KASPERSKY lab

УГРОЗЫ ДЛЯ БИЗНЕСА

МАСШТАБ УГРОЗЫ

1994

1

НОВЫЙ ВИРУС КАЖДЫЙ ЧАС

2006

1

НОВЫЙ ВИРУС КАЖДУЮ МИНУТУ

2011

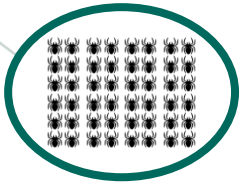
1

НОВЫЙ ВИРУС КАЖДУЮ СЕКУНДУ

2014

325 000

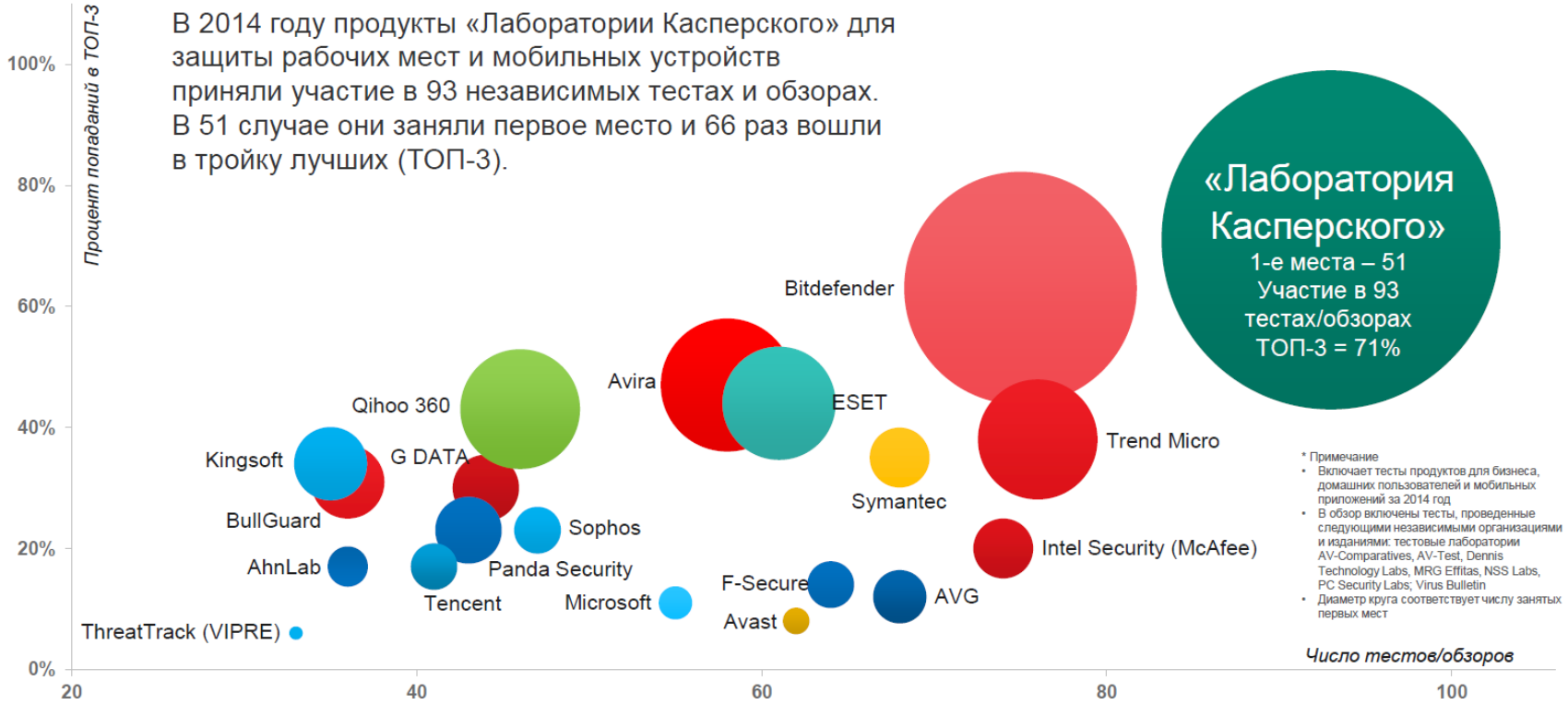
НОВЫХ ВРЕДОНОСНЫХ ОБРАЗЦОВ В ДЕНЬ



KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

«ЛАБОРАТОРИЯ КАСПЕРСКОГО» ОБЕСПЕЧИВАЕТ ЛУЧШУЮ ЗАЩИТУ*

В 2014 году продукты «Лаборатории Касперского» для защиты рабочих мест и мобильных устройств приняли участие в 93 независимых тестах и обзорах. В 51 случае они заняли первое место и 66 раз вошли в тройку лучших (ТОП-3).



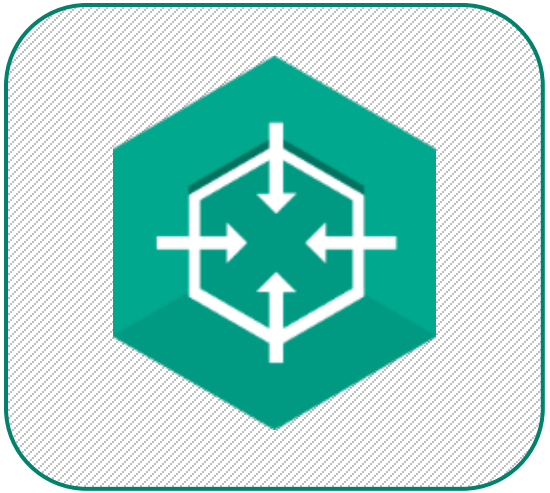
KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА

- Технологии защиты включают в себя:

- Все управляется с помощью единой консоли управления: программы Kaspersky Security Center

ГЛОБАЛЬНЫЙ МОНИТОРИНГ УГРОЗ (KSN)

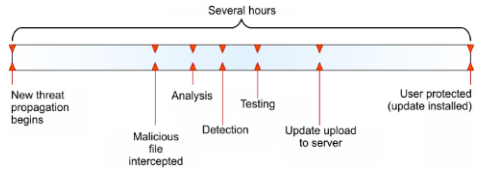
- репутационные сервисы:
  - файловая репутация
  - URL-репутация
  - шаблоны поведения ПО
  - индикаторы компрометации
- осведомленность в режиме реального времени
- глобальная статистика



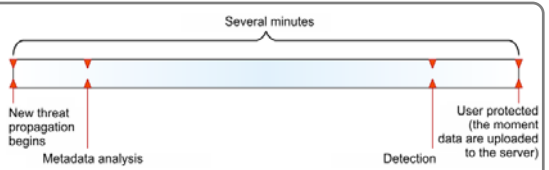
KASPERSKY lab

ОПЕРАТИВНОЕ ПОЛУЧЕНИЕ ИНФОРМАЦИИ

Стандартный процесс выпуска сигнатур при плановых обновлениях вирусных баз требует нескольких часов



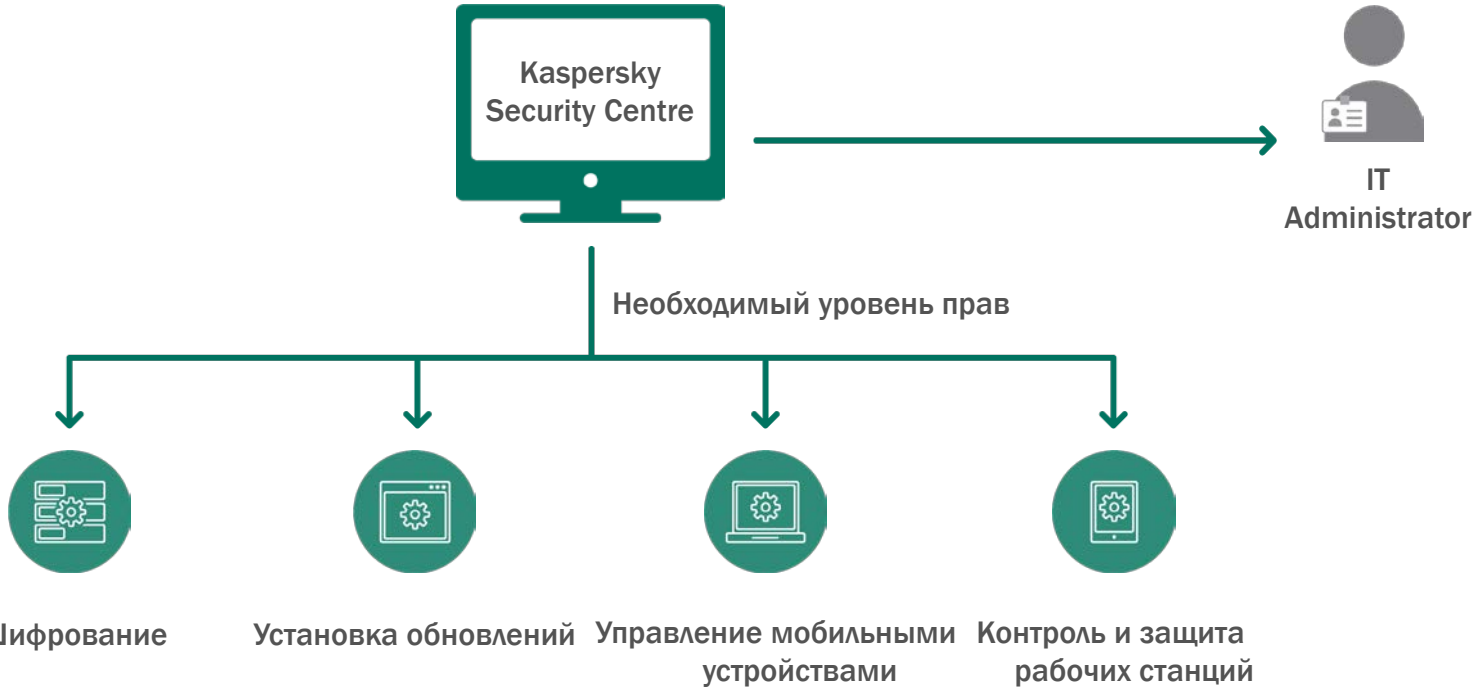
KSN распространяет информацию о конкретной новой угрозе, опасном сайте, вредоносной ссылке или новом шаблоне поведения подозрительного ПО за секунды



Для критичных видов угроз промедление в несколько часов может привести к серьезным негативным последствиям и требует незамедлительного реагирования

KASPERSKY SECURITY CENTER

- Ролевая модель доступа (RBAC) для крупных IT-департаментов с возможностью разграничения прав доступа сотрудников.



В ДЕТАЛЯХ


ТОТАЛ
Сервера совместной работы
Почта
Интернет-шлюзы
РАСШИРЕННЫЙ
Закрытие уязвимостей & Установка обновлений
Инвентаризация & Контроль лицензий
Установка приложений
Развертывание ОС
Интеграция с SIEM
Шифрование
СТАНДАРТНЫЙ
Защита мобильных устройств
Mobile Device Management
Управление установкой приложений на мобильных устройствах
Защита файловых серверов
Контроль приложений
Контроль устройств
Веб-контроль
СТАРТОВЫЙ
Защита от вредоносного ПО + Сетевой экран
Kaspersky Security Center
Интеграция с облачной сетью Kaspersky Security Network (KSN)
Endpoint
Управление
Инфраструктура

KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА - СТАНДАРТНЫЙ

Также включает:

- Контроль приложений, устройств и веб-контроль
- Kaspersky security для мобильных устройств

KASPERSKY lab

КОНТРОЛЬ РАБОЧИХ МЕСТ

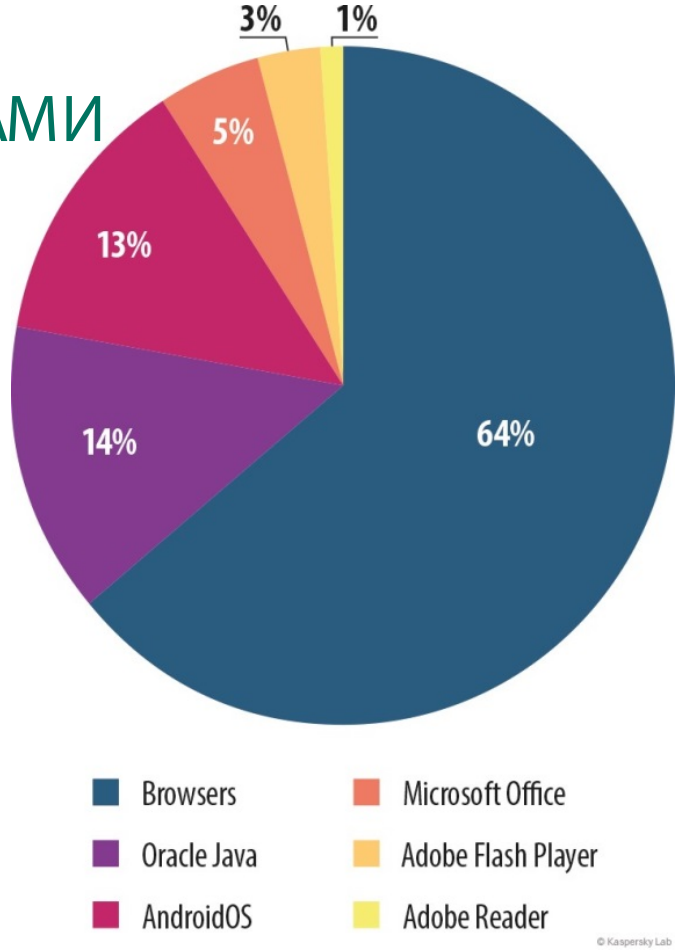
КОНТРОЛЬ УСТРОЙСТВ

ВЕБ-КОНТРОЛЬ

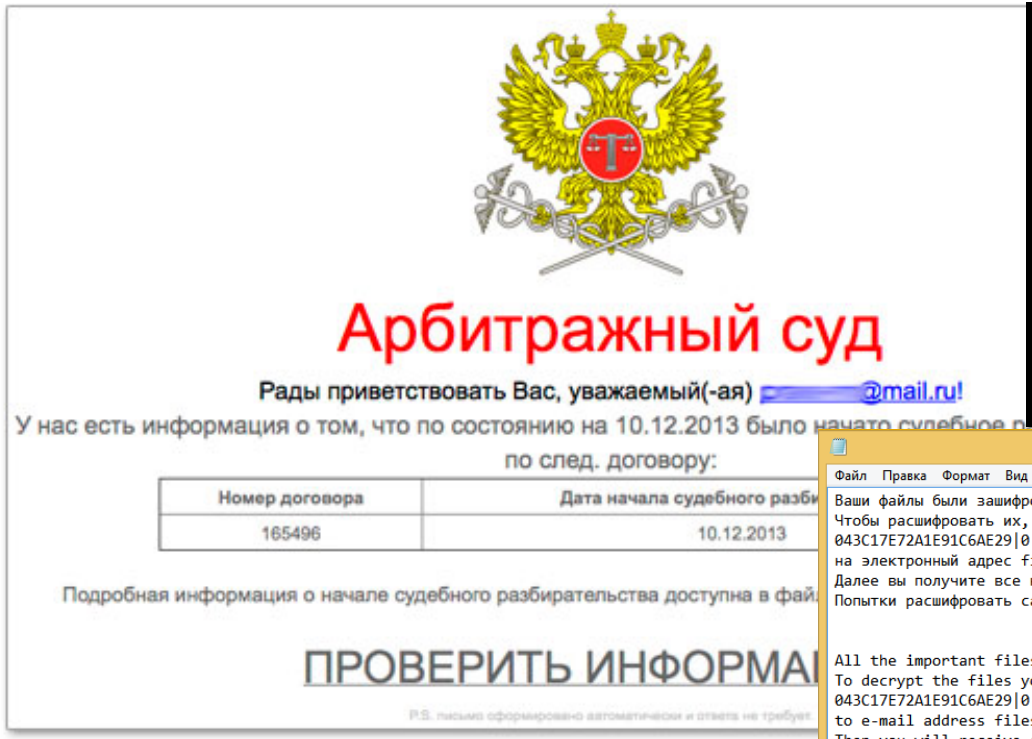
КОНТРОЛЬ ПРИЛОЖЕНИЙ С
ДИНАМИЧЕСКИМИ БЕЛЫМИ СПИСКАМИ

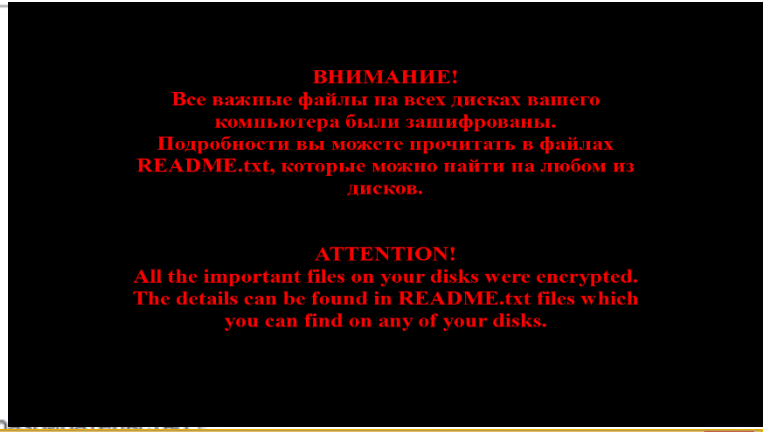
УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

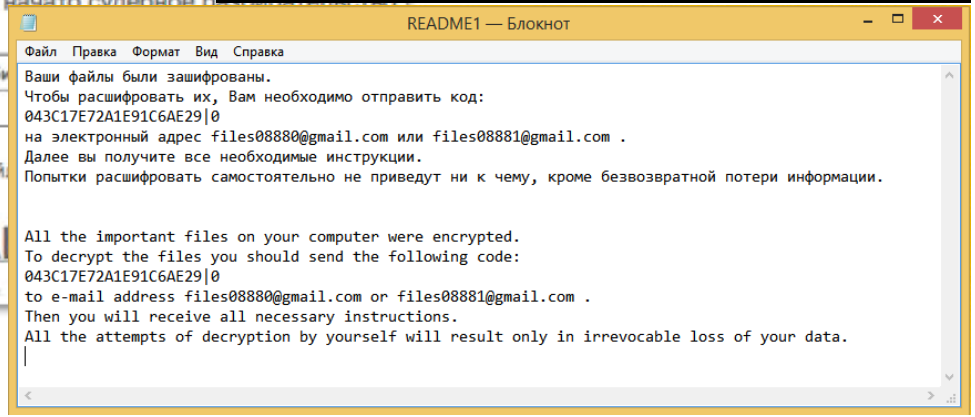
- 64% всех зарегистрированных попыток использования уязвимостей были нацелены на категорию «Браузеры», которая включает эксплойты для Internet Explorer.
- 14% Java
- Необходимо отметить, что в первом квартале 2015 года выросло число эксплойтов для Microsoft Office (на 2% по сравнению с четвёртым кварталом 2014 г.) и Adobe Flash Player (на 1%).



ШИФРОВАЛИЩИК ПО ПОЧТЕ







KASPERSKY lab

KASPERSKY SECURITY ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ

Проактивная защита, управление и контроль мобильных устройств

Защита мобильных устройств

- Веб-защита
- Выявление попыток перепрошивки

Mobile Device Management

- Exchange ActiveSync
- iOS MDM
- Samsung KNOX

Управление приложениями

- Удаление приложений
- Контроль приложений
- Выборочное удаление

Анти-Вор

- Блокировка/Удаление данных
- Определение местонахождения /Оповещение

NEW!

Портал самообслуживания

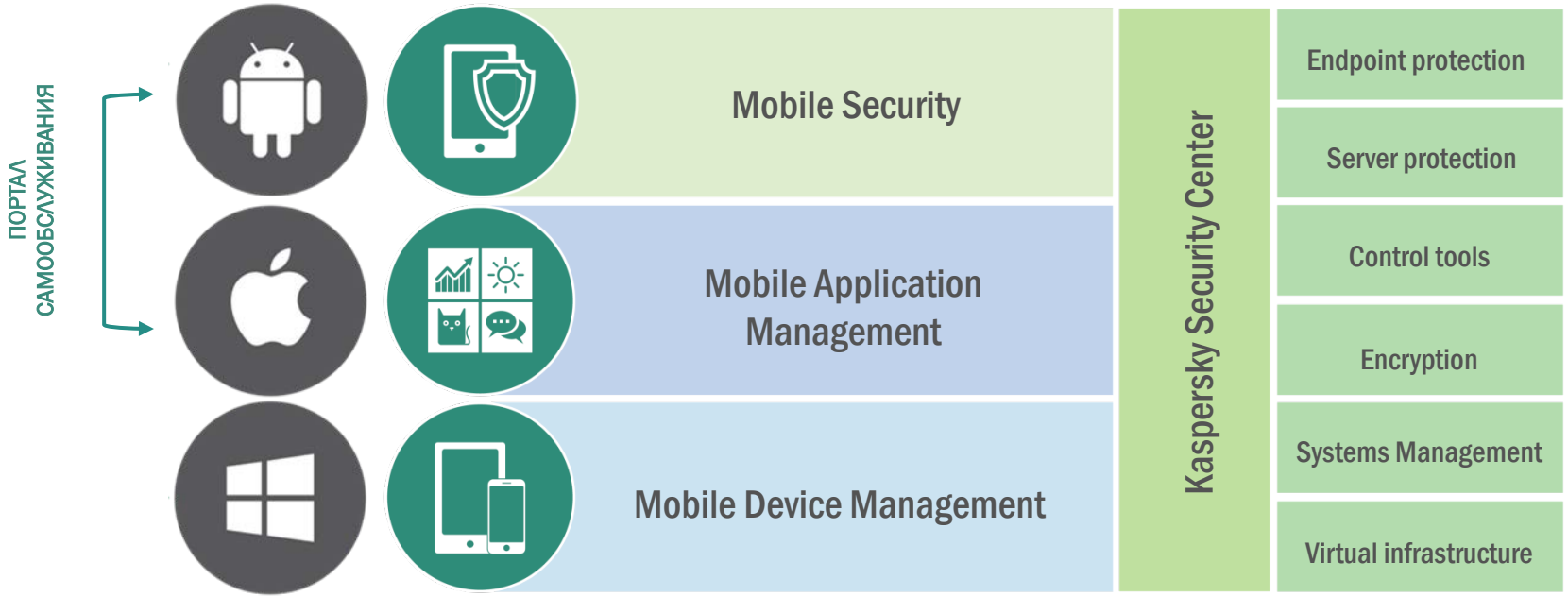
- Подключение BYOD-устройств
- Установка сертификатов
- Анти-Вор

Централизованное управление

- Поддержка основных мобильных платформ

ПОЛНОСТЬЮ ИНТЕГРИРОВАННОЕ МОБИЛЬНОЕ РЕШЕНИЕ

- Защита мобильных устройств, рабочих станций, серверов и виртуальных машин из единой консоли управления



KASPERSKY ENDPOINT SECURITY ДЛЯ БИЗНЕСА - РАСШИРЕННЫЙ

Включает также:

- Шифрование
- Kaspersky systems management

KASPERSKY lab

ШИФРОВАНИЕ ДАННЫХ

- Простое в администрировании решение

МОЩНОЕ ШИФРОВАНИЕ ДАННЫХ

- Файлы/Папки (FLE)
- Диски (FDE)

ИНТЕГРАЦИЯ С КОМПОНЕНТАМИ КОНТРОЛЯ

- Контроль приложений
- Контроль устройств

ОПТИМИЗИРОВАНО ДЛЯ МИНИМАЛЬНОГО ВЛИЯНИЯ НА ПОЛЬЗОВАТЕЛЕЙ

- Прозрачно/single sign-on
- Минимум шагов для интеграции

NEW! ГИБКАЯ АУТЕНТИФИКАЦИЯ

- Pre-boot аутентификация
- Поддержка многих языков
- Двухфакторная аутентификация с токеном или смарт-картой

УПРОЩЕННОЕ АДМИНИСТРИРОВАНИЕ

- Простое восстановление пароля
- Удаленное управление

KASPERSKY SYSTEMS MANAGEMENT

Повышение безопасности

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ И УСТАНОВКА ОБНОВЛЕНИЙ

- Поиск уязвимостей & приоретизация
- Установка патчей & обновлений
- NEW! Отчеты о установленных патчах

ИНВЕНТАРИЗАЦИЯ КОНТРОЛЬ ЛИЦЕНЗИЙ

- Инвентаризация программного и аппаратного обеспечения
- Контроль использования лицензий
- Политики гостевого доступа

УСТАНОВКА ПРИЛОЖЕНИЙ

- Поддержка мультикаста
- Политики для автоматической установки
- Установка по расписанию

РАЗВЕРТЫВАНИЕ ОС

- Простое создание и развертывание образов
- Поддержка Wake-on-LAN
- Возможность внесения изменений в образ

NEW! ИНТЕГРАЦИЯ С SIEM

- HP ArcSight & IBM QRadar
- Улучшенная IT-безопасность

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

- Удаленное решение «проблем»
- NEW! Role-Based Access Control
- Контроль подключения устройств к корпоративной сети

KASPERSKY TOTAL SECURITY ДЛЯ БИЗНЕСА

Включает также:

- Защиту для почтовых серверов
- Защита для интернет-шлюзов
- Защита серверов совместной работы

KASPERSKY lab

KASPERSKY TOTAL SECURITY ДЛЯ БИЗНЕСА

Комплексная защита инфраструктуры

Защита почтовых серверов

- Kaspersky Security for Linux Mail Server
- Kaspersky Security for Microsoft Exchange Servers
- Kaspersky Anti-Virus for Lotus Notes/Domino

Защита для интернет-шлюзов

- Kaspersky Anti-Virus for Proxy Server
- Kaspersky Anti-Virus for Microsoft ISA Server and Forefront TMG

Защита серверов совместной работы

- Kaspersky Security for Microsoft SharePoint Server

NEW

KASPERSKY SECURE MAIL GATEWAY

KASPERSKY lab

KASPERSKY SECURE MAIL GATEWAY IN A NUTSHELL

POWERFUL AND INTUITIVE MANAGEMENT

ADVANCED ANTI-PHISHING AND CONTENT FILTERING

EASY DEPLOYMENT < TCO

TOP-RATED ANTI-MALWARE*

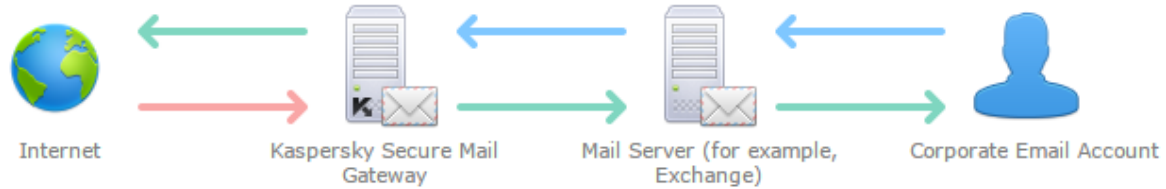
FLEXIBLE AND FAULT-TOLERANT SOLUTION

AWARD-WINNING ANTI-SPAM

*2014 TOP3 METRIC

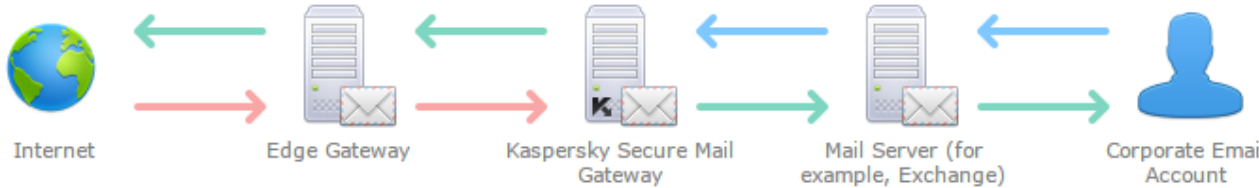
ACTS AS STANDALONE MAIL GATEWAY OR RELAY

Integrate directly



Kaspersky Secure Mail Gateway will accept email messages directly from the Internet and redirect them to your internal mail servers. It also will accept messages from your internal mail servers and redirect them to the Internet.

Integrate through Edge Gateway



Kaspersky Secure Mail Gateway will accept email messages from the Edge Gateway and redirect them to your internal mail servers. It also will accept messages from your internal mail servers and redirect them to the Edge Gateway.

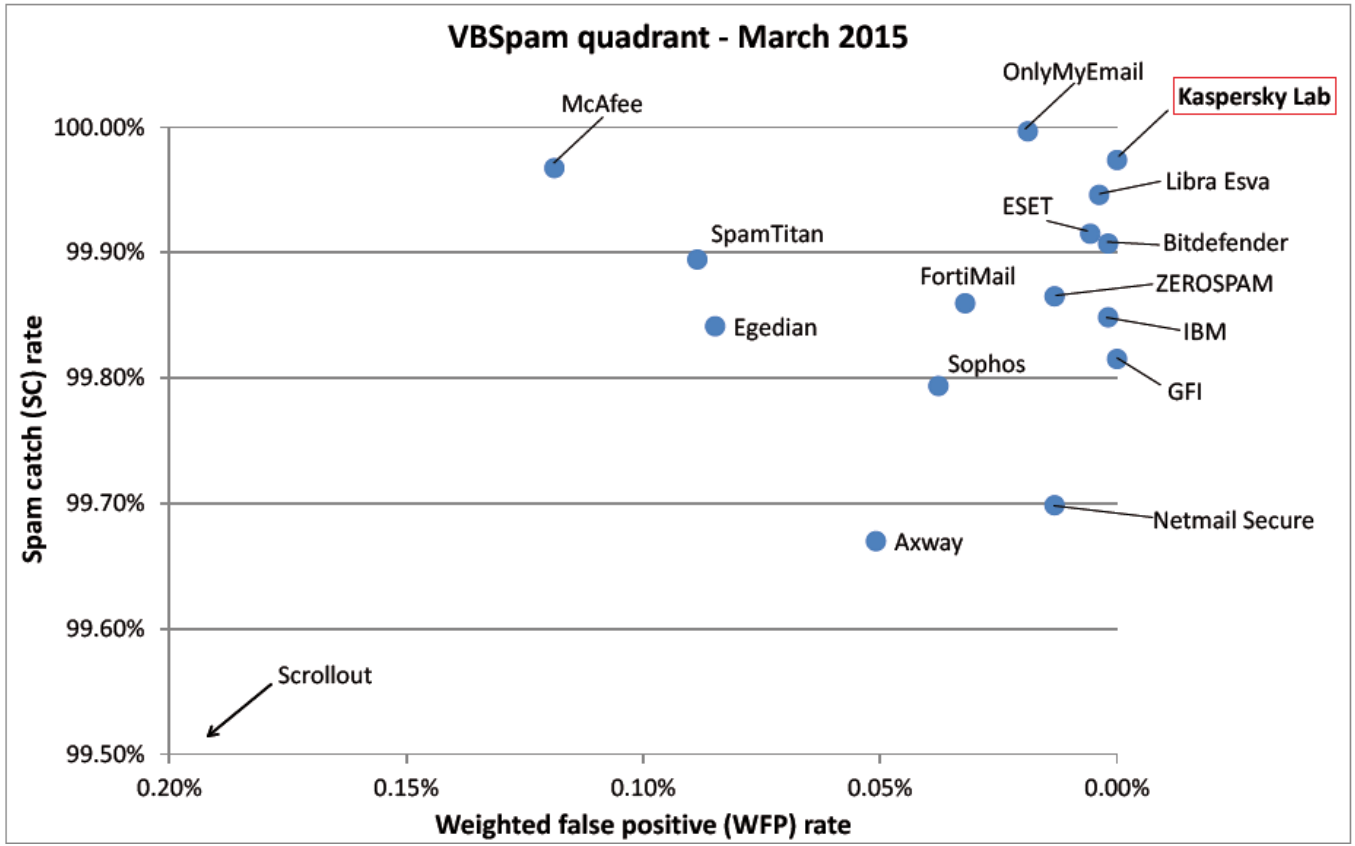
PROTECTION: ANTI-MALWARE AND MORE

- TOP-rated* and KSN-assisted anti-malware technologies: Real-time scan (incl. archived files) of in- and-outbound SMTP mail traffic
- Malicious URL filter blocks mails containing links to malicious sites
- Zero-day exploit and targeted attack prevention through dedicated advanced protection module.

- KSN-assisted anti-phishing blocks mails containing links to phishing web sites
- Attachment filtering based on file name, type, message size and individual processing rules.

*2014 TOP3 METRIC

VBSPAM QUADRANT: KL VS COMPETITION



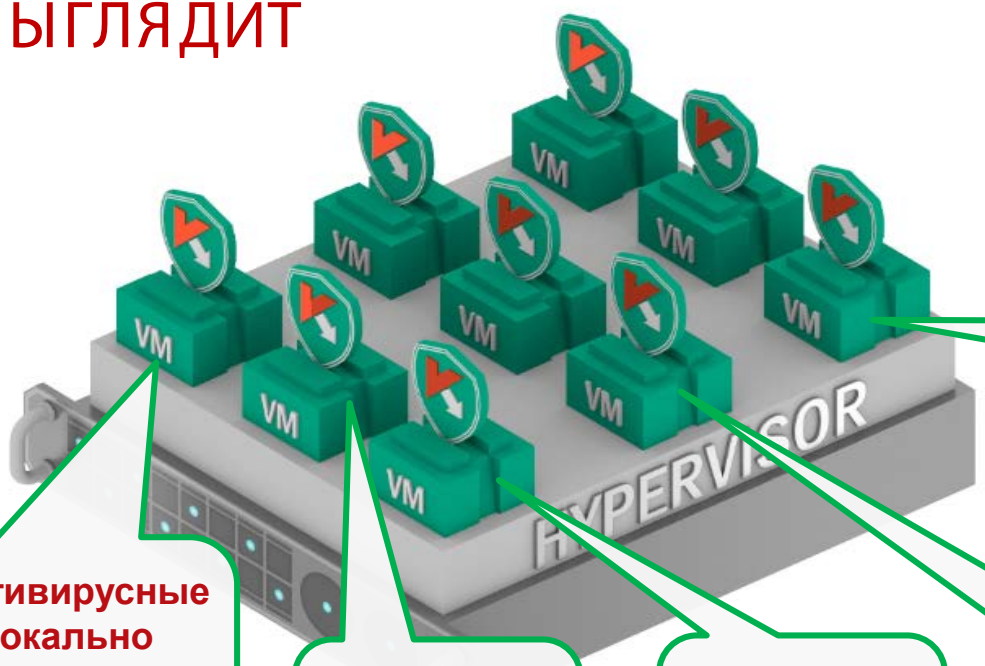
[Spam Catch] rate: 99.97%

[False Positive] rate: 0.00%

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

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

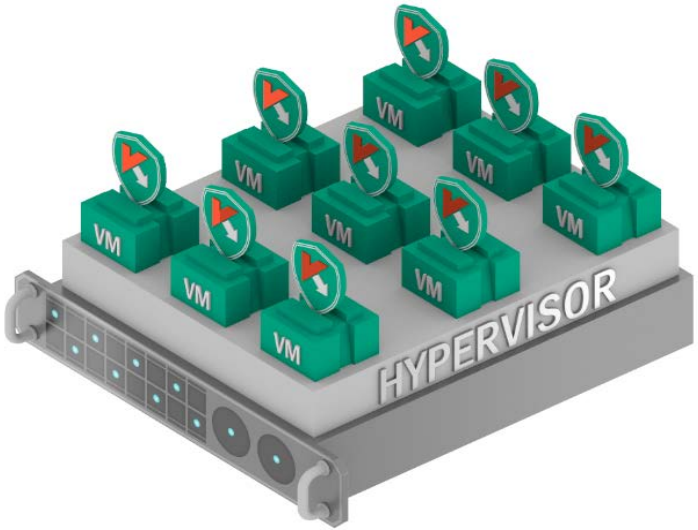
И я делаю ВСЕ то же самое

И я делаю ВСЕ то же самое

И я делаю ВСЕ то же самое

KASPERSKY lab

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

KASPERSKY lab

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

Безагентская Защита

- Защита файлов: on-access, on-demand
- Web-защита *
  (Блокирование посещения вредоносных сайтов)
- Технология «Shared Cache»
- Защита от сетевых атак *
  (Port Scan, RDP brute force и т.д.)

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

Легкий Агент

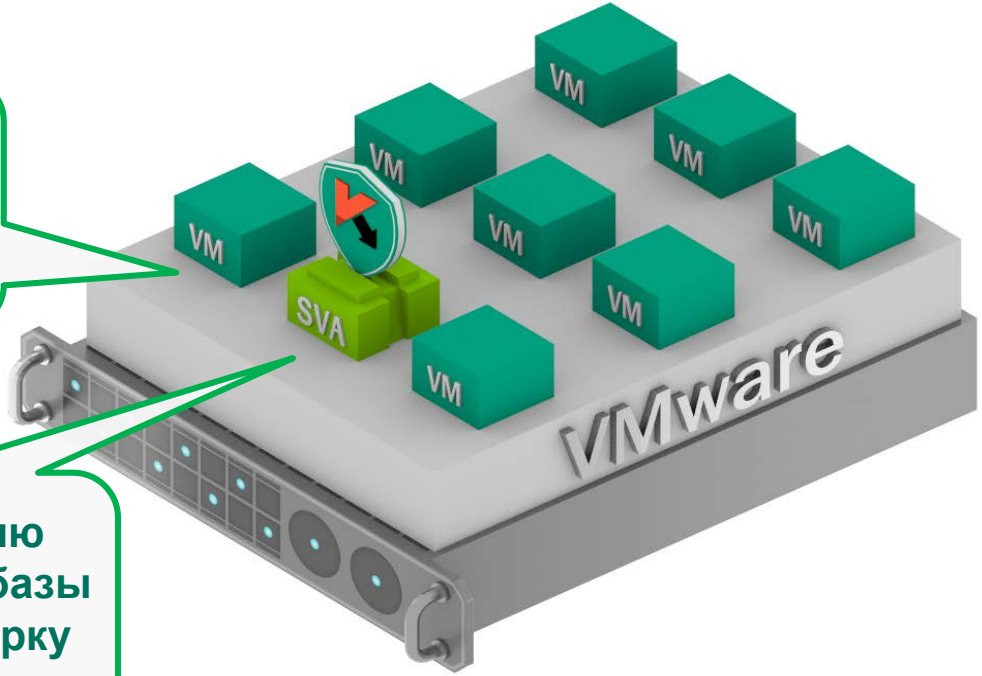
- Защита файлов: on-access, on-demand
- Полный сетевой антивирус
  (Web, IM, AV, антифишинг и т.д.)
- Технология « Shared Cache»
- Защита от сетевых атак
  (Port Scan, RDP brute force и т.д.)

+

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

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
КАК ЭТО ВЫГЛЯДИТ

Во мне содержатся только нагрузки от бизнес-приложения



Только я храню антивирусные базы и делаю проверку файлов

KASPERSKY lab

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
КАК ПРОВЕРЯЮТСЯ ФАЙЛЫ

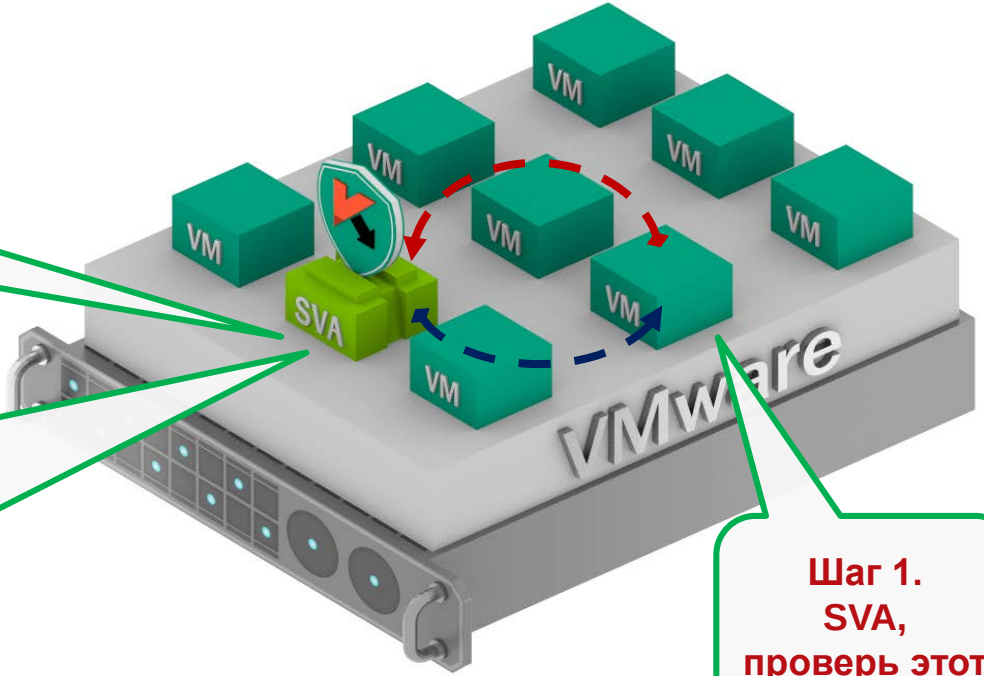
Шаг 3.

Вот вердикт по этому файлу.

Шаг 2.

Проверяется Shared Cache:

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



Шаг 1.
SVA, проверь этот файл!

БЕЗАГЕНТСКАЯ ЗАЩИТА (AGENTLESS)
ПОДДЕРЖИВАЕМЫЕ ГИПЕРВИЗОРЫ И ОС

Гипервизоры:

vmware®

- ESXi 5.1
- ESXi 5.5
- ESXi 6.0

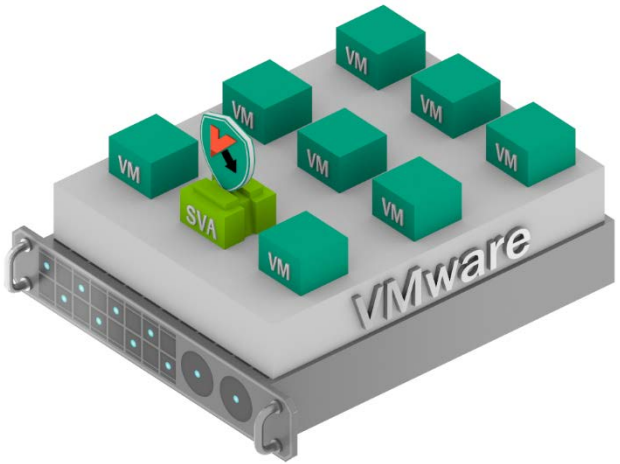
Серверные ОС:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32/64 bit)
- Windows Server 2003 R2 (32/64 bit)
- Windows Server 2003 (32/64 bit)

Гостевые ОС:

- Windows 8.1 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows 7 (32/64 bit)
- Windows XP (32 bit)
- Windows 10 – soon

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:

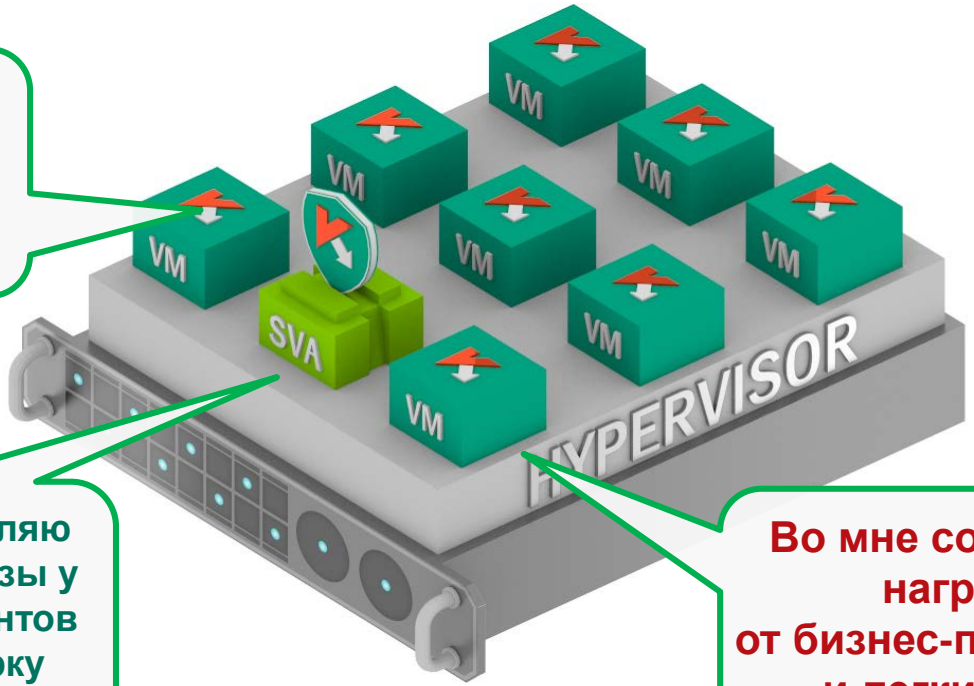
1. Только для VMware vSphere
2. Ограниченная защита ВМ

Эффективная защита всей виртуальной среды
Сохранение ROI проекта виртуализации

KASPERSKY

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

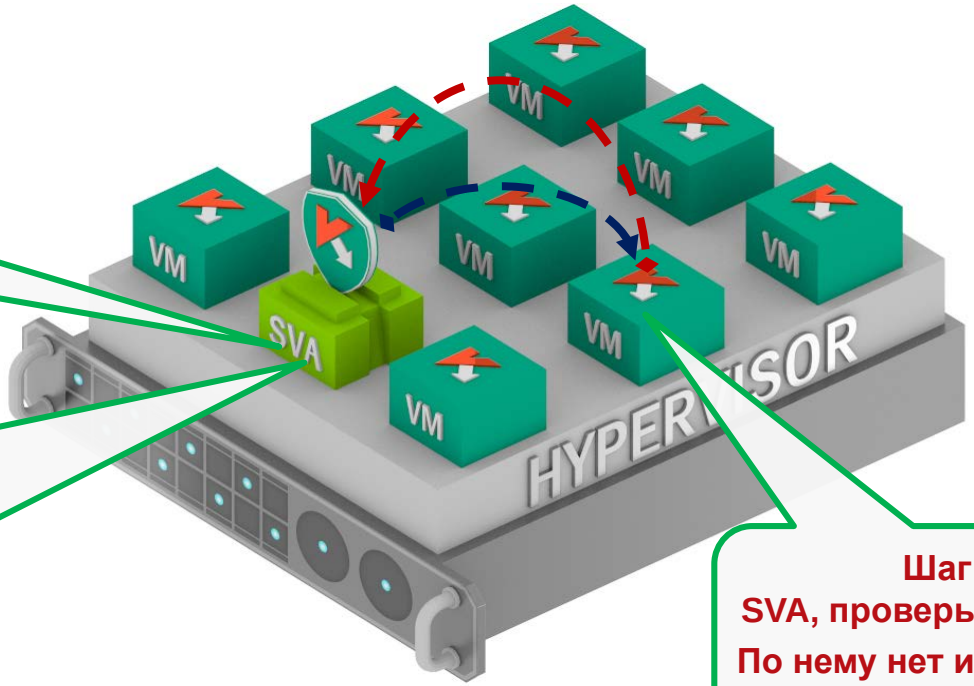
Во мне содержатся нагрузки от бизнес-приложения и легкий агент

KASPERSKY lab

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
КАК ПРОВЕРЯЮТСЯ ФАЙЛЫ

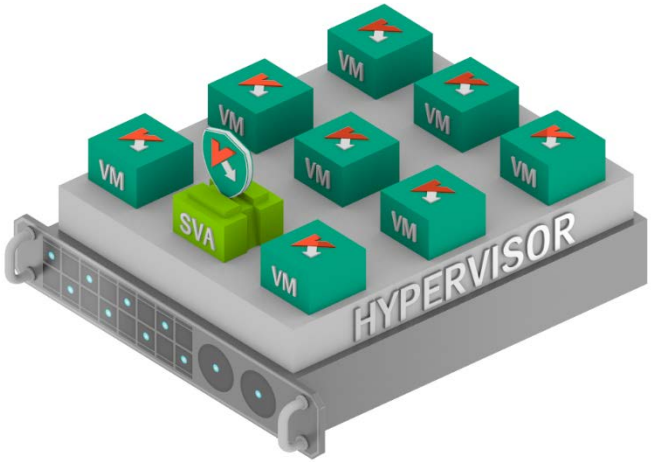
Шаг 3.
Вот вердикт по этому файлу.

Шаг 2.
Проверяется Shared Cache:
File A – чисто
File B – чисто
…
File N - вирус
…



Шаг 1.
SVA, проверь этот файл!
По нему нет информации в моем Local Cache!

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
ПЛЮСЫ И МИНУСЫ



Плюсы:

1. Работает на любом гипервизоре
2. Не зависит от сетевой среды
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. Требуется учитывать инфраструктуру

Эффективная и полноценная защита для ЛЮБОЙ виртуальной среды

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Kaspersky Security Center

Позволяет осуществлять управление защитой физических, мобильных и виртуальных устройств из единой консоли

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД

ИНТЕГРАЦИЯ С KASPERSKY SECURITY NETWORK

САМАЯ СОВРЕМЕННАЯ ГЛОБАЛЬНАЯ ОБЛАЧНАЯ СЕТЬ БЕЗОПАСНОСТИ

ДИНАМИЧЕСКАЯ РЕПУТАЦИЯ И КАТЕГОРИЗАЦИЯ

ЗАЩИТА ОТ САМЫХ НОВЫХ УГРОЗ в т.ч. УГРОЗ НУЛЕВОГО ДНЯ

ПОЛНАЯ ИНТЕГРАЦИЯ С МОДУЛЯМИ ЗАЩИТЫ ПРОДУКТА

KASPERSKY SECURITY ДЛЯ ВИРТУАЛЬНЫХ СРЕД
КОМПЛЕКТ ПОСТАВКИ ПРОДУКТА

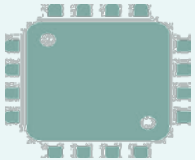
Решение состоит из следующих приложений:

- **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)

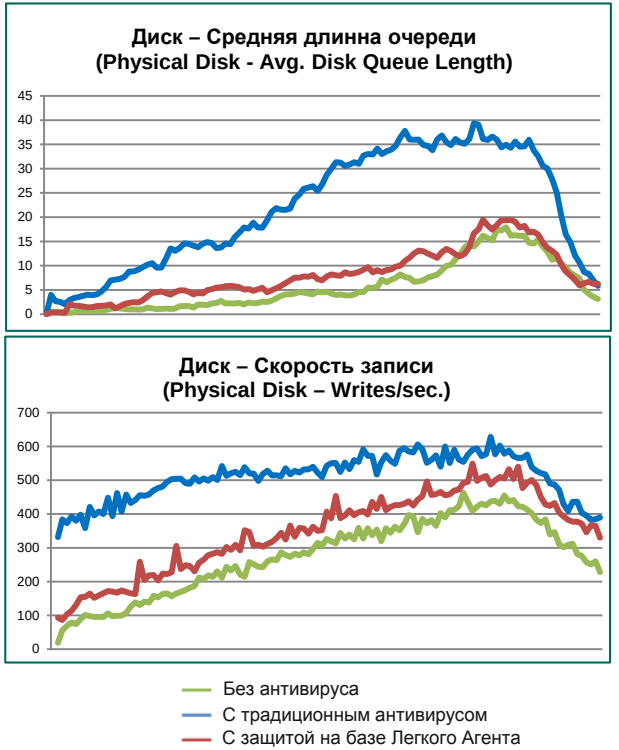
- Высокая плотность ВМ
- Количество ВМ часто меняется
- Фиксированная аппаратная часть
- Удобно для Дата Центров и провайдеров облачных услуг

ПО ОБЪЕКТАМ ЗАЩИТЫ (Server / Desktop)

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

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

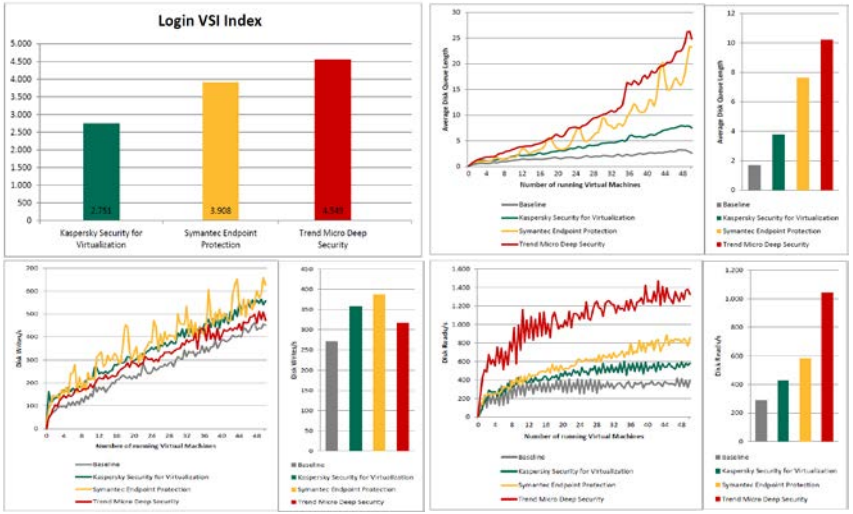
Сравниваемый параметр производительности	Традиционный антивирус	Защита на базе Легкого Агента
Доп.нагрузка на CPU	10-15%	1-5%
Доп.нагрузка на RAM	15-25%	5-10%
Увеличение длины очереди диска	в 7 раз	в 3 раза
Увеличение количества файловых операций	в 8 раз	в 1,5 раза
Увеличение длина очереди CPU	150%	20%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



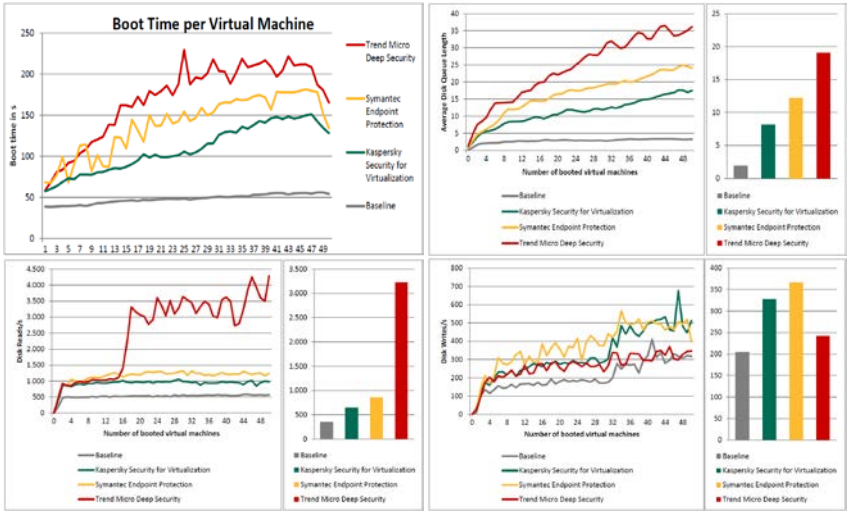
* По результатам внутреннего тестирования Лаборатории Касперского

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT) БЫСТРЕЕ КОНКУРЕНТОВ *

Login VSI Test



Boot Storm Test



* По результатам тестирования AV-Test GmbH, проведенного в 2014 году

ЗАЩИТА С ЛЕГКИМ АГЕНТОМ (LIGHT AGENT)
ПОДДЕРЖИВАЕМЫЕ ГИПЕРВИЗОРЫ И ОС

Microsoft Hyper-V

- 2008 R2
- 2012
- 2012 R2

Гипервизоры:

vmware®

- ESXi 5.1
- ESXi 5.5
- ESXi 6.0

CITRIX® XenServer

- XenServer 6.1
- XenServer 6.2 SP1
- XenServer 6.5

Серверные ОС:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008 (32/64 bit)
- Windows Server 2003 R2 (32/64 bit)
- Windows Server 2003 (32/64 bit)
- Linux Server (в 2016 году)

Гостевые ОС:

- Windows 8.1 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows 7 (32/64 bit)
- Windows XP (32 bit)
- Windows 10 - soon
- Linux OS (в 2016 году)

DLP

KASPERSKY lab

ПОДХОД ЛК К DLP

- ЛК разрабатывает **собственный DLP**
- **Channel DLP**
- **Data Loss Protection** = channel DLP (защита от утечек) + функционал Endpoint Security

Channel DLP

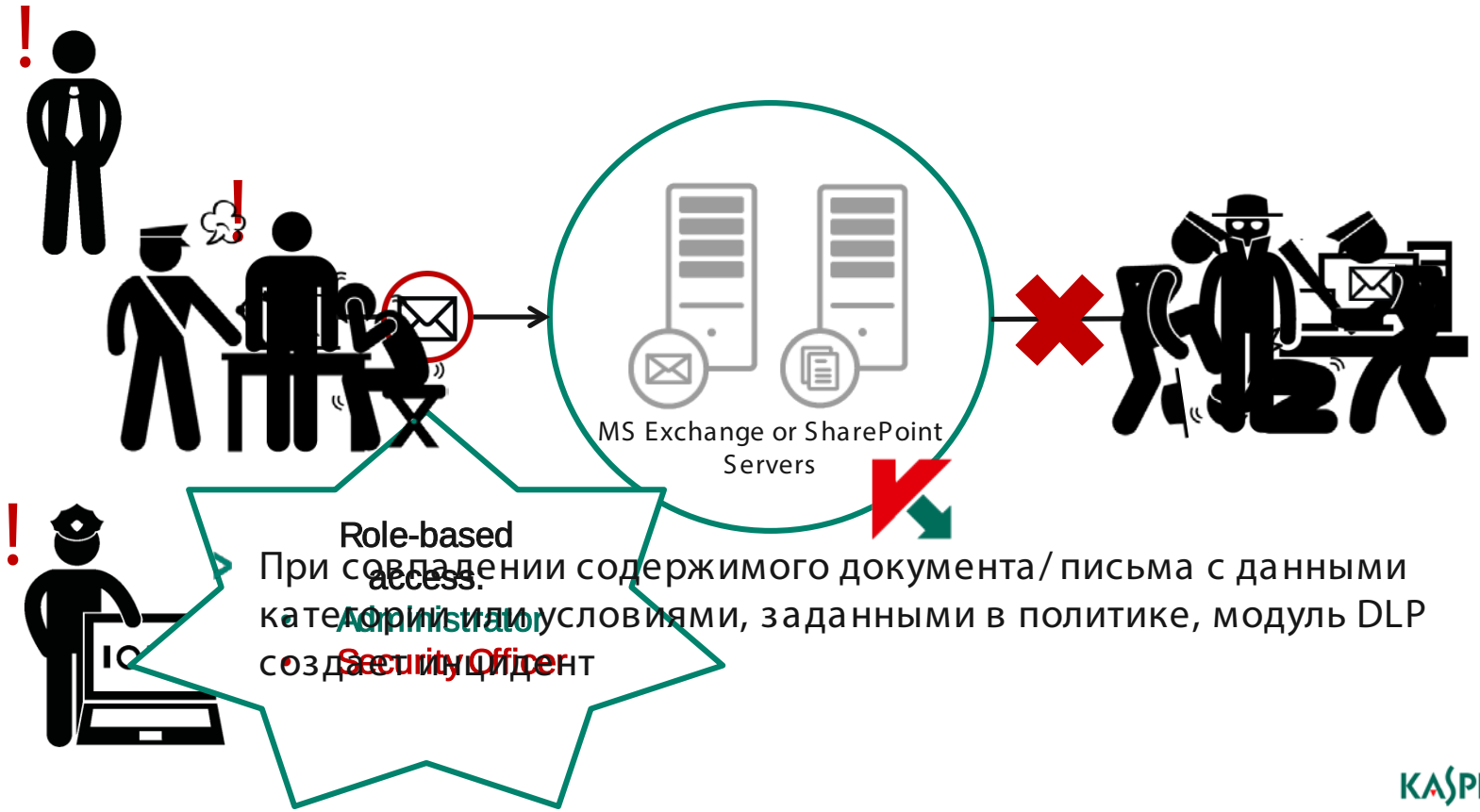
- Content-aware DLP
- Проверяет исходящий трафик и документооборот
- В первую очередь, защита от непреднамеренных утечек

Endpoint Data Protection

- Encryption
- Web, Application and Device control
- Mobile Device Management

KASPERSKY lab

КАК ЭТО РАБОТАЕТ



При совпадении содержимого документа/письма с данными категории или условиями, заданными в политике, модуль DLP создает инцидент

ЧТО КОНКРЕТНО МЫ ПРОВЕРЯЕМ:

- Весь e-mail – заголовок, тело и вложение
- Проверяем все **основные офисные форматы** + **pdf**
- Проверяем **архивы (включая вложенные)**
- Не сканируем **изображения**

KASPERSKY lab

ATM PROTECTION

KASPERSKY lab

ATM PROTECTION

Features:

1. Default Deny only installation mode
   - Low system requirements (256MB system memory)
   - Low traffic consumption (no regular av updates)
2. Modules: Default Deny (optional), File Antivirus OAS + ODS (both optional)
3. Device control (optional)
4. KSN integration
5. Management from local GUI and KSC

System Requirements:

1. DD only (256 MB RAM)
2. DD + ODS (on demand av-scan) (512 MB RAM)
3. DD + ODS + OAS (on access av-scan) (1 MB RAM)

KASPERSKY DDOS PREVENTION

KASPERSKY lab

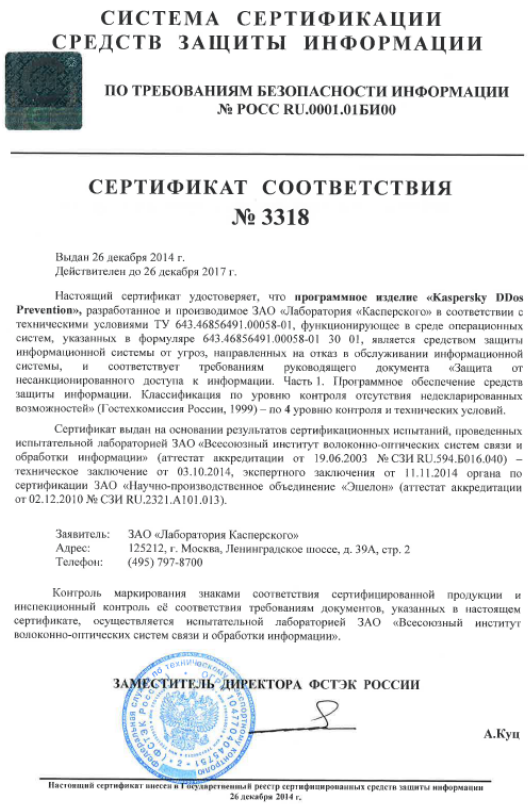
ДОСТУПНОСТЬ DDOS

- ~$200 – стоит целый день DDOS атаки на чёрном рынке
- Существуют специализированные online marketplaces для продажи/ покупки ботнетов и атак.
- Анонимная оплата через Bitcoins, PayPal.

KASPERSKY lab

КРАТКО О РЕШЕНИИ KASPERSKY DDOS PREVENTION

- KDP существует 5 лет
- Преимущественно enterprise клиенты (коэффициент удержания > 95%)
- Технологии оттестированные на сложных и больших атаках
- KL DDoS Intelligence – технологии, инструментарий, эксперты
- Kaspersky DDoS Prevention – первое и, на данный момент единственное, сертифицированное ФСТЭК решение по защите от атак отказ в обслуживании



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3318

Выдан 26 декабря 2014 г.
Действителен до 26 декабря 2017 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky DDos Prevention»**, разработанное и производимое ЗАО «Лаборатория «Касперского» в соответствии с техническими условиями ТУ 643.46856491.00058-01, функционирующее в среде операционных систем, указанных в формуляре 643.46856491.00058-01 30 01, является средством защиты информационной системы от угроз, направленных на отказ в обслуживании информационной системы, и соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровню контроля и технических условий.

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Всесоюзный институт волоконно-оптических систем связи и обработки информации» (аттестат аккредитации от 19.06.2003 № СЗИ RU.594.Б016.040) – техническое заключение от 03.10.2014, экспертного заключения от 11.11.2014 органа по сертификации ЗАО «Научно-производственное объединение «Эшелон» (аттестат аккредитации от 02.12.2010 № СЗИ RU.2321.А101.013).

Заявитель: ЗАО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

Контроль маркирования знаками соответствия сертифицированной продукции и инспекционный контроль её соответствия требованиям документов, указанных в настоящем сертификате, осуществляется испытательной лабораторией ЗАО «Всесоюзный институт волоконно-оптических систем связи и обработки информации».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ А.Куц

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 26 декабря 2014 г.

ПРЕИМУЩЕСТВА KDP

ПО собственной разработки

Быстро адаптируемся к новым изменениям и контролируем развитие

Команда дежурных экспертов 24x7

Следят за ситуацией и вмешиваются, когда необходимо

Защищаем конкретные ресурсы

Мониторим трафик именно к защищаемым ресурсам, что позволяет обнаруживать даже самые тонкие атаки.

Технологическое партнёрство с ISP

Фильтруем большую часть атаки как можно ближе к источнику

KL DDoS Intelligence

Позволяет обнаруживать атаки на самых ранних стадиях

KASPERSKY SECURITY INTELLIGENCE SERVICES

KASPERSKY lab

SERVICES MAP

SECURITY EDUCATION

Cybersecurity Fundamentals
Digital Forensics
Malware Analysis & Reverse Engineering

INVESTIGATION SERVICES

Malware Analysis
Digital Forensics
Incident Response

THREAT INTELIGENCE

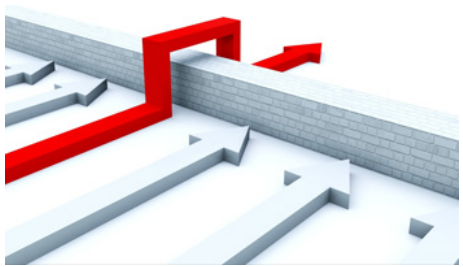
Threat Data Feeds
Botnet Tracking
Intelligence Reporting

SECURITY ASSESSMENT

Pen Testing
Application Security Assessment

PENETRATION TESTING

- **What?**
  - Black/ gray box security assessment of internal/ external network, system and application infrastructure*
- **Customer's goals**
  - Understand infrastructure security "from an attacker's perspective" **
  - Achieve compliance with security standards (like PCI DSS)
- **The service may additionally include:**
  - Social engineering checks (staff security awareness assessment)
  - Wireless networks security assessment
  - Technological audit (white-box) of certain systems with achieved privileges

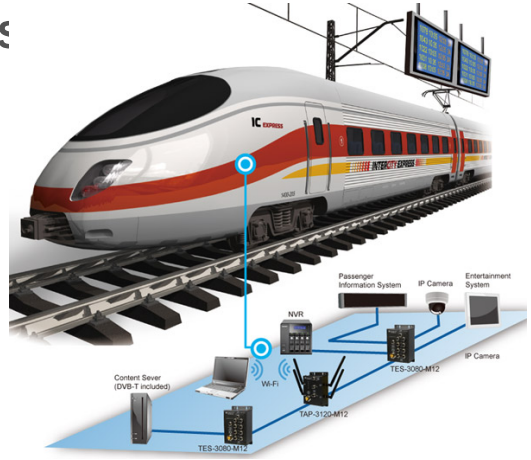


* http:/ / en.wikipedia.org/ wiki/ Penetration_test

** BTW, we will not "attack you as a hacker", we have moral and lawful restrictions

ICS COMPONENTS SECURITY ASSESSMENT

- **Deep technical assessment of SCADA, PLC, Smart Meters, RTU**
  - System-specific threat modelling
  - Network communication analysis
  - Black and white-box (source code) checks
  - Security features testing
- **Customer Benefits**
  - Threat model
  - Known and 0-day vulnerabilities
  - Security Checklists
  - Industry-specific attack scenarios
  - Technical fraud scenarios

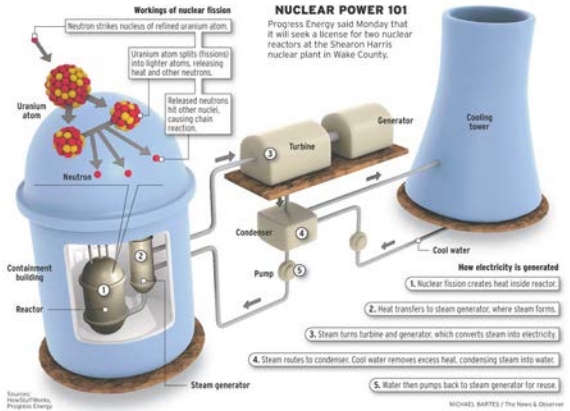


KASPERSKY lab

ICS/ SCADA SECURITY AUDITS

- **IT/ OT Security Audit of network, Infrastructure, ICS and Process security**
  - Industrial-specific threat modelling
  - Technical audit of network, system and application infrastructure
  - Technical compliance checks

- **Customer Benefits**
  - Threat model
  - Knowledge about ICS network vulnerabilities
  - Technical compliance gap map
  - Security program recommendation
  - Technical controls recommendations



APPLICATION SECURITY ASSESSMENT

- **Approaches**
  - Black-box
  - Grey-box
  - White-box (including source code analysis)

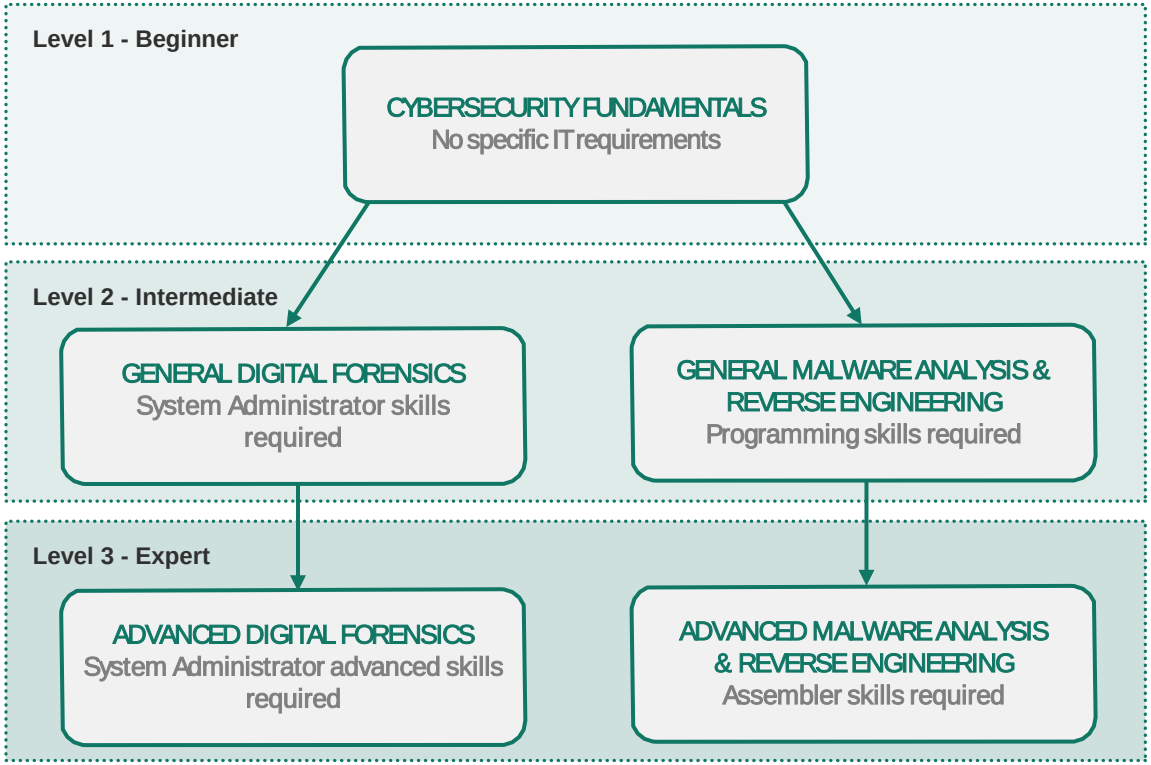
- **We can analyze:**
  - Various web applications (including online banking), taking into account business logic
  - Mobile applications
  - Applications having fat clients
  - Web applications with an enabled WAF (to assess its effectiveness)

ATM AND POS SECURITY ASSESSMENT

- **Deep assessment of ATM, POC Systems and Networks**
  - System-specific threat modelling
  - Network communication analysis
  - Black-box vulnerability assessment
  - Security features testing
- **Customer Benefits**
  - Threat model
  - Knowledge about known and 0-day vulnerabilities
  - Security Checklists
  - Attack scenarios
  - Technical fraud scenarios

KASPERSKY lab

CYBERSECURITY EDUCATION: AN OVERVIEW



KASPERSKY lab

СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕВЫМ АТАКАМ И APT (ADVANCED PERSISTENT THREAT)

KASPERSKY lab

КОМПЛЕКСНЫЙ ПОДХОД К ПРОТИВОДЕЙСТВИЮ ЦЕЛЕВЫМ АТАКАМ

- защита рабочих мест
- защита мобильных устройств
- защита виртуализации
- безопасности Web и почты
- защита для дата центров

РЕАКЦИЯ

ПРОТИВОДЕЙСТВИЕ

АНАЛИЗ

ОБНАРУЖЕНИЕ

КОМПЛЕКСНЫЙ ПОДХОД К ПРОТИВОДЕЙСТВИЮ ЦЕЛЕВЫМ АТАКАМ

- защита рабочих мест
- защита мобильных устройств
- защита виртуализации
- безопасности Web и почты
- защита для дата центров

ПРОТИВОДЕЙСТВИЕ

ОБНАРУЖЕНИЕ

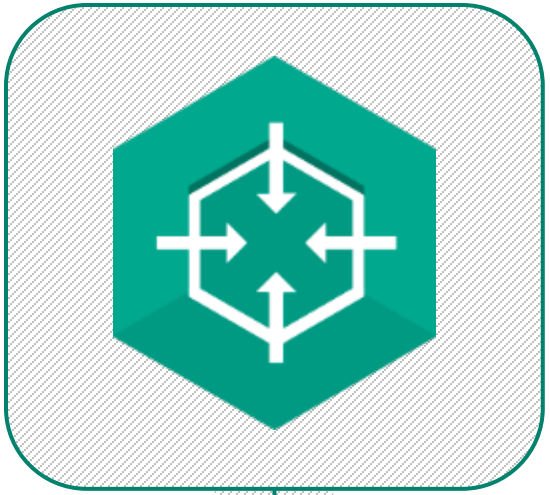
- Мониторинг угроз безопасности (KSN)
- Kaspersky Anti Targeted Attacks (KATA) Platform

- *Сенсоры и агенты*
- *«Песочница»*

АНАЛИЗ

РЕАКЦИЯ

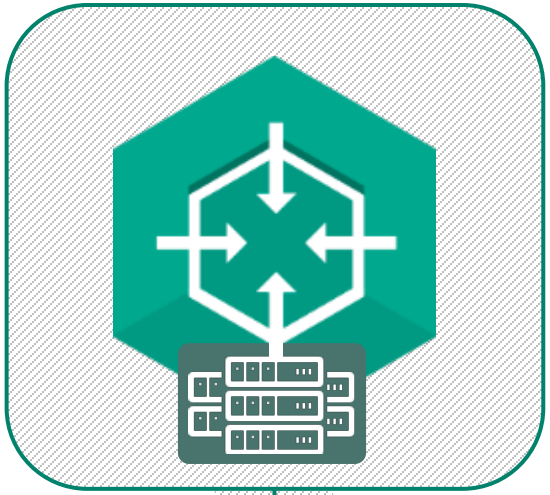
ОБНАРУЖЕНИЕ
ГЛОБАЛЬНЫЙ МОНИТОРИНГ УГРОЗ (KSN)



- репутационные сервисы:
  - файловая репутация
  - URL-репутация
  - шаблоны поведения ПО
  - индикаторы компрометации
- осведомленность в режиме реального времени
- глобальная статистика, 600k (1.4 GB) запросов в секунду

KASPERSKY lab

ОБНАРУЖЕНИЕ (ОПЦИОНАЛЬНО)
ЛОКАЛЬНАЯ РЕПУТАЦИОННАЯ БАЗА УГРОЗ (KPSN)

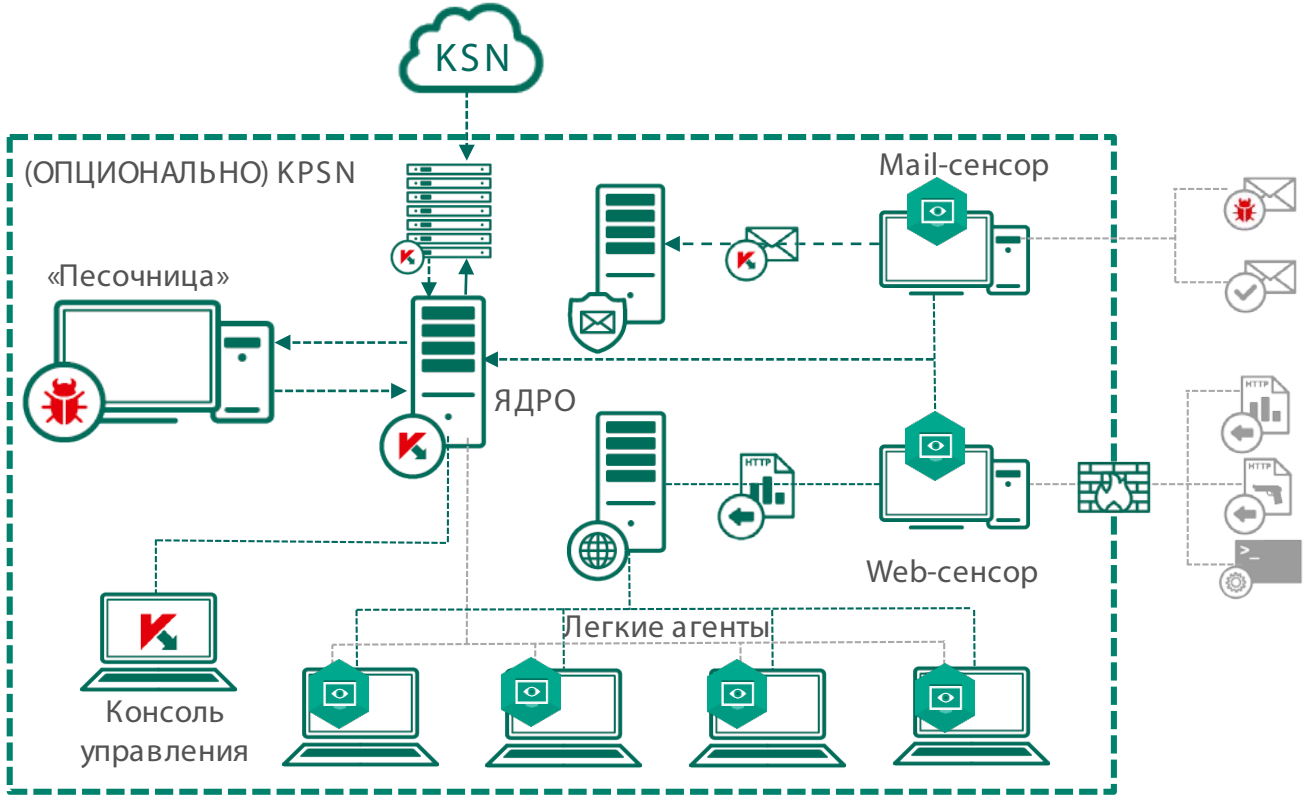


- доверенная установка в виде отдельного решения:
  - опыт ЛК внутри инфраструктуры
  - отсутствие исходящего трафика
  - подходит для физ. изолированных сетей
- полная копия репутационной базы ЛК
- только входящие обновления от KSN
- возможность создания и накопления уникальных вердиктов

KASPERSKY lab

ОБНАРУЖЕНИЕ

KASPERSKY ANTI TARGETED ATTACK (KATA) PLATFORM



Обнаружение и сдерживание целевых атак на ранних стадиях до причинения серьезного вреда

КОМПЛЕКСНЫЙ ПОДХОД К ПРОТИВОДЕЙСТВИЮ ЦЕЛЕВЫМ АТАКАМ

- защита рабочих мест
- защита мобильных устройств
- защита виртуализации
- безопасности Web и почты
- защита для дата центров

РЕАКЦИЯ

ПРОТИВОДЕЙСТВИЕ

АНАЛИЗ

ОБНАРУЖЕНИЕ

- Обучение офицеров анти-АПТ решения
- Kaspersky Anti Targeted Attacks (KATA) Platform

- *Поведение рабочих мест*
- *Поведение внутри сети*

- Мониторинг угроз безопасности (KSN)
- Kaspersky Anti Targeted Attacks (KATA) Platform

- *Сенсоры и агенты*
- *«Песочница»*

КОМПЛЕКСНЫЙ ПОДХОД К ПРОТИВОДЕЙСТВИЮ ЦЕЛЕВЫМ АТАКАМ

- Расследование киберинцидентов
- Kaspersky Anti Targeted Attacks (KATA) Platform

- *Восстановление рабочих мест*
- *Сетевое блокирование*

РЕАКЦИЯ

- защита рабочих мест
- защита мобильных устройств
- защита виртуализации
- безопасности Web и почты
- защита для дата центров

ПРОТИВОДЕЙСТВИЕ

АНАЛИЗ

- Обучение офицеров анти-АПТ решения
- Kaspersky Anti Targeted Attacks (KATA) Platform

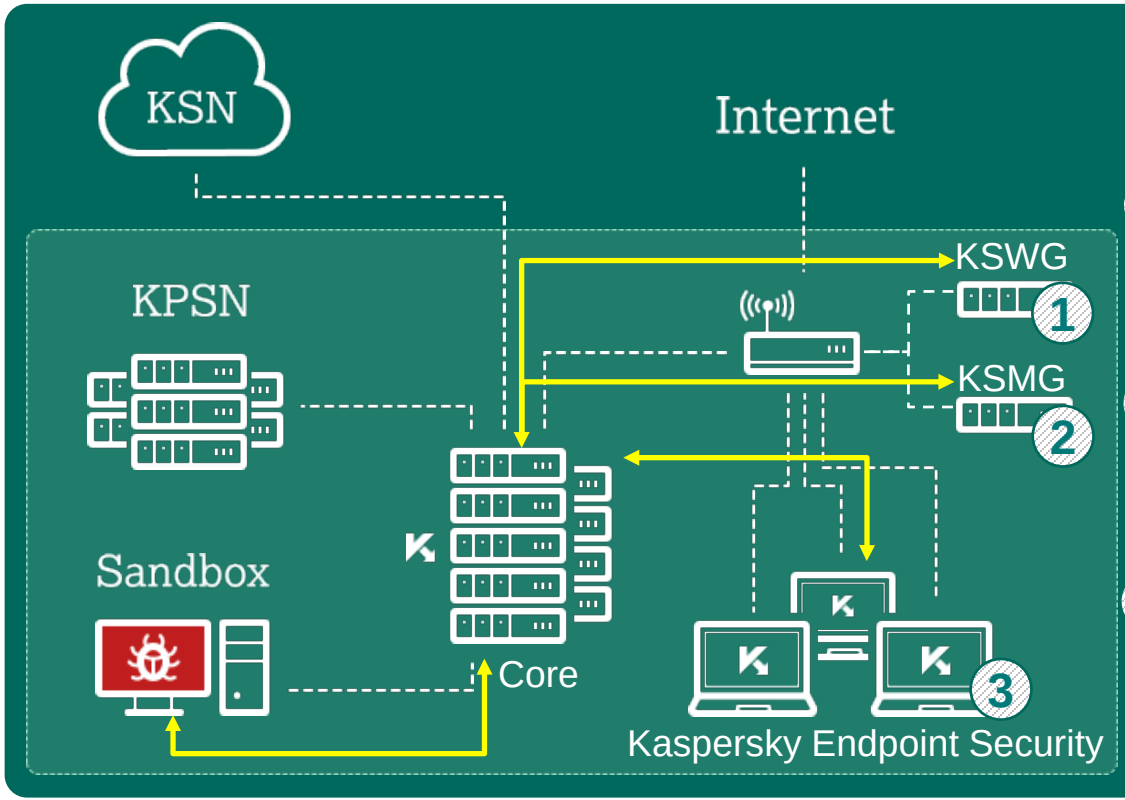
- *Поведение рабочих мест*
- *Поведение внутри сети*

ОБНАРУЖЕНИЕ

- Мониторинг угроз безопасности (KSN)
- Kaspersky Anti Targeted Attacks (KATA) Platform

- *Сенсоры и агенты*
- *«Песочница»*

РЕАКЦИЯ
КАТАВОЗМОЖНОСТИ РЕАГИРОВАНИЯ В ПЛАНЕ



1. **Kaspersky Secure Web Gateway:** Блокирование сетевого трафика (H2 2016)
2. **Kaspersky Secure Mail Gateway:** Блокирование почты (H2 2016)
3. **Kaspersky Endpoint Security:** Восстановление рабочих мест (H2 2016)

www.kaspersky.com/business

KASPERSKY lab