kaspersky 25 лет

Защита от продвинутых угроз

Алексей Киселев

Руководитель отдела по работе с клиентами среднего и малого бизнеса

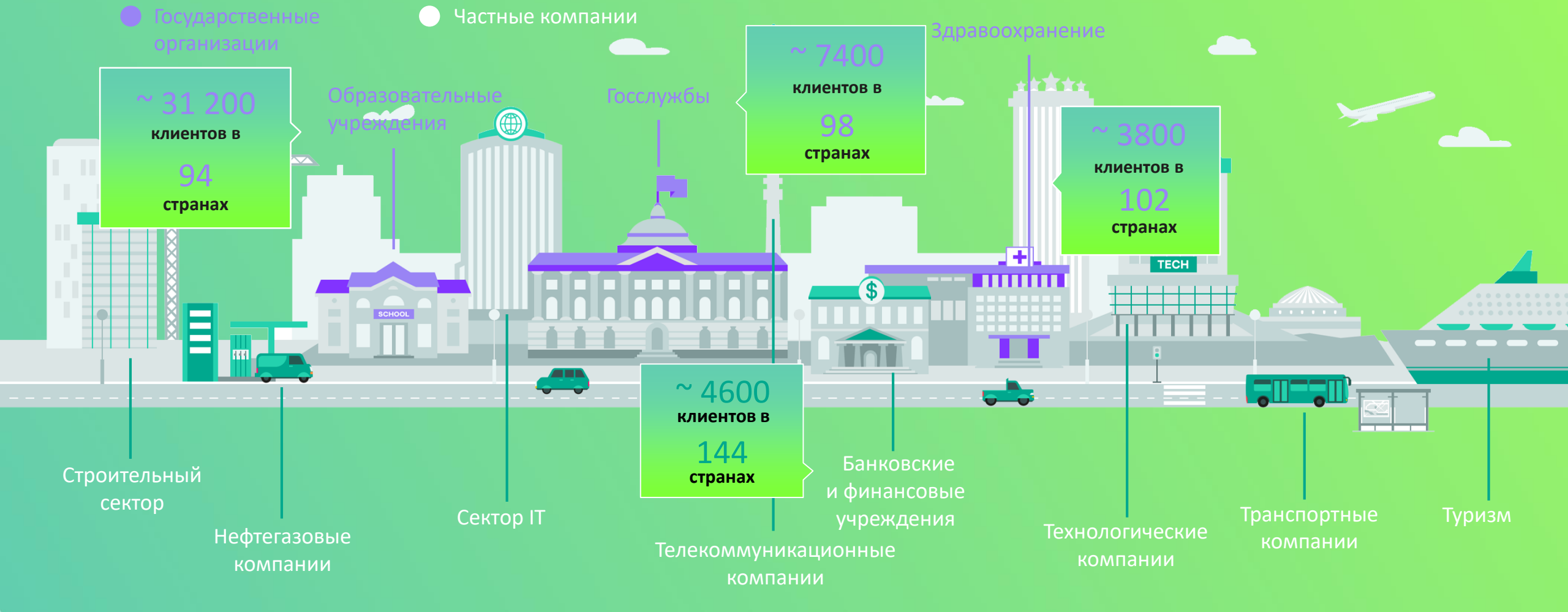
1.

О компании

Глобальный охват, признанная экспертиза

>240 000
корпоративных клиентов по всему миру

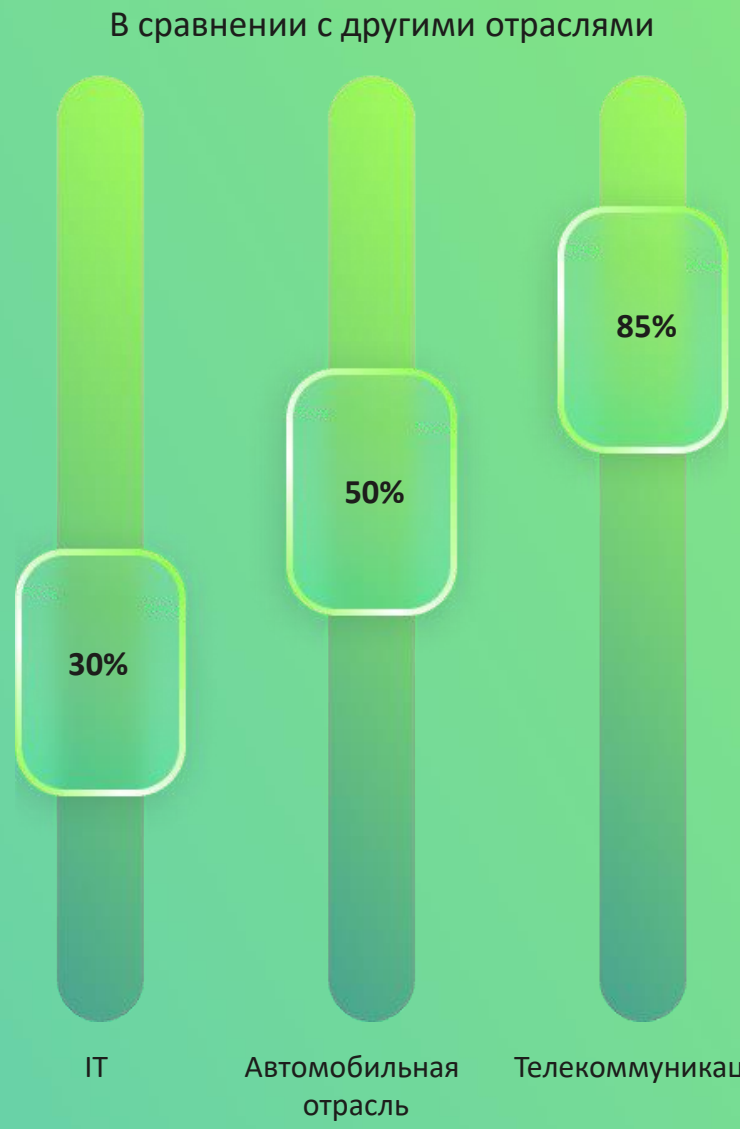
>400 000 000
защищенных пользователей по всему миру



2.

Состояние кибербезопасности в 2022 году

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]

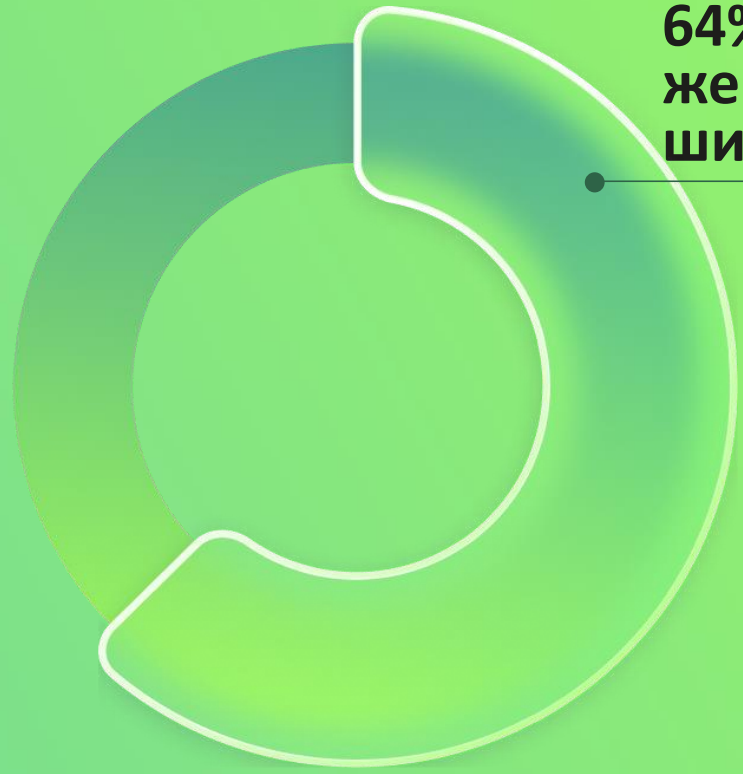
Крупные предприятия

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»

Выплата выкупа ничего не гарантирует

Двойное вымогательство

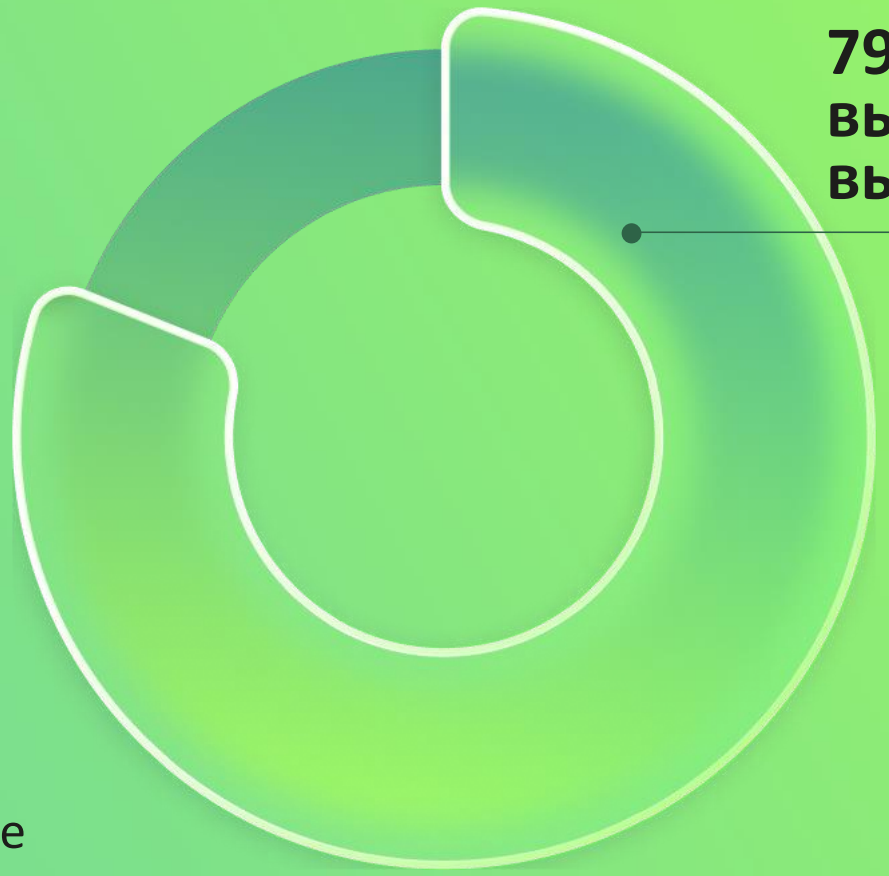
Преступники не только шифруют ваши данные, но и крадут их – и требуют выкуп за уничтожение копий

20 дней[2]

в среднем длится простой после атаки

Никаких гарантий

Злоумышленники могут так и не вернуть данные

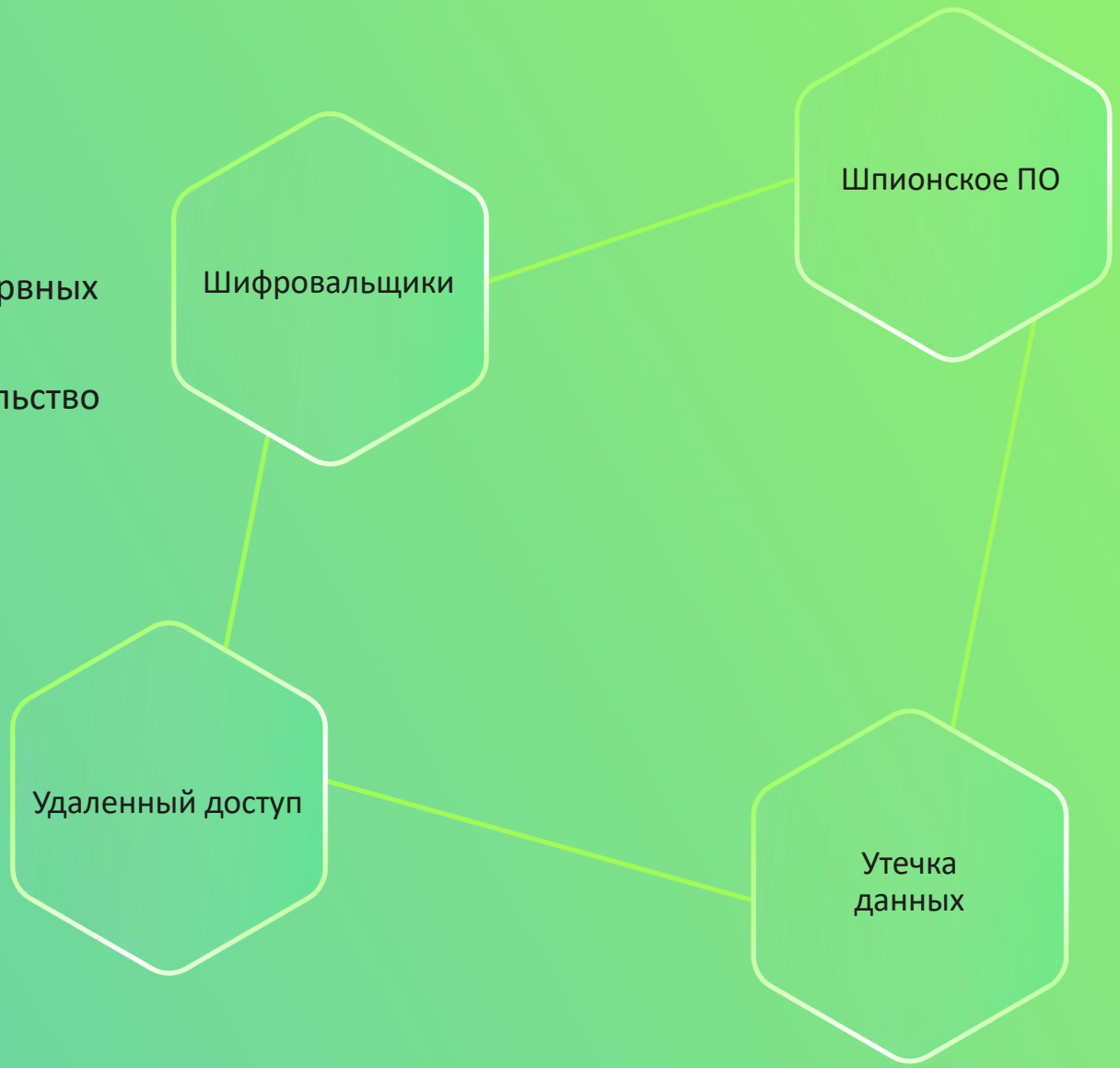


79% компаний выплачивают выкуп[1]

[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

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

Существуют разные способы борьбы со скрытыми угрозами

Контролируйте использование интернета, устройств и приложений, чтобы не подпустить преступника к инфраструктуре.

Используйте несколько методов, в том числе обнаружение на базе машинного обучения и поведенческого анализа.

Повысьте осведомленность сотрудников о киберугрозах, чтобы избежать ошибок, которые могут дорого обойтись.

Анализируйте более сложные угрозы и быстро реагируйте на них.

[1] Технологии обнаружения и реагирования на рабочих местах

Kaspersky Optimum Security защитит вашу компанию от скрытых угроз

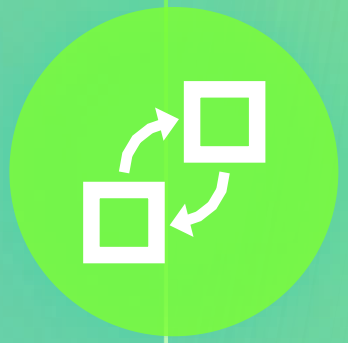
Продвинутые технологии

Сокращение поверхности атаки

Адаптивный контроль аномалий, управление установкой исправлений, контроль программ, контроль устройств и веб-контроль

Расширенное обнаружение

Поведенческий анализ на базе машинного обучения, облачная песочница, аналитика угроз



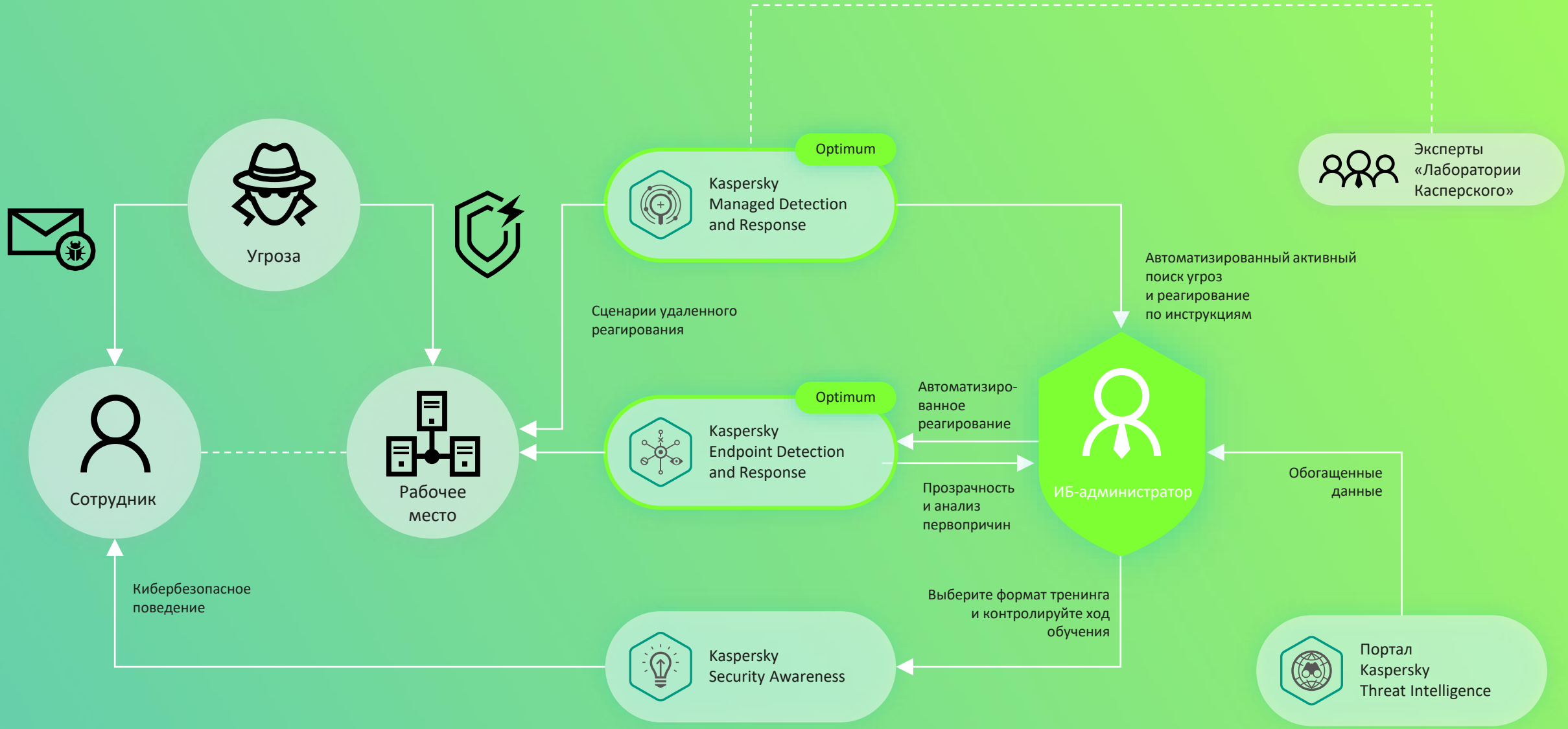
EDR/MDR

Простое EDR-решение для анализа угроз и реагирования на них и MDR-сервис для автоматизированного активного поиска угроз

Тренинги для сотрудников

Автоматизированные инструменты, позволяющие без особых хлопот развить навыки кибербезопасного поведения у сотрудников всех уровней

Предотвращение угроз и борьба с ними на разных уровнях



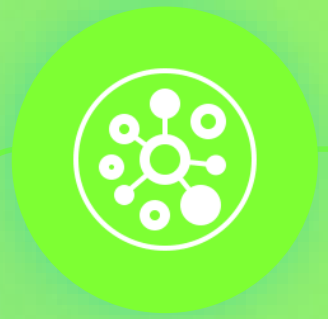
Риски для компаний, которые не используют EDR

Данные об инциденте

Если вы не знаете, как преступник проник в вашу инфраструктуру, вы остаетесь уязвимыми к подобным атакам.

Первопричина

Если вы не найдете первопричину, злоумышленники смогут воспользоваться сохраненными на устройствах компонентами и инструментами для будущих атак.



Масштаб инцидента

Скрытые компоненты могут находиться на нескольких устройствах – это не только делает их уязвимыми, но и позволяет преступникам продолжать атаку.

Пример использования: Kaspersky Optimum Security в борьбе со скрытыми атаками

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.

Повышение осведомленности сотрудников

Сокращение поверхности атаки

Автоматическое предотвращение угроз

Расширенные механизмы обнаружения, в том числе поведенческий анализ на основе машинного обучения и облачная песочница

Автоматизированный поиск угроз с помощью IoA[2]

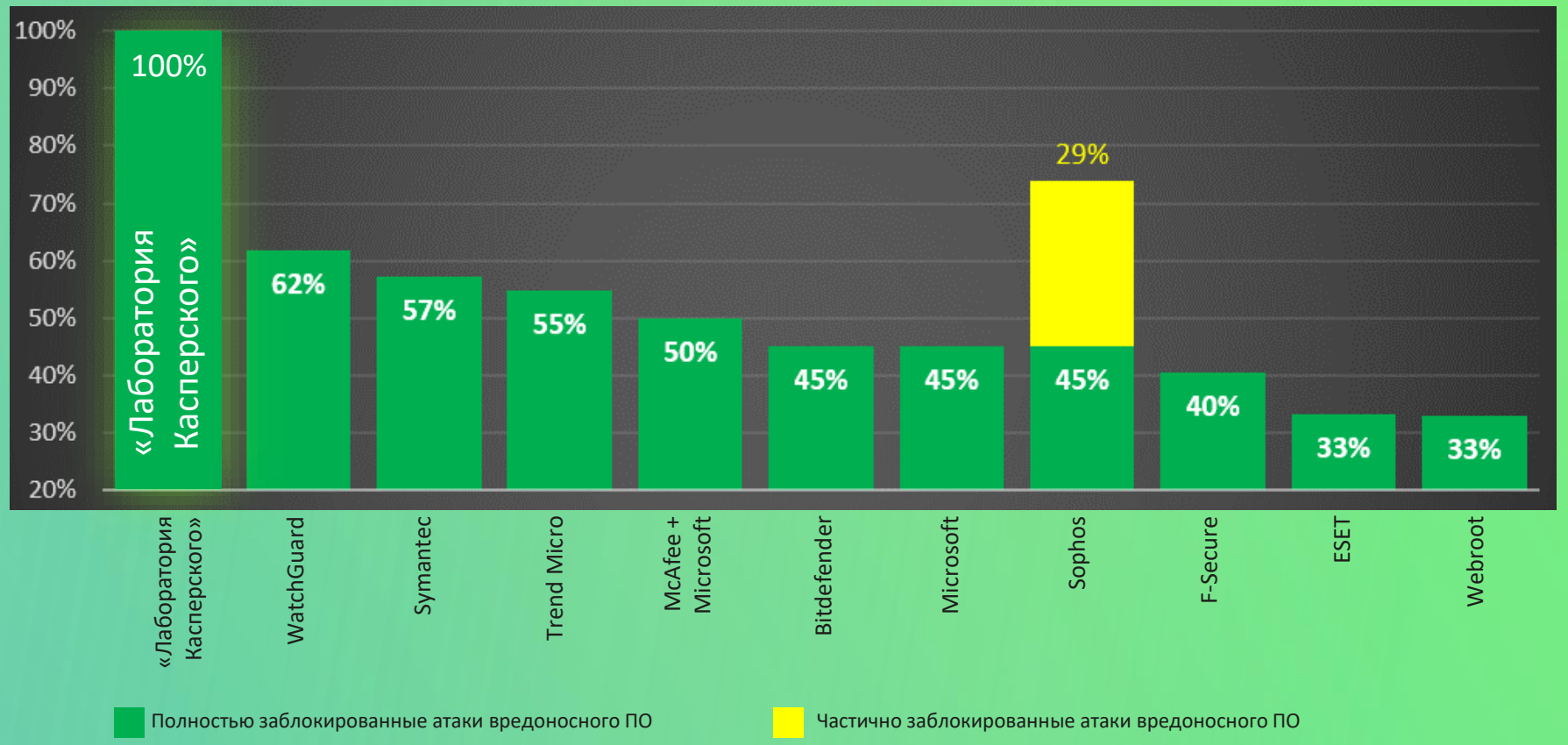
Анализ первопричин и поиск IoC[3]

Автоматизированное, удаленное реагирование и реагирование по инструкциям

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

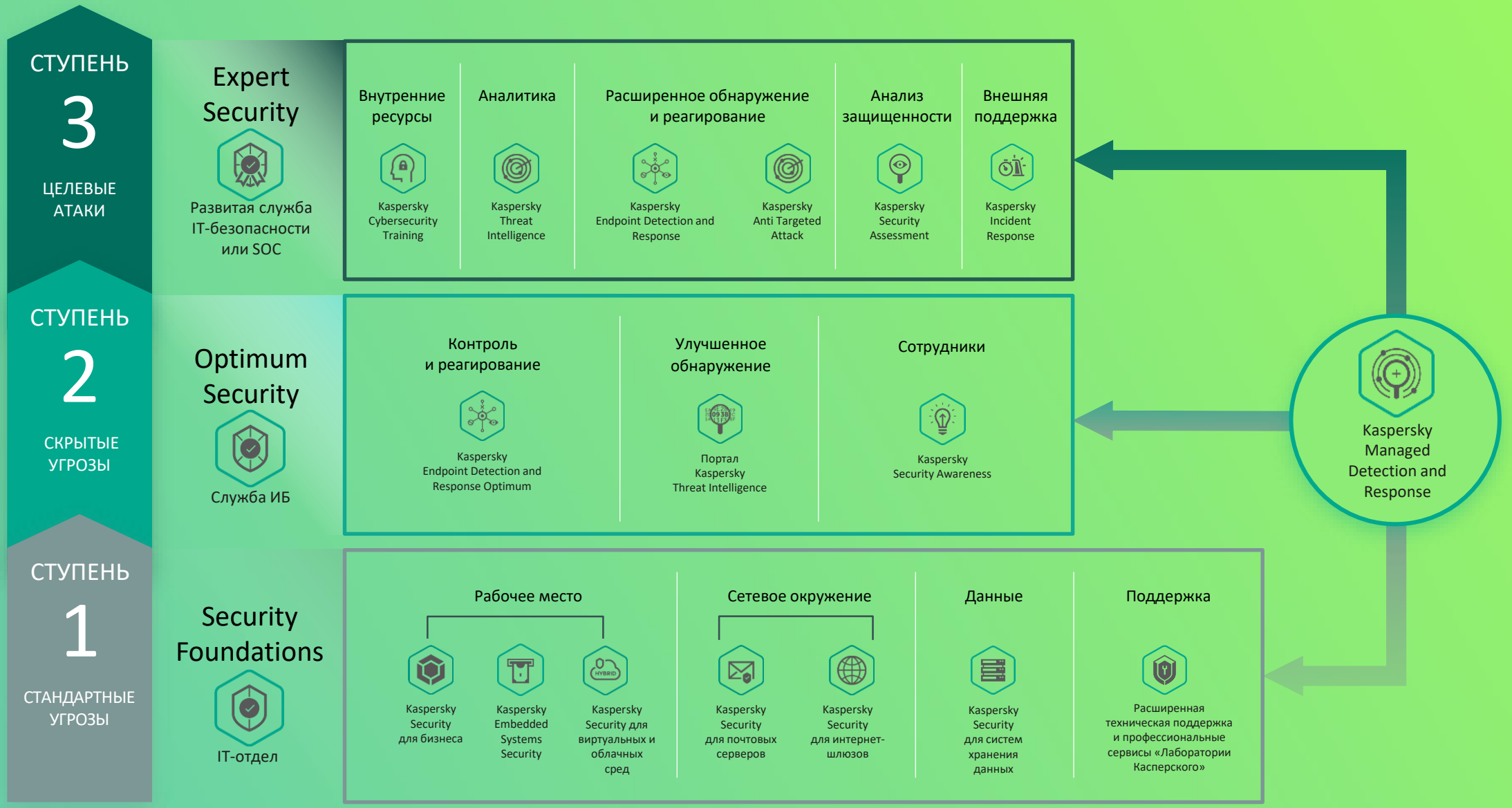
Только наши защитные решения не пропустили ни одного шифровальщика в ходе тестирования, проведенного AV-Test

100%-ная защита от программ-вымогателей



Подробнее: http://kas.pr/9dv9

Kaspersky Optimum Security – лишь малая часть нашего портфолио



5.

Ключевые выводы

Вывод № 1. Преимущества для бизнеса

Снижение рисков

Надежная защита от атак шифровальщиков, других распространенных и скрытых угроз.

Развитие бизнеса

Непрерывность и своевременность выполнения бизнес-процессов без юридических и финансовых проблем.

Экономия ресурсов

Повышение эффективности за счет простых автоматизированных инструментов или передачи управления защитой внешним специалистам.

Технологии с заделом на будущее

Какой бы вектор развития вы ни выбрали, вы всегда сможете положиться на наши продукты и опыт наших экспертов.

Вывод № 2. Технические преимущества

Защита рабочих мест

Технологии нового поколения для защиты рабочих мест сокращают поверхность атаки и автоматически блокируют угрозы.

Анализ и реагирование

EDR- и MDR-технологии позволяют расследовать скрытые угрозы и быстро реагировать на них на всех конечных устройствах.

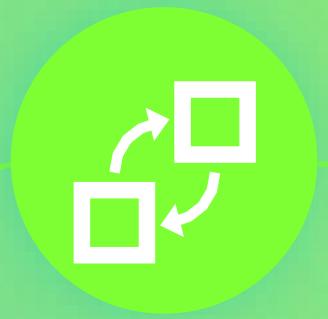
Управляемые услуги

Опыт наших экспертов и ресурсы «Лаборатории Касперского» помогут вывести защиту на абсолютно новый уровень.

Вывод № 3. Операционные преимущества

Тренинги

Наши тренинги помогут выработать у сотрудников навыки безопасного поведения, снизить риски и сформировать культуру кибербезопасности.



Развертывание

Вы сможете быстро и без труда развернуть продукты в любой инфраструктуре – облачной, локальной или гибридной.

Автоматизация

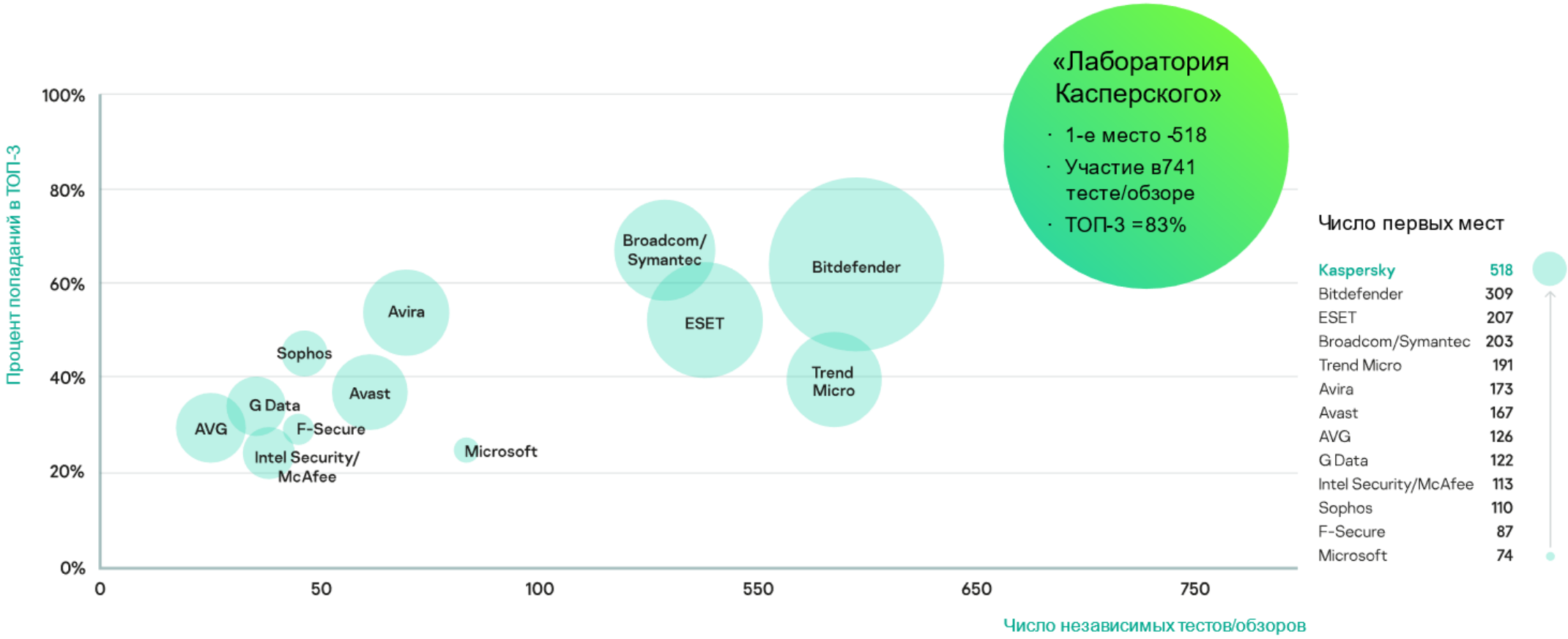
Автоматизация рутинных задач сэкономит ваше время и обеспечит самую современную защиту рабочих мест.

6.

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.



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.

Kaspersky
Optimum Security

Давайте обсудим

alexey.kiselev@kaspersky.com

kaspersky 25 лет