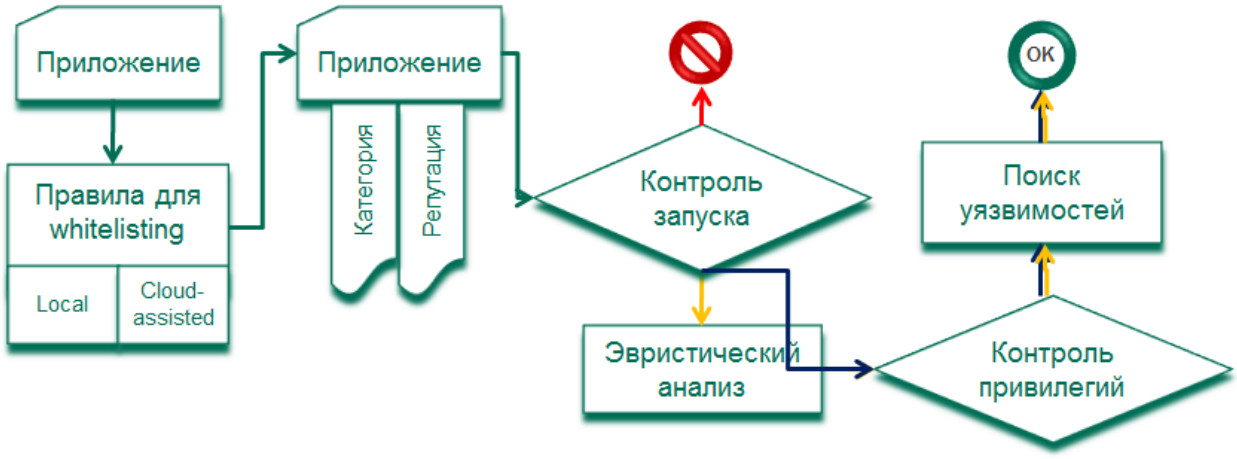

Рисунок 6 Контроль приложений

Компонент «Контроль активности программ» предотвращает выполнение программами опасных для системы действий, а также обеспечивает контроль доступа к ресурсам ОС и персональным данным.

Данный компонент контролирует работу программ, в том числе доступ к защищаемым ресурсам с помощью правил контроля программ (набора ограничений для различных действий программ в Оси прав доступа к ресурсам ПК).

Во время первого запуска программы на компьютере компонент Контроль активности программ проверяет безопасность программы и помещает программу в одну из групп доверия. Группа доверия определяет правила контроля программ, которые Kaspersky Endpoint Security применяет для контроля работы программ.

Во время повторного запуска исследуется целостность программы. Если она не изменилась, применяется соответствующее правило, если изменилась, программа исследуется как в первый раз.

Заключение

Как видите, Kaspersky Endpoint Security скорее уже является центром управления безопасностью вашего ПК, а не только антивирусным ПО. С одной стороны продукт, естественно, стал сложнее, с другой – позволяет решить комплексные задачи в области обеспечения безопасности