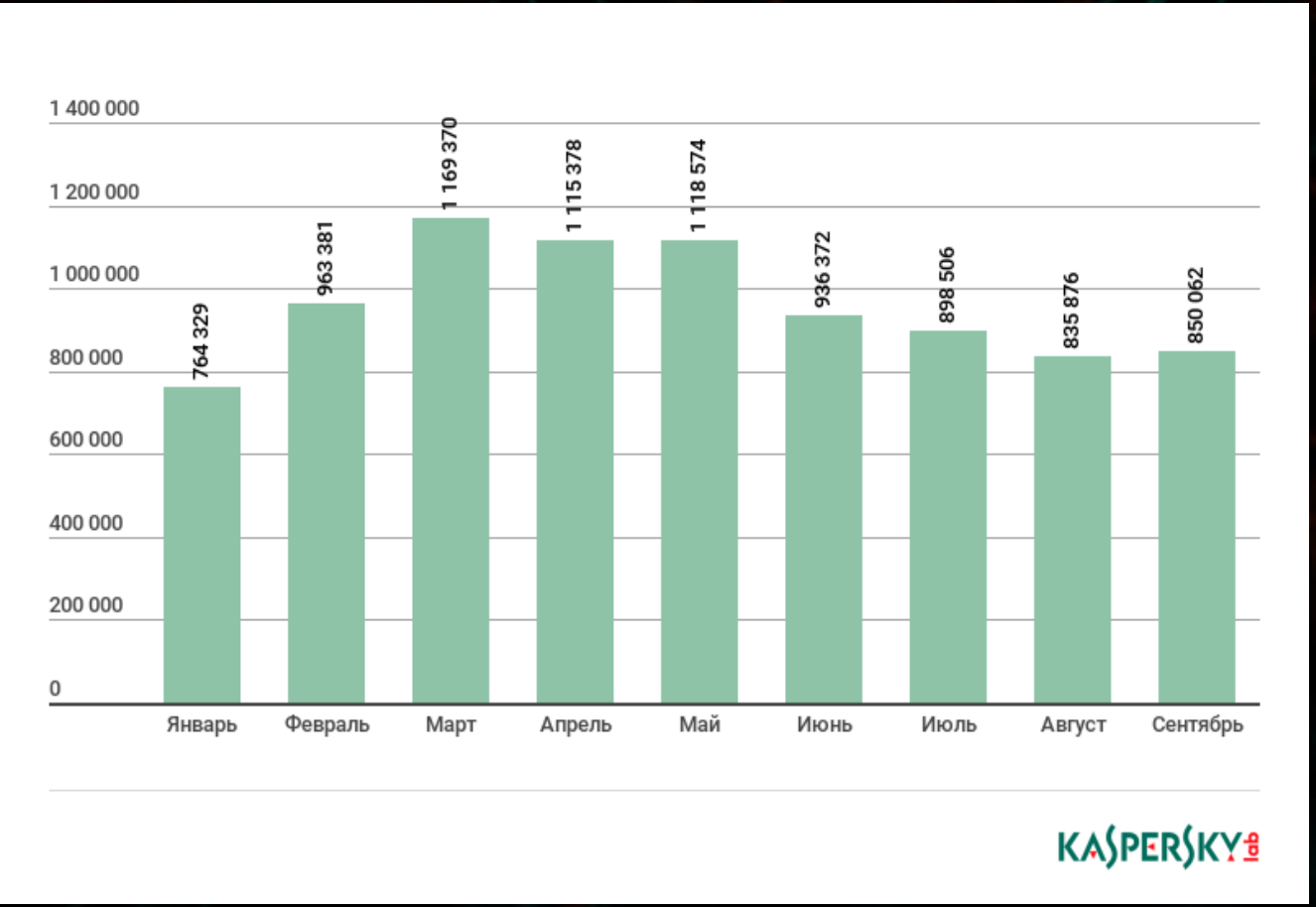
Защита от сложных угроз

Криптовалютные майнеры

1. “Перепрофилирование” бот-сетей с DDoS-атак на майнинг криптовалюты
2. Появление майнингового функционала во вредоносном и рекламном ПО
3. Около 70-80 % мощности центрального или графического процессора его ПК используются для генерации виртуальных монет



Количество уникальных пользователей, атакованных майнерами

KASPERSKY lab

Примеры инцидентов

Вирус-майнер найден в официальном магазине приложений Ubuntu

Майнер, добывающий Bytecoin, обнаружил пользователь по имени Tarwirdur.

...дрядчика ...заражен ...айнинга

...пасности»,
...ты информации, в том
...уктур, оказался
...майнинга. В компании
...о разместили вирусы в

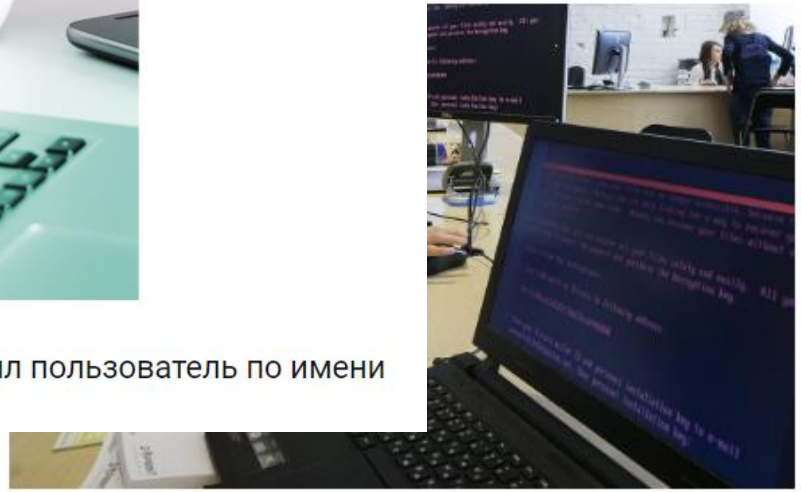


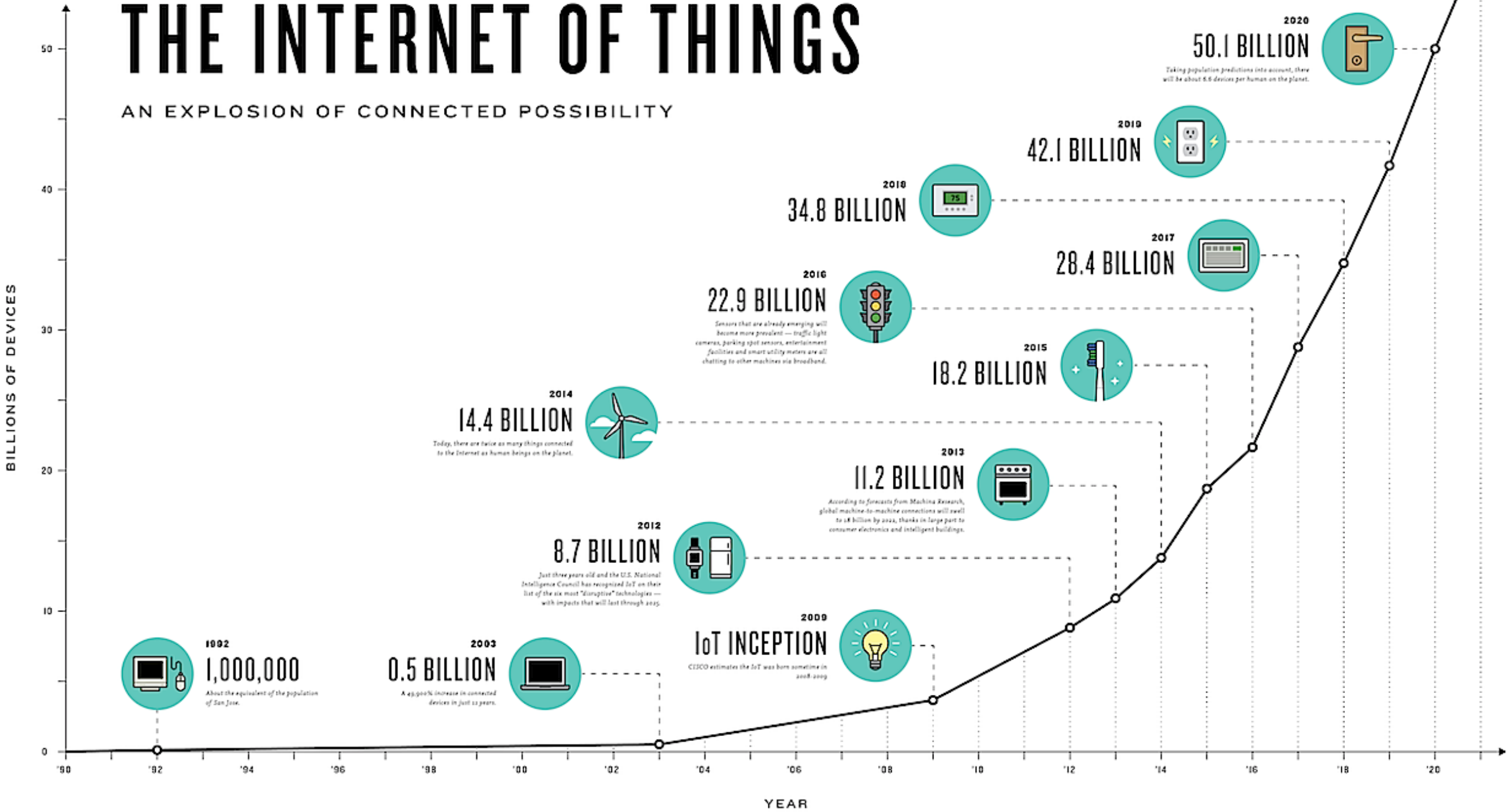
Фото: Vincent Mundy / Bloomberg

...майнер атаковал тысячи гаджетов ...id

...сова Мария

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY

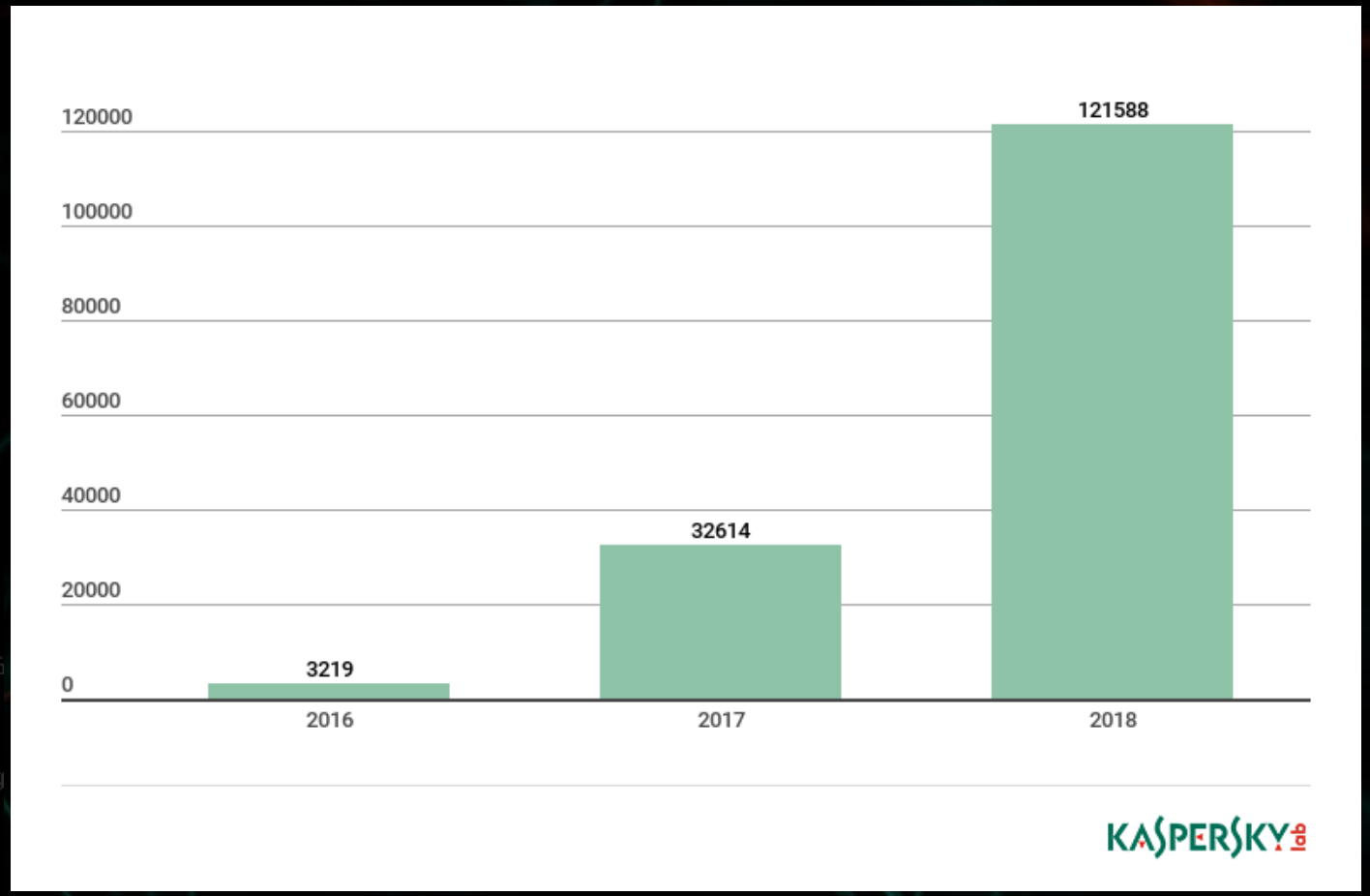


IoT-устройства

1. Простые уязвимости
2. С 2016 года кол-во вредоносного ПО увеличилось больше чем в 40 раз!
3. Одним из самых популярных векторов атак и, соответственно, заражения устройств все еще остается перебор пароля Telnet

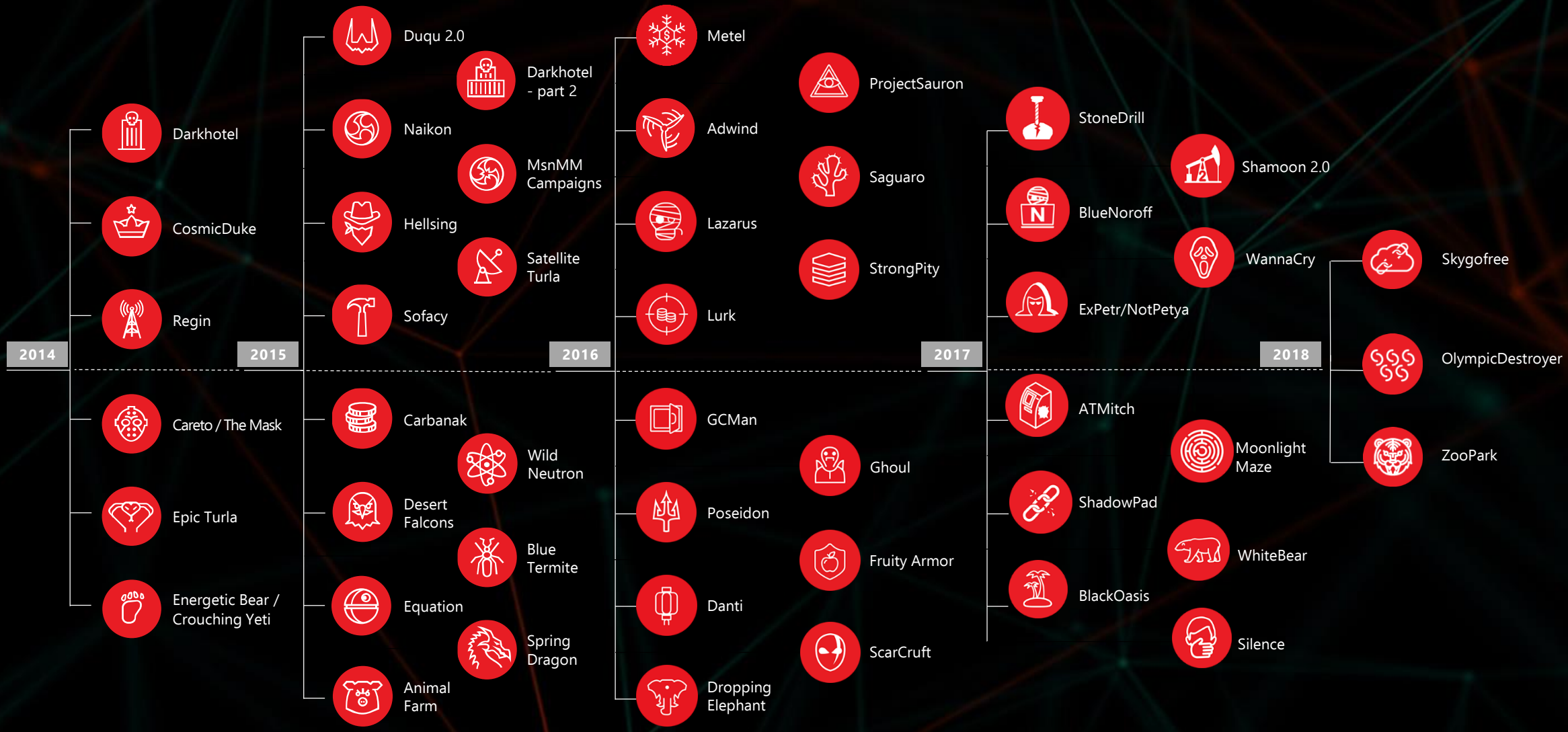
HAJIME

MIRAI



Количество образцов вредоносного ПО для IoT-устройств

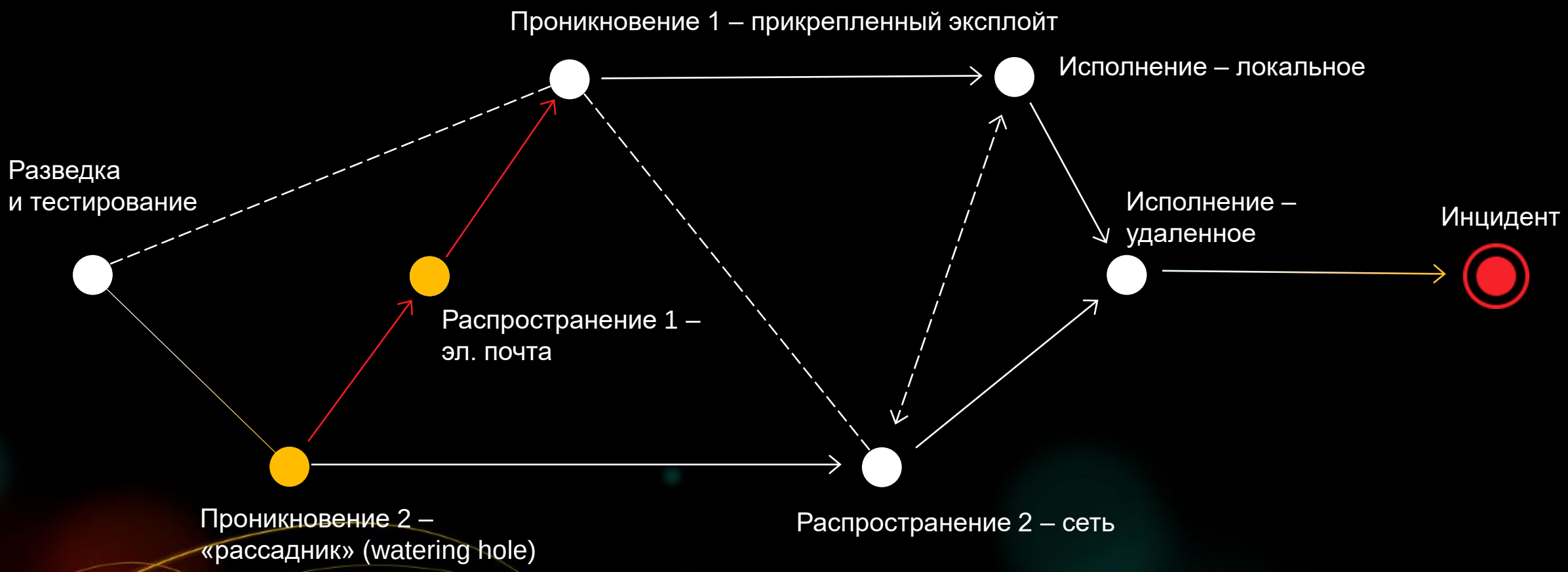
Наши исследования



KASPERSKY lab

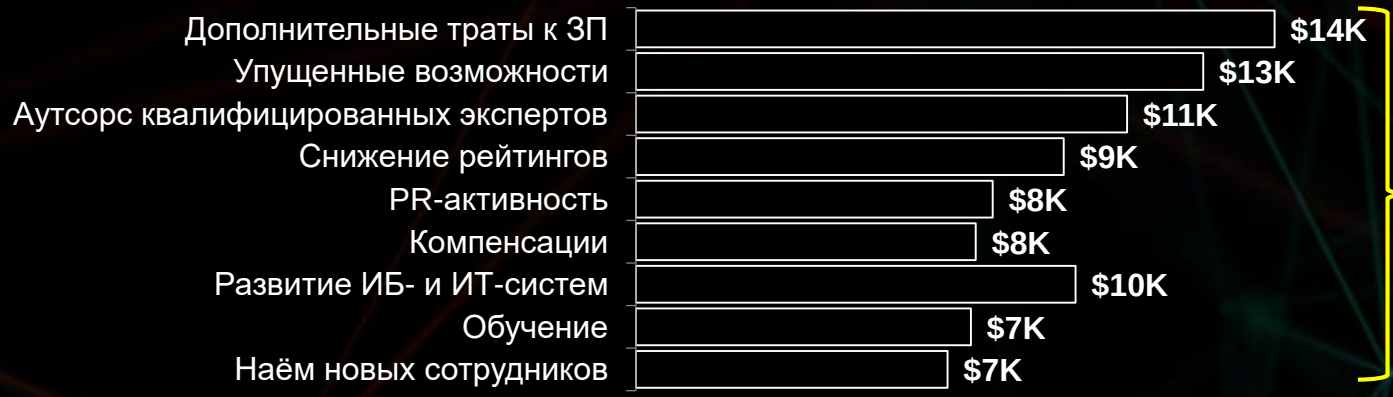
Чем «сложнее» угрозы – тем больше вопросов к «решениям» и списку предлагаемых «инновационных технологий»

ПЕРЕДОВЫЕ УГРОЗЫ: СЛОЖНЫЕ И НЕЛИНЕЙНЫЕ



Статистика потерь за 2018 год от одного инцидента ИБ

SMB



Средний ущерб:
$86.5 тыс.

Крупные компании

Средний ущерб:
$891 тыс.

Перераспредленеие трудозатрат ИТ и ИБ служб крупнейшая часть затрат по результату выявленного инцидента

Источник: Исследование рисков информационной безопасности 2018, «Лаборатория Касперского»

Опрошено: 926 SMBs/ 590 Enterprises
Пострадали минимум от одной утечки данных

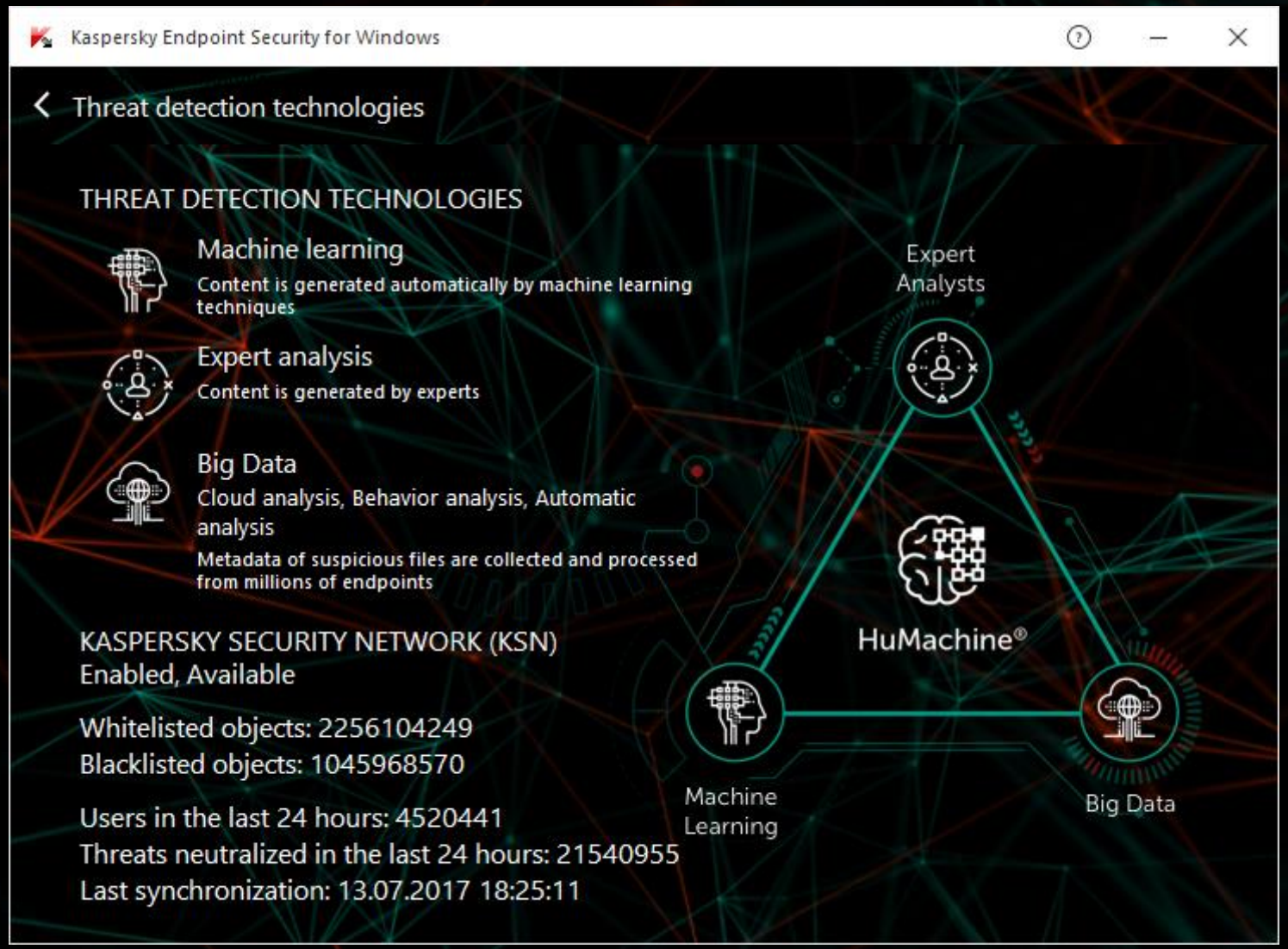
KASPERSKY lab

Что делать?

Kaspersky Adaptive Security Framework 2013

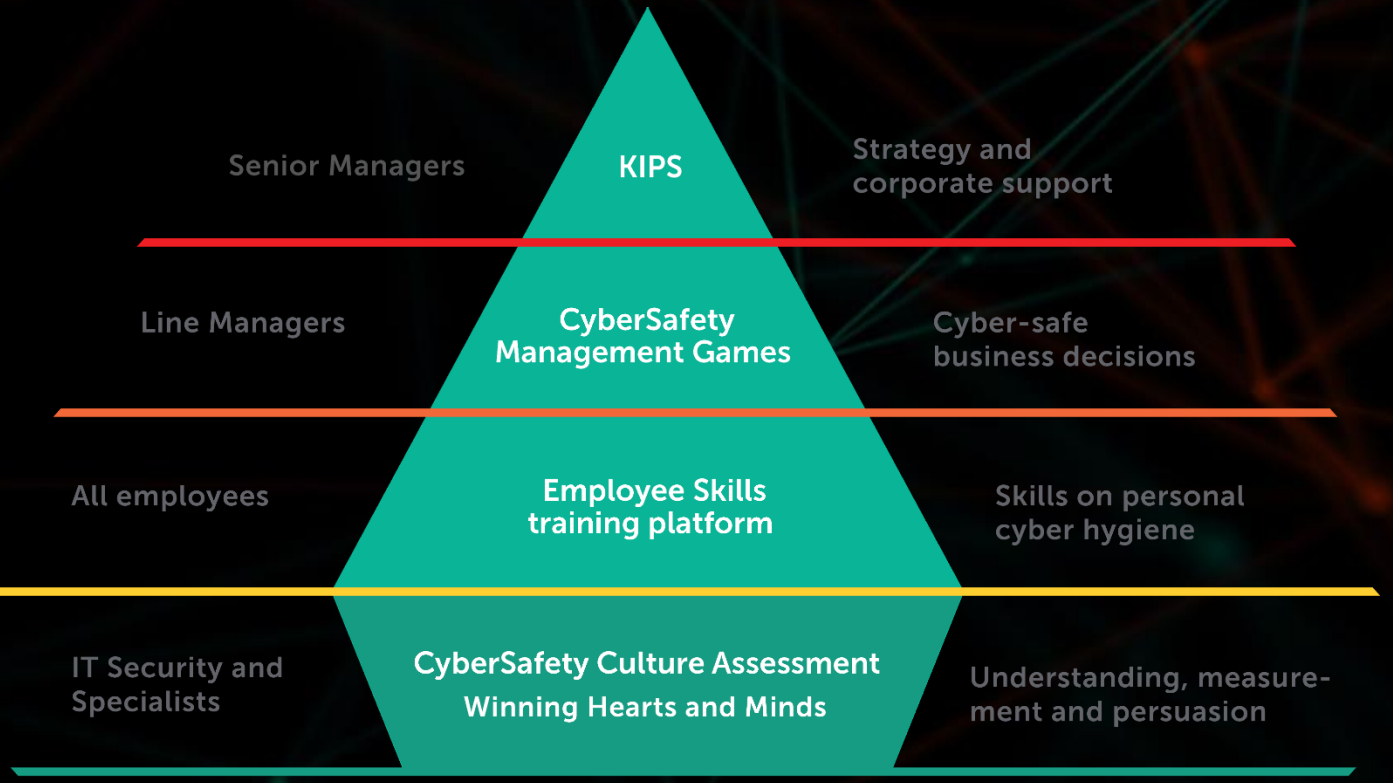
KASPERSKY lab

Kaspersky Endpoint Security 11



Повышение осведомлённости сотрудников об угрозах ИБ

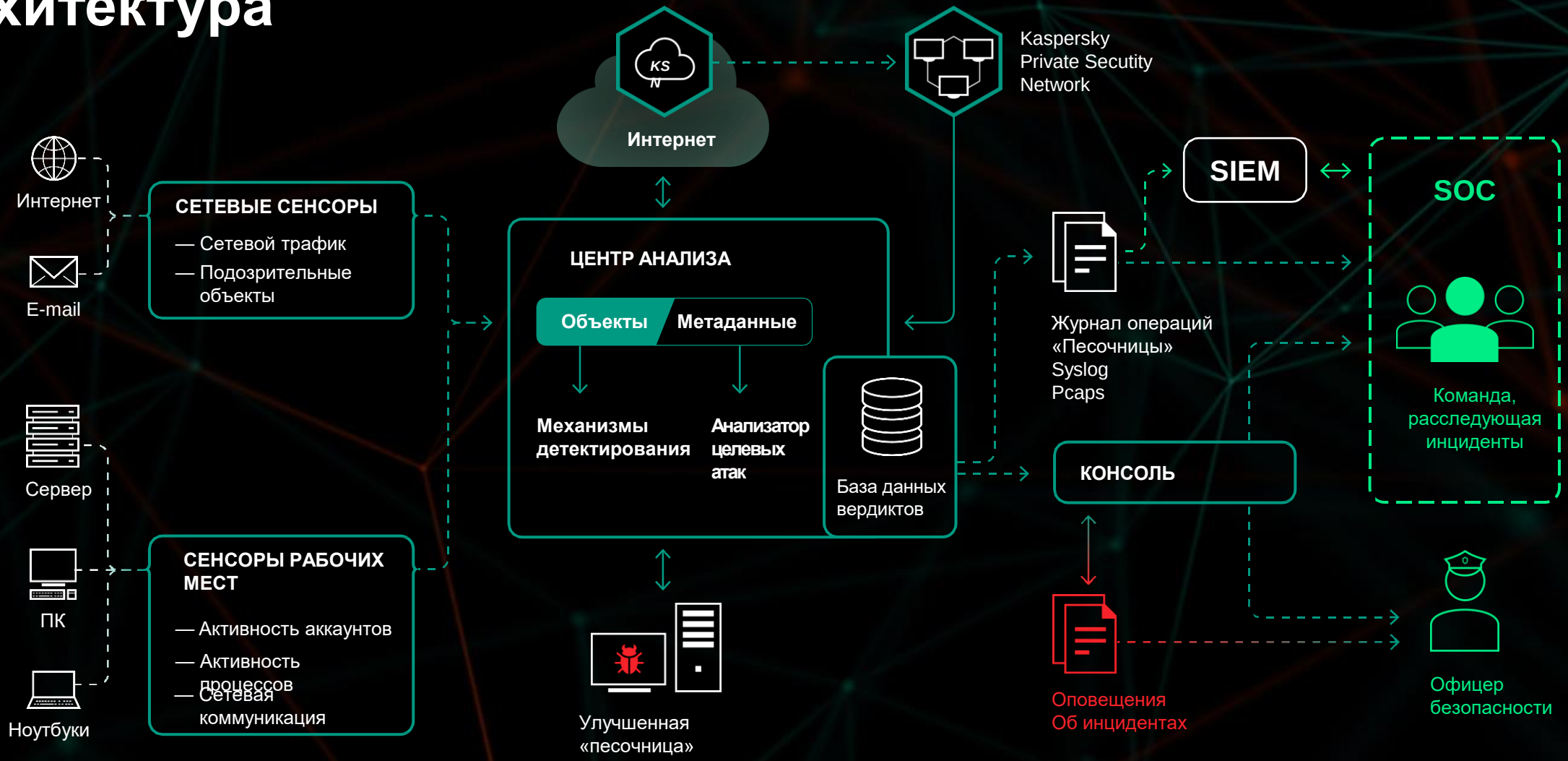
- до 93% применяют навыки в повседневной работе
- до 90% снижения количества инцидентов
- не менее чем на 50% снижение ущерба от инцидентов в денежном эквиваленте
- 30x ROI



KASPERSKY lab

Kaspersky Anti Targeted Attack platform

Архитектура



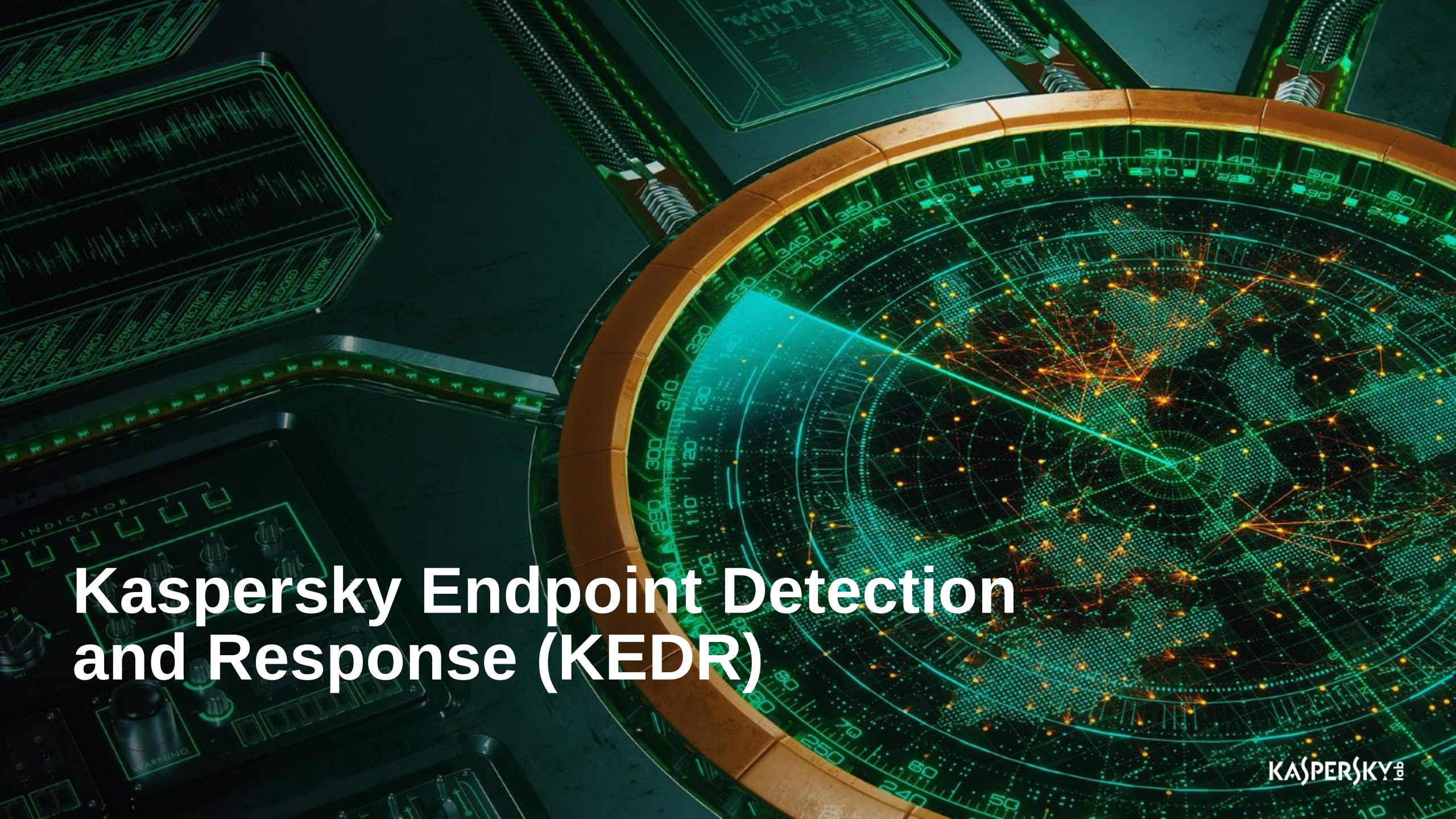
Векторы атаки | Получение данных | Анализ данных | Приоритизация вердиктов | Реагирование

KASPERSKY lab

Детектирующие технологии

- Intrusion detection system
- Anti malware engine
- Threat intelligence services
- Targeted attack analyzer
- YARA engine
- Risk score engine
- Certcheck
- Sandbox

Технология Sandbox



Kaspersky Endpoint Detection and Response (KEDR)

Решение Лаборатории Касперского

Название решения: Kaspersky Endpoint Detection and Response, Kaspersky EDR, KEDR.

Kaspersky Endpoint Detection and Response – это агентское решение для централизованного расследования и реагирования, предлагающее автоматизацию ключевых процессов ИБ, глубинный мониторинг состояния рабочих станций в сети и средств цифровой криминалистики для служб ИБ и команд SOC (Security Operational Center).

Kaspersky EDR помогает крупным организациям:

- Обеспечить полную осведомленность о состоянии сети посредством постоянного Мониторинга
- Централизованно собирать и хранить необходимую для работы телеметрию и данные
- Эффективно Обнаруживать угрозы и помогать оперативно их искать
- Реагировать соразмерно уровню опасности
- Предотвращать появления аналогичных угроз в будущем

KASPERSKY lab

Сегодня защита рабочих станций – больше чем антивирусная защита

CISO

Риск менеджер

SOC команда

ИТ-администратор

Группа реагирования

ИТ-инженер

Офицер ИБ

Аналитик

Endpoint Protection (EPP)

Как автоматизировать процесс защиты и антивирусной проверки против распространенных угроз

Как

Как

Как

Как

Как предоставить сотрудникам/группам уникальные политики и настройки безопасности

Противодействие и контроль

Endpoint Detection and Response (EDR)

Как сканировать сеть на предмет наличия следов компрометации и IoC

Как обна

ущерб

Как сопс

Как быстр

Как цент

Как сделать процесс реагирования менее затратным и более унифицированным

Организация процессов… Incident Response, Threat Hunting, Threat Analysis…

От автоматического обнаружения – к реагированию и предотвращению

НА ОСНОВЕ АНАЛИТИКИ

Передовые технологии и решения

Kaspersky
Anti Targeted Attack

Kaspersky
Endpoint Detection and Response

KASPERSKY lab

ОБЛАЧНЫЕ ДАННЫЕ ОБ УГРОЗАХ

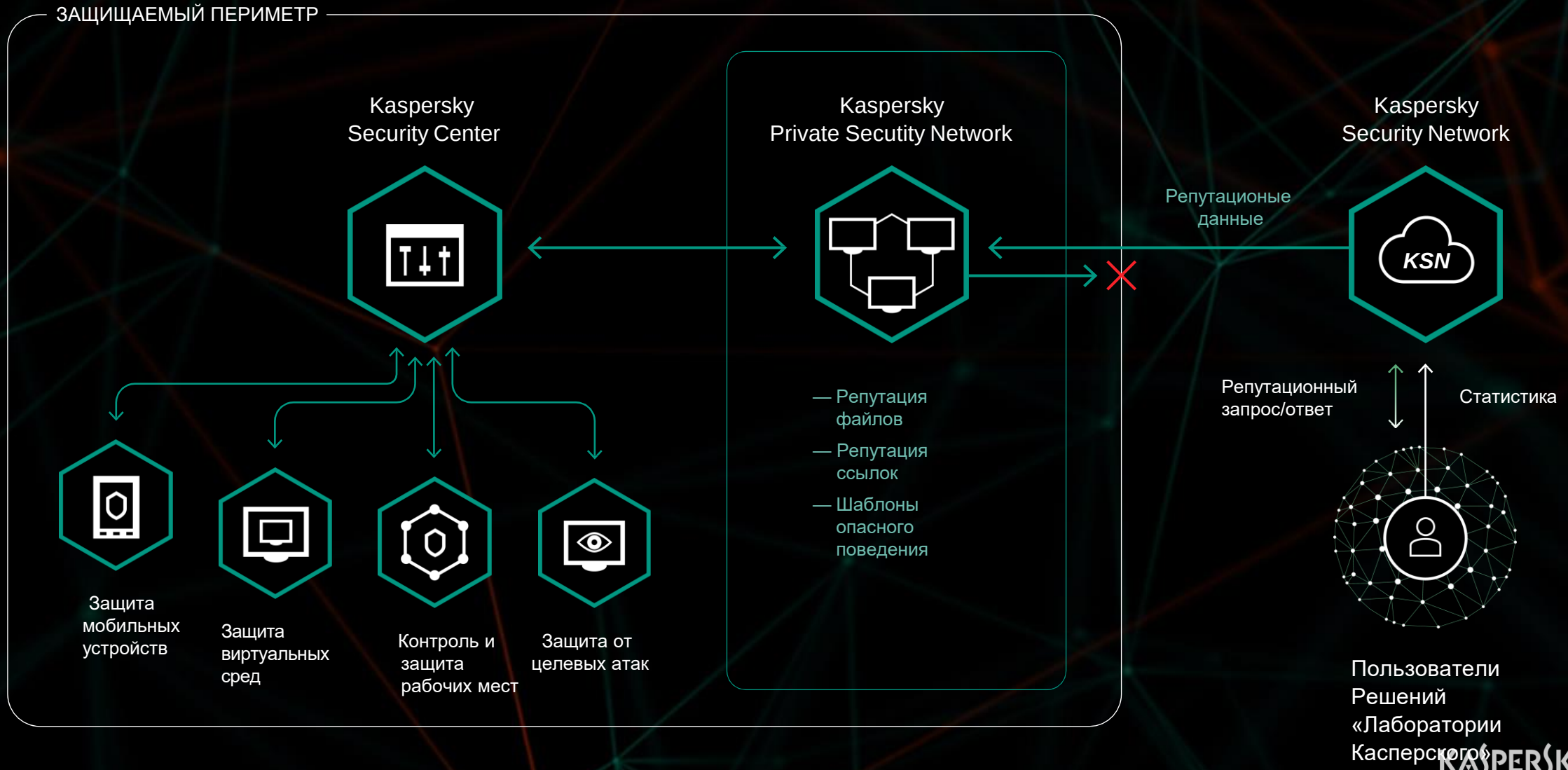
Информация об угрозах поступает от более 60 млн пользователей

Глобальные данные об угрозах в режиме реального времени

Постоянное использование данных в защитных решениях

Пользователи KSN

KASPERSKY PRIVATE SECURITY NETWORK



Модель построения передовой защиты с помощью решений и технологий «Лаборатории Касперского»

APT-угрозы

Целевые атаки

Шифровальщики

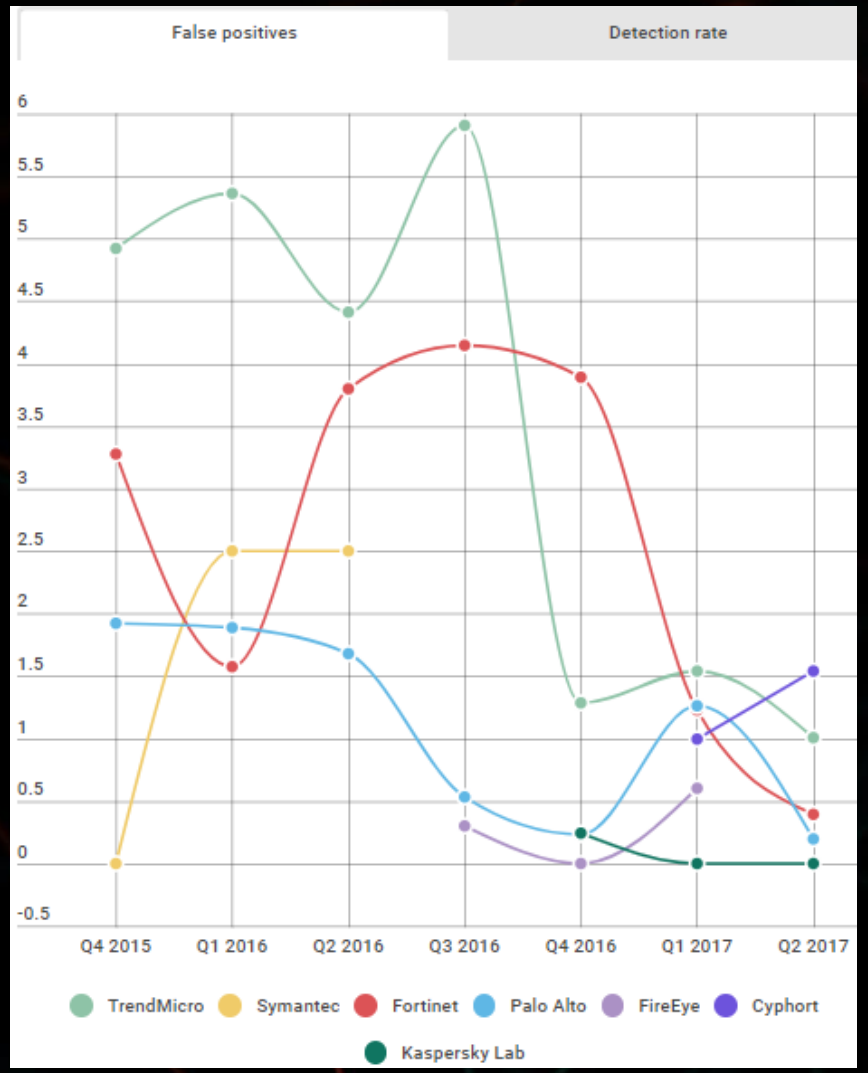
Массовые угрозы

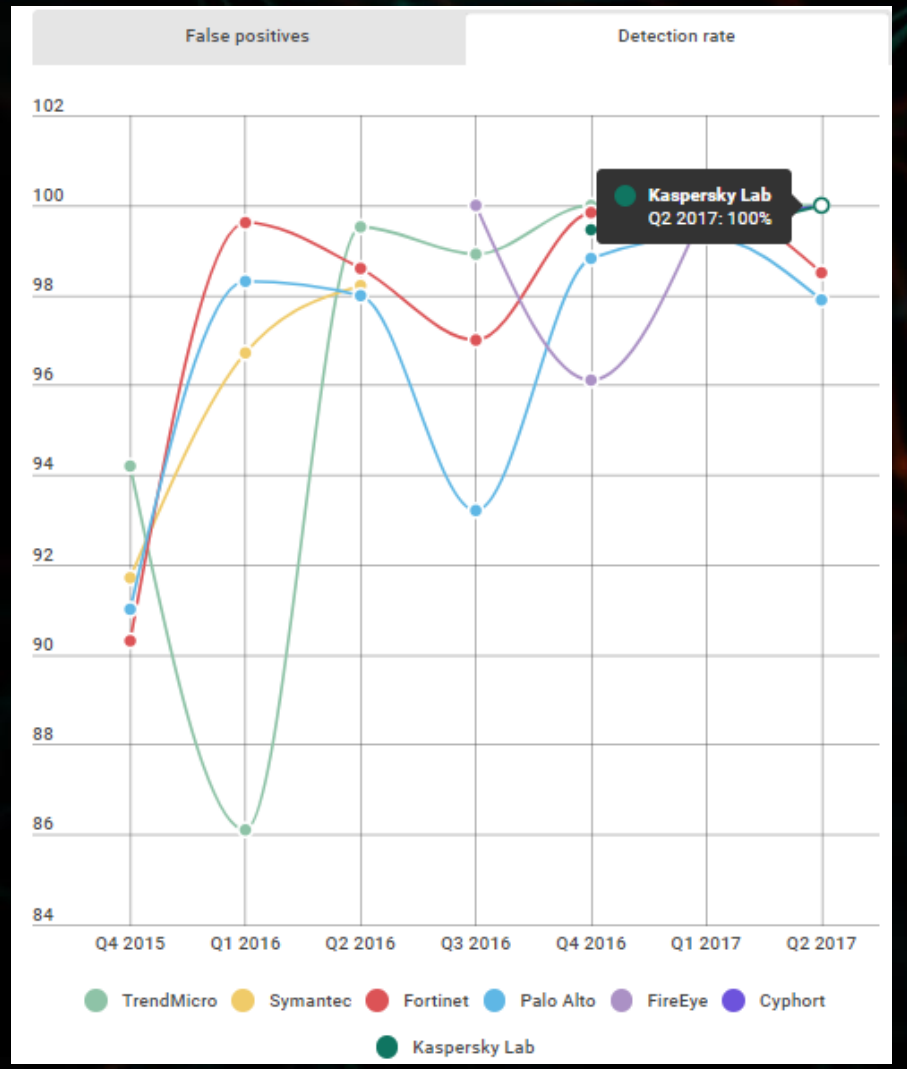
- Anti Targeted Attack (KATA)
- Endpoint Detection and Response (KEDR)
- Private Security Network (KPSN)
- Secure Mail Gateway (KSMG)
- Security для бизнеса (KESB)
- Мониторинг системы

- Профессиональные сервисы
- MSA (SAM)
- Повышение осведомленности
- Отчеты об APT-атаках
- Threat Hunting (KMP)
- Портал Threat Intelligence (TIP)
- Реагирование на инциденты
- Тренинги для IT-специалистов

KASPERSKY lab

Сертификация ICSA Labs – Advanced Threat Defense, 2017





KASPERSKY lab

KASPERSKYOS // Первый взгляд

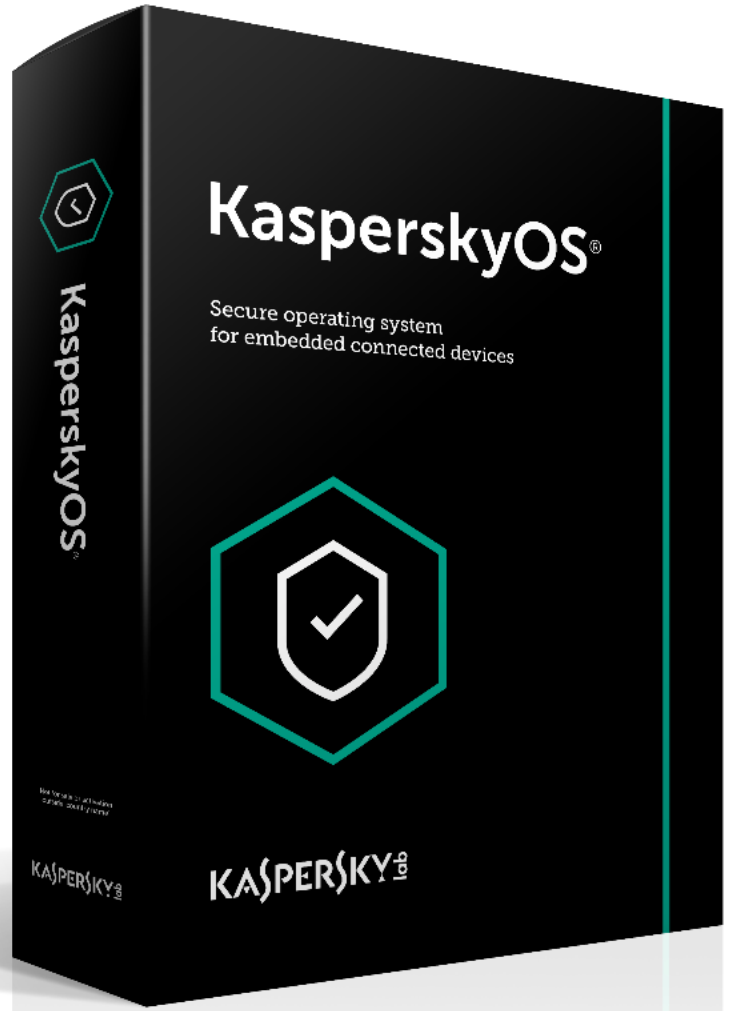
- Разработана для встраиваемых, подключенных к сети Интернет устройств со специфическими требованиями к кибербезопасности
- Основана на микроядре, которое гарантирует контроль всех внутренних коммуникаций
- Поведение всех модулей описано в политиках безопасности
- MILS архитектура

  - ✓ Разделение и изоляция доменов безопасности
  - ✓ Гибкий контроль междоменных коммуникаций посредством Kaspersky Security System (KSS)

KASPERSKYOS // Первый взгляд

- Разработана для встраиваемых, подключенных к сети Интернет устройств со специфическими требованиями к кибербезопасности
- Основана на микроядре, которое гарантирует контроль всех внутренних коммуникаций
- Поведение всех модулей описано в политиках безопасности
- MILS архитектура

  - ✓ Разделение и изоляция доменов безопасности
  - ✓ Гибкий контроль междоменных коммуникаций посредством Kaspersky Security System (KSS)



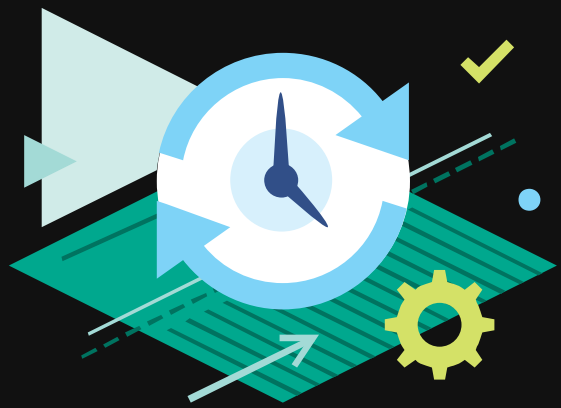
KASPERSKYOS - TRUSTED. FLEXIBLE. SECURE.

ДОВЕРЕННАЯ

KasperskyOS может выступать основой для построения доверенной системы в силу своих архитектурных особенностей: ОС не допускает исполнения функций приложений, не декларированных в политиках безопасности

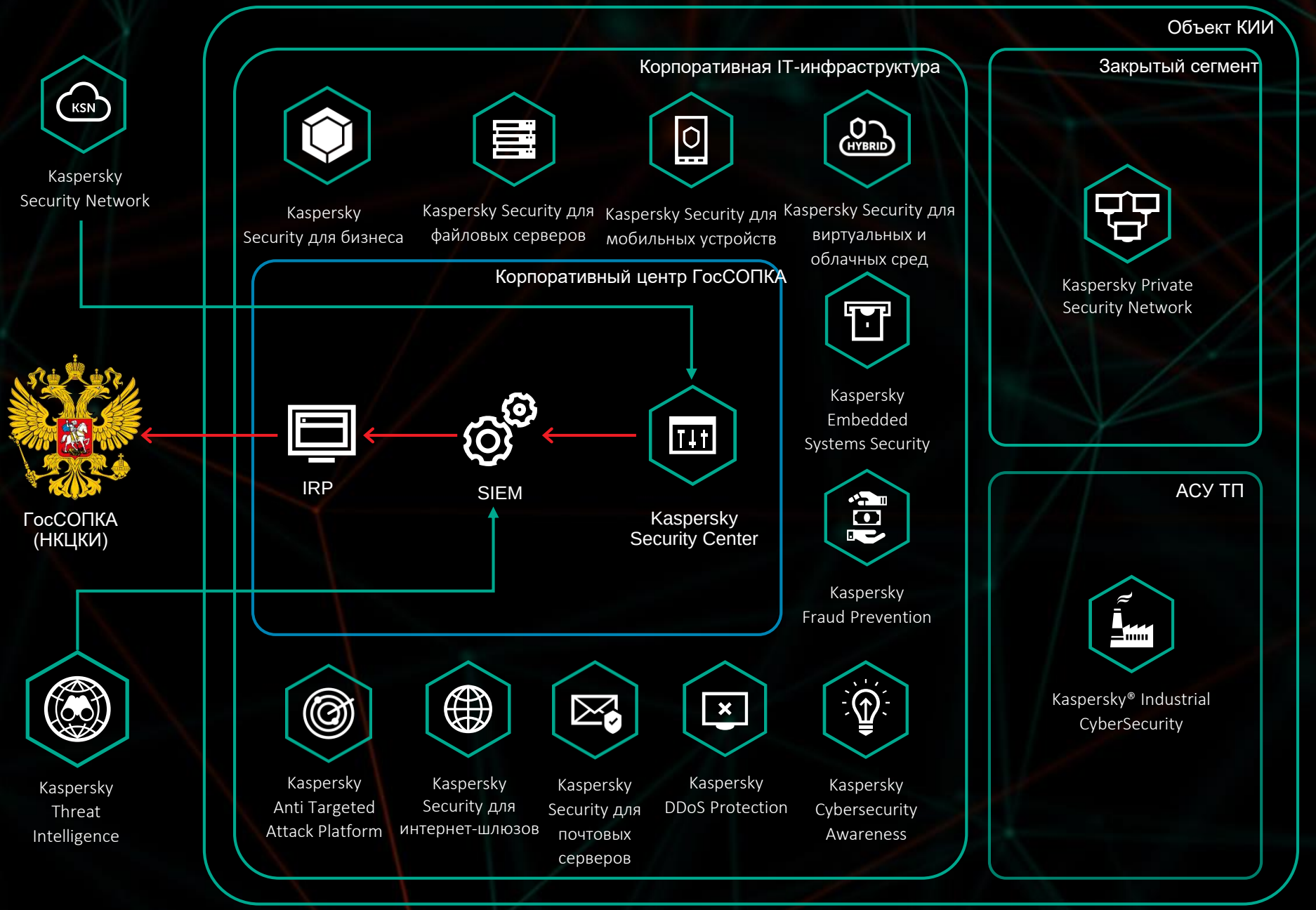
ГИБКАЯ

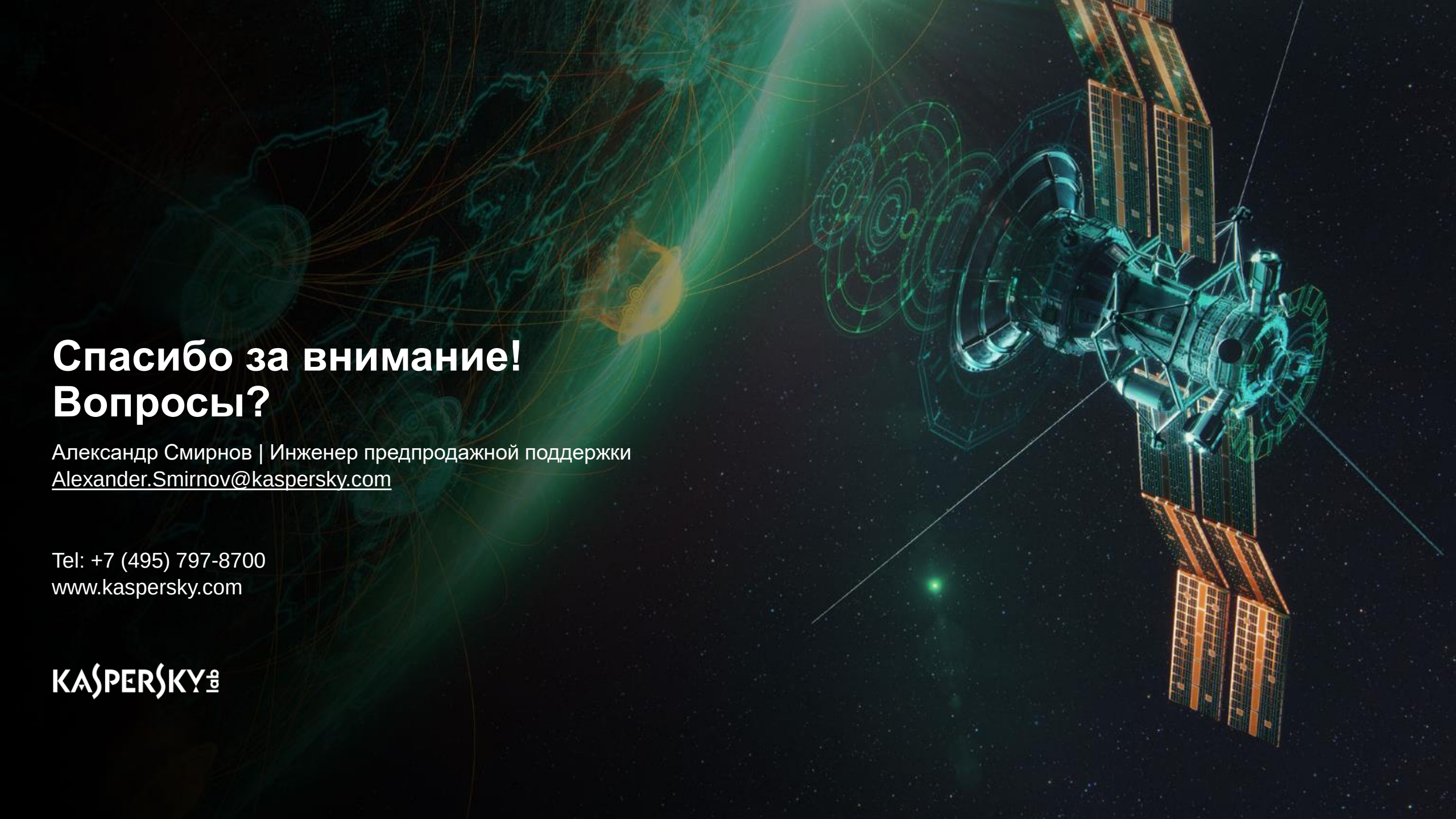
Благодаря возможности использования любого типа политик безопасности, возможно использовать KasperskyOS для любых задач. Разработав один раз политику для приложения или модуля, ее можно использовать вновь в будущем



БЕЗОПАСНАЯ

Благодаря разделению функций безопасности и функциональной части приложения, возможна параллельная работа над этими частями, что экономит время. Позволяет улучшить функциональную безопасность системы за счет использования политик безопасности, в которых описан алгоритм работы


Объект КИИ
Корпоративная IT-инфраструктура
Закрытый сегмент
KSN
Kaspersky Security Network
Kaspersky Security для бизнеса
Kaspersky Security для файловых серверов
Kaspersky Security для мобильных устройств
HYBRID
Kaspersky Security для виртуальных и облачных сред
Kaspersky Private Security Network
Корпоративный центр ГосСОПКА
Kaspersky Embedded Systems Security
ГосСОПКА (НКЦКИ)
IRP
SIEM
Kaspersky Security Center
Kaspersky Fraud Prevention
АСУ ТП
Kaspersky® Industrial CyberSecurity
Kaspersky Threat Intelligence
Kaspersky Anti Targeted Attack Platform
Kaspersky Security для интернет-шлюзов
Kaspersky Security для почтовых серверов
Kaspersky DDoS Protection
Kaspersky Cybersecurity Awareness



Спасибо за внимание!
Вопросы?

Александр Смирнов | Инженер предпродажной поддержки
Alexander.Smirnov@kaspersky.com

Tel: +7 (495) 797-8700
www.kaspersky.com

KASPERSKY lab