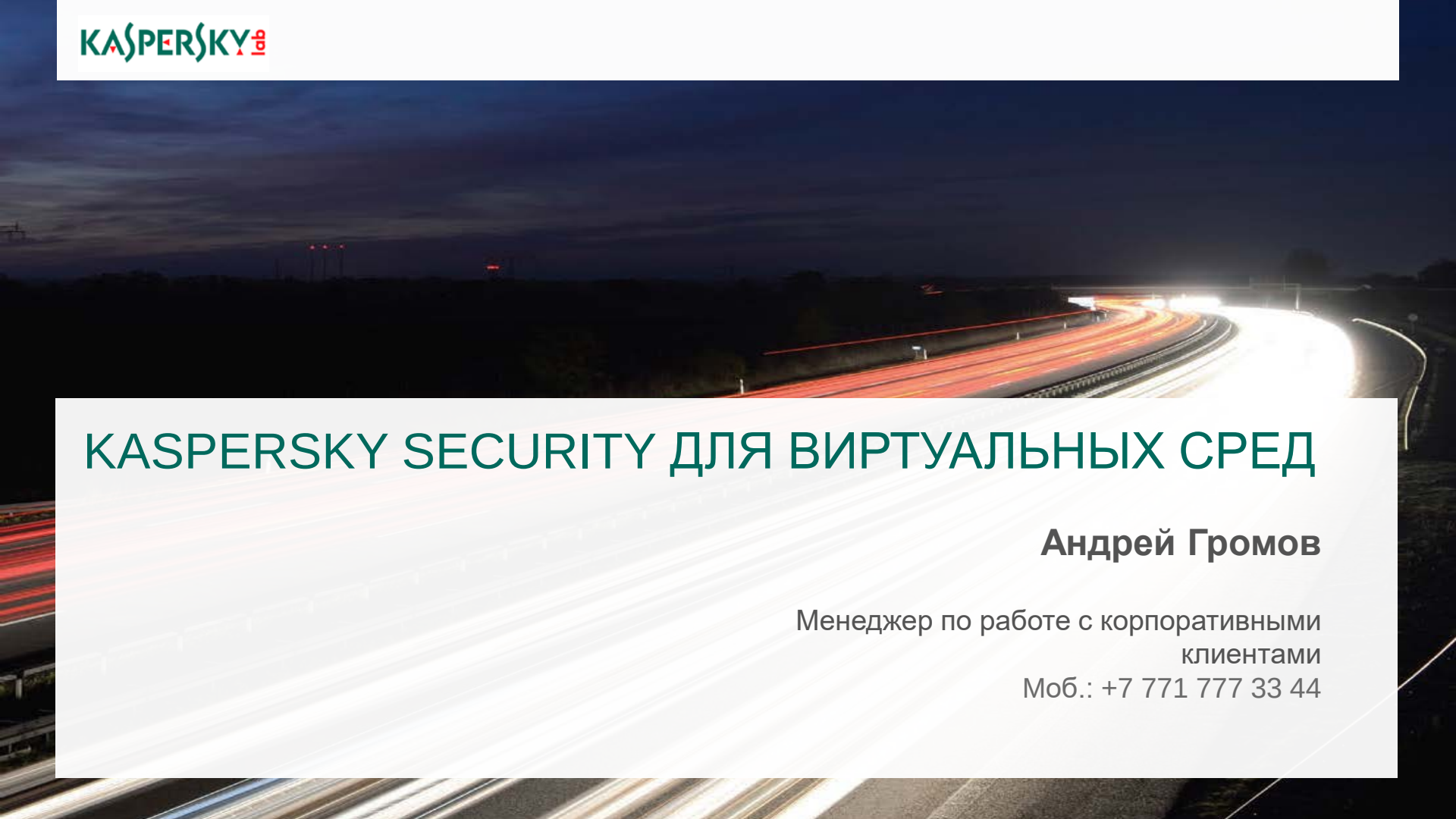


KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Андрей Громов

Менеджер по работе с корпоративными клиентами
Моб.: +7 771 777 33 44

ВИРТУАЛИЗАЦИЯ:
ЧТО ОНА ДАЕТ И НУЖНО ЛИ ЕЁ ЗАЩИЩАТЬ?

KASPERSKY lab

ПРЕИМУЩЕСТВА ВИРТУАЛИЗАЦИИ

СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ

Прославившиеся на весь мир атаки, вирусы и трояны

Каждый день появляется еще более 350 000 новых угроз и вредоноса.

Многие из них используют до этого неизвестные способы атак или заражений («угрозы нулевого дня») и могут оставаться неопознанными системами безопасности значительное время.

НУЖНА ЛИ ОСОБАЯ ЗАЩИТА ДЛЯ ВИРТУАЛИЗАЦИИ ?

ДА БЫВАЮТ ЛИ ВИРУСЫ В ВИРТУАЛЬНЫХ СРЕДАХ?

- УЯЗВИМЫ ГОСТЕВЫЕ ОС, БОЛЬШИНСТВО ТРАДИЦИОННЫХ ВИРУСОВ НЕЗАВИСИМЫ ОТ СРЕДЫ ВИРТУАЛИЗАЦИИ

ДА ИСПОЛЬЮТ ЛИ СПЕЦИФИКУ ВИРТУАЛЬНЫХ СРЕД?

- ПЕРВЫЙ ТРОЯН, ЗАРАЖАЮЩИЙ ШАБЛОНЫ ВИРТУАЛЬНЫХ МАШИН VMWARE БЫЛ НАЙДЕН В 2012 (**MORCUT** a.k.a. **CRISIS**)

ДА МОГУТ ЛИ ВЫЖИВАТЬ В ВИРТУАЛЬНОЙ СРЕДЕ?

- ТРОЯН МОЖЕТ КОПИРОВАТЬ СЕБЯ С ОДНОЙ ВМ НА ДРУГУЮ ИЛИ ВЫЙТИ ЗА ПРЕДЕЛЫ ВМ И ВЫПОЛНИТЬ ЗЛОВРЕДНЫЙ КОД НА ХОСТЕ ИЛИ ЛЮБОЙ ДРУГОЙ ВМ (**KIDO**, **VENOM**)

ПОДХОДЫ В ЗАЩИТЕ ВИРТУАЛЬНЫХ СРЕД

Без Защиты

Традиционная защита

Безагентская защита

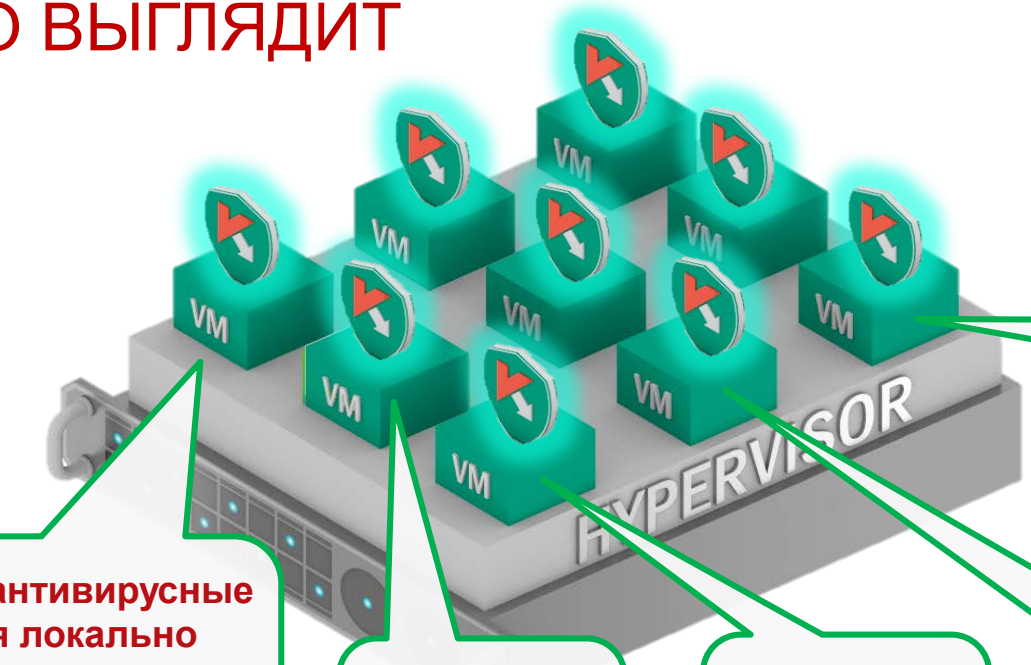
Легкий Агент

KASPERSKY lab

ТРАДИЦИОННАЯ АНТИВИРУСНАЯ ЗАЩИТА: ИСПОЛЬЗОВАНИЕ ПОЛНОЦЕННОГО АГЕНТА

KASPERSKY lab

ТРАДИЦИОННАЯ АНТИВИРУСНАЯ ЗАЩИТА
КАК ЭТО ВЫГЛЯДИТ



Я храню ВСЕ антивирусные базы у себя локально

Я сам обновляю ВСЕ базы

Я сам делаю ВСЕ проверки

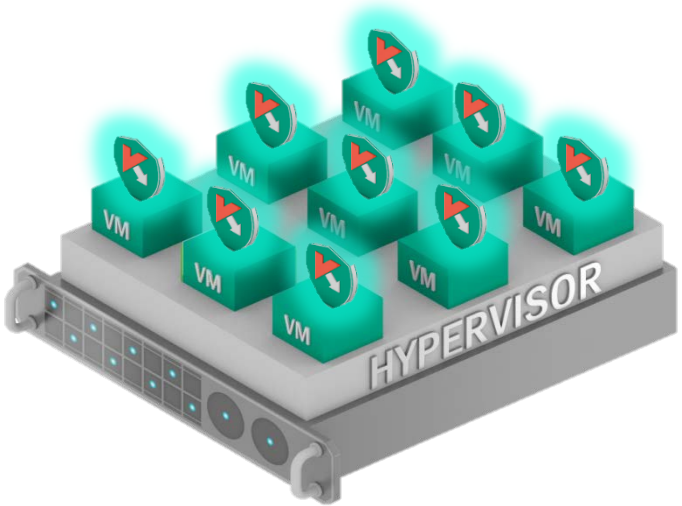
И я делаю ВСЕ то же самое

И я делаю ВСЕ то же самое

И я делаю ВСЕ то же самое

И я делаю ВСЕ то же самое

ТРАДИЦИОННАЯ ЗАЩИТА
ПЛЮСЫ И МИНУСЫ



Плюсы:

1. Надежная «тяжелая» защита
2. Не привязано к гипервизору

Минусы:

1. «Штормы обновлений»
2. «Окно уязвимости»
3. Высокая ресурсоемкость
4. Снижение плотности ВМ
5. Сложности с управлением

Увеличение нагрузки на среду виртуализации
Снижение ROI самого проекта

ЕСТЬ БОЛЕЕ ЭФФЕКТИВНЫЕ СПОСОБЫ…

Используя возможности сред виртуализации можно значительно повысить эффективность обеспечения антивирусной защиты всей виртуальной инфраструктуры:

1. Использовать функционал платформы (например, vShield Endpoint)
2. Проверку вынести на «Виртуальный Сервер Защиты»
3. Использовать легкого агента для передачи файлов на проверку
4. Организовать «Централизованный Кэш Вердиктов» для всех ВМ
5. Реализовать дополнительную защиту виртуального сетевого трафика

KASPERSKY SECURITY FOR VIRTUALIZATION

СПЕЦИАЛИЗИРОВАННОЕ РЕШЕНИЕ:
KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД (KSV)

KASPERSKY lab

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Безагентская Защита

- Защита файлов: on-access, on-demand
- Web-защита *
  (Блокирование посещения вредоносных сайтов)
- Централизованный кэш вердиктов
- Защита от сетевых атак *
  (Port Scan, RDP brute force и т.д.)

** При наличии установленной лицензии VMware vCloud Networking and Security*

Легкий Агент

- Защита файлов: on-access, on-demand
- Полный сетевой антивирус
  (Web, IM, AV, антифишинг и т.д.)
- Централизованный кэш вердиктов
- Защита от сетевых атак
  (Port Scan, RDP brute force и т.д.)

+

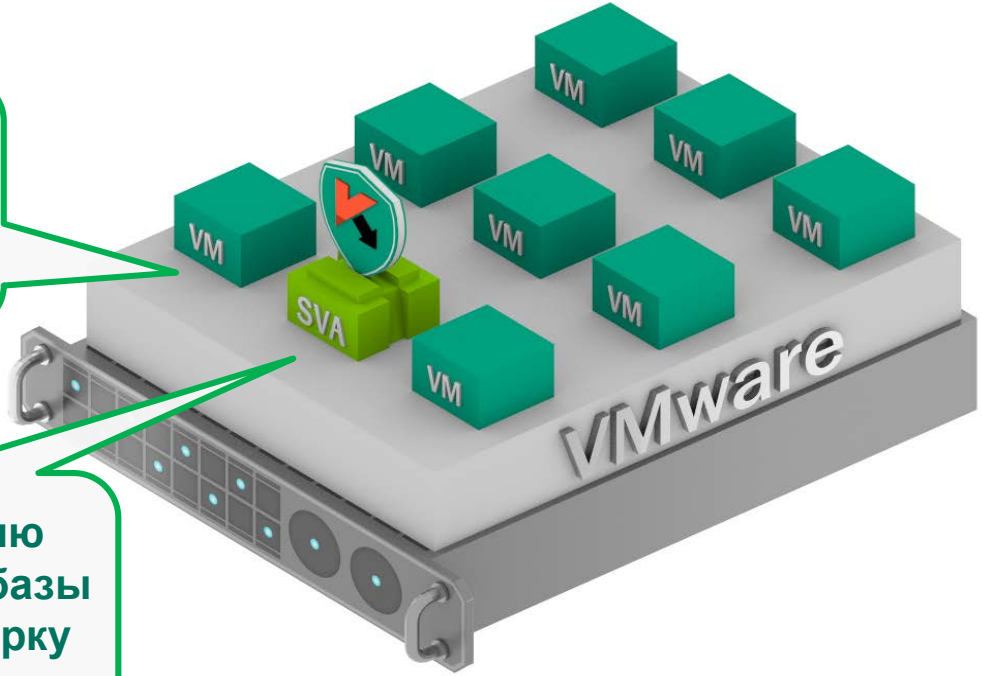
- **Защита процессов, анализ приложений**
- **Защита от удаления/отключения**
- **Контроль web/приложений/устройств**
- **Функционал поиска уязвимостей, HIPS**

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД (KSV):
БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)

KASPERSKY lab

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
КАК ЭТО ВЫГЛЯДИТ

Во мне содержатся только нагрузки от бизнес-приложения



Только я храню антивирусные базы и делаю проверку файлов

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
ВЫДЕЛЕННЫЙ СЕРВЕР ЗАЩИТЫ (SVA)

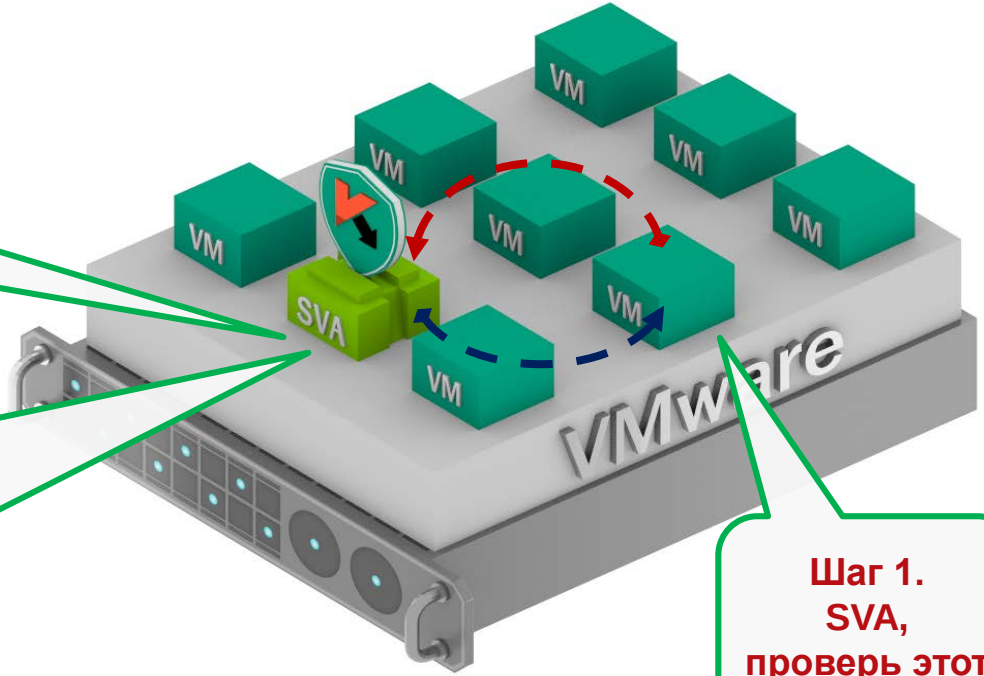
- Идеально спроектирован для работы с гипервизором
- Гибко настраивается и глубоко интегрируется со средой виртуализации
- Держит самую актуальную антивирусную базу
- Получает файлы на проверку от ВМ (сами ВМ ничего не проверяют)
- Выполняет антивирусную проверку файлов защищаемых ВМ
- Распределяет лицензии на работающие ВМ
- Работа в режиме 24x7 и отказоустойчивость заложены на уровне кода

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
КАК ПРОВЕРЯЮТСЯ ФАЙЛЫ

Шаг 3.
Вот вердикт по этому файлу.

Шаг 2.
Проверяется Централизованный кэш вердиктов:

File A – чисто
File B – чисто
…
File N - вирус
…



Шаг 1.
SVA, проверь этот файл!

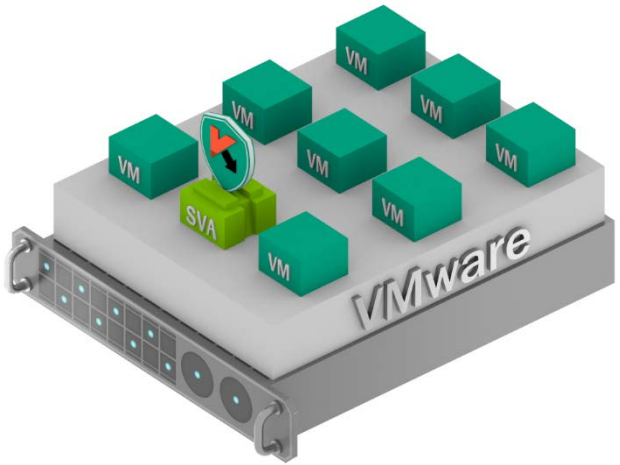
KASPERSKY lab

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
КАК РАСПРОСТРАНЯЮТСЯ ОБНОВЛЕНИЯ

Только **Выделенный сервер защиты (SVA)** хранит на себе антивирусную базу, обновляет ее и только он занимается антивирусной проверкой всех ВМ.

Нет необходимости распространять обновления антивирусных баз на ВМ.

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
ПЛЮСЫ И МИНУСЫ



Плюсы:

1. Нет «штормов» и «окон уязвимости»
2. «Родное» для гипервизора
3. Постоянная защита всех ВМ
4. Минимум нагрузки на ресурсы
5. Сохраняется высокая плотность ВМ
6. Легко развернуть и просто управлять

Минусы:

1. Только для VMware vSphere
2. Ограниченная защита ВМ

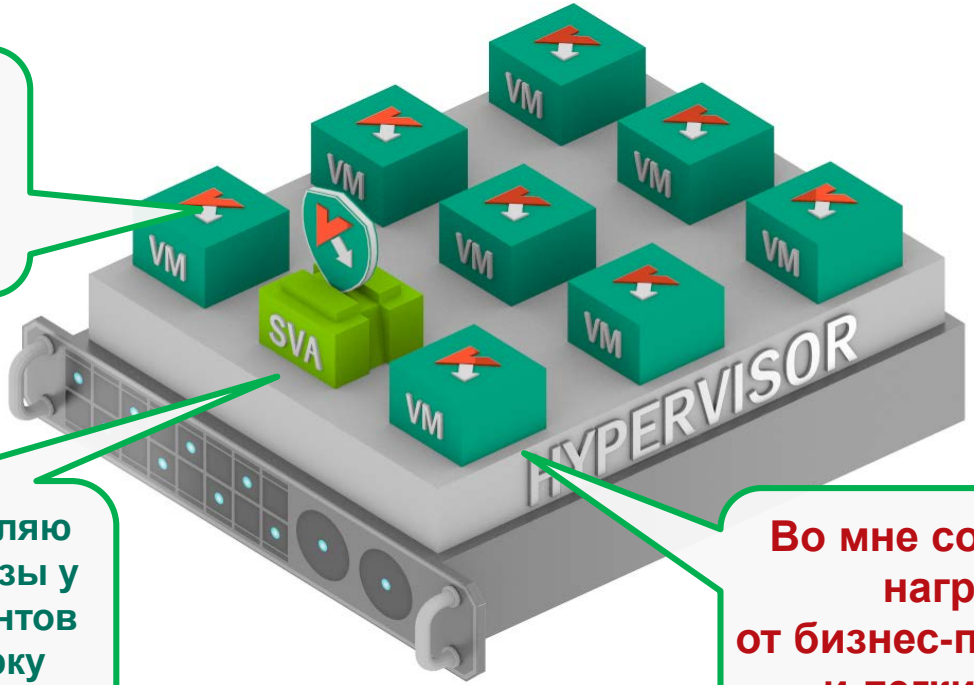
Эффективная защита всей виртуальной среды

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД (KSV):
ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)

KASPERSKY lab

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
КАК ЭТО ВЫГЛЯДИТ

Я нахожусь внутри каждой ВМ и слежу за ее полной защитой от угроз



Я храню и обновляю антивирусные базы у себя и легких агентов и делаю проверку ВСЕХ файлов

Во мне содержатся нагрузки от бизнес-приложения и легкий агент

KASPERSKY

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT) КАК ЭТО РАБОТАЕТ

- На хосте виртуализации разворачивается «Выделенный сервер защиты» (SVA).
- SVA хранит на себе единую антивирусную базу обновлений. Передает «оптимизированные» обновления на Легких Агентов.
- На ВМ устанавливается **ЛЕГКИЙ АГЕНТ**, основанный на антивирусном движке традиционного антивируса, но оптимизирован для работы в среде виртуализации.
- С использованием легкого агента теперь можно проверять не только файлы ВМ, но также проверять ее память, процессы, приложения, почтовый и веб файлы, и в целом выполнять более глубокую защиту всей ВМ.
- На основании проверки на ВМ теперь формируется еще и Локальный Кэш Вердиктов, а на SVA все так же формируется Централизованный Кэш Вердиктов (CVC).
- На самих ВМ работают только легкие агенты и агенты администрирования.

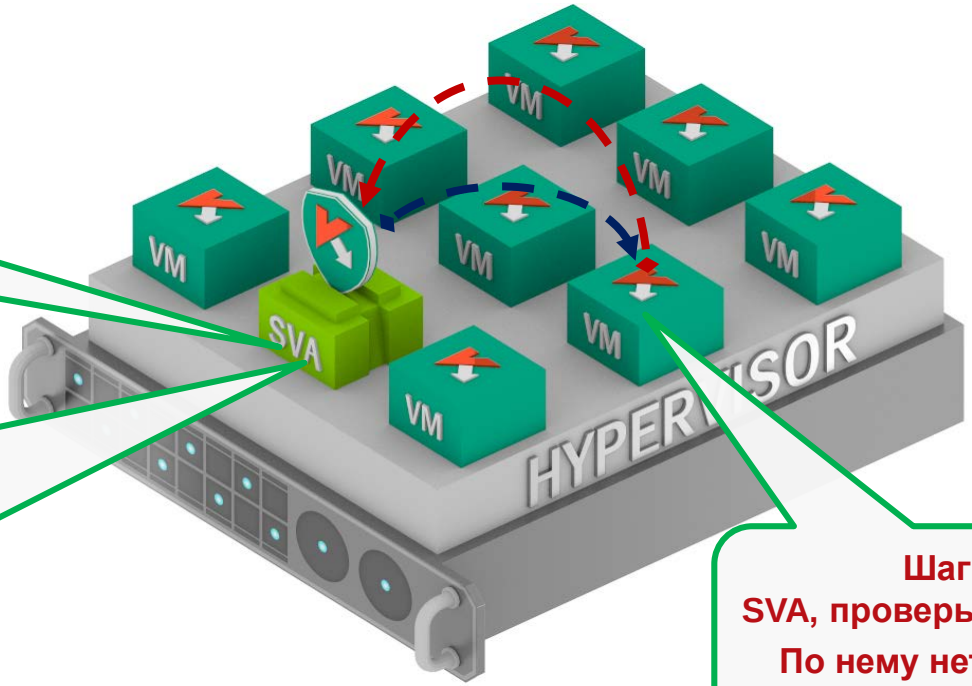
Пройти обучение на русском: http://support.kaspersky.ru/learning/courses/kl_131.30

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
КАК ПРОВЕРЯЮТСЯ ФАЙЛЫ

Шаг 3.
Вот вердикт по этому файлу.

Шаг 2.
Проверяется Централизованный кэш вердиктов:

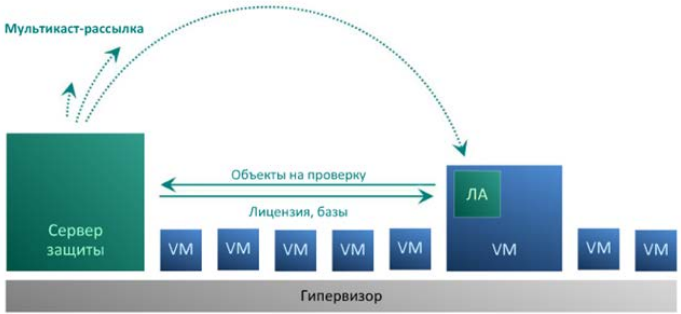
File A – чисто
File B – чисто
…
File N - вирус
…



Шаг 1.
SVA, проверь этот файл!
По нему нет никакой информации в моем LVC!

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
КАК АГЕНТЫ ПОДКЛЮЧАЮТСЯ К SVA

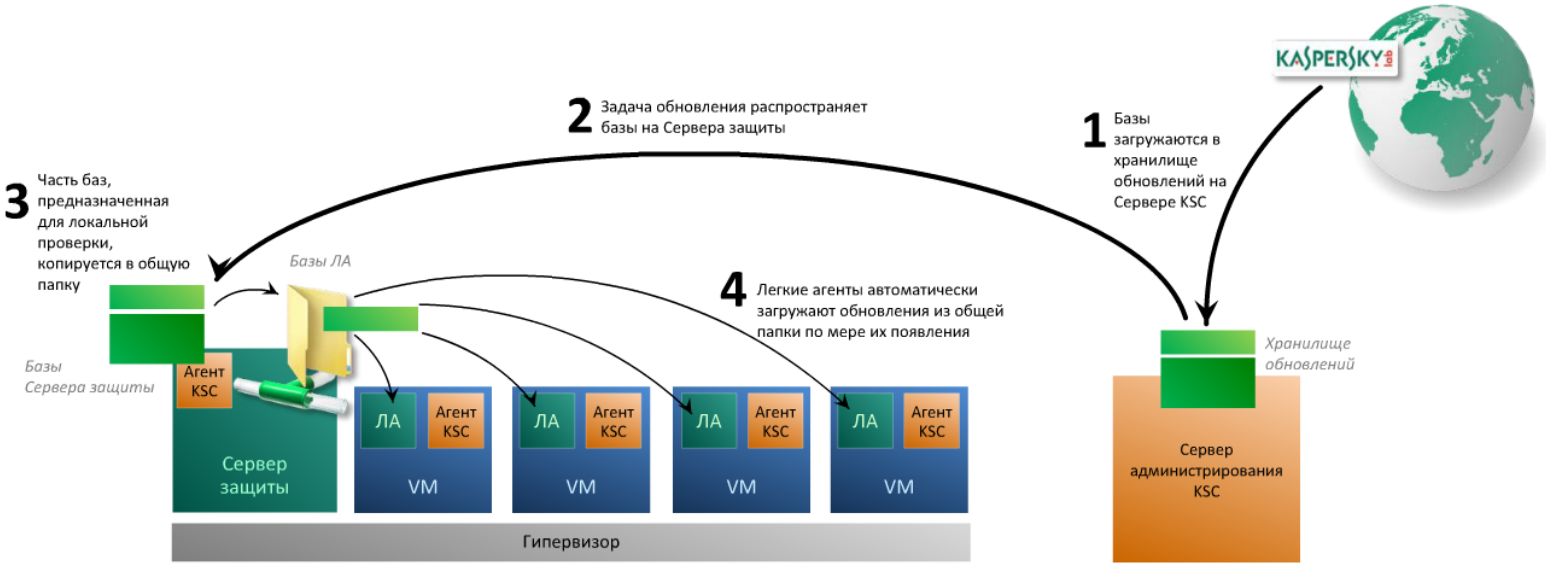
- Легкий Агент отправляет multicast-запрос
- SVA отвечает и сообщает свои данные
- Легкий агент выбирает себе SVA:
  - на том же самом гипервизоре
  - наименее загруженный



- Легкий Агент устанавливает соединение с SVA
- Оптимизированное хранилище антивирусных баз

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
КАК РАСПРОСТРАНЯЮТСЯ ОБНОВЛЕНИЯ

- Централизованное и эффективное обновление баз
- Оптимизация файловых операций на ВМ и в рамках всего хоста.



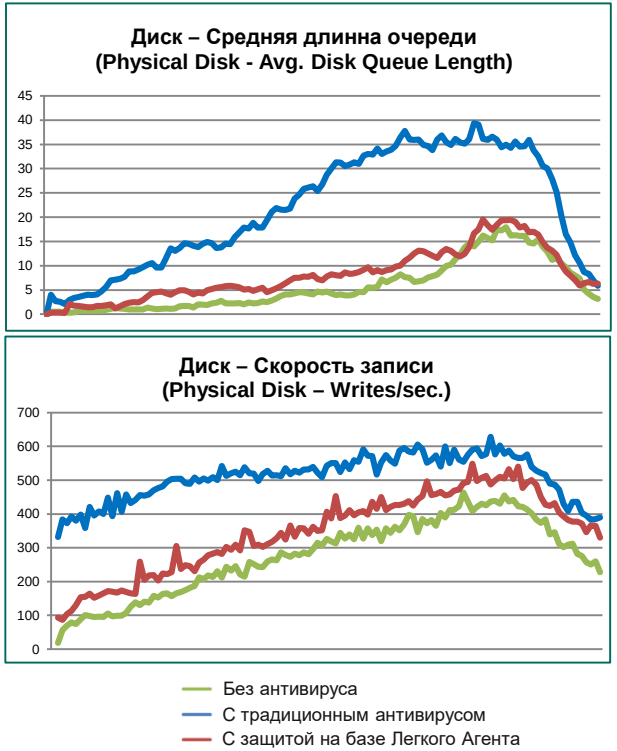
KASPERSKY

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT) ЭФФЕКТИВНЕЕ ТРАДИЦИОННОГО АГЕНТА

- Специально разработан для виртуальных сред
- Оптимизированное хранилище антивирусных баз
- Локальный Кэш Вердиктов (LVC)
  - Не нужно перепроверять файлы и приложения внутри ВМ
- Централизованный Кэш Вердиктов (CVC)
  - Не нужно проверять одинаковые файлы на разных ВМ
  - Существенно увеличивается производительность в VDI
- Централизованное обновление антивирусных баз
- Оптимизация файловых операций как на каждой ВМ, так и в рамках всего хоста виртуализации

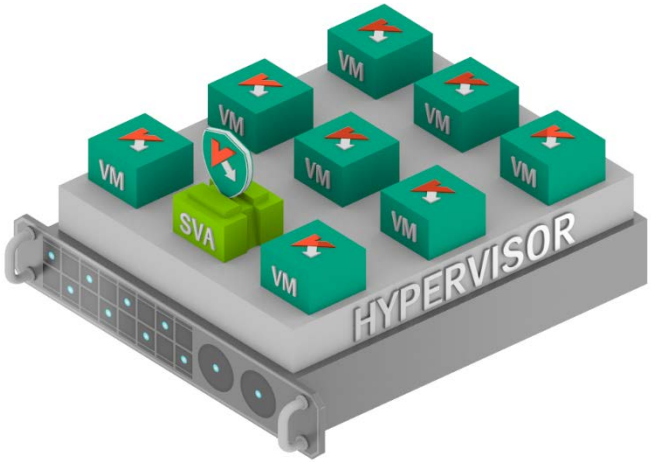
ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
БЫСТРЕЕ ТРАДИЦИОННОГО АНТИВИРУСА *

Сравниваемый параметр производительности	Традиционный антивирус	Защита на базе Легкого Агента
Доп.нагрузка на CPU	10-15%	1-5%
Доп.нагрузка на RAM	15-25%	5-10%
Увеличение длины очереди диска	в 7 раз	в 3 раза
Увеличение количества файловых операций с данными	в 8 раз	в 1,5 раза
Увеличение длина очереди CPU	150%	20%
Добавленная нагрузка на гипервизор	25%	5%



* По результатам внутреннего тестирования Лаборатории Касперского

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
ПЛЮСЫ И МИНУСЫ



Плюсы:

1. Работает на любом гипервизоре
2. Не зависит от гипервизора
3. Полноценная защита всех ВМ
4. Минимум нагрузки на ресурсы
5. Сохраняется высокая плотность ВМ
6. Легко развернуть и просто управлять
7. Большой набор технологий защиты

Минусы:

1. Нельзя скачать бесплатно

Эффективная и полноценная защита для ЛЮБОЙ виртуальной среды

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
КОМПЛЕКТ ПОСТАВКИ ПРОДУКТА

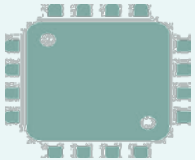
Решение состоит из следующих приложений:

- **KSV Agentless** – безагентская защита ВМ
- **KSV Light Agent** – защита ВМ на базе Легкого Агента
- **Kaspersky Security Center** – сервер управления

ДЛЯ УСТАНОВКИ ВСЕХ КОМПОНЕНТОВ ПРОДУКТА
ИСПОЛЬЗУЕТСЯ ЕДИНЫЙ ЛИЦЕНЗИОННЫЙ КЛЮЧ

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
ЛИЦЕНЗИРОВАНИЕ ПРОДУКТА

- ЕДИНАЯ ЛИЦЕНЗИЯ ДЛЯ УСТАНОВКИ НА ЛЮБОЙ ГИПЕРВИЗОР
- ЕДИНАЯ ЛИЦЕНЗИЯ ДЛЯ БЕЗАГЕНТСКОЙ ЗАЩИТЫ И ЛЕГКОГО АГЕНТА



ПО ЯДРАМ (Cores)

- Высокая плотность ВМ
- Количество ВМ часто меняется
- Фиксированная аппаратная часть
- Удобно для Дата Центров и провайдеров облачных услуг

ПО ОБЪЕКТАМ ЗАЩИТЫ (Server / Desktop)

- Низкая плотность ВМ
- Фиксированное количество ВМ
- Рост числа ВМ прогнозируем
- Удобно для виртуальных сред низкой степени вариативности

СПАСИБО ЗА ВНИМАНИЕ!

Андрей Громов

Менеджер по работе с корпоративными клиентами
Моб.: +7 771 777 33 44

Лаборатория Касперского
www.kaspersky.ru

KASPERSKY lab