KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Надежная, гибкая и эффективная защита виртуальных серверов и рабочих станций

ПРЕИМУЩЕСТВА

УСИЛЕННАЯ ЗАЩИТА

- Передовые технологии защиты виртуальных машин (ВМ) от самых сложных угроз
- Интеграция с облачной сетью безопасности Kaspersky Security Network (KSN) для проактивной защиты от новых глобальных угроз
- Расширенная защита от вредоносного ПО, в том числе автоматическая защита от эксплойтов, формирующая мощную многоуровневую систему безопасности
- Контроль программ (с использованием динамических белых списков), веб-контроль и контроль устройств, позволяющие администратору применять политики для защиты пользователей и обеспечения их продуктивной работы
- Мощная комбинация технологии блокирования сетевых атак, персонального сетевого экрана и системы предотвращения вторжений (HIPS), а также технологии антифишинга для защиты виртуальных машин от сетевых угроз
- Централизованная защита ВМ с помощью виртуального устройства безопасности, антивирусные базы которого постоянно поддерживаются в актуальном состоянии

УЛУЧШЕННАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

- Инновационные технологии, обеспечивающие низкую нагрузку на систему и сохраняющие высокую плотность ВМ на хост-сервере
- Технология Shared Cache, позволяющая исключить повторную проверку файлов
- Отсутствие проблем «шквального» сканирования и обновления, а также появления «окна уязвимости» при выходе ВМ из спящего режима

УДОБСТВО ИСПОЛЬЗОВАНИЯ

- Поддержка платформ VMware ESXi, Microsoft® Hyper-V и Citrix Xen
- Быстрое и простое развертывание без необходимости перезагрузки ВМ и гипервизора в процессе установки решения
- Единая консоль управления безопасностью физических, мобильных и виртуальных узлов IT-инфраструктуры
- Упрощенное администрирование, повышающее эффективность работы и снижающее вероятность ошибок конфигурации
- Гибкое лицензирование по количеству ВМ (рабочих станций или серверов) или по количеству ядер физических процессоров

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД – ГИБКОЕ РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ВАШЕЙ IT-ИНФРАСТРУКТУРЫ И ПОВЫШЕНИЯ ЕЕ ПРОИЗВОДИТЕЛЬНОСТИ

ОСНОВНЫЕ ФУНКЦИИ

- **Централизованная защита ВМ с помощью виртуального устройства безопасности**
- **Расширенная защита от вредоносного ПО**
- **Персональный сетевой экран и система предотвращения вторжений (HIPS)**
- **Контроль приложений, веб-ресурсов и периферийных устройств**
- **Интеграция с облачной сетью безопасности Kaspersky Security Network (KSN)**
- **Блокирование сетевых атак**
- **Антифишинг**
- **Проверка IM-сообщений, почтовый и веб-антивирус**
- **Централизованное управление через Kaspersky Security Center**

ВИРТУАЛЬНОЕ УСТРОЙСТВО БЕЗОПАСНОСТИ

Оба варианта установки Kaspersky Security для виртуальных сред предполагают использование виртуального устройства безопасности, которое обеспечивает централизованную проверку всех виртуальных машин, размещенных на хост-сервере. Это позволяет эффективно защищать виртуальные машины без дополнительной нагрузки на гипервизор и сохраняет высокую плотность ВМ. Благодаря такому подходу исключаются ситуации «шквального» обновления и сканирования, а также появления «окна уязвимости» при выходе ВМ из спящего режима.

ГИБКОЕ ЛИЦЕНЗИРОВАНИЕ

Kaspersky Security для виртуальных сред может лицензироваться двумя способами, в зависимости от ваших потребностей:

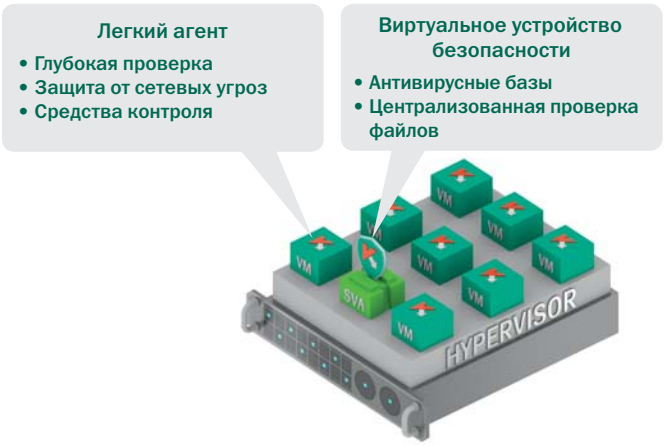
- По количеству виртуальных машин:
  - по количеству рабочих станций
  - по количеству серверов
- По количеству ядер физических процессоров

НЕСКОЛЬКО ПЛАТФОРМ – ЕДИНАЯ ЛИЦЕНЗИЯ

Kaspersky Security для виртуальных сред обеспечивает поддержку платформ виртуализации VMware ESXi, Microsoft Hyper-V и Citrix Xen в рамках единой лицензии.

РАСШИРЕННАЯ ЗАЩИТА НА БАЗЕ ЛЕГКОГО АГЕНТА

Kaspersky Security для виртуальных сред предусматривает два варианта развертывания. Легкий агент, устанавливаемый на каждую виртуальную машину, позволяет использовать расширенный функционал для обеспечения безопасности ВМ, в том числе мониторинг уязвимостей, контроль программ, устройств и веб-контроль, проверку IM-сообщений, почтовый и веб-антивирус, а также передовые эвристические методы защиты. Вместе эти компоненты образуют мощную многоуровневую систему безопасности, не оказывающую негативного влияния на производительность виртуальной среды.

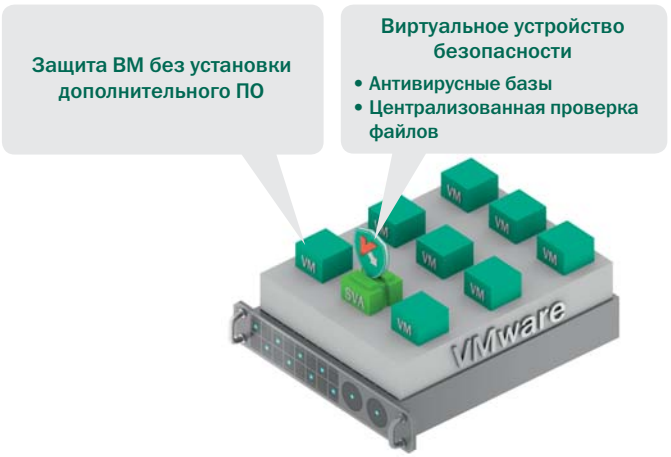


Kaspersky Security для виртуальных сред
Конфигурация с установкой Легкого агента

ЗАЩИТА БЕЗ АГЕНТА ДЛЯ СРЕД VMWARE

Тесная интеграция с технологиями VMware позволяет легко развертывать решение Kaspersky Security для виртуальных сред и управлять им на этой платформе без установки агента. Все действия по обеспечению безопасности осуществляются на выделенном виртуальном устройстве, которое взаимодействует с vShield для мгновенной автоматической защиты виртуальных машин, а также с vCloud для обеспечения защиты на уровне сети.

В этой конфигурации недоступны расширенные функции защиты, такие как карантин для подозрительных файлов, HIPS, проверка на наличие уязвимостей и средства контроля.



Kaspersky Security для виртуальных сред
Конфигурация без агента

Традиционная защита на базе агента	**Защита без установки агента**	**Защита на базе Легкого агента***
• Работает на любом гипервизоре • Защита ВМ на базе ОС Windows®, Linux® и Mac • Типовое применение: виртуальная среда, где плотность ВМ не имеет значения	• Только для сред VMware • Высокая плотность ВМ • Защита только ВМ на базе ОС Windows • Минимум IT-ресурсов для установки и управления • Типовое применение: виртуализация серверов с контролируемым подключением к интернету	• Для сред VMware, Microsoft и Citrix • Высокая плотность ВМ • Защита только ВМ на базе ОС Windows • Расширенная защита и применение политик • Типовое применение: виртуализация рабочих станций и серверов, выполняющих критически важные задачи

* Для непостоянных ВМ защита осуществляется сразу же после добавления Легкого агента в образ ВМ. Для защиты постоянных ВМ Легкий агент должен быть установлен на каждую виртуальную машину в процессе инсталляции.

ПОДДЕРЖИВАЕМЫЕ ПЛАТФОРМЫ ВИРТУАЛИЗАЦИИ

- Microsoft Hyper-V Server 2008 R2 / 2012
- Citrix XenServer 6.0.2 / 6.1
- VMware ESXi 4.1, 5.0, 5.1 и 5.5

ПОДДЕРЖИВАЕМЫЕ ГОСТЕВЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Конфигурация	Защита на базе Легкого агента			Защита без агента
Гостевые операционные системы, установленные на виртуальной машине	Windows Server® 2008 R2 Hyper-V и Windows Server 2012 Hyper-V	XenServer 6.0.2 и 6.1	VMware ESXi 5.1 и 5.5	VMware ESXi 4.1, ESXi 5.0 или ESXi 5.1
Windows XP Professional SP3 (x32)	Да	Да	Нет	Да
Windows XP Professional SP2 (x64)	Да	Нет	Нет	Нет
Windows 7 Professional / Enterprise / Ultimate (x32 / x64) SP1 или выше	Да	Да	Да	Да
Windows 8 Pro / Enterprise (x32 / x64)	Да	Да	Да	Нет
Windows Vista® Business / Enterprise / Ultimate SP2 (x32)	Да	Нет	Нет	Да
Windows Server 2008 R2 Standard / Enterprise SP2 (x64)	Да	Да	Да	Да
Windows Server 2008 Standard / Enterprise SP2 (x32 / x64)	Да	Да	Да	Да
Windows Server 2003 R2 Standard / Enterprise SP2 (x32 / x64)	Да	Нет	Да	Да
Windows Server 2003 Standard SP2 (x32 / x64)	Да	Да	Нет	Да
Windows Server 2012 (x64)	Да	Да	Да	Нет
Windows Small Business Server 2008 Standard (x64)	Да	Нет	Нет	Нет
Windows Small Business Server 2011 Essentials / Standard (x64)	Да	Нет	Нет	Нет

Подробнее о Kaspersky Security для виртуальных сред см. на **www.kaspersky.ru/business-security/virtualization/**

KSV/Version 3.1/April 14/Global

KASPERSKY lab