KASPERSKY lab

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
ЗАЩИТА СРЕД VMWARE, MICROSOFT И CITRIX

апрель 2014 г.

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ СРЕД: МИФЫ И РЕАЛЬНОСТЬ

МИФ

ВИРТУАЛЬНЫЕ СРЕДЫ ЛУЧШЕ ЗАЩИЩЕНЫ, ЧЕМ ФИЗИЧЕСКИЕ

ВРЕДОНОСНЫЕ ПРОГРАММЫ НЕ ДЕЛАЮТ РАЗЛИЧИЙ МЕЖДУ ФИЗИЧЕСКИМИ И ВИРТУАЛЬНЫМИ МАШИНАМИ

МИФ

КИБЕРПРЕСТУПНИКИ НЕ АТАКУЮТ ВИРТУАЛЬНЫЕ МАШИНЫ

MORCUT (AKA CRISIS) – ПЕРВЫЙ ТРОЯНЕЦ, НАЦЕЛЕННЫЙ НА ВИРТУАЛЬНЫЕ МАШИНЫ. ОБНАРУЖЕН В 2012 ГОДУ

МИФ

ПРИ УДАЛЕНИИ НЕПОСТОЯННЫХ ВМ ВРЕДОНОСНОЕ ПО ТОЖЕ УДАЛЯЕТСЯ

РЕЗИДЕНТНОЕ ПО МОЖЕТ ОСТАВАТЬСЯ. НАПРИМЕР, KIDO/CONFICKER МОЖЕТ «ПЕРЕПРЫГИВАТЬ» С ОДНОЙ ВМ НА ДРУГУЮ, С ОДНОГО ХОСТ-СЕРВЕРА НА ДРУГОЙ

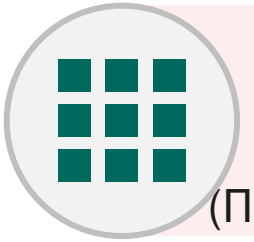
KASPERSKY lab

ВРЕДОНОСНОЕ ПО РАСТЕТ И РАЗВИВАЕТСЯ

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ СРЕД – ВОЗМОЖНЫЕ ВАРИАНТЫ

БЕЗ ЗАЩИТЫ

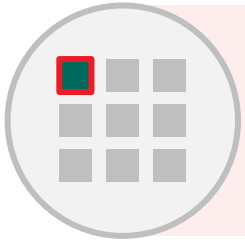
НЕПРИЕМЛЕМО!



ТРАДИЦИОННАЯ ЗАЩИТА

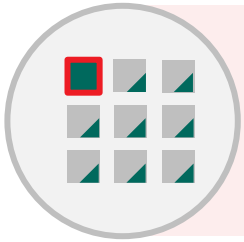
(Полноценный агент)

ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ / СНИЖЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ



БЕЗ УСТАНОВКИ АГЕНТА

ПРОСТОЕ РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ. ТОЛЬКО ДЛЯ СРЕД VMWARE

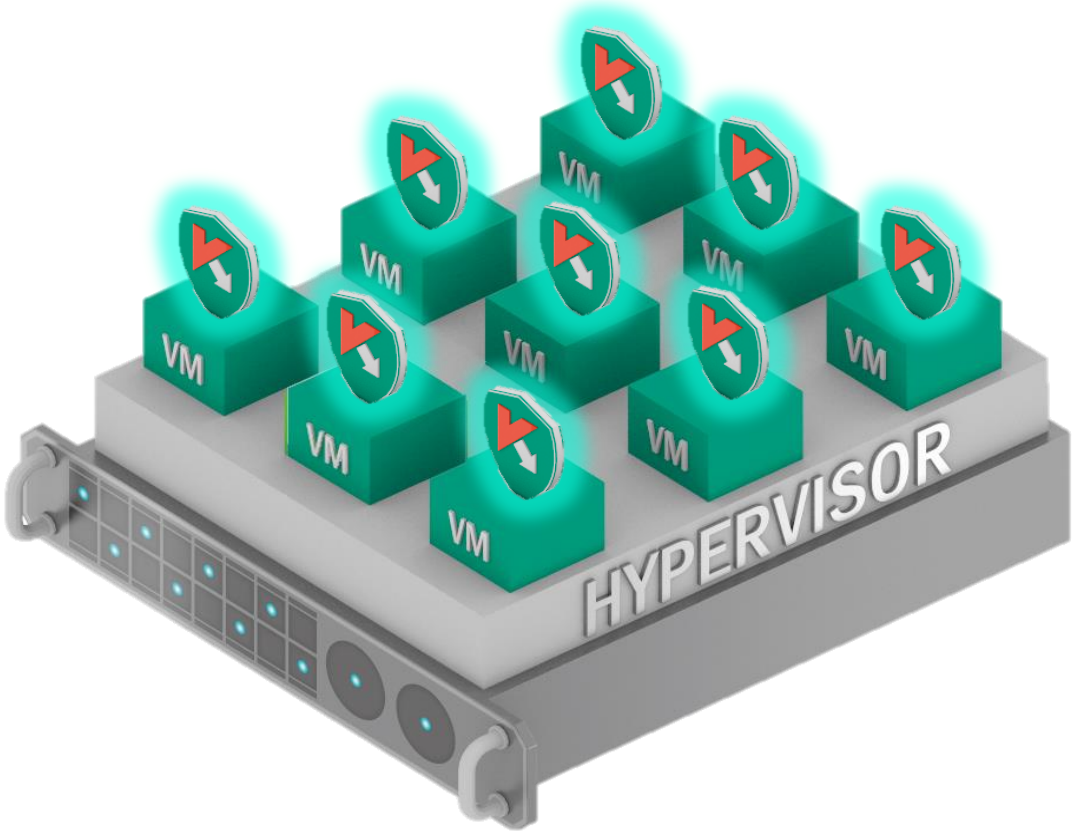


ЛЕГКИЙ АГЕНТ

НАДЕЖНАЯ ЗАЩИТА

ТРАДИЦИОННАЯ ЗАЩИТА С УСТАНОВКОЙ АГЕНТА

Полноценный агент безопасности устанавливается на каждую виртуальную машину



Агент безопасности

- **Неэффективное использование ресурсов**
  - Дублирование ПО
  - Дублирование сигнатурных баз
- **Результат:**
  - Чрезмерное потребление ресурсов
  - «Шквальные» обновления
  - «Окно уязвимости» при выходе ВМ из спящего режима
  - Низкая плотность ВМ

KASPERSKY lab

РЕШЕНИЕ: KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

РАЗРАБОТАНО СПЕЦИАЛЬНО ДЛЯ ВИРТУАЛЬНЫХ СРЕД

ЕДИНАЯ КОНСОЛЬ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ФИЗИЧЕСКИХ, МОБИЛЬНЫХ И ВИРТУАЛЬНЫХ УСТРОЙСТВ

vmware citrix

Windows Server Hyper-V

ПОДДЕРЖКА ВСЕХ ОСНОВНЫХ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ ОТ VMWARE, MICROSOFT И CITRIX

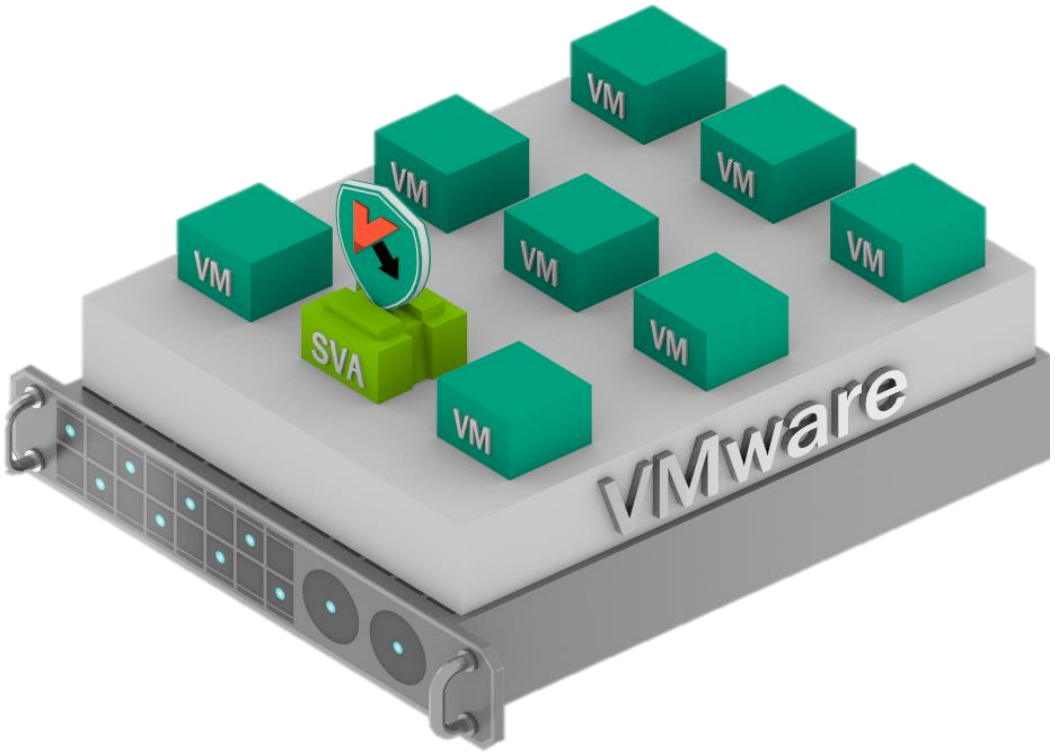
ОТМЕЧЕННОЕ НАГРАДАМИ АНТИВИРУСНОЕ ЯДРО

ИНТЕГРАЦИЯ С ОБЛАЧНОЙ СЕТЬЮ БЕЗОПАСНОСТИ KASPERSKY SECURITY NETWORK

KASPERSKY lab

ЗАЩИТА БЕЗ УСТАНОВКИ АГЕНТА

Защиту обеспечивает виртуальное устройство безопасности, установленное на хост-сервере



Эффективно:

- Установка и запуск решения занимают меньше часа
- Без необходимости перезагрузки системы

Исключает:

- Чрезмерное потребление ресурсов
- «Шквальное» обновление и сканирование
- «Окно уязвимости» при выходе ВМ из спящего режима

Результат:

- Высокая плотность ВМ

ЗАЩИТА БЕЗ АГЕНТА

ТЕСНАЯ ИНТЕГРАЦИЯ С ПЛАТФОРМОЙ VMWARE

ПРОВЕРКУ ФАЙЛОВ И БЛОКИРОВАНИЕ СЕТЕВЫХ УГРОЗ ОСУЩЕСТВЛЯЕТ ВИРТУАЛЬНОЕ УСТРОЙСТВО БЕЗОПАСНОСТИ

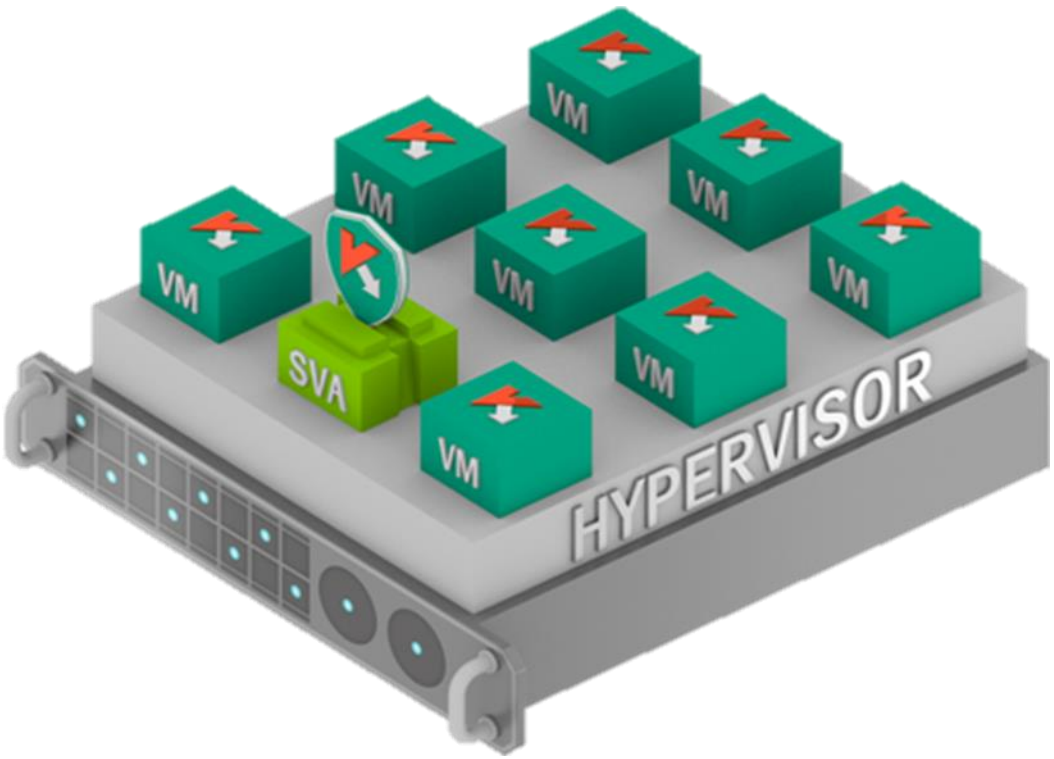
ОТСУТСТВИЕ ДУБЛИРОВАНИЯ ПО И АНТИВИРУСНЫХ БАЗ, СОХРАНЕНИЕ ВЫСОКОЙ ПЛОТНОСТИ ВМ

ПРОСТОЕ РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ, МГНОВЕННАЯ ЗАЩИТА

ЭФФЕКТИВНОЕ РАЗВЕРТЫВАНИЕ В СРЕДАХ VMWARE, ТРЕБУЮЩИХ ТОЛЬКО БАЗОВОЙ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПО

ЗАЩИТА НА ОСНОВЕ ЛЕГКОГО АГЕНТА

Легкий агент на каждой ВМ плюс виртуальное устройство безопасности



- **Расширенная защита**
  - Мониторинг уязвимостей
  - Контроль программ
  - Веб-контроль
  - Контроль устройств
  - Эвристический анализ
  - Проверка IM-сообщений, почтового и веб-трафика
- **Устраняет:**
  - Чрезмерное потребление ресурсов
  - «Шквальное» обновление и сканирование
  - «Окно уязвимости» при выходе ВМ из спящего режима

KASPERSKY lab

ЗАЩИТА НА ОСНОВЕ ЛЕГКОГО АГЕНТА

ПОДДЕРЖКА СРЕД VMWARE, CITRIX И MICROSOFT

ВИРТУАЛЬНОЕ УСТРОЙСТВО БЕЗОПАСНОСТИ ПРОВЕРЯЕТ ФАЙЛЫ ДЛЯ КАЖДОЙ ВМ НА ХОСТ-СЕРВЕРЕ

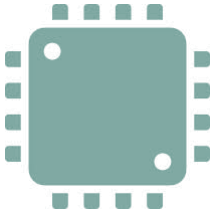
РАСШИРЕННАЯ ЗАЩИТА С СОХРАНЕНИЕМ ВЫСОКОЙ ПЛОТНОСТИ ВМ

ПРИМЕНЕНИЕ ПОЛИТИК ВЕБ-КОНТРОЛЯ, КОНТРОЛЯ УСТРОЙСТВ И ПРОГРАММ

АВТОМАТИЧЕСКАЯ ЗАЩИТА ОТ ЭКСПЛОЙТОВ ПРЕДОТВРАЩАЮЩАЕТ ЭКСПЛУАТАЦИЮ УЯЗВИМОСТЕЙ ВРЕДОНОСНЫМ ПО

ГИБКОЕ ЛИЦЕНЗИРОВАНИЕ ПО ЧИСЛУ ВМ И ПО ЧИСЛУ ЯДЕР ПРОЦЕССОРОВ

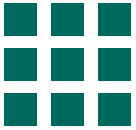
ПО ЧИСЛУ ВМ
Стоимость зависит от числа защищаемых ВМ



ПО ЧИСЛУ ЯДЕР ПРОЦЕССОРОВ
Стоимость зависит от объема защищаемых физических ресурсов

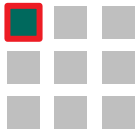
ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ
Защита платформ Microsoft Hyper-V, Citrix Xen и VMware ESXi в рамках одной лицензии

ВЫБОР ОПТИМАЛЬНОГО СПОСОБА ЗАЩИТЫ



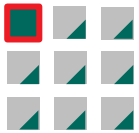
Традиционная защита на базе агента

- Работает на любом гипервизоре
- Защита ВМ на базе ОС Windows, Linux и Mac
- Типовое применение: виртуальная среда, где плотность ВМ не имеет значения



Защита без установки агента

- Только для сред VMware
- Высокая плотность ВМ
- Защита только ВМ на базе ОС Windows
- Минимум IT-ресурсов для установки и управления
- Типовое использование: виртуализация серверов с контролируемым подключением к интернету



Защита на базе Легкого агента

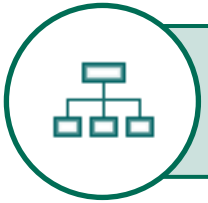
- Для сред VMware, Microsoft и Citrix
- Высокая плотность ВМ
- Защита только ВМ на базе ОС Windows
- Расширенная защита:
  - Проверка IM-сообщений, почтового и веб-трафика
  - Автоматическая защита от эксплойтов
  - Контроль программ, устройств и веб-контроль
- Типовое использование: виртуализация рабочих станций и серверов, выполняющих критически важные задачи

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

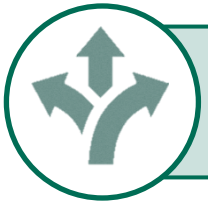
БЕЗОПАСНОСТЬ

ПРОИЗВОДИТЕЛЬНОСТЬ

ЭФФЕКТИВНОСТЬ



УПРАВЛЕНИЕ



ГИБКОСТЬ

KASPERSKY lab

СПАСИБО!

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