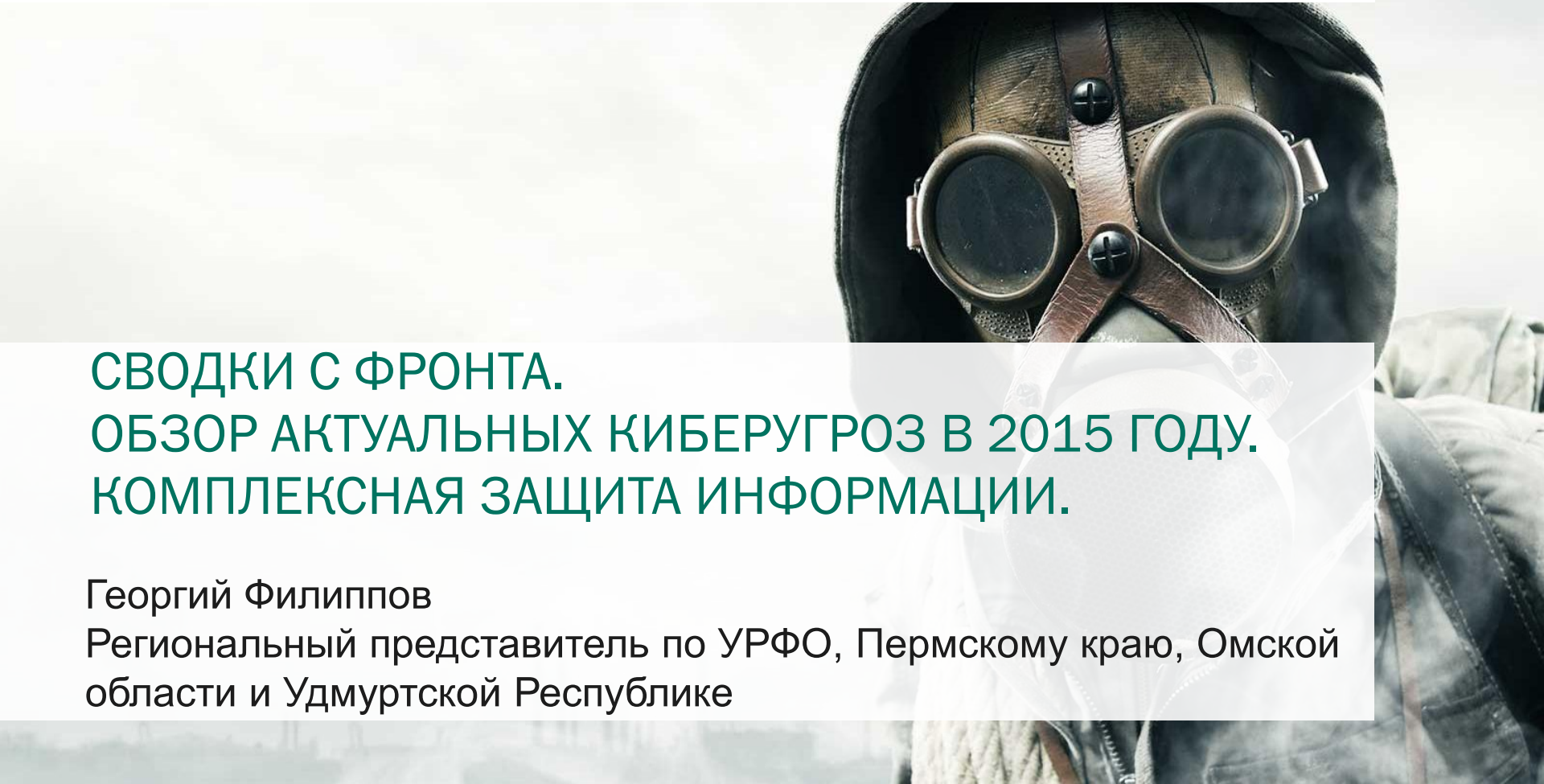
KASPERSKY lab



СВОДКИ С ФРОНТА.
ОБЗОР АКТУАЛЬНЫХ КИБЕРУГРОЗ В 2015 ГОДУ.
КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ.

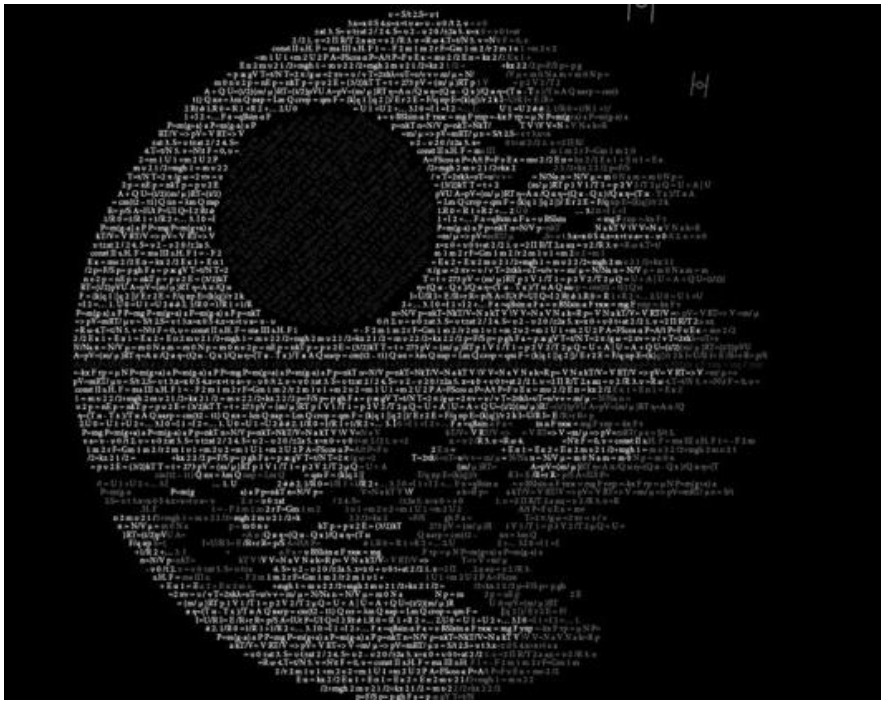
Георгий Филиппов
Региональный представитель по УРФО, Пермскому краю, Омской области и Удмуртской Республике

Q1 2015 В ЧИСЛАХ - ОБЗОР

Боремся с киберзлоумышленниками по всему миру

- По данным KSN, в первом квартале 2015 года продукты «Лаборатории Касперского» заблокировали 2 205 858 791 вредоносную атаку на компьютерах и мобильных устройствах пользователей.
- Решения «Лаборатории Касперского» отразили 469 220 213 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- Зафиксировано 93 473 068 уникальных URL, на которых происходило срабатывание веб-антивируса.
- **40%** веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в России.

EQUATION
ЗВЕЗДА СМЕРТИ ГАЛАКТИКИ ВРЕДОНОСНОГО ПО



Пятнадцать лет
кибершпионажа.

Заражение прошивки жестких дисков 12 различных марок

Точечные «закладки»

KASPERSKY lab

Equation group victims map

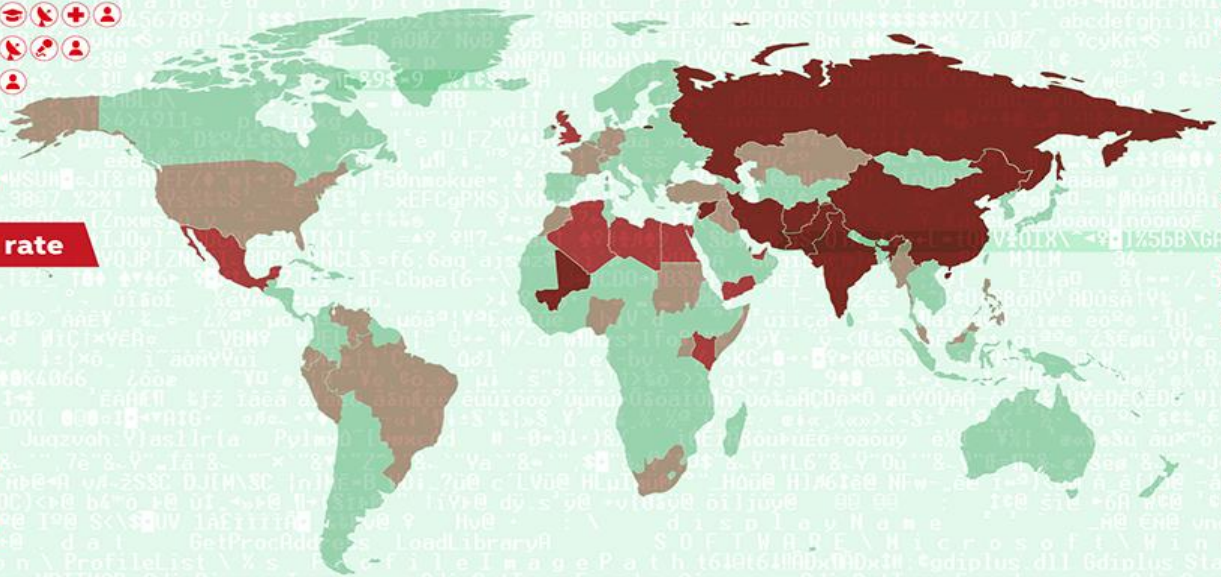
Finance · Diplomatic / Embassies · Energy / Infrastructure · Military · Telecommunications · Islamic Scholars · Other / Unknown
Government · Research institution · University · Aerospace · Medical · Media

High infection rate

- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate

- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt



Low infection rate

- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Equador
- Belgium
- Bahrain

© 2015 Kaspersky Lab

GREAT KASPERSKY lab

CARBANAK
УГРОЗА НА МИЛЛИАРД

Более ста финансовых учреждений.

На ограбление банка уходило 2 - 4 месяца

Убытки каждого из банков составляют от 2,5 примерно до 10 миллионов долларов

Как кибербанда Carbanak украла миллиард долларов

Целевая атака на банк

1. Заражение

Электронное письмо с бэкдором Carbanak

Работник банка

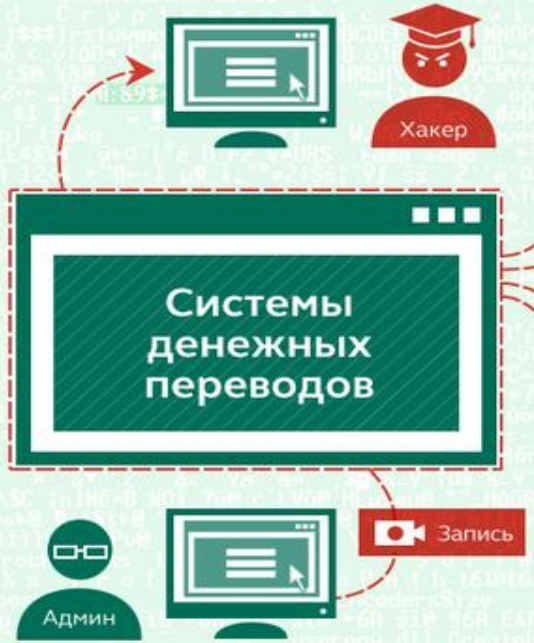
Электронные письма с эксплойтами

Краденые учетные данные

Сотни машин заражены в поисках компьютера администратора

2. Сбор разведданных

Перехват данных с экранов служащих



3. Действия от имени сотрудников

Как были украдены средства

Онлайн-банкинг
Перевод средств на счета мошенников

Системы электронных платежей
Перевод средств в китайские и американские банки

Завышение баланса счетов
Присвоение «лишних» средств через фальшивую транзакцию

Управление банкоматами
Приказы на выдачу наличных в заранее определенное время

© 2015 Лаборатория Касперского

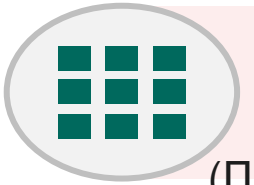
GREAT KASPERSKY lab

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

БЕЗОПАСНОСТЬ ВИРТУАЛЬНЫХ СРЕД – ВОЗМОЖНЫЕ ВАРИАНТЫ

БЕЗ ЗАЩИТЫ

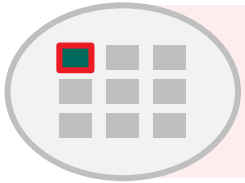
НЕПРИЕМЛЕМО!



ТРАДИЦИОННАЯ ЗАЩИТА

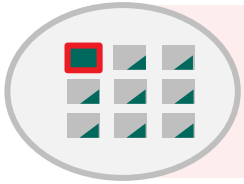
(Полноценный агент)

ВЫСОКИЙ УРОВЕНЬ ЗАЩИТЫ / СНИЖЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ



БЕЗ УСТАНОВКИ АГЕНТА

ПРОСТОЕ РАЗВЕРТЫВАНИЕ И УПРАВЛЕНИЕ. ТОЛЬКО ДЛЯ СРЕД VMWARE



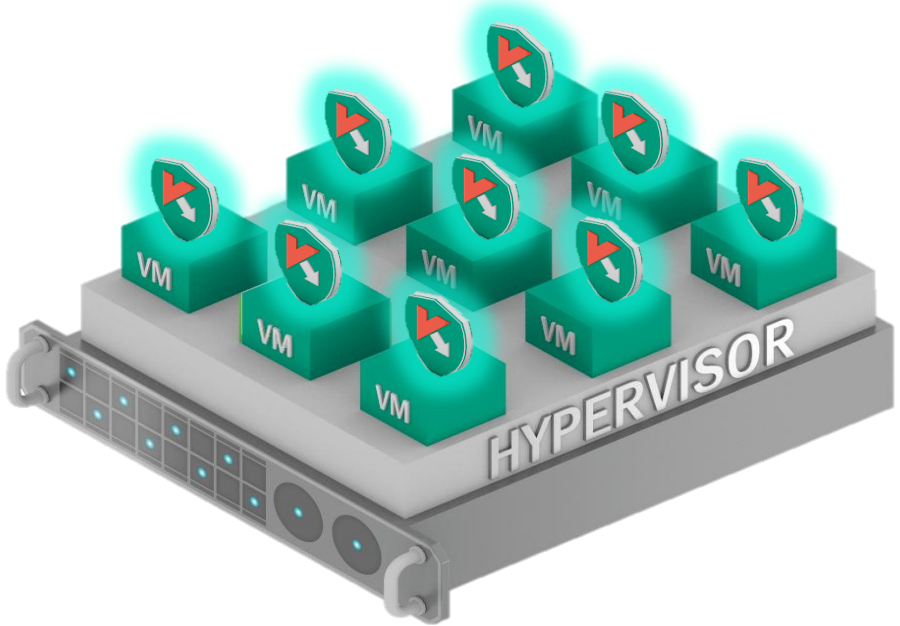
ЛЕГКИЙ АГЕНТ

НАДЕЖНАЯ ЗАЩИТА

KASPERSKY lab

ТРАДИЦИОННАЯ ЗАЩИТА С УСТАНОВКОЙ АГЕНТА

Полноценный агент безопасности устанавливается на каждую виртуальную машину



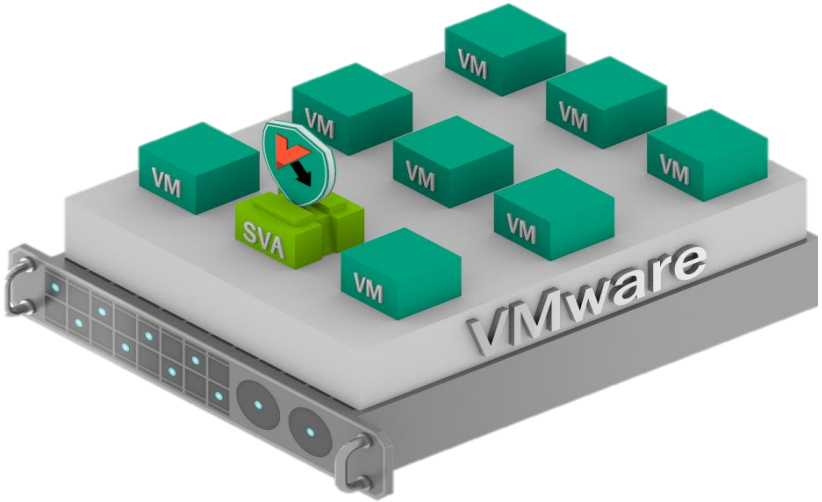
Агент безопасности

- 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

ЗАЩИТА БЕЗ УСТАНОВКИ АГЕНТА

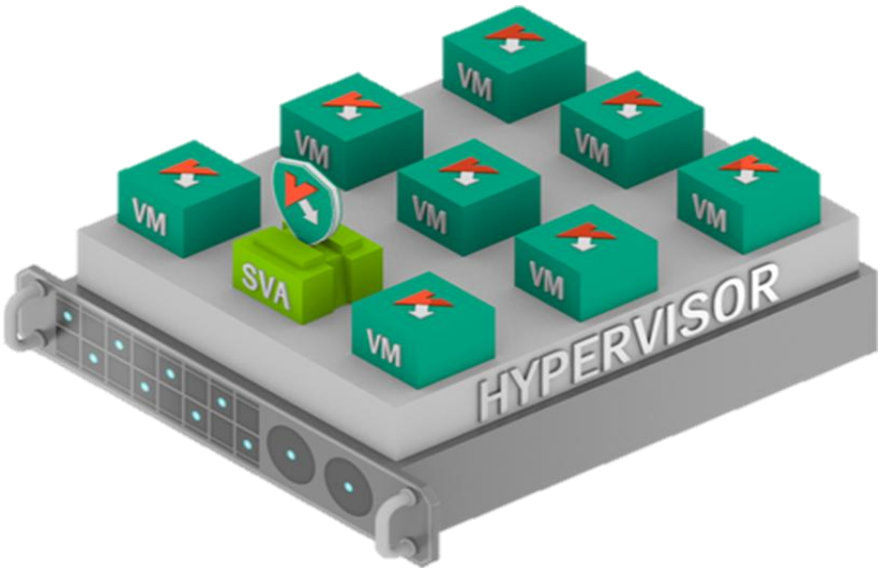
Защиту обеспечивает виртуальное устройство безопасности, установленное на хост-сервере



- **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 НА ОСНОВЕ ЛЕГКОГО АГЕНТА

Легкий агент на каждой ВМ плюс виртуальное устройство безопасности



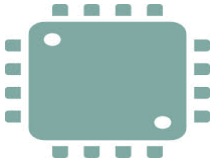
- Расширенная защита
  - Мониторинг уязвимостей
  - Контроль программ
  - Веб-контроль
  - Контроль устройств
  - Эвристический анализ
  - Проверка IM-сообщений, почтового и веб-трафика
- Устраняет:
  - Чрезмерное потребление ресурсов
  - «Шквальное» обновление и сканирование
  - «Окно уязвимости» при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

KASPERSKY lab

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

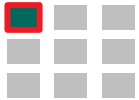
ПОДДЕРЖКА РАЗЛИЧНЫХ ПЛАТФОРМ

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

ВЫБОР ОПТИМАЛЬНОГО СПОСОБА ЗАЩИТЫ

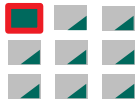
Традиционная защита на базе агента

- 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

KASPERSKY lab

ЗАЩИТА КОРПОРАТИВНОЙ ПОЧТЫ И KASPERSKY DLP

KASPERSKY SECURITY 9.0 ДЛЯ MICROSOFT EXCHANGE SERVERS

Надежная защита от вредоносных ссылок и вложений в электронных письмах

Интеллектуальное распознавание и блокирование спама

Гибкий контроль над распространением конфиденциальной информации

Простое и удобное управление

KASPERSKY lab

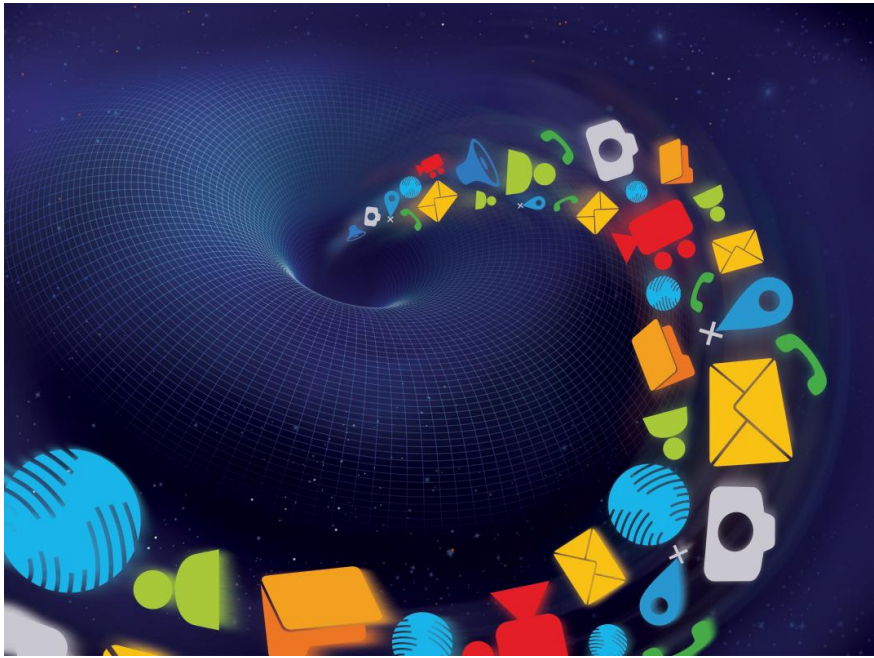
НАДЕЖНАЯ ЗАЩИТА ОТ ВРЕДОНОСНЫХ ССЫЛОК И ВЛОЖЕНИЙ В ЭЛЕКТРОННЫХ ПИСЬМАХ

Высокая скорость сканирования

Проверка трафика в режиме реального времени

Резервное копирование

Сканирование упакованных (в том числе многократно) файлов для повышения уровня обнаружения вредоносных объектов



KASPERSKY lab

ЗАЩИТА ОТ СПАМА

Интеллектуальные технологии распознавания спама

Защита из «облака» в режиме реального времени

Классификация сообщений

По сведениям Gartner сегодня до 66% всей электронной корреспонденции по-прежнему относится к спаму и массовым рассылкам.

КОНТРОЛЬ ЗА РАСПРОСТРАНЕНИЕМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ЗАЩИТА ОТ УТЕЧКИ ДАННЫХ

Обеспечение соответствия стандартам или регулятивным актам (PCI-DSS,ФЗ 152)

Тематические словари (Административный,Финансы)

Собственные словари

Поиск структурированной информации (Выгрузки, таблицы)

Согласно совместному исследованию, проведенному «Лабораторией Касперского» с агентством «B2B International» в 2014 году, в 30% российских организаций произошла утечка данных по невнимательности сотрудников.

СПАСИБО!

ВОПРОСЫ?

Georgy.Filippov@kaspersky.com
+7(912) 696-6600

KASPERSKY lab