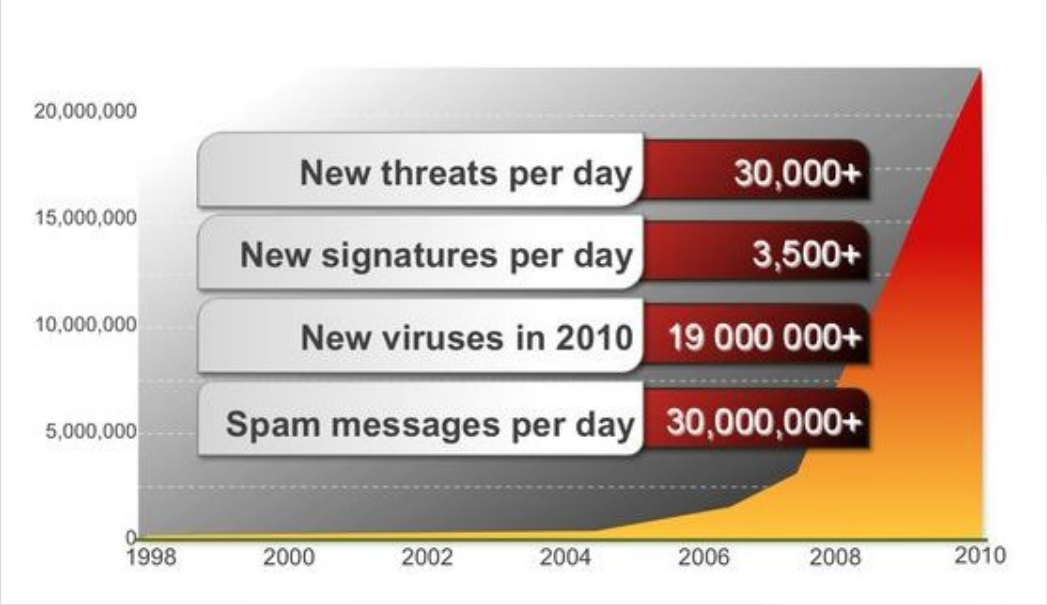
Новые решения для информационной безопасности бизнеса

Виталий Федоров
инженер предпродажной поддержки

KASPERSKY lab

Текущая ситуация в сфере IT-угроз и ответная реакция

Ситуация в сфере IT-угроз: рост числа угроз



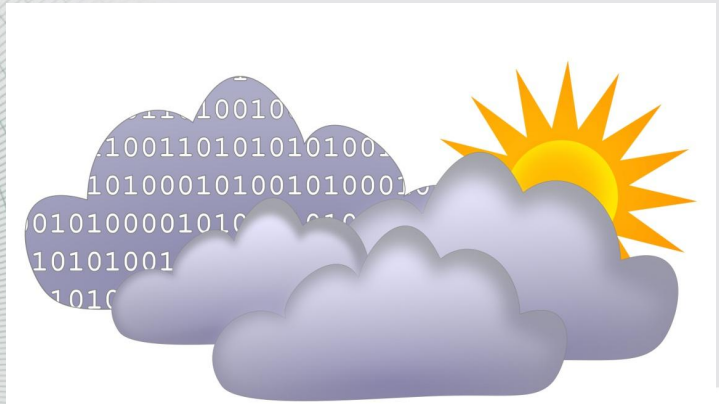
- 200 000 000 сетевых атак блокируется ежемесячно
- ~ 2 000 уязвимостей в приложениях обнаружено только в 2010 году
- > 35 000 вредоносных программ появляется ежедневно

Возникают серьёзные вопросы:

- Где хранить террабайты информации о компьютерных угрозах?
- Как обеспечить мгновенную реакцию на эти угрозы?
- Что делать в условиях, когда ни одна из проактивных технологий не может справиться с таким потоком угроз?

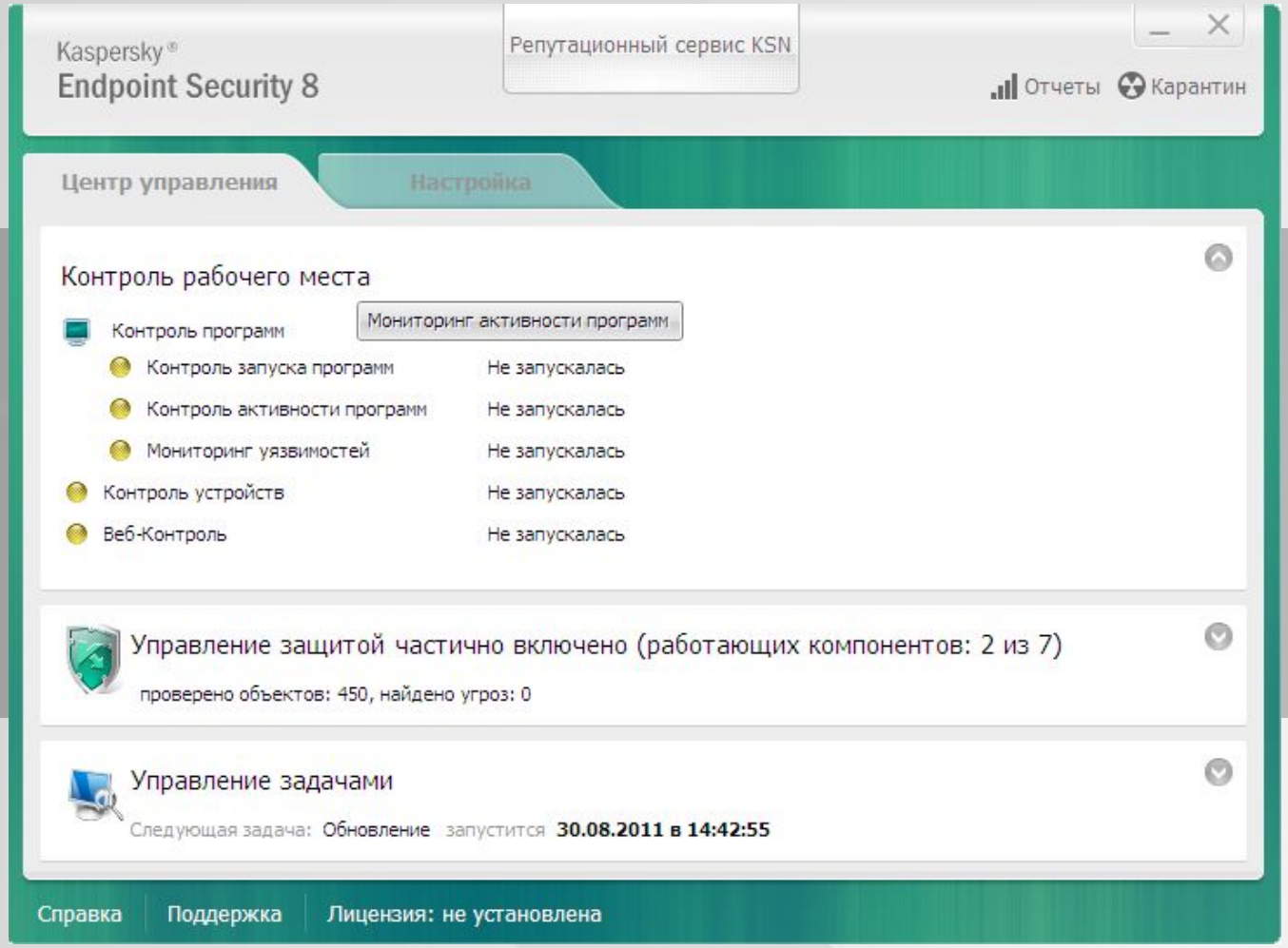
KASPERSKY lab

«Облачная» защита – наш ответ угрозам



KASPERSKY lab

Kaspersky Endpoint Security 8 для Windows



Kaspersky Endpoint Security 8 для Windows

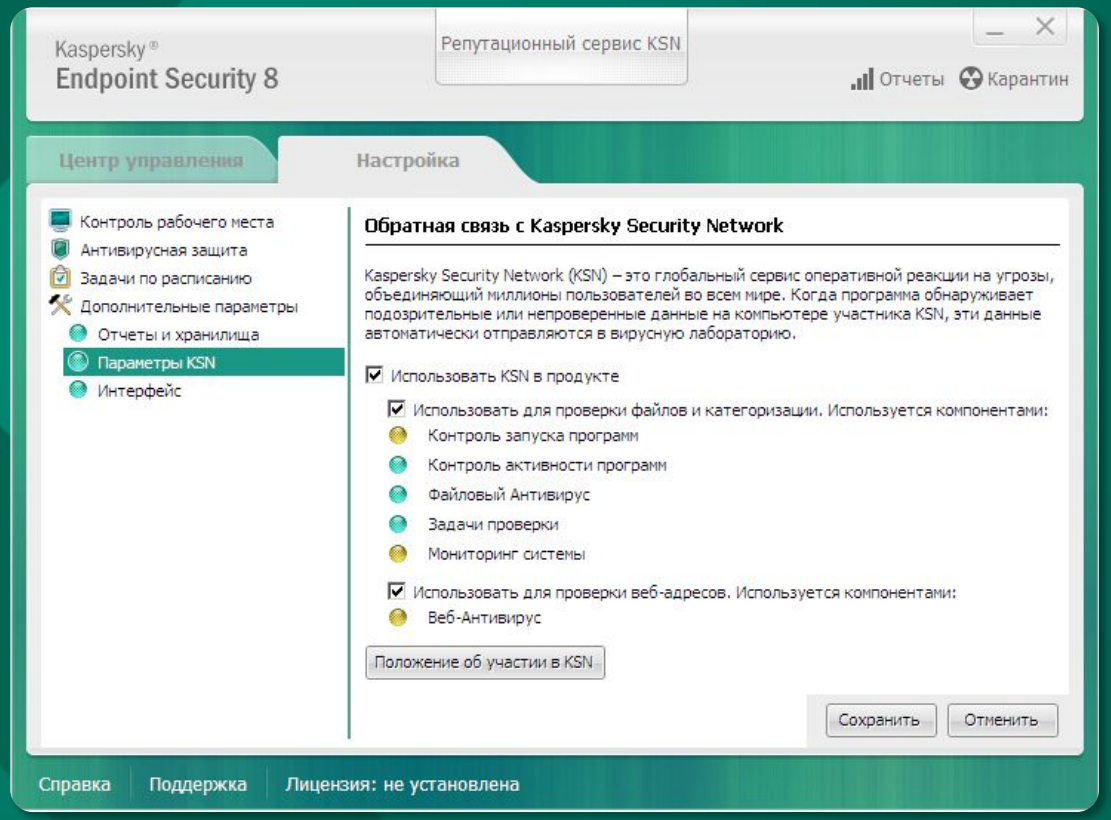
Защита от угроз сегодняшнего и завтрашнего дня

- Защита рабочих мест
  - Сигнатурный анализ
  - Проактивная защита
  - Облачная защита (Kaspersky Security Network)
- Контроль рабочих мест
  - Контроль программ
  - Контроль устройств
  - Веб-Контроль

KASPERSKY lab

Kaspersky Security Network (KSN)

- Облачная репутационная база
- Информация о 3 миллиардах объектов
- Мгновенное детектирование угроз и быстрое реагирование
- Минимальный риск ложных срабатываний



Мгновенная реакция на новые угрозы

Kaspersky Security Network (KSN) – глобальный облачный сервис мгновенной реакции на угрозы

- **Автоматический сбор данных о зараженных файлах, веб-страницах, подозрительном поведении программ**
- **Автоматическая обработка этой информации в вирлабе ЛК**
- **Мгновенный доступ к информации об угрозах со всех компьютеров с продуктами ЛК**

► Для чего это нужно?

- **Быстрый ответ** на новые угрозы: защита в течение десятков секунд после появления вируса в интернете
- **Отсутствие необходимости** передавать и хранить большой объем данных на компьютере пользователя
- **Минимальная загрузка компьютера** при «общении с облаком»

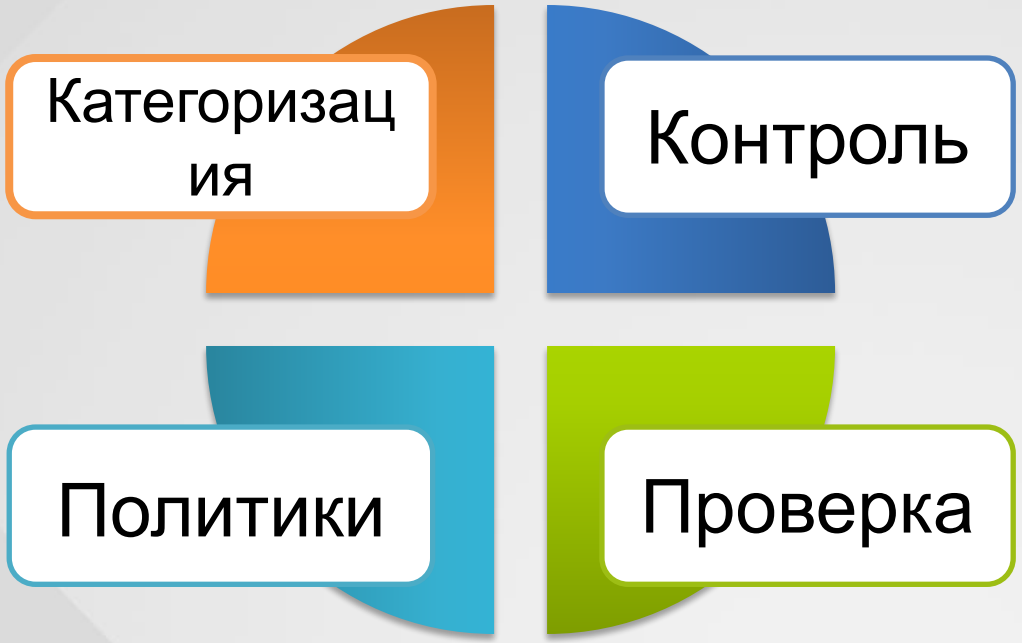
Kaspersky Endpoint Security 8 для Windows

Защита от угроз сегодняшнего и завтрашнего дня

- Защита рабочих мест
  - Сигнатурный анализ
  - Проактивная защита
  - Облачная защита (Kaspersky Security Network)
- Контроль рабочих мест
  - Контроль программ
  - Контроль устройств
  - Веб-Контроль

Контроль программ

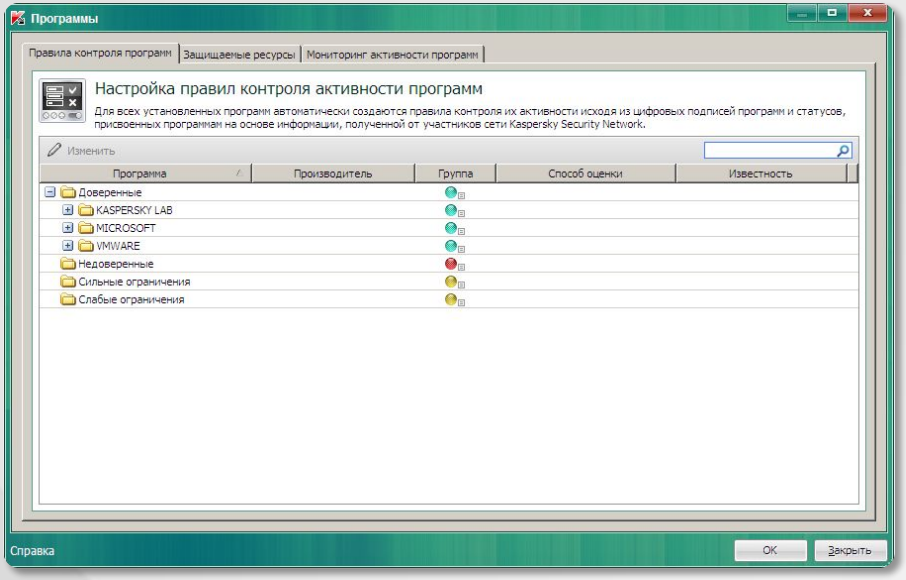
- Категоризация программ и белые списки
- Контроль запуска программ
- Контроль активности программ
- Мониторинг уязвимостей



Категоризация программ и белые списки

Категоризация

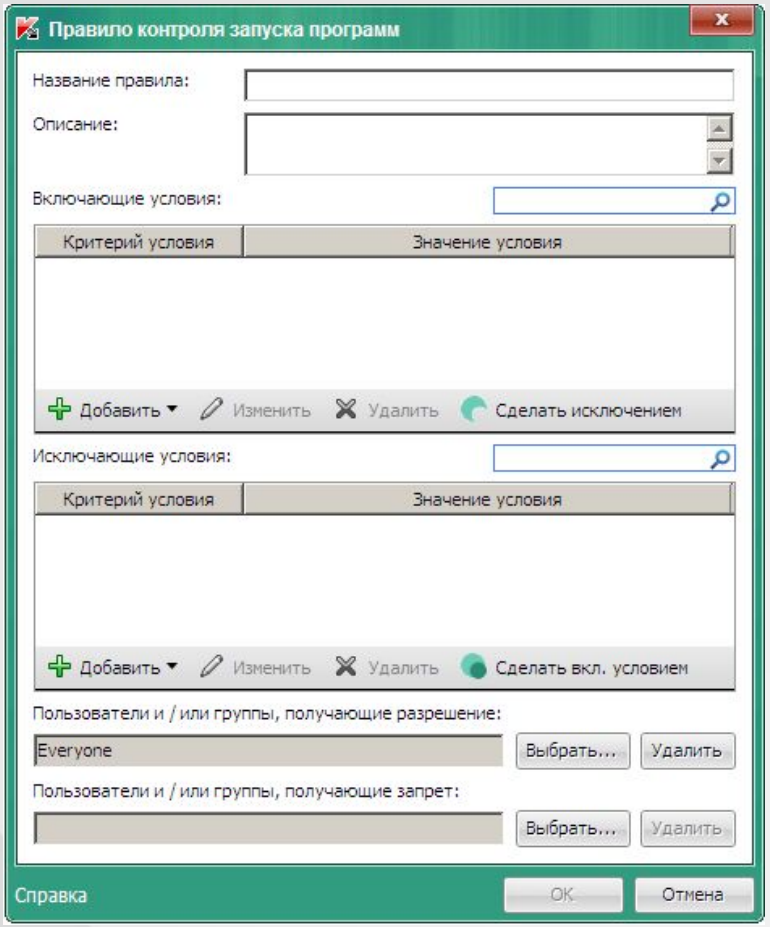
- Предустановленные KL-категории
  - созданные специалистами «Лаборатории Касперского»
- Собственные категории
  - созданные администратором
- Локальный и облачный белые списки
- Непрерывный мониторинг



Контроль запуска програм

Контроль

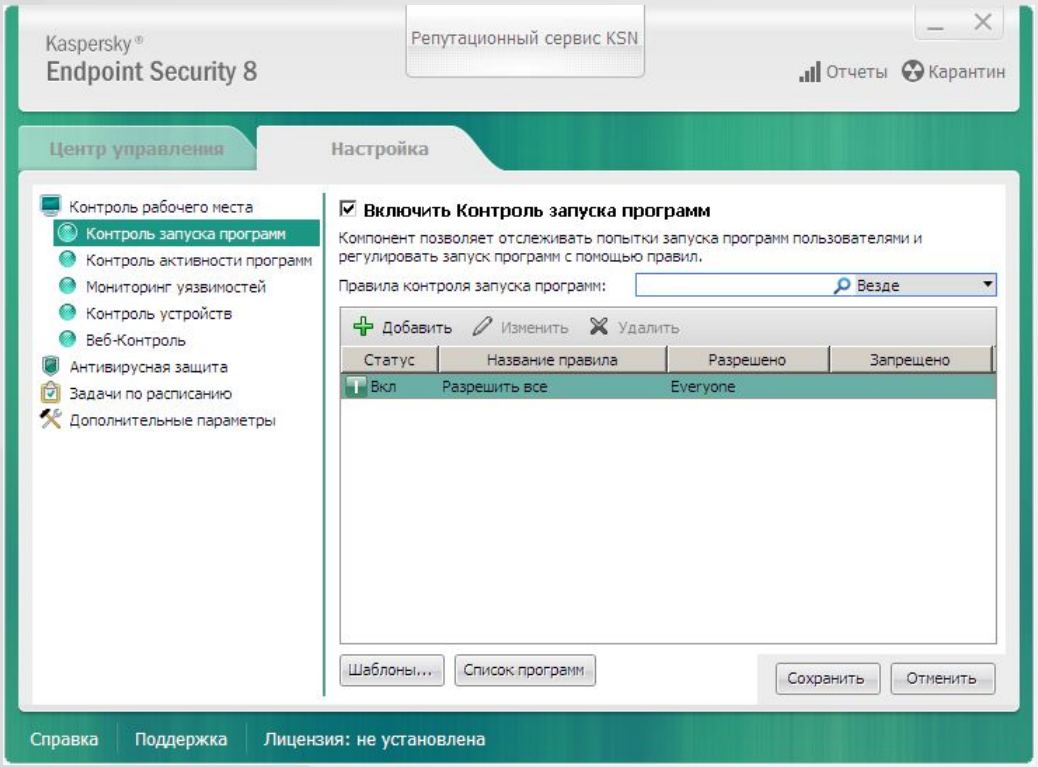
- Аудит запуска программ
- Разрешение и блокирование по белым спискам и категориям
- Интеграция с Active Directory
- Экономия сетевых ресурсов



Контроль активности программ

Политики

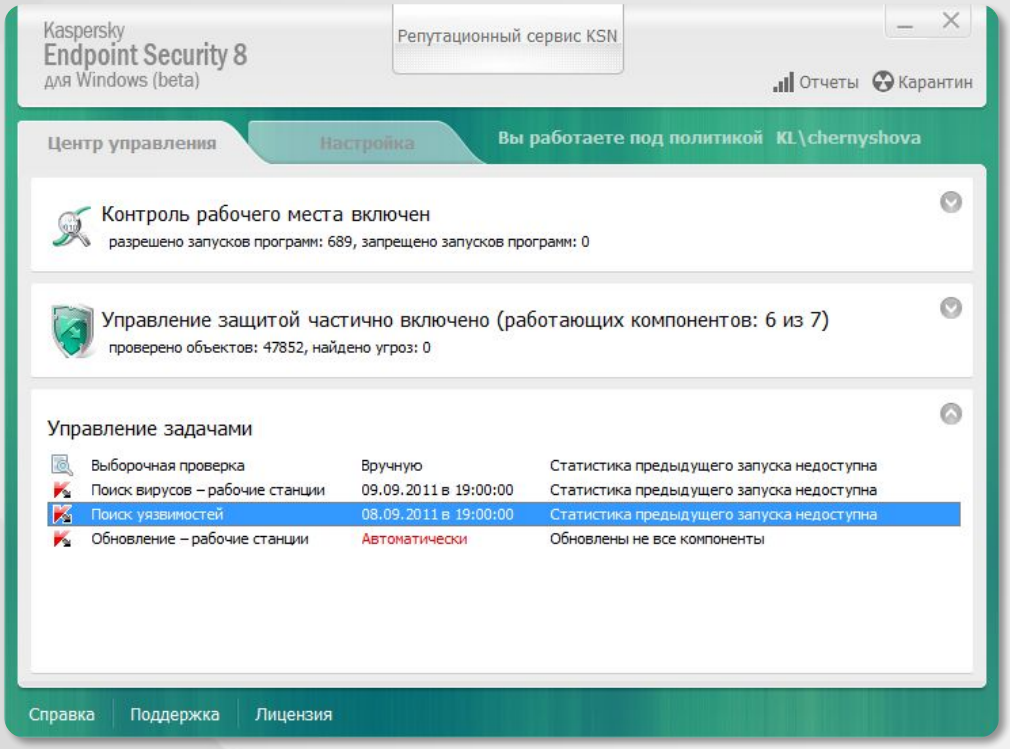
- Применение правил к запущенным программам
- Автоматическое распределение программ по группам:
  - Доверенные
  - Слабые ограничения
  - Сильные ограничения
  - Недоверенные
- Выбор политики в зависимости от присвоенной категории и группы
- Ограничение работы программ с:
  - реестром
  - ресурсами системы
  - данными пользователя
- Снижение вероятности использования в сети нежелательного ПО



Мониторинг уязвимостей

Проверка

- Проверка программ на наличие уязвимостей
- 3 источника данных:
  - база уязвимостей компании Secunia
  - список уязвимостей приложений Microsoft
  - список уязвимостей, составленный специалистами «Лаборатории Касперского»
- Задачи мониторинга:
  - информация
  - предупреждение
  - «первая помощь»
- Повышение надежности защиты



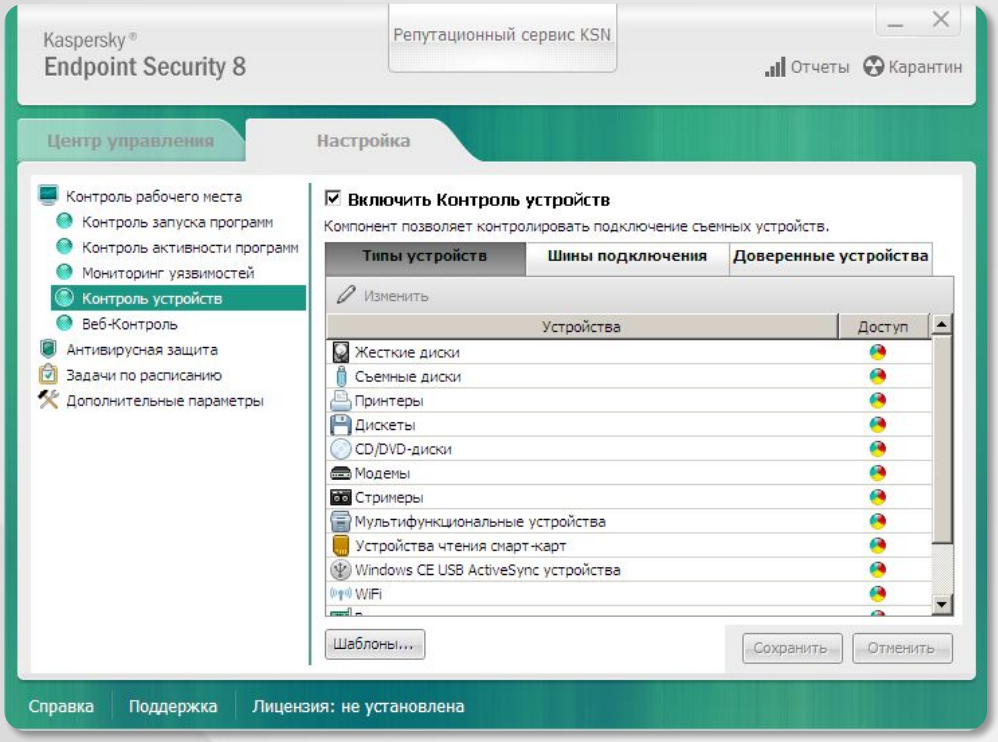
Kaspersky Endpoint Security 8 для Windows

Защита от угроз сегодняшнего и завтрашнего дня

- Защита рабочих мест
  - Сигнатурный анализ
  - Проактивная защита
  - Облачная защита (Kaspersky Security Network)
- Контроль рабочих мест
  - Контроль программ
  - Контроль устройств
  - Веб-Контроль

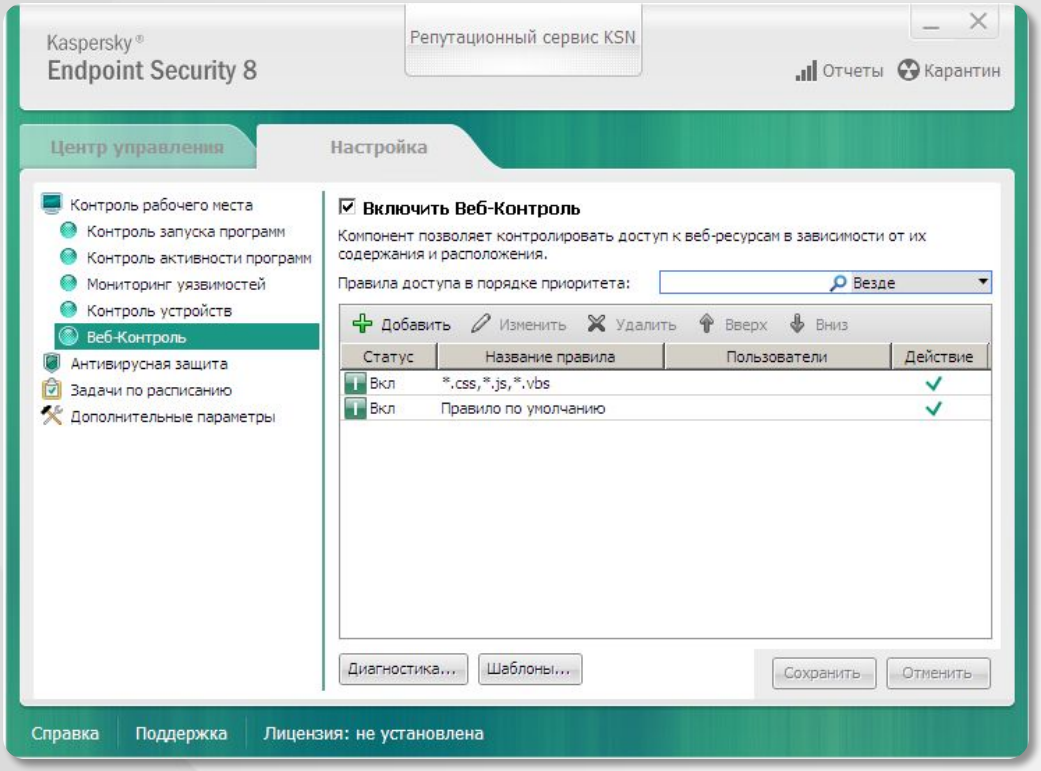
Гранулярный контроль устройств

- Ограничение доступа к подключаемым устройствам
  - внешние жесткие диски и другие накопители, модемы, принтеры
- Ограничение доступа по:
  - Типу устройства
  - Способу подключения (шине)
  - Серийному номеру
- Поддержка идентификаторов устройств
- Настройка расписания для применения правил



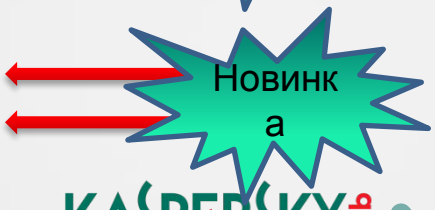
Веб-Контроль

- Аудит использования веб-ресурсов
- Политики доступа к веб-ресурсам:
  - Разрешение, запрещение или ограничение доступа
  - Расписание применения политик
  - Интеграция с Active Directory
- Правила доступа к веб-ресурсам по параметрам
- Тестирование правил
- Интеграция с KSN: использование репутационных сервисов для проверки ссылок



Функциональные возможности в защите рабочих станций и файловых серверов

Функции	Kaspersy Endpoint Security 8 для Windows	
	Рабочие станции	Файловые серверы
Файловый Антивирус	+	+
Почтовый Антивирус	+	-
Веб-Антивирус	+	-
IM-Антивирус	+	-
Технология лечения активного заражения (Advanced disinfection)	+	-
Мониторинг системы	+	-
Проактивная защита	+	-
Мониторинг активности программ: технология UDS (KSN)	+	-
Мониторинг активности программ: репутационная база KSN	+	-
Сетевой экран	+	+
Система обнаружения вторжений (IDS)	+	+
Контроль программ	+	-
Контроль устройств	+	-
Веб-Контроль	+	-
Мониторинг уязвимостей	+	+
Интеграция с KSN	+	+

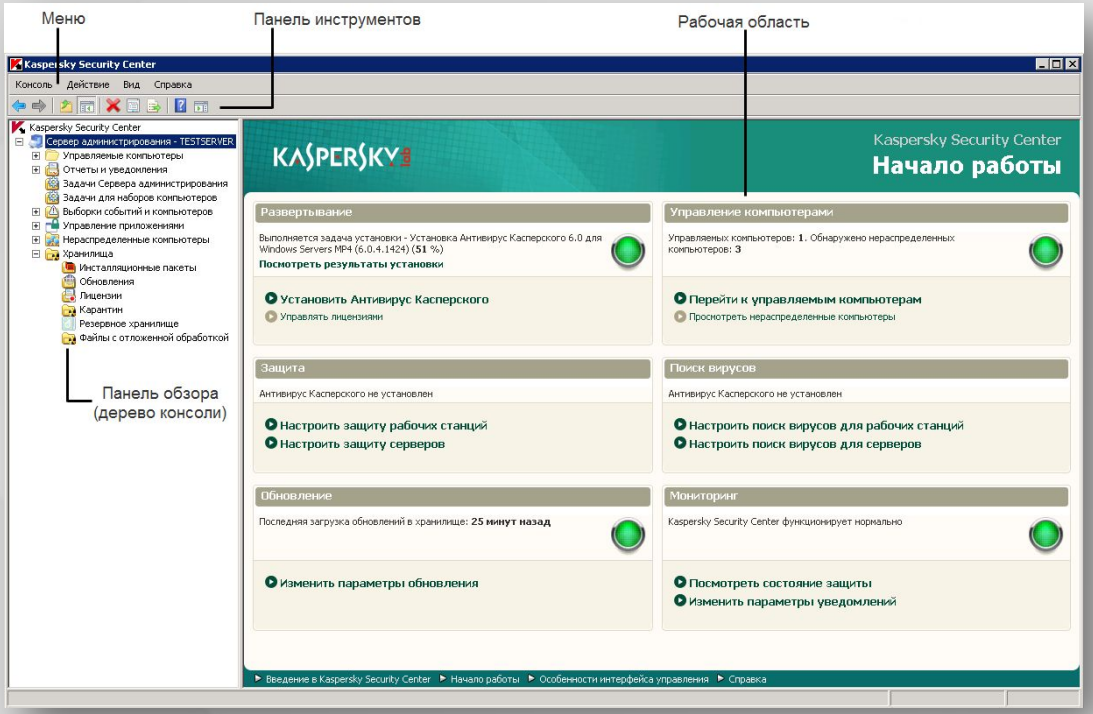


Kaspersky Security Center

Kaspersky Security Center

Новые возможности

- Управление виртуальными машинами VMware
- Создание виртуальных Сервером администрирования
- Инвентаризация программных и аппаратных средств
- Поиск уязвимостей
- Служба KSN Proxy
- Веб-консоль



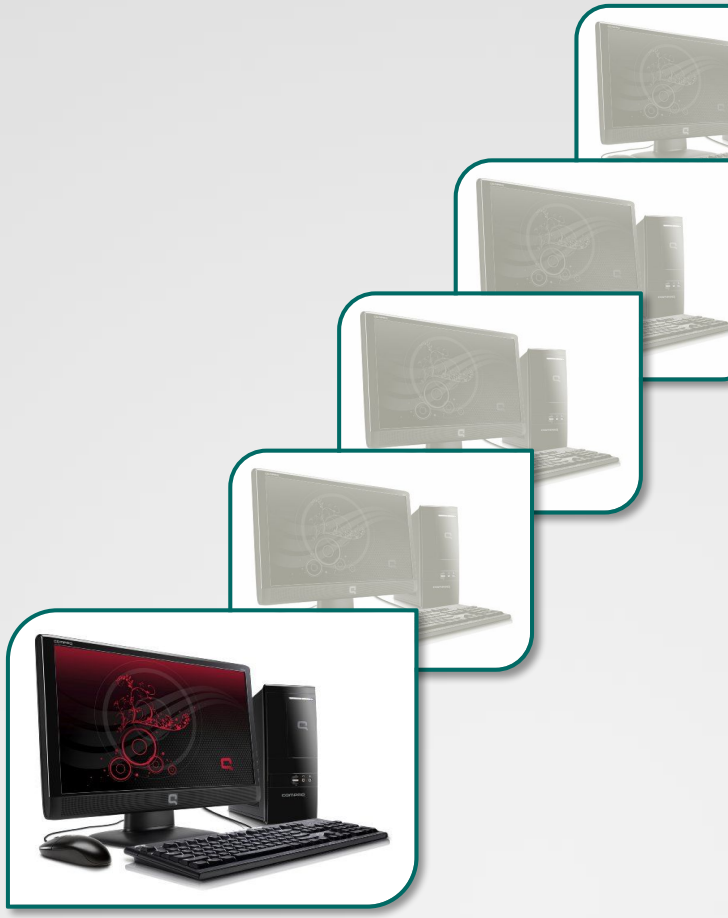
Виртуальные Серверы администрирования

Простое управление крупными или распределенными системами

- Двухуровневая иерархия Серверов администрирования
- До 10 виртуальных Серверов администрирования на одном физическом сервере
- Отсутствие необходимости в сторонних средствах виртуализации
- Возможность добавления дополнительных виртуальных серверов
- До 25 000 рабочих мест в иерархии
- Изоляция от других виртуальных серверов

Преимущества использования виртуальных Серверов администрирования

- Снижение нагрузки на единый Сервер администрирования
- Уменьшение объемов внутрисетевого трафика
- Простое управление локальными сетями удаленных филиалов
- Распределение обязанностей между администраторами безопасности



Учет ресурсов и поиск уязвимостей

Защита от угроз на уровне программ и ОС

- Инструмент для оценки уровня безопасности
- Детальный учет
  - Аппаратных средств
  - Программного обеспечения
- Минимизация возможностей для атак
- Сокращение времени реакции на угрозу
- Автоматические обновления через Kaspersky Security Network

Kaspersky Endpoint Security 8 для Windows и Kaspersky Security Center

- Ключевые и преимущества

KASPERSKY lab

Ключевые преимущества: Kaspersky Endpoint Security 8 для Windows

- Усиленная защита благодаря сочетанию проактивных, сигнатурных и облачных технологий
- Минимальный риск ложных срабатываний
- Мощные инструменты для контроля рабочего места:
  - контроль устройств
  - веб-контроль
  - контроль запуска программ
  - контроль активности программ / белые списки
- Полная интеграция с Kaspersky Security Center 9

Ключевые преимущества: Kaspersky Security Center

- Централизованное управление комплексной системой защиты
- Оперативное развертывание системы защиты
- Поддержка иерархической структуры управления
- Специальные политики для мобильных пользователей
- Просмотр состояния защиты при помощи веб-консоли
- Информационные панели и система отчетов
- Поддержка мультиплатформенных сред
- Автоматическая поддержка жизненного цикла виртуальных машин

Как приобрести

- Kaspersky Endpoint Security 8 для Windows и Kaspersky Security Center входят в состав всех продуктов линейки Kaspersky Open Space Security
- Kaspersky Endpoint Security 8 приходит на смену Антивирусу Касперского для Windows Workstation и Антивирусу Касперского для Windows Server

Продукт / Тип защищаемого узла сети	Смартфоны	Рабочие станции / Ноутбуки	Файловые серверы	Почтовые серверы	Интернет-шлюзы	Системы хранения данных
Kaspersky Work Space Security [KOSS 1]	•	•				
Kaspersky Business Space Security [KOSS 2]	•	•	•			
Kaspersky Enterprise Space Security [KOSS 3]	•	•	•	•		
Kaspersky Total Space Security [KOSS 4]	•	•	•	•	•	
Kaspersky Endpoint Security for Smartphone	•					
Антивирус Касперского для файловых серверов			•			
Kaspersky Security для почтовых серверов				•		
Kaspersky Security для интернет-шлюзов					•	
Антивирус Касперского для систем хранения данных						•

Спасибо!

http://www.kaspersky.ru

http://www.securelist.com/ru

KASPERSKY lab

Виталий Федоров, инженер предпродажной поддержки в УрФО и Пермском крае

vitaly.fedorov@kaspersky.com
+7(343)328-34-34