Современные Подходы к Защите Виртуализированной ИТ Инфраструктуры

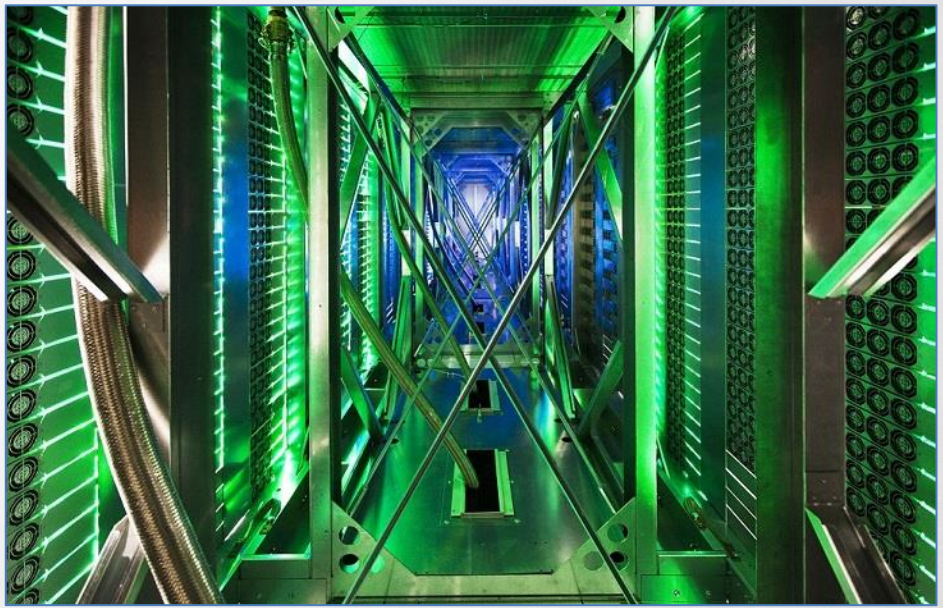
Павел Поляков
Инженер по предпродажной поддержки в Восточной Европе

KASPERSKY lab

Содержание

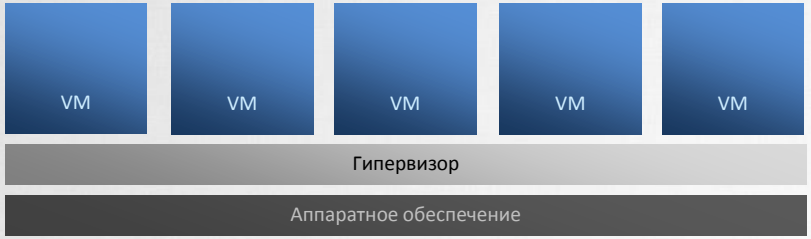
Сегодня рассмотрим:

- Риски ИТ безопасности в Виртуальной среде.
- Вредоносное ПО в Виртуальной среде.
- Методы защиты Виртуализированной ИТ инфраструктуре.



KASPERSKY lab

Ключевые понятия



- Гостевая операционная система
- Виртуальная машина (VM)
- Гипервизор

I типа — работает как операционная система, непосредственно взаимодействует с устройствами:
VMware ESXi, Microsoft Hyper-V, XenServer

II типа — работает как программа в операционной системе:
VMware Workstation, VirtualBox, VirtualPC, Parallels

Возможности виртуализации

- Запуск нескольких операционных систем на одном компьютере

- Преимущества:
  - Быстрое развертывание тестовых и промышленных конфигураций
  - Стандартизация драйверов, и как следствие, переносимость
  - Эффективное использование ресурсов
  - Быстрое восстановление при сбоях
  - Высокая доступность и балансировка нагрузки

РИСКИ безопасности в виртуализированной ИТ инфраструктуры

- Риски связанные с взаимодействием виртуальных машин (например, технология vmotion)
- Риск нарушения непрерывности бизнеса (Denial-of-Service).
- Традиционные риски Информационной Безопасности

KASPERSKY lab

Вредоносное ПО в виртуальных средах

ДА — РАБОТАЮТ ЛИ ВИРУСЫ В ВИРТУАЛЬНЫХ СРЕДАХ?

- УЯЗВИМЫ ГОСТЕВЫЕ ОС. БОЛЬШИНСТВО ТРАДИЦИОННЫХ ВИРУСОВ НЕЗАВИСИМЫ ОТ СРЕД ВИРТУАЛИЗАЦИИ

ДА — ИСПОЛЬЮТ ЛИ СПЕЦИФИКУ ВИРТУАЛЬНЫХ СРЕД?

- ПЕРВЫЙ ТРОЯН, ЗАРАЖАЮЩИЙ ШАБЛОНЫ ВИРТУАЛЬНЫХ МАШИН VMWARE БЫЛ НАЙДЕН В 2012 (MORCUT)
- Blue Pill

ДА — МОЖЕТ ЛИ ВЫЖИВАТЬ ЗЛОВРЕДНОЕ ПО В ВИРТУАЛЬНОЙ СРЕДЕ?

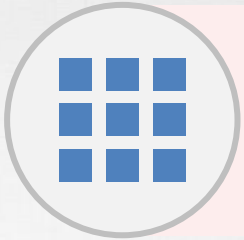
- СЕТЕВОЙ ЧЕРВЬ, ПРОШЕДШИЙ ЧЕРЕЗ КОРПОРАТИВНЫЙ ПЕРИМЕТР, МОЖЕТ ЖИТЬ СКОЛЬ УГОДНО ДОЛГО

KASPERSKY lab

Virtual security – подходы к защите

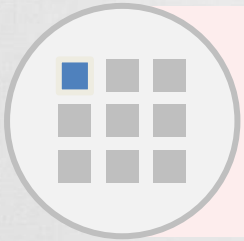
NO SECURITY

NOT AN OPTION!



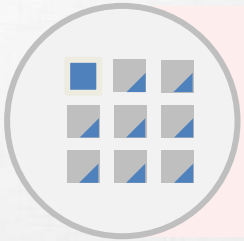
Традиционный подход (Agent-Based)

ОТЛИЧНАЯ ЗАЩИТА ДЛЯ НЕВИРТУАЛИЗИРОВАННОЙ СРЕДЫ



БезАгентское решение (AGENTLESS)

ЛЕГКО ВНЕДРИТЬ В СРЕДЕ VMWARE

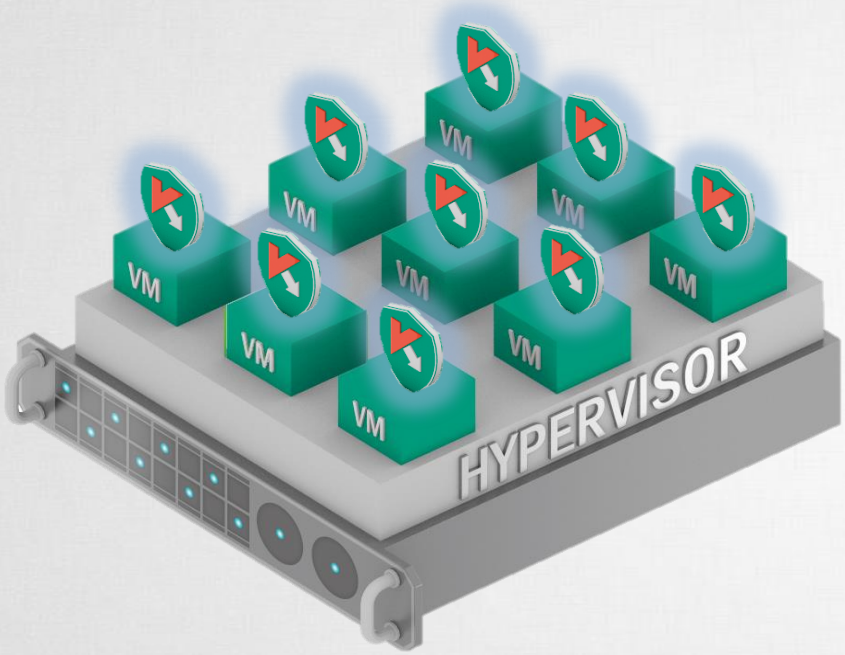


Решение «Легкий агент» (LIGHT AGENT)

КОМБИНИРОВАННОЕ РЕШЕНИЕ ЗАЩИТЫ ВИРТУАЛЬНОЙ СРЕДЫ

KASPERSKY lab

Традиционные решения



Неэффективно для Виртуальных Сред из-за:

1. Специфики виртуальных сред
2. инсталляция полноценного антивирусного ПО на каждую VM - черезмерное использования ресурсов.
3. «шторм» трафика при одновременном обновлении баз антивируса и т.д.

KASPERSKY lab

Kaspersky security for virtualization

- Разработан специально для Виртуальных Сред

- Единая панель управления защитой как для физической так и для виртуальной среды (Kaspersky Security Center)

- Поддержка самых популярных гипервизоров

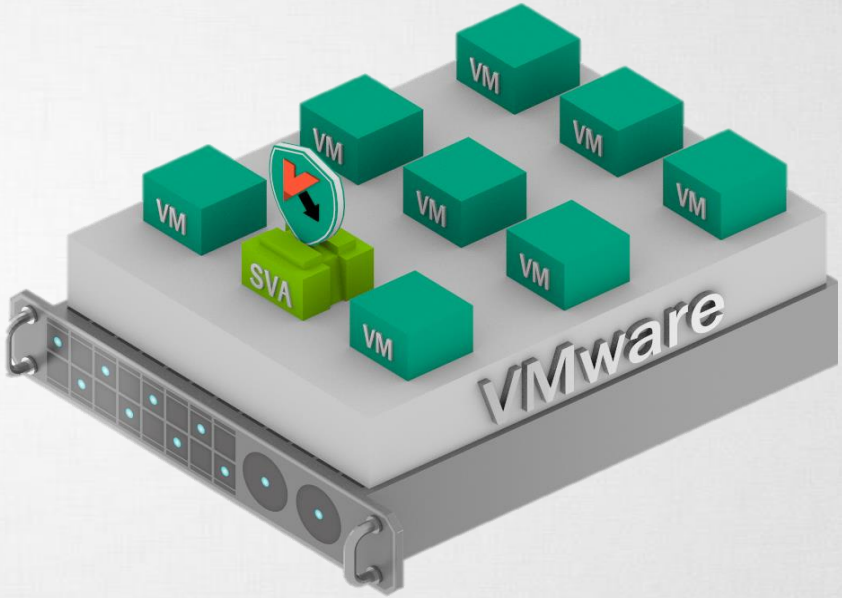
- AWARD-WINNING ANTI-MALWARE ENGINE

- KASPERSKY SECURITY NETWORK

KASPERSKY lab

Специализированная защита – «Без Агентская» технология = KSV Agentless

1. **Используется встроенный функционал от VMware** («vShield» и «vCloud Networking and Security») **.**
2. **Функциональность антивируса вынесены на отдельную Виртуальную Машину (VSA)**
   - Антивирусные базы на одной машине – нет проблемы «штормов»
   - Защита на файловом и сетевом уровнях.
3. **Небольшая нагрузка на ресурсы гипервизора**
   - Меньше «след» машин в памяти
   - Избегаем повторного сканирования (общий кэш вердиктов)



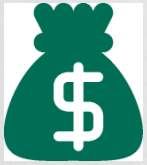
KASPERSKY lab

Ограничения «Без Агентского» (AGENTLESS) подхода

- Совместимо только с платформой VMware

- Нет доступа к оперативной памяти виртуальных машин – ограничения vShield

- Ограниченный функционал - отсутствие инструментов контроля (приложений, веб, устройств).

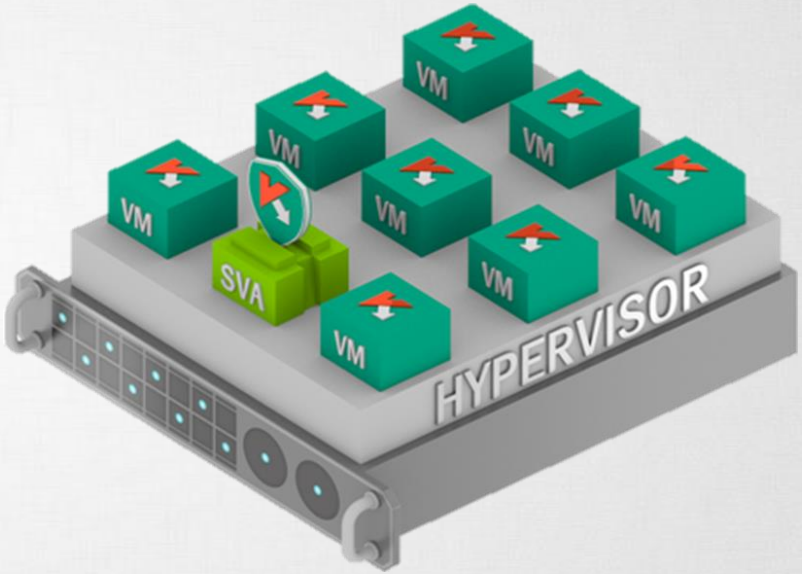


- Сетевая защита требует покупки «vcloud networking and security»

KASPERSKY lab

Специализированная защита – «Легкий Агент» = KSV Light Agent

1. **Особенности реализации**:
   - Дополнительное лёгкое приложение на защищаемой ВМ.
   - Не использует VMware API
   - Содержит дополнительные модули защиты
2. **Расширенный функционал защиты:**
   - Система защиты от вторжений и сетевой экран
   - Контроль приложений/web/устройств
   - Проверка памяти и системных процессов
3. **Оптимальное потребление ресурсов**

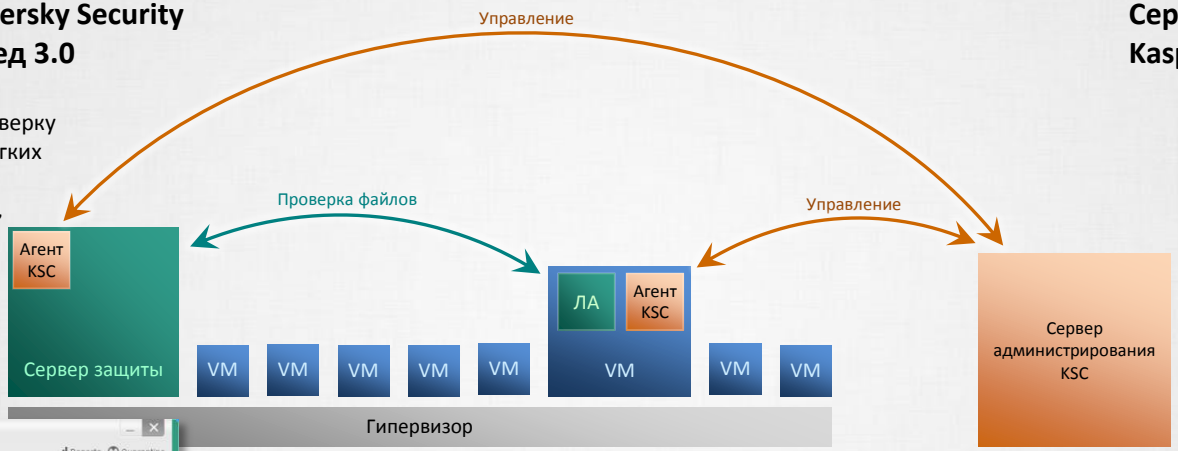


KASPERSKY lab

Компоненты Kaspersky Security 3.0 для виртуальных сред

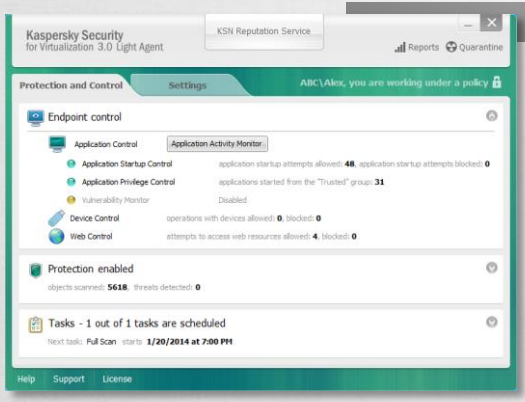
Сервер защиты Kaspersky Security для виртуальных сред 3.0

Специальная виртуальная машина, выполняющая проверку файлов, поступающих от Легких агентов. Также отвечает за распространение лицензий, обновлений. Содержит предустановленный Агент администрирования



Сервер администрирования Kaspersky Security Center

Единая консоль управления защитой на базе продуктов Лаборатории Касперского, хорошо знакомая по управлению защитой узлов Windows на базе Kaspersky Endpoint Security.
В случае Kaspersky Security для виртуальных сред Сервер администрирования необходим для:
— Развертывания
— Обновления
— Настройки

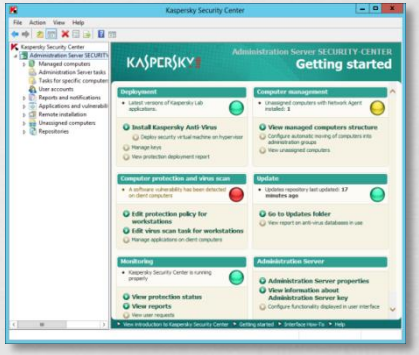


Легкий агент Kaspersky Security для виртуальных сред 3.0

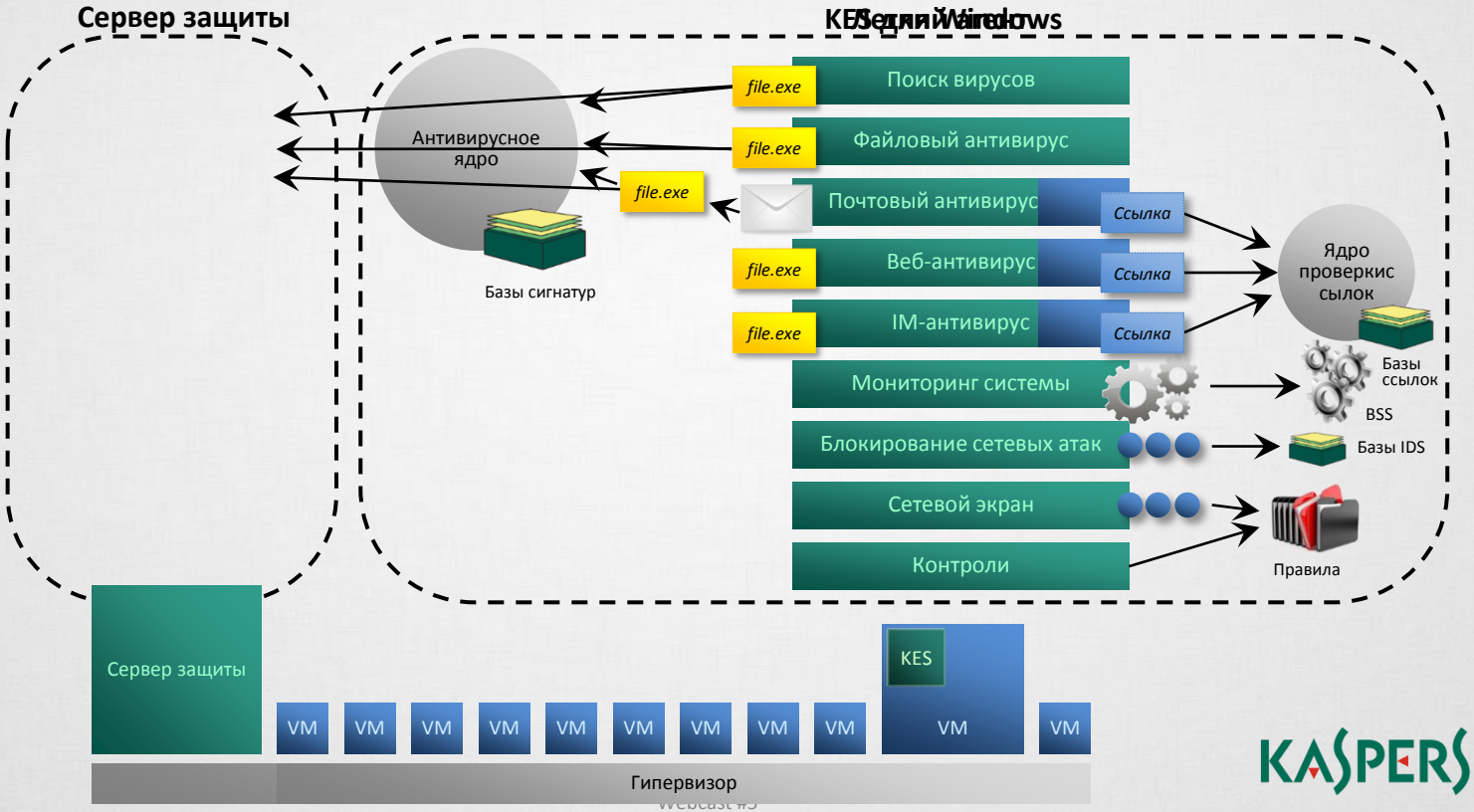
Средство защиты, практически идентичное Kaspersky Endpoint Security 10 для Windows: те же настройки и компоненты, кроме шифрования. Отличается тем, что все файлы пересылает на проверку Серверу защиты, а с Сервера защиты, кроме вердиктов, получает лицензию и обновления.

Агент администрирования Kaspersky Security Center

Обычный агент, такой же, как и для управления Kaspersky Endpoint Security:
— Получает настройки
— Пересылает события



Устройство Легкого агента

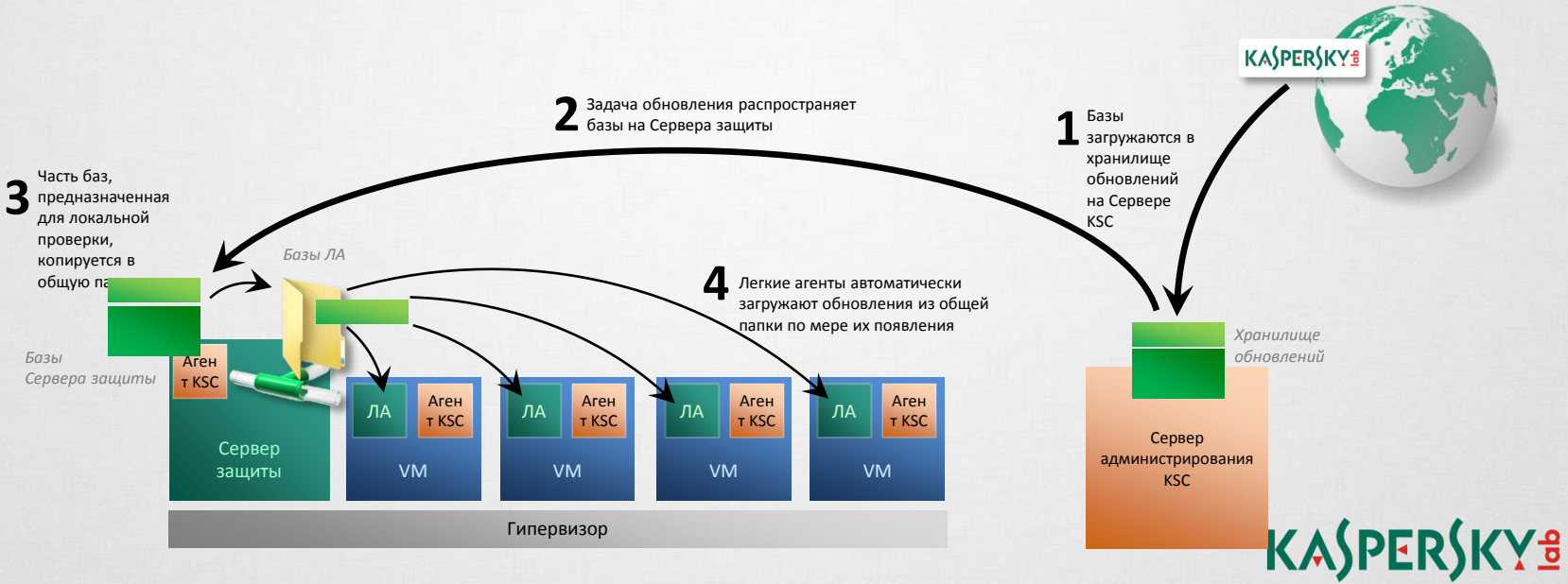


Как проверяются файлы

За счет общего кэша и единой очереди проверки не будет «штормов» при одновременном старте поиска вирусов или при одновременном запуске виртуальных машин в сценарии VDI

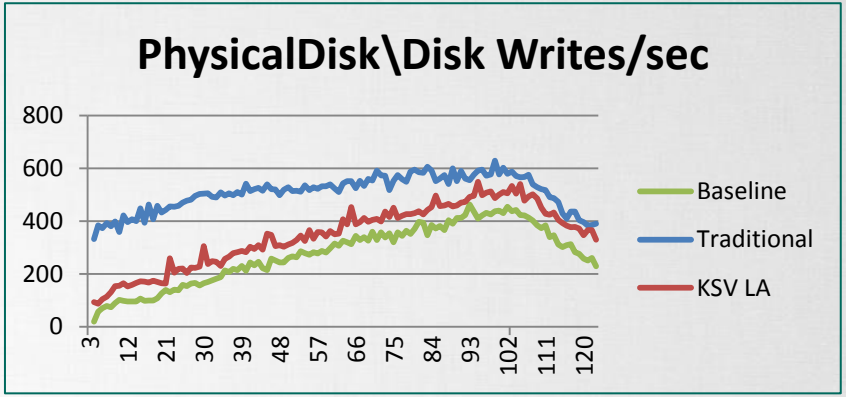
Как распространяются обновления

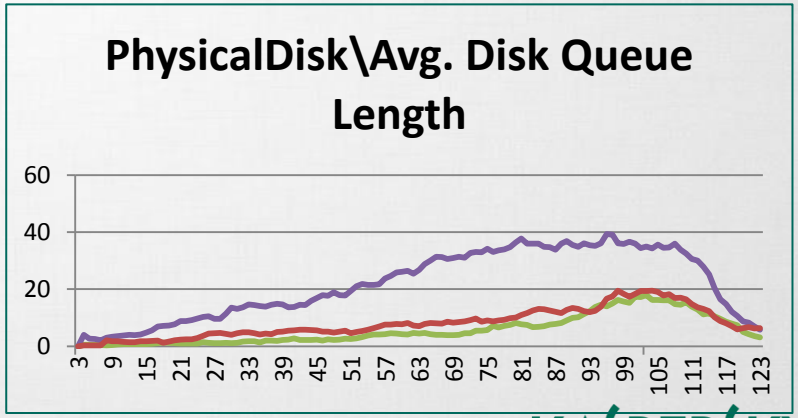
За счет малого объема баз, распространяемых на защищаемые виртуальные машины, **не возникает «штормов»** при одновременном обновлении Легких агентов в сценарии VDI



KSV | Легкий Агент
Реальная Проверка Производительности

- Сымитирован «офисный» уровень нагрузки
- Достигнут уровень консолидации: **100+** машин под защитой на одном хосте (около 15 VM на ядро)
- Дисковые операции:
  - Выигрыш от **20%** до **50%** по сравнению с традиционным решением
  - Сокращение дисковой очереди: в разы

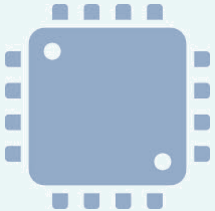




KASPERSKY lab

KSV
ГИБКОЕ ЛИЦЕНЗИРОВАНИЕ

- ЕДИНАЯ ЛИЦЕНЗИЯ ДЛЯ БЕЗАГЕНТСКОГО РЕШЕНИЯ И ЛЕГКОГО АГЕНТА



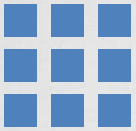
ПО РЕСУРСАМ (ЯДРО)

ПО ВИРТУАЛЬНЫМ МАШИНАМ

- По серверам
- По рабочим станциям

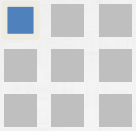
KASPERSKY lab

Сравнение методов защиты ИТ инфраструктуры



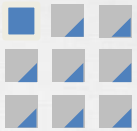
Традиционный
Agent-Based

- Любой гипервизор
- Плотность VM малая
- Windows, Linux или Mac гостевые ОС



Без Агентский
Agentless

- VMware только
- Высока плотность VM
- Windows гостевая ОС
- Минимум IT ресурсов



Легкий Агент
Light Agent

- VMware, Citrix или Hyper-V
- Высока плотность VM
- Windows гостевая ОС
- Расширенный функционал:
  - IM, Web, Mail AV
  - Automatic Exploit Prevention
  - Application, Web and Device controls

KASPERSKY lab

Готов ответить на ваши вопросы :)

KASPERSKY lab