kaspersky 25 лет

Защита от массовых и продвинутых угроз

Алексей Киселев

Руководитель отдела по работе с клиентами среднего и малого бизнеса

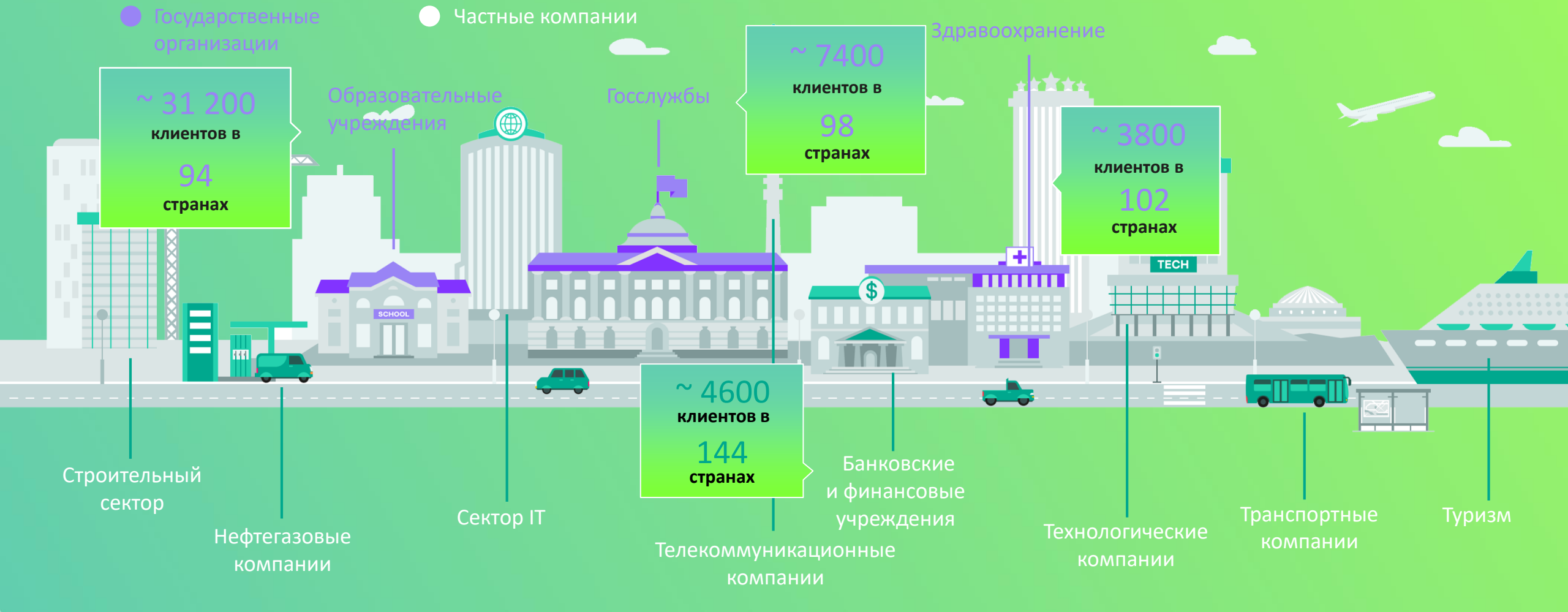
1.

О компании

Глобальный охват, признанная экспертиза

>240 000
корпоративных клиентов по всему миру

>400 000 000
защищенных пользователей по всему миру



2.

Состояние кибербезопасности за последний год

Новая реальность

Неопределенность. Больше рисков. Поиск решения

Интерактивная карта киберугроз

Подробнее

Рост количества атак и их усложнение

Количество и сложность киберинцидентов в российских компаниях растут. Рост 2021 vs 2022 составил **+300%***

Киберагрессия

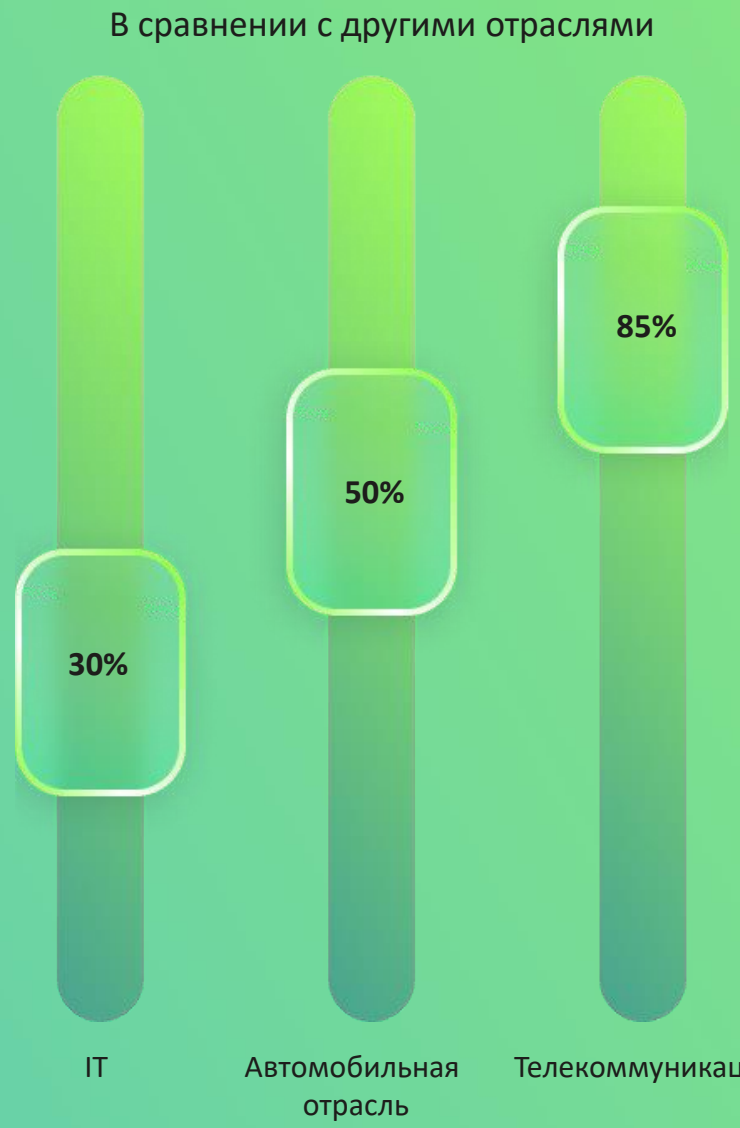
Россия номер 1 в мире по количеству атак

Киберугрозы для всех

Атакам сегодня подвержены компании любого размера из любой отрасли

* По данным центра реагирования на инциденты «Лаборатории Касперского»

Киберпреступность превратилась в полноценную индустрию со множеством участников



Общегодовой доход:

1,5 трлн

долл. США[1]

[1] CSO Online
[2] Yahoo Finance

Организация атаки не требует ни больших вложений, ни технических навыков

0–5000 долл. США[1]

- RDP
- VPN
- Учетные данные

10–150 долл. США[3]

- RDP
- VPN
- Учетные данные

200–3500 долл. США[2]

- Фишинг
- Шифровальщик
- Банковский троянец

1–30 долл. США[3]

- Вредоносное ПО
- Фишинг
- Взлом учетных записей

[1] «Лаборатория Касперского»
[2] CSOOnline
[3] Top10VPN

А ущерб от атаки может быть очень серьезным

Расходы атакованной организации[1]

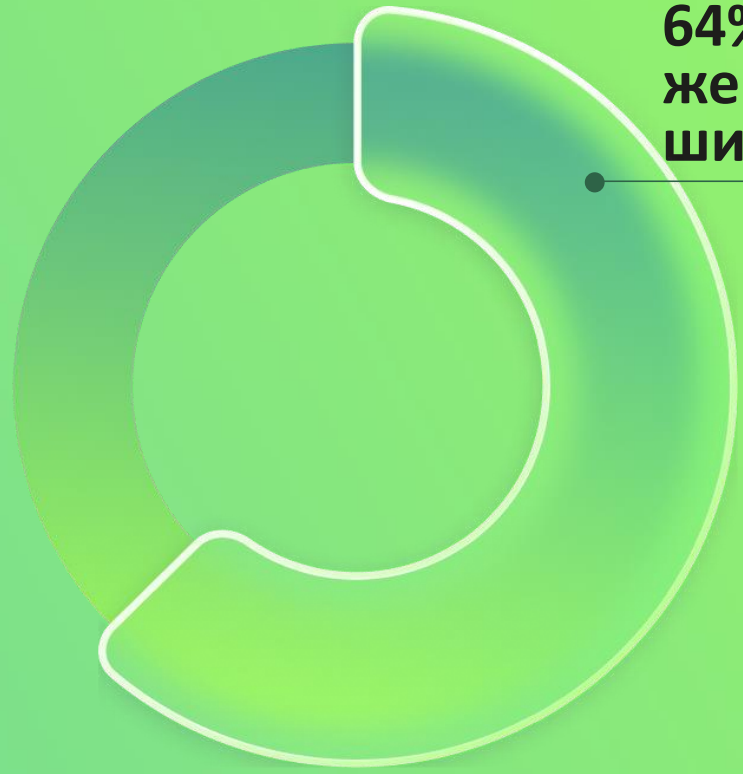
Крупные предприятия

927 тыс. долл. США

Малый и средний бизнес

105 тыс. долл. США

Главная угроза: шифровальщики[2]



64% компаний стали жертвами шифровальщиков

- Выкуп
- Помощь сторонних экспертов
- Улучшение инфраструктуры
- Повышение осведомленности сотрудников
- Пени и штрафы
- Коммерческие потери
- Выплата страховых взносов
- Ущерб репутации

[1] «Лаборатория Касперского»
[2] «Лаборатория Касперского»

СМБ под прицелом: в России увеличилось число атак шифровальщиков на небольшие компании

Обращения за восстановлением зашифрованных данных Q4vsQ3 2022: **x2**

За январь 2023 года этот показатель уже **превысил половину** количества запросов Q4 2022

Наиболее частый вектор атаки — **через службу удалённого рабочего стола** (RDP)

>400 000

попыток заражения корпоративных устройств программами-шифровальщиками в 2022 году[1]

[1] «Лаборатория Касперского»

Выплата выкупа ничего не гарантирует

Двойное вымогательство

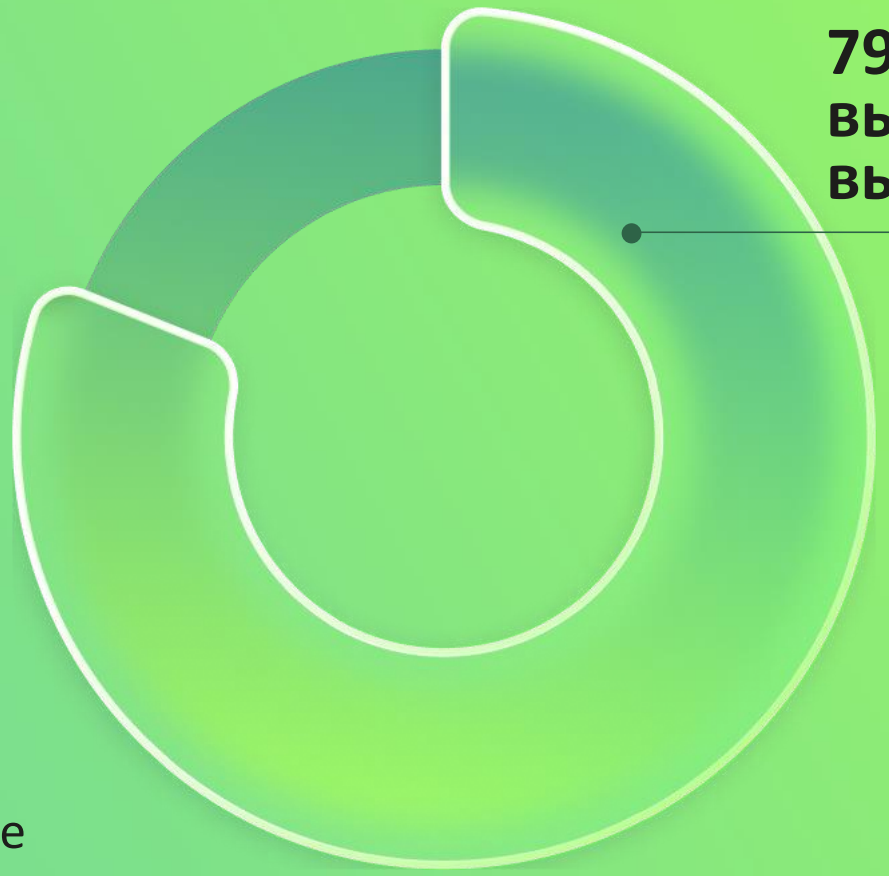
Преступники не только шифруют ваши данные, но и крадут их – и требуют выкуп за уничтожение копий

20 дней[2]

в среднем длится простой после атаки

Никаких гарантий

Злоумышленники могут так и не вернуть данные

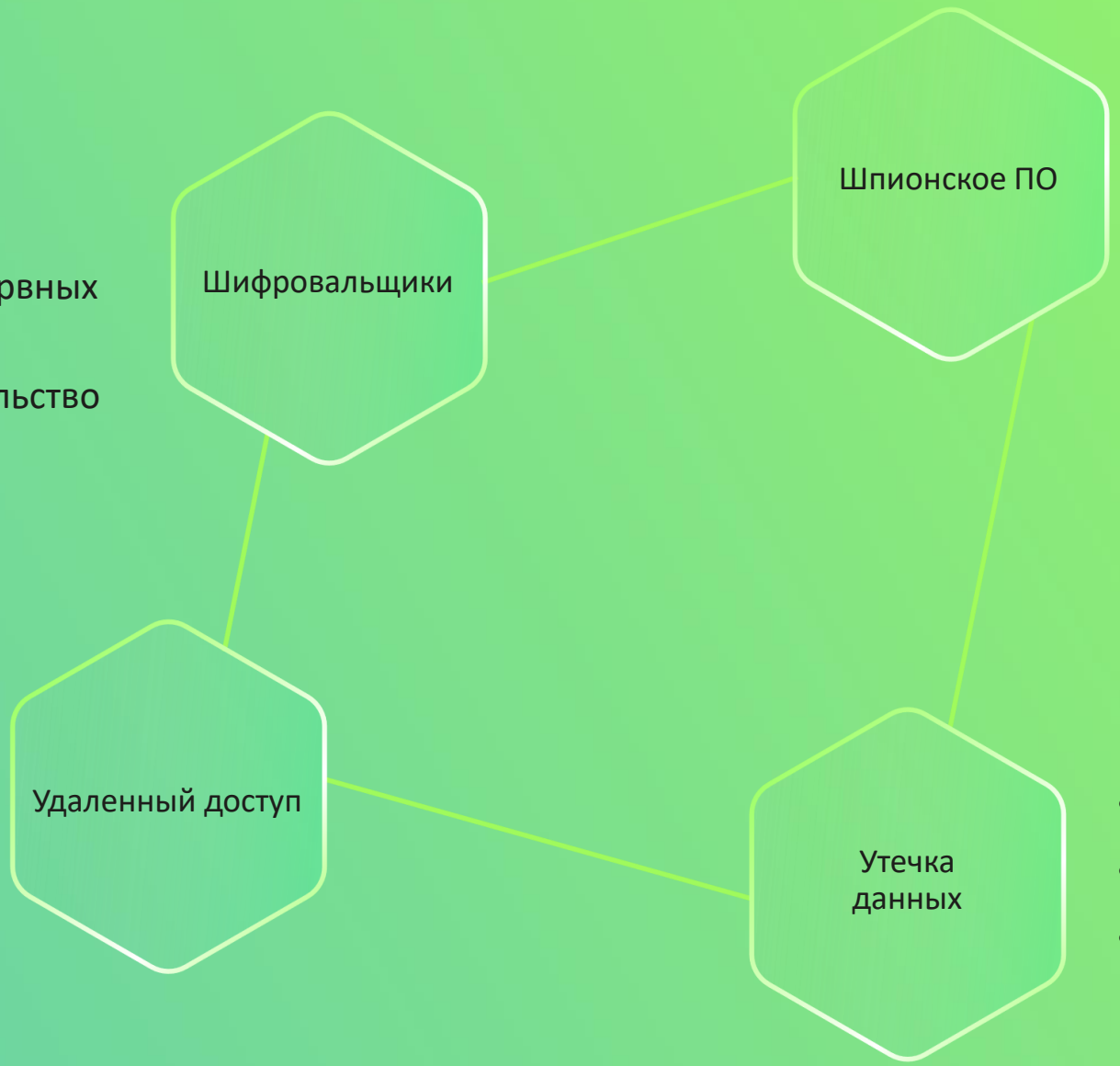


79% компаний выплачивают выкуп[1]

[1] «Лаборатория Касперского»
[2] Statista

Шифровальщики – основная угроза, но нельзя забывать и об остальных

- Шифрование
- Повреждение резервных копий
- Двойное вымогательство



- Учетные данные
- Финансовая информация
- Бизнес- и IT-процессы

Доступ к системам в будущем – злоумышленники воспользуются им сами или продадут другим

- Персональные данные
- Коммерческая тайна
- Конфиденциальная информация

Ландшафт киберугроз

38% Нарушение сотрудниками политик безопасности

5.62 среднее количество инцидентов в одной компании за год.

26% Заражение корпоративных устройств вредоносным ПО

4.28 среднее количество инцидентов в одной компании за год.

31% DDoS-атаки

4.71 среднее количество инцидентов в одной компании за год.

19% Фишинг и социальная инженерия, нацеленные на клиентов

4.71 среднее количество инцидентов в одной компании за год.

18% Таргетированные атаки (APT, «кастомизированное» ПО)

3.21 среднее количество инцидентов в одной компании за год.

% компаний, столкнувшихся с киберинцидентами, и среднее количество таких инцидентов в России за последние 12 месяцев.

Источник: Данные опроса Kaspersky, 2022 Anti-Malware

Киберпреступники все лучше обходят системы защиты

Идентифицируемые характеристики постоянно меняются.

Использование легитимных системных инструментов для атаки.

Проникнув в инфраструктуру, злоумышленники долго бездействуют, чтобы остаться незамеченными.

Многокомпонентное вредоносное ПО позволяет совершить атаку, даже если один из компонентов будет удален.

[1] Living-off-the-land – атака посредством легитимных инструментов

3.

Как мы можем помочь

Типы угроз

Массовые

Наиболее распространены

Простое обнаружение

Легко устраняются

Решение:

- Автоматическое предотвращение
- Усиление защиты (system hardening)

Скрытые

Легко найти в даркнете

Избегают обнаружения

Значительные последствия

Решение:

- Различные механизмы обнаружения
- Прозрачность, анализ и реагирование

Продвинутые

Часто – целевые атаки

Сложны в обнаружении

Многовекторные и устойчивые

Решение:

- Продвинутые технологии обнаружения
- Глубокое расследование

Система защиты конечных точек (EPP [1])

Против угроз: Массовых

- Критически важная часть корпоративной ИБ
- Уменьшение поверхности атаки и усиление защиты (system hardening)
- Автоматическое предотвращение и обнаружение угроз
- Автоматическое устранение угроз

[1] Endpoint Protection Platform

Но такие инструменты не предназначены для защиты от скрытых угроз

Низкая прозрачность

Что произошло – и на каких хостах?

Сложный анализ

Как мне проанализировать угрозу и найти первопричину?

Медленное реагирование

Как мне быстро провести реагирование и ничего не сломать?

Высокий риск

Endpoint Detection and Response

Против угроз: Скрытых Продвинутых

Продвинутые технологии обнаружения

Прозрачность угроз и инфраструктуры

Инструменты для расследования угроз

Быстрое и точное реагирование

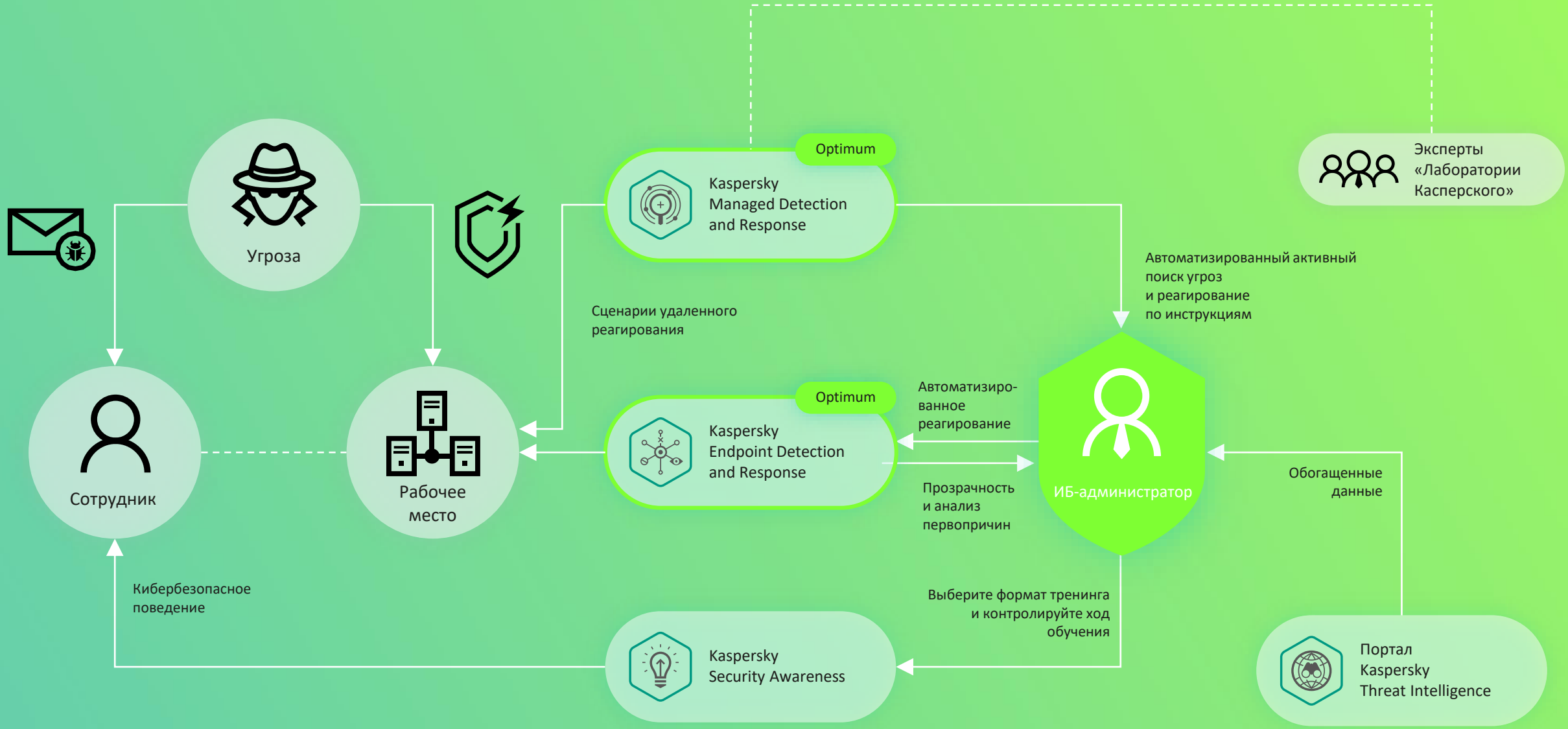
Когда используется EPP, а когда - EDR

Критерий	EPP	EDR
Класс угроз	Массовые	Скрытые и продвинутые
Ключевая цель	Автоматически защищать от постоянного потока угроз	Найти и обезвредить более сложные атаки
Ключевое действие	Предотвращение	Анализ и реагирование
Время использования	Защита в реальном времени	Расследовать и устранить активные атаки
Участие человека	Минимальное наблюдение	Активное участие
Обнаружение	Автоматическое детектирование	Продвинутое детектирование и обнаружение угроз, которое сложно найти обычными средствами
Контекст угрозы	Фокусируется на автоматической защите и не показывает контекст угрозы	Помогает службе ИБ получить полные данные об атаке и проанализировать их
Реагирование	Автоматическое устранение обнаруженных угроз	Автоматизированное и ручное реагирование на угрозы, которые невозможно нейтрализовать автоматически

Современная защита конечных точек

Kaspersky Optimum Security защитит вашу компанию от скрытых угроз

Предотвращение угроз и борьба с ними на разных уровнях



Существует несколько направлений защиты рабочих мест

Используйте надежные инструменты для предотвращения инцидентов и сокращения поверхности атаки.

Анализ угроз помогает определить их первопричины и истинный масштаб инцидента и принять соответствующие меры.

Сформируйте культуру безопасного поведения, чтобы избежать дорогостоящих ошибок.

Получите экспертную поддержку в области поиска угроз и реагирования на инциденты

[1] Технологии обнаружения и реагирования на рабочих местах
[2] Управляемый поиск угроз и реагирование на них

2.

EDR Оптимальный

Продукт:
Kaspersky EDR для бизнеса Оптимальный

Базовый EDR: Kaspersky EDR для бизнеса Оптимальный

Продвинутая защита конечных точек

- Защита от новейших угроз, в том числе от бесфайловых вирусов
- Адаптивный контроль аномалий
- Автоматическое устранение угроз
- Развертывание в облаке или локально

Расследование

- Анализ первопричин
- Детали по инциденту
- Обогащение данными Threat Intelligence

Прозрачность

- Визуализация пути атаки
- Сканирование индикаторов компрометации
- Единая карточка обнаружения

Реагирование

- Рекомендации по реагированию
- Реагирование «в одно нажатие» и автоматическое реагирование
- Сетевая изоляция, запрет запуска, карантин

Связанные продукты и сервисы:

- Kaspersky MDR Optimum
- Kaspersky Symphony

Расширенное обнаружение

Поведенческий анализ

Алгоритмы машинного обучения выявляют прежде неизвестные шаблоны поведения на ранних стадиях выполнения программы.

Умные записи

Некоторые свойства проанализированных файлов пропускаются через тщательно отлаженное дерево принятия решений, чтобы выявить вредоносные особенности.

Kaspersky Security Network

Доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения ускоряет обнаружение подозрительных объектов.

Повышенная видимость угроз

- ## Единый источник достоверной информации

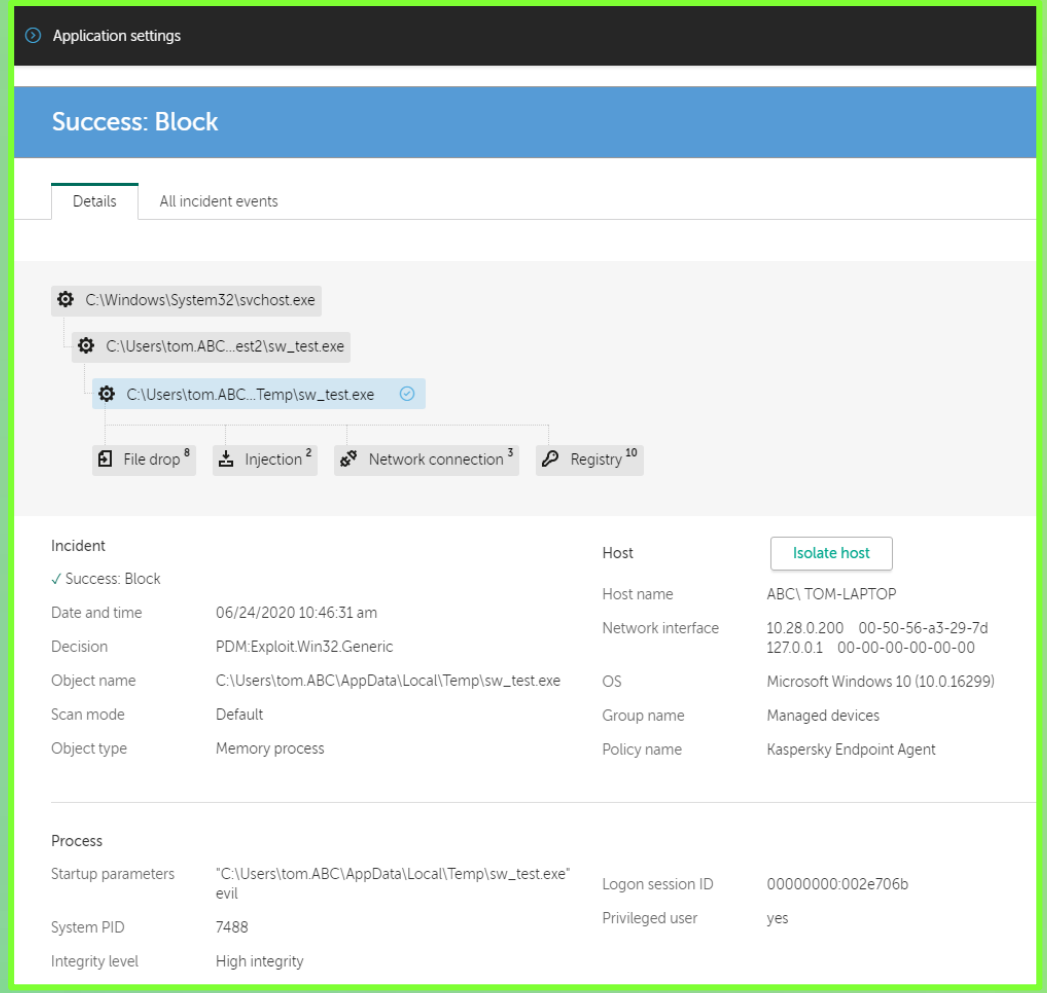
  Данные из множества источников автоматически собираются на единой карточке инцидента. Это обеспечивает скорость и эффективность анализа без использования множества разных инструментов.

- ## Обогащение данных

  Базовые данные по обнаружениям дополняются подходящими данными о файлах, хостах, пользователях и т. д.

- ## Контекстные данные

  Для анализа отбираются актуальные контекстные данные, в том числе по сопоставлению событий, родительским процессам и истории ответных действий.



Анализ первопричин

- ## Где?

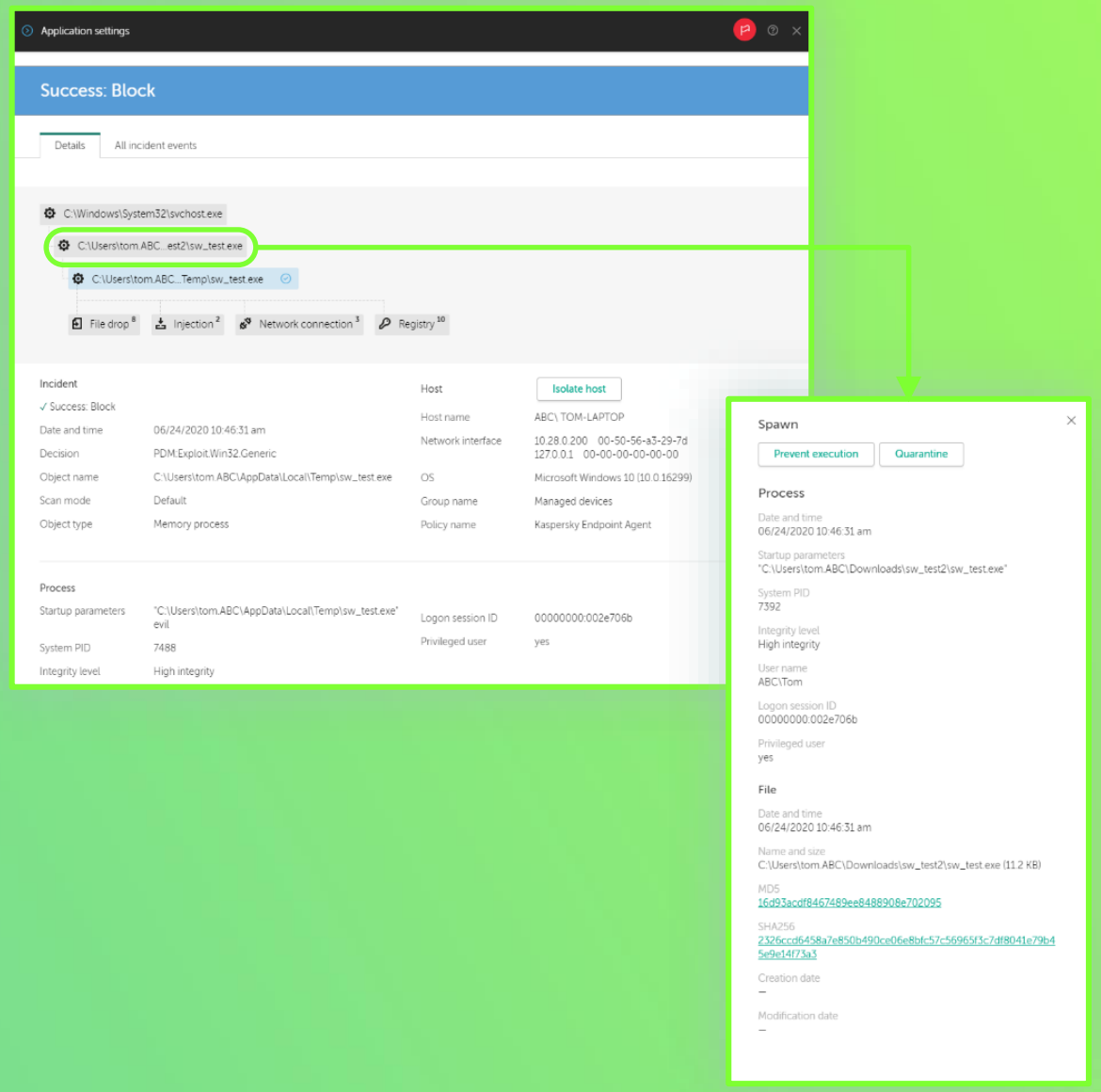
  Обогащенные данные об обнаружении дают комплексную и точную картину инцидента: что, на каком хосте и у какого пользователя произошло.

- ## Как?

  Автоматически создается дерево процессов, позволяющее быстро увидеть и проанализировать, как угроза развивалась на хосте, и установить ее первопричину.

- ## Что?

  Используя все доступные данные и инструменты визуализации, вы можете установить первопричину угрозы и определить, нужны ли какие-то дополнительные меры реагирования.



Проверка всех конечных устройств

Выявление текущих угроз

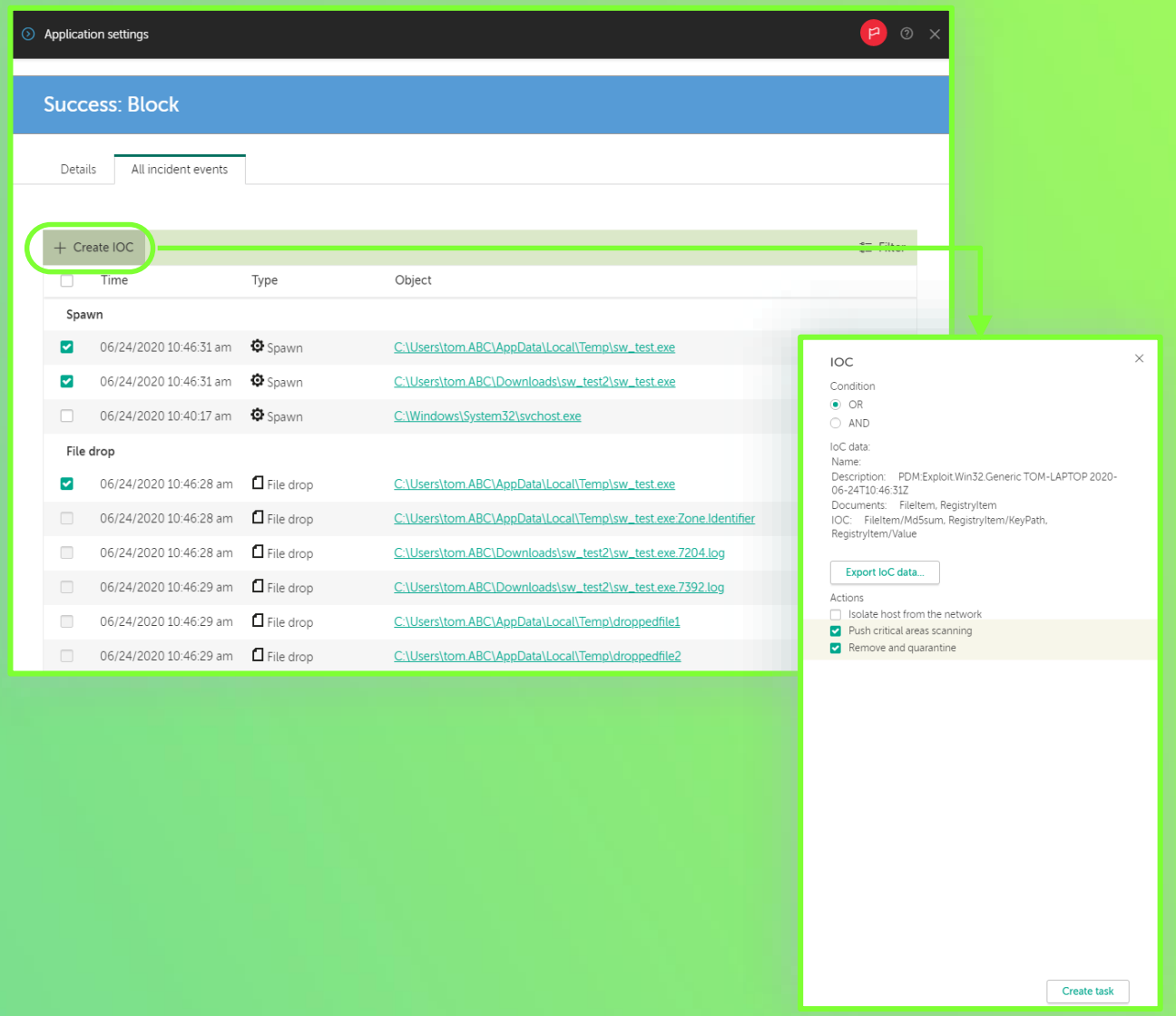
Импорт индикаторов компрометации из доверенного источника и проверка всех хостов, чтобы обнаружить текущие маскирующиеся угрозы, которые могут скрываться на конечных устройствах.

Определение масштаба инцидента

Создание индикатора компрометации для проанализированного оповещения за несколько кликов
и поиск схожих угроз, чтобы установить истинный масштаб выявленной атаки

Быстрое обнаружение угроз

Проверка по запросу, позволяющая обнаружить текущие угрозы, или проверки по расписанию



Автоматизированное реагирование

Реагирование в один клик

Реагирование в один клик прямо из карточки инцидента и незамедлительные действия по проанализированным угрозам

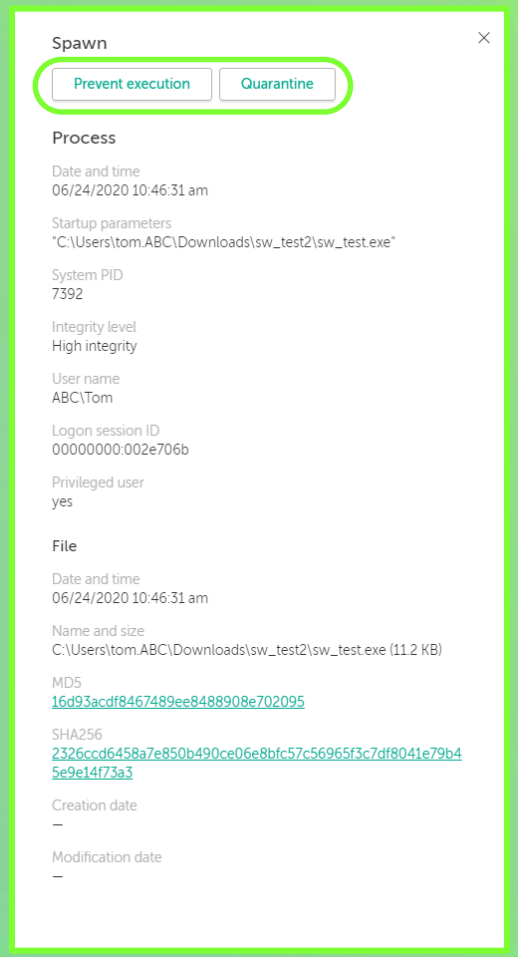
Автоматизированное реагирование

Настройка автоматизированного реагирования с помощью простой установки флажков напротив нужных действий, которые будут выполняться в случае обнаружения индикаторов компрометации при проверке

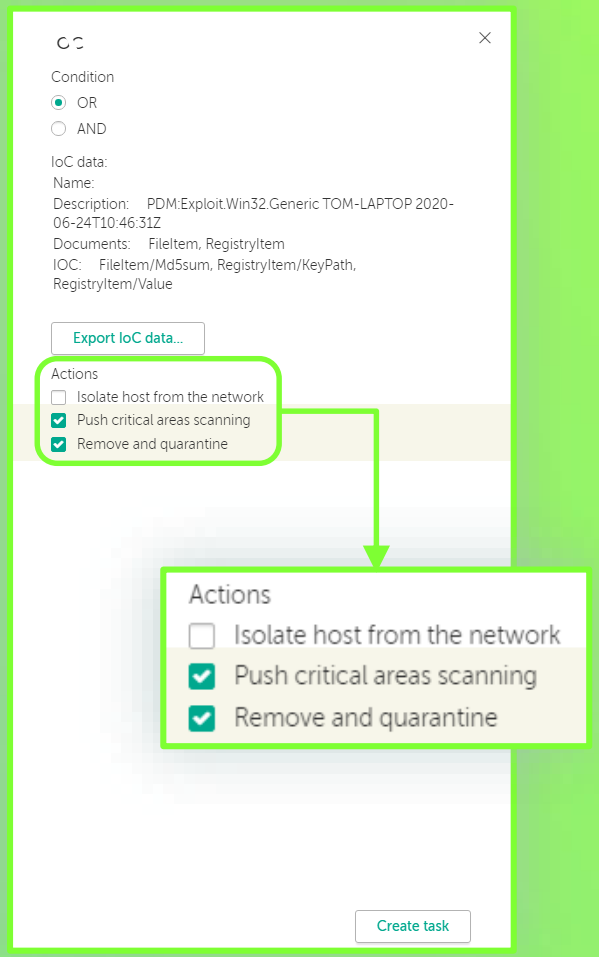
Варианты реагирования

- Изоляция хоста
- Отправка файла на карантин
- Проверка критичных областей
- Предотвращение выполнения файла

На основе карточки инцидента



На основе поиска индикаторов



Новые возможности

Рекомендации по реагированию

Доступны прямо в карточке инцидента – вы сможете быстро принять ответные меры!

Аналитические данные в карточке инцидента

Содержат данные Kaspersky Threat Intelligence о репутации файлов – это сокращает время и повышает точность анализа первопричин.

Качество данных

Можно исключить воздействие на критически важные системные объекты

Мифы о EDR

Миф: EDR сложный и затратный

Часть 1

Недостаточно персонала

Миф:

Нам нужен отдельно выделенный человек – настоящий эксперт с глубоким знанием ИБ

Реальность:

На самом деле да, желательно иметь хотя бы базовые навыки ИБ, понимать что такое цепочка атаки и индикатор компрометации.
Однако, это зависит от компании и Ваших целей.
Выбранное EDR решение должно помогать специалистам обучаться через рекомендации и простой интерфейс.

Часть 2

Сложное решение

Миф:

EDR решения слишком сложные и требуют больших затрат времени и ресурсов

Реальность:

- Поддерживает любую инфраструктуру
- Единый агент
- Низкое влияние на производительность
- Автоматизированные сценарии работы

Базовый EDR не сложнее любого другого ИТ-инструмента,
а Экспертный понадобится, когда у Вас уже будет время и ресурсы.

Миф: EDR это только для крупного бизнеса

Часть 1

Сложные угрозы

Миф:

Нужен для защиты от сложных угроз, которые актуальны только для больших компаний

Реальность:

- Помогает защититься от различных типов угроз
- Скрытые угрозы атакуют даже малый бизнес

Часть 2

Высокая цена

Миф:

У нас нет бюджета ни для чего кроме антивируса

Реальность:

Мы предлагаем единое решение с простой модернизацией – построенное на нашем EPP

Часть 3

Затратно по времени

Миф:

Специалист не может себе позволить тратить на это время

Реальность:

Правильный инструмент наоборот экономит время, которое иначе пришлось бы тратить на расследование в ручную.
А автоматизация и реагирование сразу на группу ПК помогает быть ещё эффективнее.

Что останавливает заказчиков в России от внедрения EDR

8% Непонятная функциональность

Быстрое расследование и реагирование на обнаруженные инциденты.

16% Высокая цена и стоимость владения

Продукт входит в линейку Kaspersky Security для бизнеса, использует ту же консоль и не требует значительных ресурсов.

10% Агенты снижают производительность ПК

Используется один агент с Kaspersky Security для бизнеса других уровней.

10% Подход в целом слишком затратный и сложный

Начать строить процессы реагирования на инциденты можно с простых инструментов и подходов, а затем использовать более продвинутые.

40% Требует высокой экспертизы

Продукт прост в установке, обучении и использовании. Прямо в интерфейсе есть рекомендации и подсказки по реагированию.

16% Другое

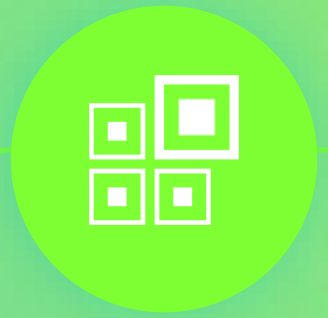
Функциональность – необходимая.
Переход с других продуктов - простой.
Затраты – минимальные.

Источник: Данные опроса Anti-Malware

Выводы о современных EDR решениях

Необходимый функционал

EDR всё больше становится стандартом в области ИБ, и без предоставляемых им возможностей трудно защищаться от скрытых, сложных и продвинутых угроз



Единая защита

EPP и EDR должны работать вместе, создавая оптимальную защиту против всех типов угроз

Разные предложения

Не существует универсального EDR предложения, т.к. у разных заказчиков – разные потребности и сценарии использования

6.

Выводы

Защита от скрытых угроз на разных уровнях

Проникновение

Заражение компьютера происходит после получения фишингового письма или посещения вредоносного интернет-ресурса.

Установка

Изначальный переносчик заражения внедряет необходимые компоненты, связывается с командным сервером[1] и изучает окружение.

Закрепление

При помощи набора инструментов, в том числе легитимных и системных средств, вредоносный объект закрепляется в системе и при необходимости начинает перемещаться по ней.

Kaspersky
Security Awaren

Kaspersky
Endpoint Detect
Response Опти

Kaspersky Optimum Security

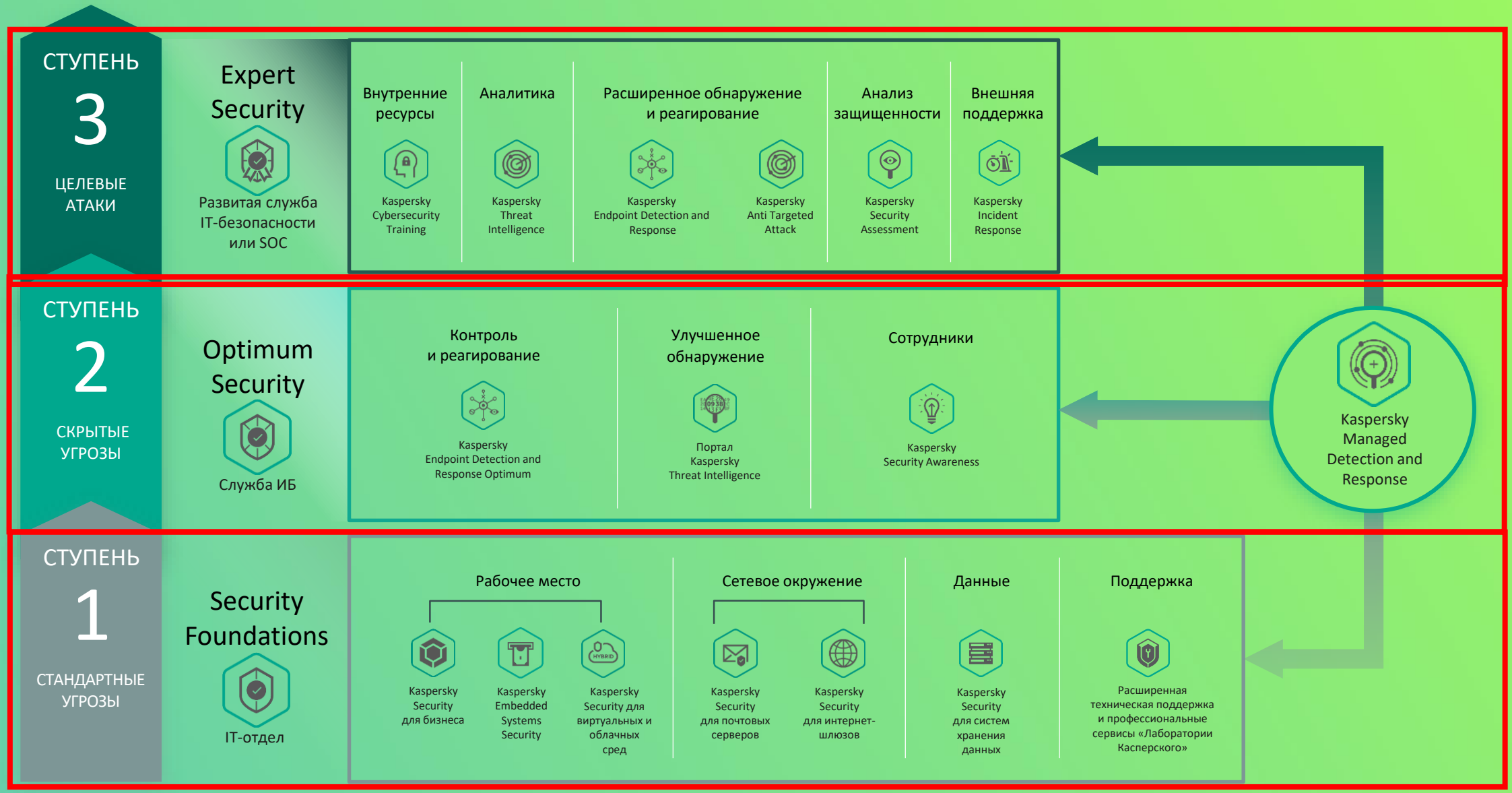
on and
альный

Kaspersky
Endpoint Detection and
Response Оптимальный

Kaspersky
Managed Detection and
Response Optimum

1 C&C, command and control
2 Индикаторы атаки
3 Индикаторы компрометации

Kaspersky Optimum Security – лишь малая часть нашего портфолио

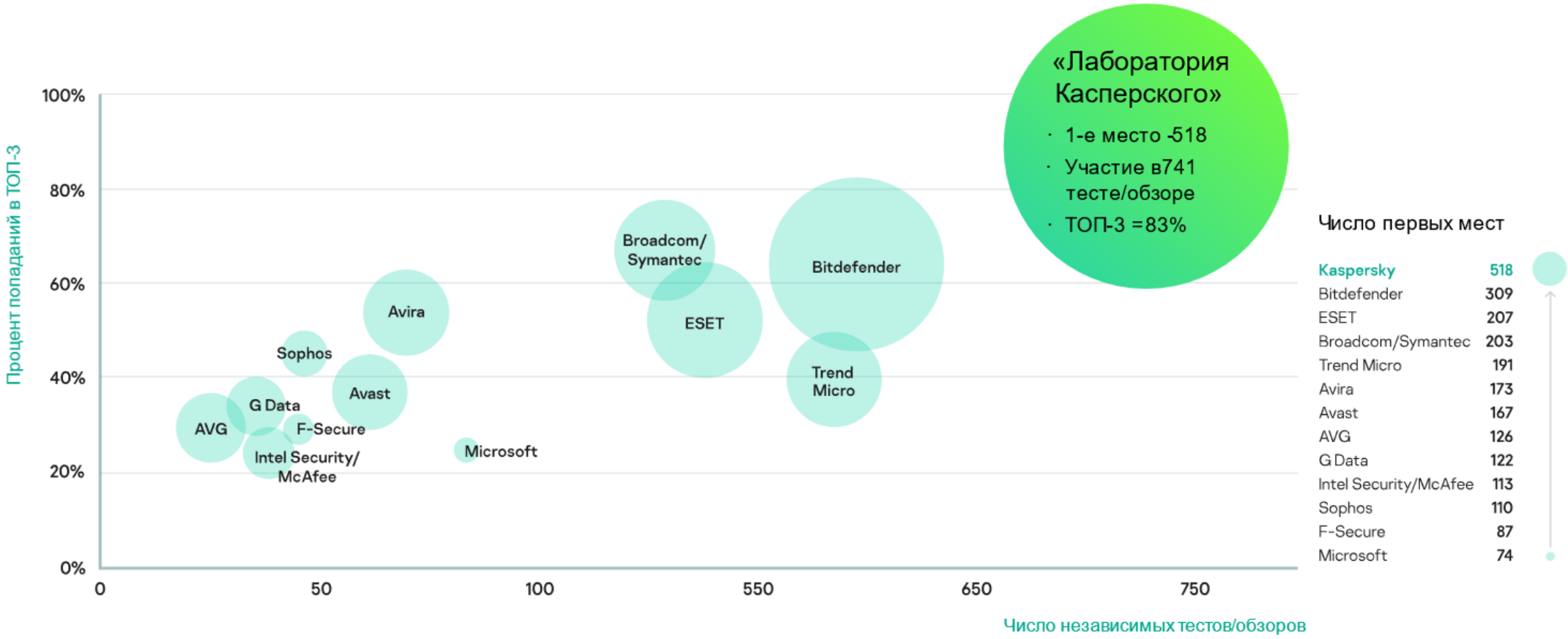


7.

Преимущества «Лаборатории Касперского»

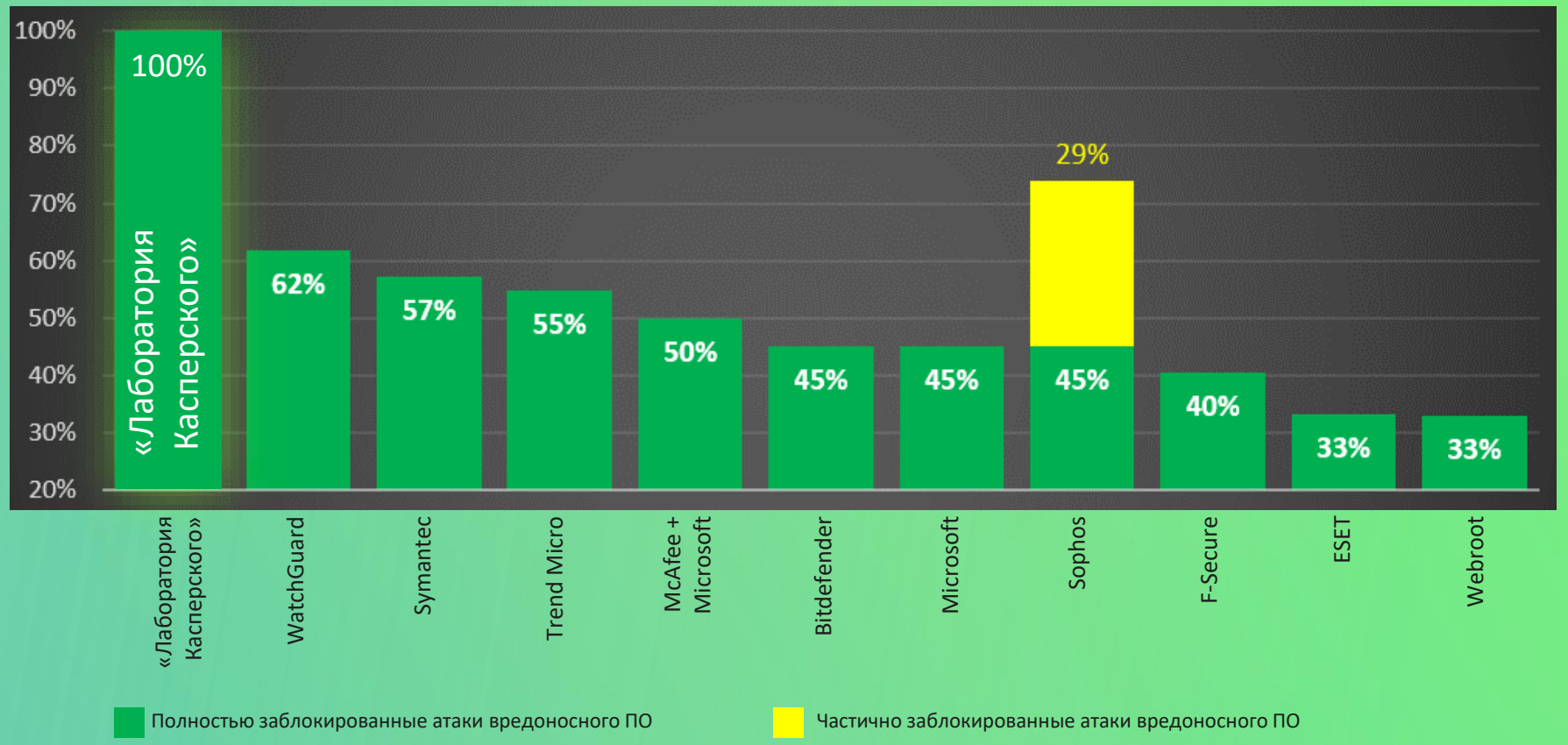
Больше тестов. Больше наград

С 2013 по 2021 г. продукты «Лаборатории Касперского» приняли участие в 741 независимом тесте и обзоре. Наши продукты завоевали 518 первых мест и 612 раз входили в тройку победителей.



Только наши защитные решения не пропустили ни одного шифровальщика в ходе тестирования, проведенного AV-Test

100%-ная защита от программ-вымогателей



Подробнее: http://kas.pr/9dv9

Наша команда

> 4500 высококвалифицированных специалистов

50% наших сотрудников – профессионалы в области R&D

40+ экспертов по безопасности мирового уровня

Уникальный опыт наших экспертов по безопасности позволяет защитить пользователей по всему миру от самых сложных и опасных киберугроз. Мы постоянно совершенствуем свои продукты, чтобы обеспечить непревзойденный уровень защиты наших клиентов.

9.

Текущие акции

Текущие акции

1

Мигрируй

Получите скидку до 40% на покупку лицензии при переходе с решений других вендоров

2

Доступная почта

При наличии или покупке одного из уровней Kaspersky Security для бизнеса или Kaspersky Endpoint Security Cloud скидка на защиту почты до 25%

3

Продление истекших лицензий

Лицензия по цене продления, если предыдущая истекла не более года назад

Мигрируй!

Подробнее

Спасибо!

alexey.kiselev@kaspersky.com

kaspersky 25 лет