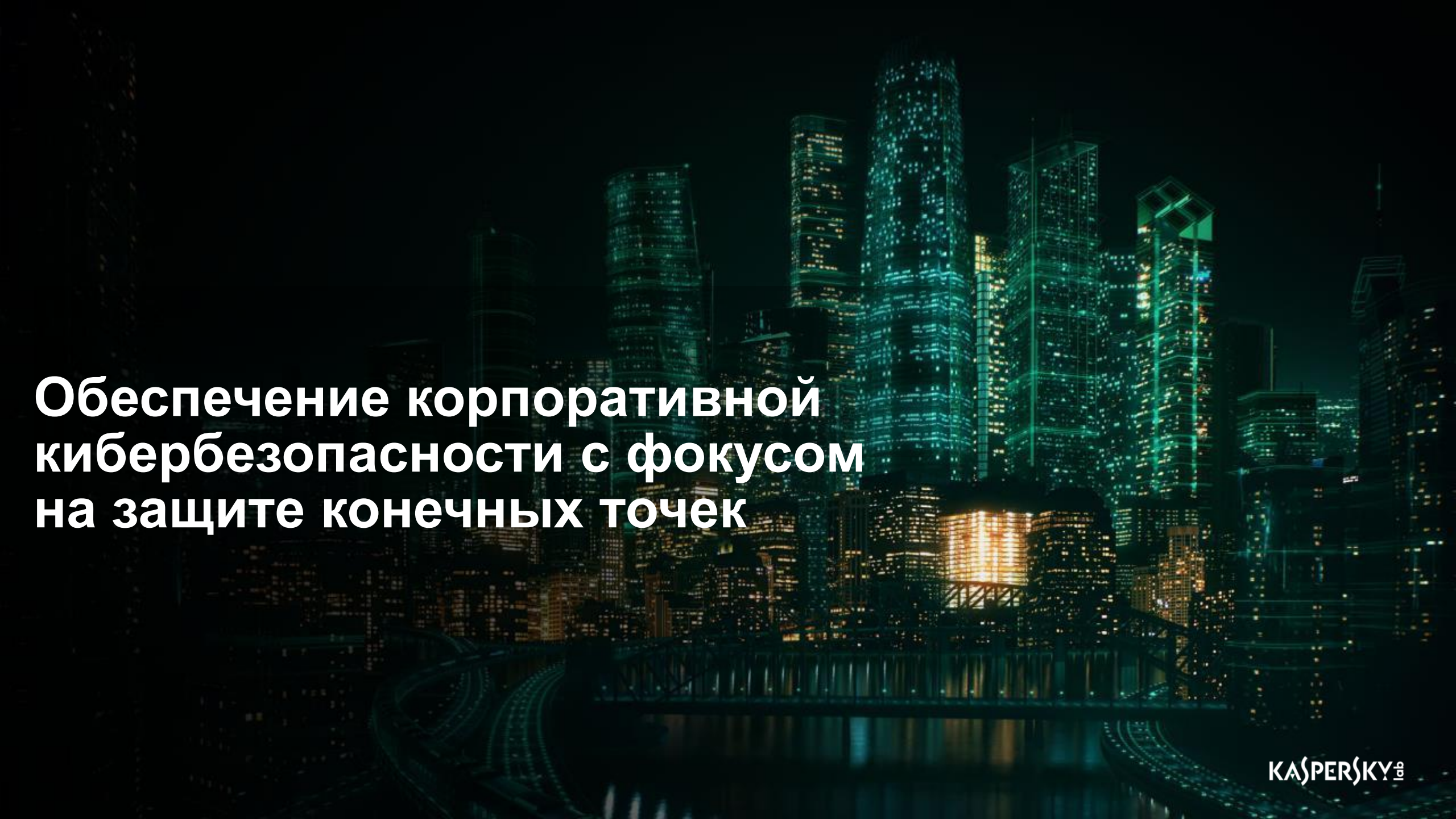


Обеспечение корпоративной кибербезопасности с фокусом на защите конечных точек

KASPERSKY lab

ЦЕЛЕНАПРАВЛЕННЫЕ КИБЕРАТАКИ: СТАТИСТИКА В РФ

В 2017 году доля целевых атак выросла на **10%** и составила **23%,** что поставило их в ряд самых стремительно развивающихся угроз*

В 2017 году каждая **4** крупная организация стала жертвой целенаправленной атаки*

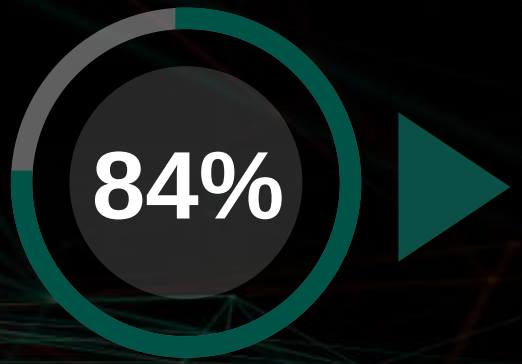
22% всех опрошенных в России компаний подозревают, что стали жертвой не случайно, а целенаправленно*

63% респондентов считают, что угрозы, с которыми они столкнулись в 2017 году, стали на порядок сложнее*

*По данным исследования «Информационная безопасность бизнеса» (Kaspersky Lab Corporate IT Security Risks Survey) аналитического агентства B2B International по заказу «Лаборатории Касперского», апрель 2017 г.

KASPERSKY lab

А нужна ли в 2019 году защита рабочих мест и серверов?



Успешных атак на конечные точки затрагивала более 1 устройства

Несанкционированный доступ даже к одному устройству может нанести огромный вред для организации

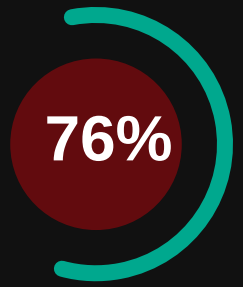
Рабочие места – первичная цель любой кибератаки

- Уязвимы к большому числу атак
- Их много и они все разные
- Есть AV ну и бог с ним
- Хранят идентификационные данные
- Начальная точка развития целевой атаки

KASPERSKY lab

**Endpoint Protection and Response: A SANS Survey, 2018*

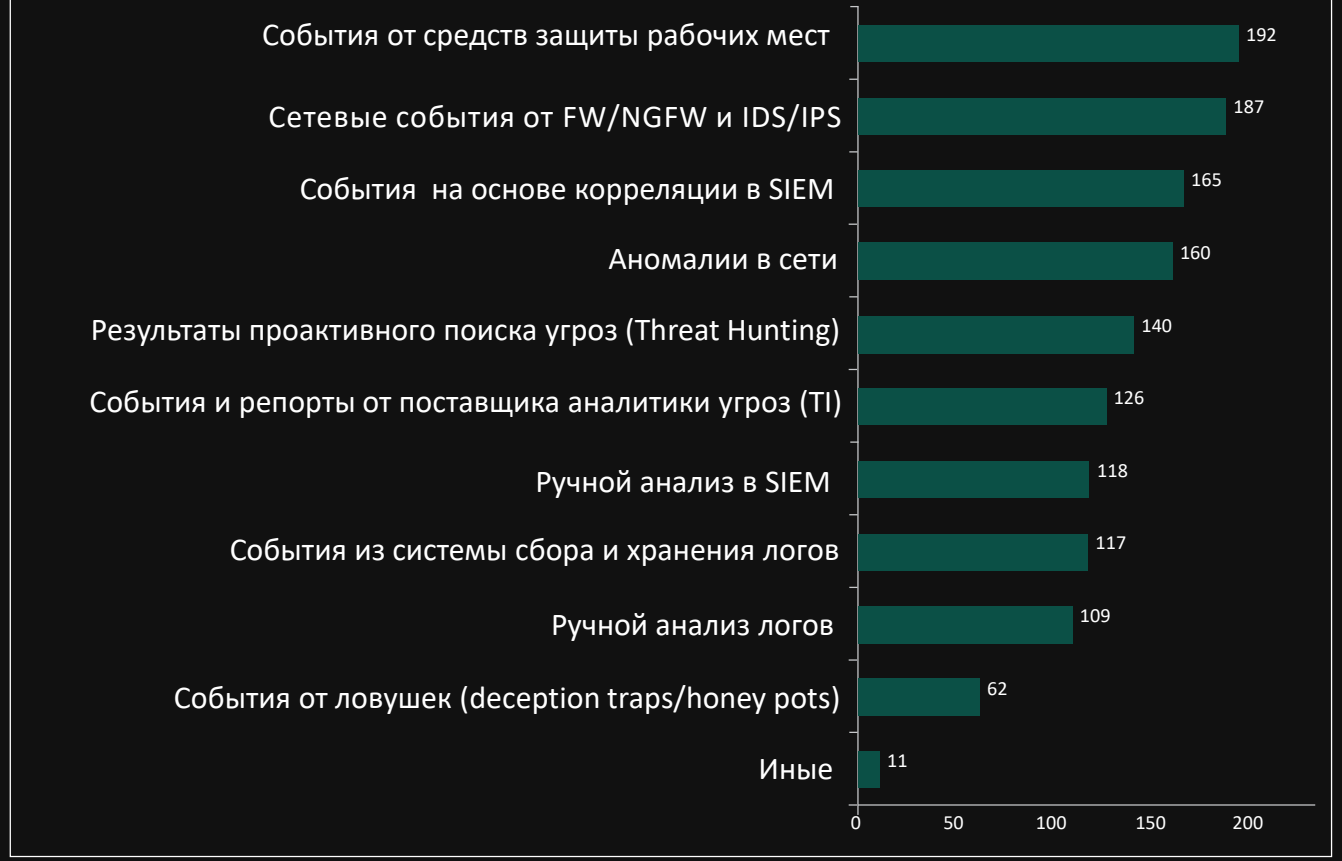
Где будут брать данные, если что-то всё же случилось?



События безопасности рабочих мест

Конечные точки являются ключевым источником данных цифровой криминалистики, необходимых для эффективного расследования, включая информацию о неизвестных файлах, а также ключевые метаданные о процессах, программах, службах, модулях, файлах, автозапуске, сетевых подключениях и временных шкалах.

Отправная точка для расследования



Source: SANS 2018 Security Operations Center Survey

Поэтапная стратегия развития корпоративной кибербезопасности

Единая долгосрочная стратегия развития кибербезопасности с учетом уровня и темпов роста компетенций в области ИБ

Блокирование максимального количества угроз в автоматическом режиме

Автоматизация передовых средств обнаружения и защиты

Развитие передовой экспертизы для комплексной защиты

Этап 1

Оценить и максимально усилить существующие превентивные технологии

Минимизировать необходимость ручного анализа

Этап 2

Выстроить максимально эффективную и удобную защиту от передовых угроз

Автоматизировать ручные операциии службы ИБ для повышения эффективности

Этап 3

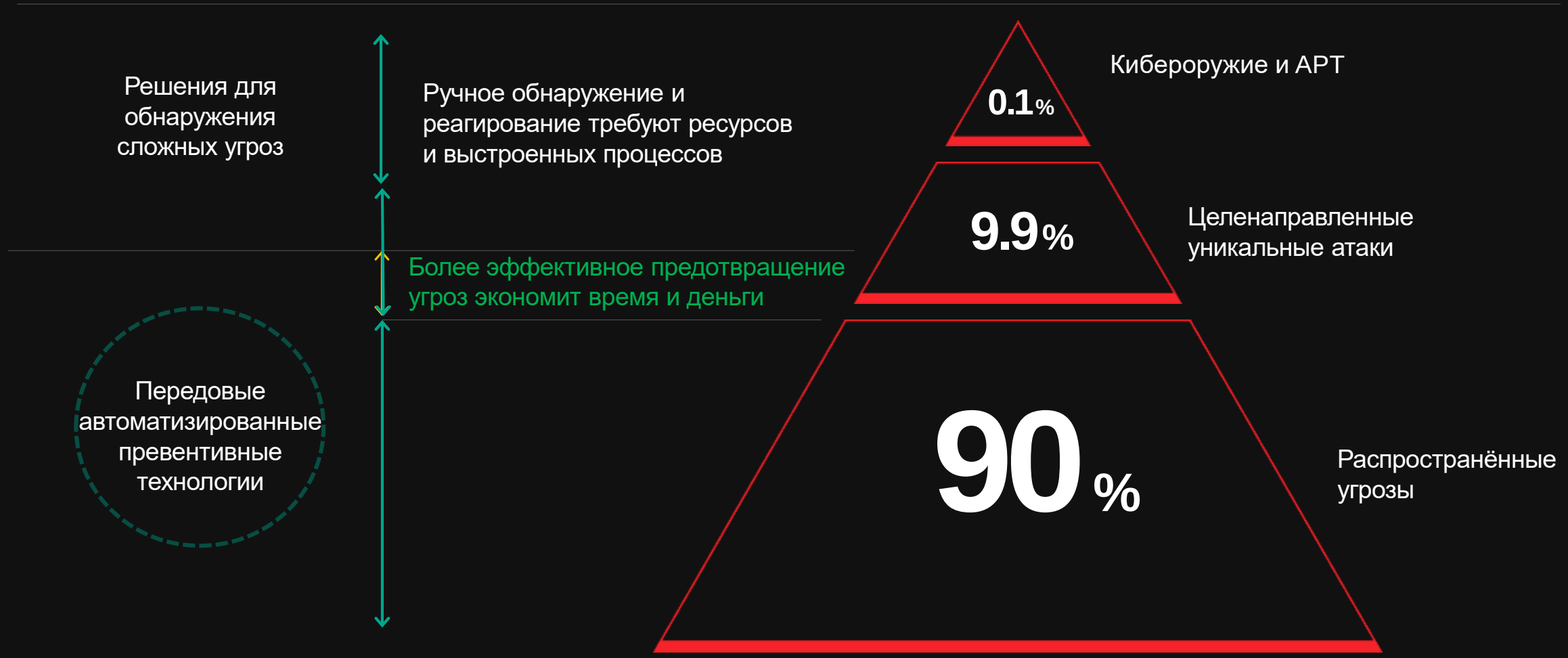
Внедрение концепции SOC, постоянного мониторинга и максимальной осведомленности о происходящем в сети

Этап 1 – заблокировать максимальное количество угроз и снизить риски

- Основополагающий этап в построении комплексной защиты
- Защита устройств и критичных данных
- Уменьшение поверхности атаки (снижение рисков)
- Предотвращение угроз как часть соотвествия требованиям законодательства
- Оптимизация затрат на построение защиты

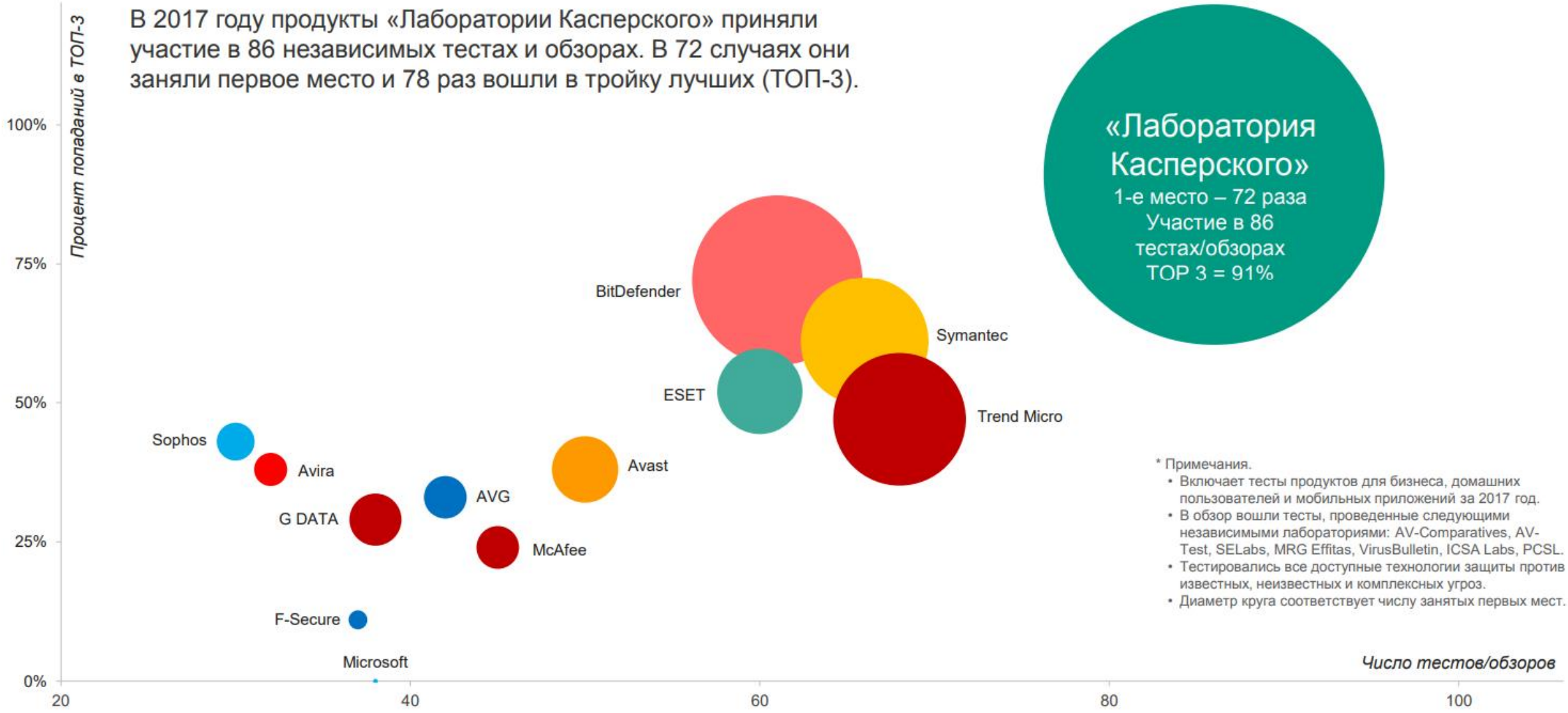
Чем больше угроз будет автоматически заблокировано, тем дешевле

Роль решений с максимальной эффективностью блокирования угроз



БОЛЬШЕ ТЕСТОВ. БОЛЬШЕ НАГРАД. БОЛЬШЕ ЗАЩИТЫ*

В 2017 году продукты «Лаборатории Касперского» приняли участие в 86 независимых тестах и обзорах. В 72 случаях они заняли первое место и 78 раз вошли в тройку лучших (ТОП-3).



«Лаборатория Касперского»
1-е место – 72 раза
Участие в 86 тестах/обзорах
TOP 3 = 91%

* Примечания.
- Включает тесты продуктов для бизнеса, домашних пользователей и мобильных приложений за 2017 год.
- В обзор вошли тесты, проведенные следующими независимыми лабораториями: AV-Comparatives, AV-Test, SELabs, MRG Effitas, VirusBulletin, ICSA Labs, PCSL.
- Тестировались все доступные технологии защиты против известных, неизвестных и комплексных угроз.
- Диаметр круга соответствует числу занятых первых мест.

Достигаемый результат от выполнения первого этапа

Построение автоматической защиты без увеличения штата специалистов

Предпосылки для перехода на этап #2

Задачи ИБ

- Повышение осведомленности
- Необходимость в развитие методов защиты и обнаружения угроз
- Корреляция данных с рабочих мест
- Построение комплексной стратегии защиты и компенсирующих друг друга механизмов
- Снижение нагрузки на персонал (автоматизация рутинных операций)

Внешние факторы и тенденции

- Усложнение законодательства РФ в области защиты данных и КИИ
- Изменение модели рисков под воздействием факторов Цифровой Трансформации
- Повсеместное усложнение угроз и методов злоумышленников

Этап 2 – подготовится к серьезным угрозам и инцидентам на рабочих местах

Передовое обнаружение, централизация реагирования и повышение экспертизы

Этап 2

Выстроить максимально эффективную и удобную защиту от передовых угроз

- **Kaspersky Security Training**
- **Kaspersky Managed Protection**
- **Kaspersky Endpoint Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Targeted Attack Discovery***
- **Kaspersky Threat Data Feeds**

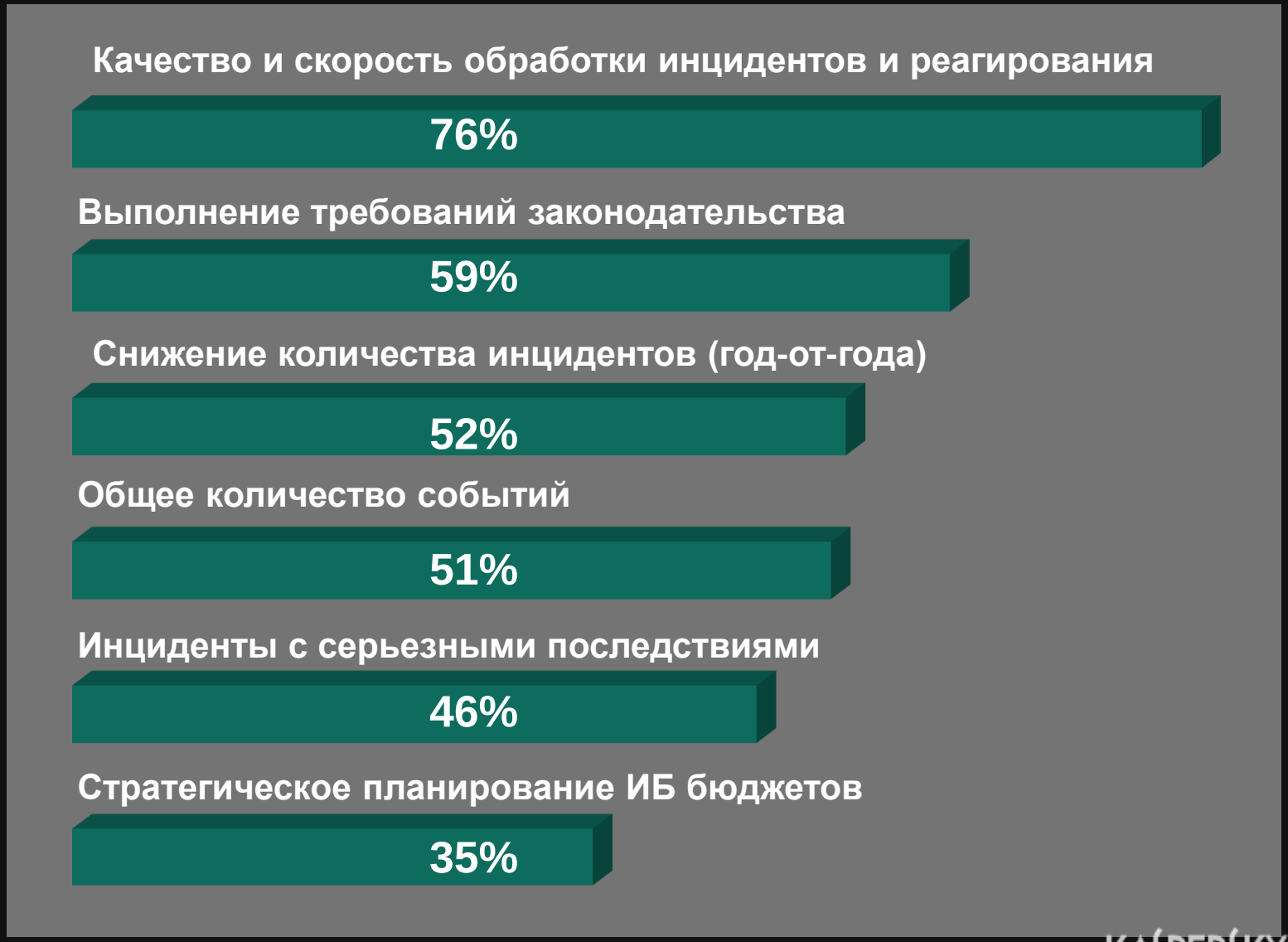
- Автоматическое обнаружение комплексных угроз
- Централизованное хранение данных и вердиктов для использования в ретроспективном анализе и оперативное предоставление подробной информации о уже произошедших инцидентах
- Встроенная корреляция событий и формирование «макро-инцидента» для ускорения процесса расследования
- Централизованные ответные задачи с единой консоли на всех этапах расследования инцидентов

- Увеличение скорости и качественной обработки инцидентов
- Снижение стоимости рутинных операций
- Соответствие нормативным требованиям

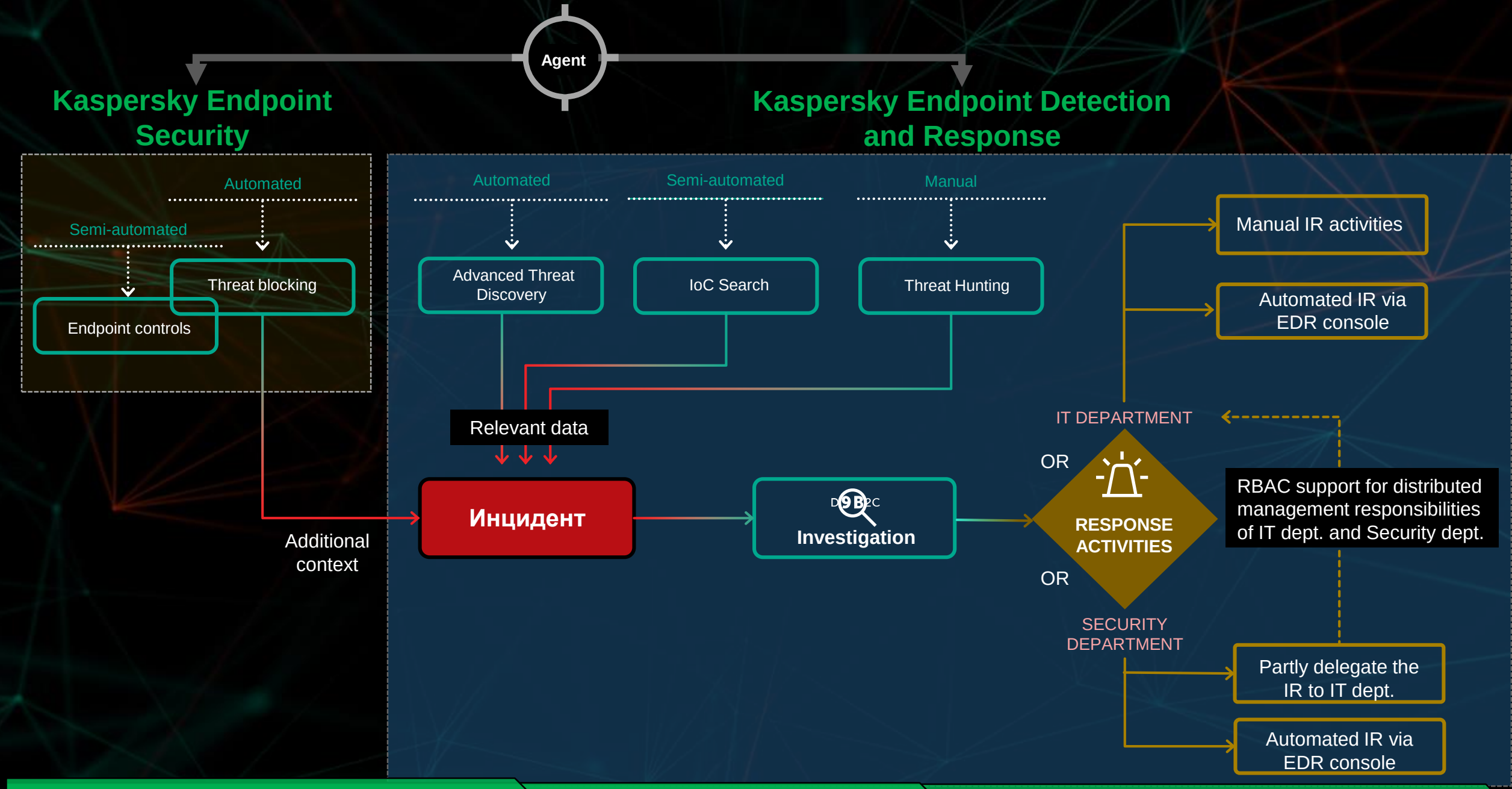
KASPERSKY lab

Ключевые задачи и KPI при работе со сложными инцидентами

- Количество инцидентов и их сложность возрастает год от года
- Реагирование существенно усложняется
- Законодательство напрямую форсирует построение новых процессов ИБ
- У организаций нет ресурсов, опыта и инструментов, необходимых для решения этих задач



Source: What It Takes to Be a CISO: Success and Leadership in Corporate IT Security, Kaspersky Lab, 2018


Agent
Kaspersky Endpoint Security
Kaspersky Endpoint Detection and Response
Automated
Semi-automated
Threat blocking
Endpoint controls
Automated
Semi-automated
Manual
Advanced Threat Discovery
IoC Search
Threat Hunting
Relevant data
Инцидент
Additional context
Investigation
IT DEPARTMENT
OR
RESPONSE ACTIVITIES
OR
SECURITY DEPARTMENT
Manual IR activities
Automated IR via EDR console
RBAC support for distributed management responsibilities of IT dept. and Security dept.
Partly delegate the IR to IT dept.
Automated IR via EDR console
ИТ департамент
ИБ департамент
SOC

Что такое EDR? В чем отличие от EPP?

Kaspersky Security для бизнеса

Endpoint Protection Platform (EPP)

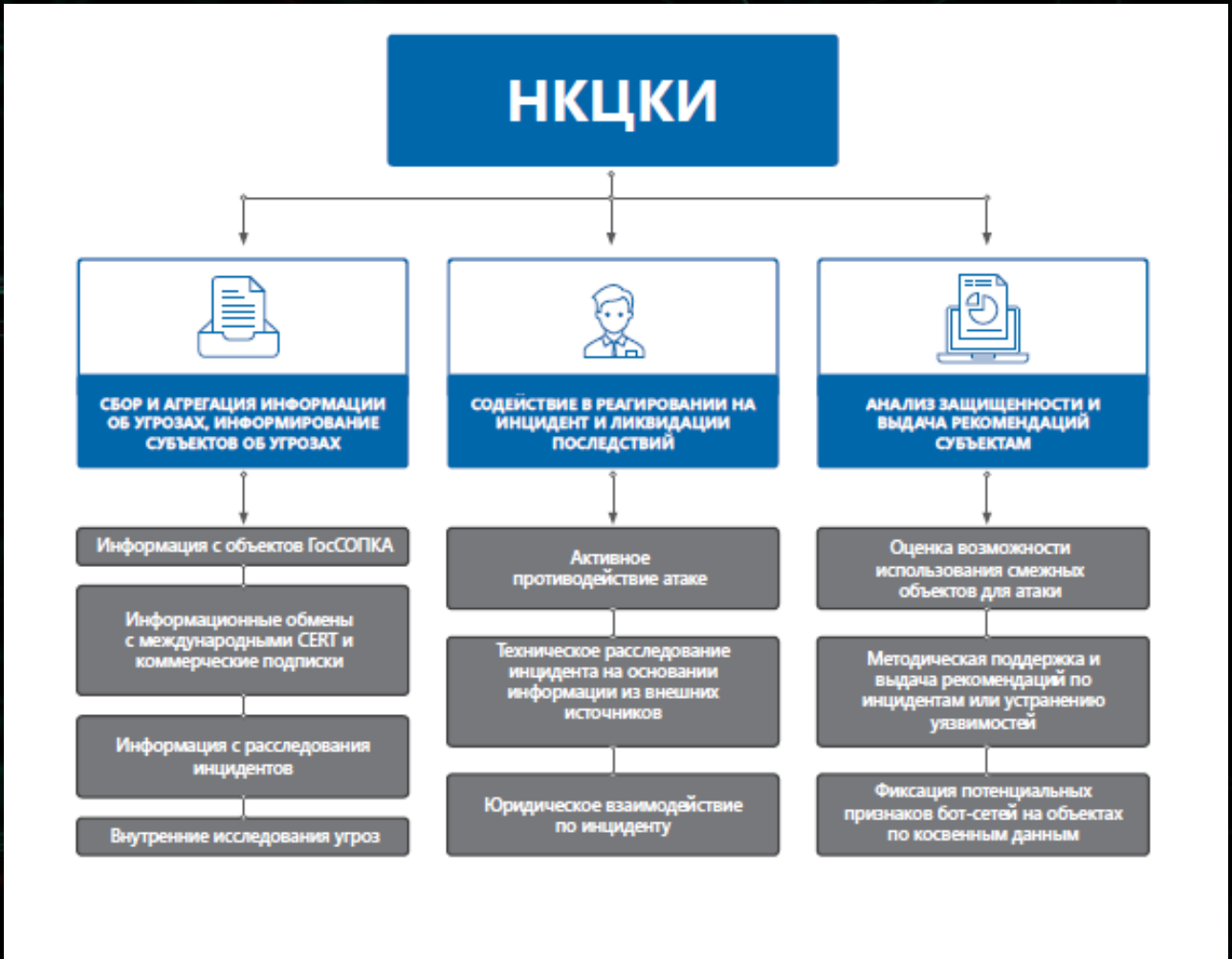
Автоматическое обнаружение и автоматическая блокировка угроз на уровне одной конечной точки

Kaspersky Endpoint Detection and Response

Endpoint Detection and Response (EDR)

Автоматическое передовое обнаружение, дальнейшее расследование и реагирование на уровне всей инфраструктуры конечных точек

Обнаружение, реагирование и предупреждение



- Инцидент
- ЧТО?, ГДЕ?, КАК?
- ЗАЧЕМ?
- ГДЕ ещё?
- сэмплы, PCAPs
- Принятые меры
- И многое другое

Преимущества для действующих клиентов Лаборатории Касперского

Заказчики, использующие Kaspersky Security для бизнеса:

- Получают функциональность EDR в рамках уже установленного программного агента
- Избегают дополнительной нагрузки на производительность рабочих мест
- Получают упрощенный процесс контроля
- Обеспечивают полноценную защиту инфраструктуры конечных точек

Действующие клиенты KES

Kaspersky Security для бизнеса

Конечные точки

Единый агент

Kaspersky Security для бизнеса

Kaspersky EDR

Достигаемый результат от выполнения второго этапа

Максимально эффективно и быстро выявлять и реагировать на возникающие инциденты

Предпосылки для перехода на этап 3

Задачи ИБ

- Комплексный подход на уровне как рабочих мест так и сетевом
- Развитие корреляции в SIEM
- Построение и развитие процессов SOC
- Необходимость глубокой аналитики угроз

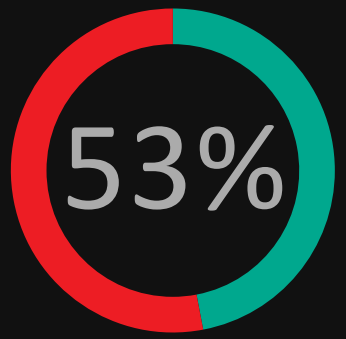
Внешние факторы

- Соответствие требованиям (ФЗ-187)
- Внешняя экспертиза вендора

Этап 3 – Повышение осведомленности об угрозах на всей сети

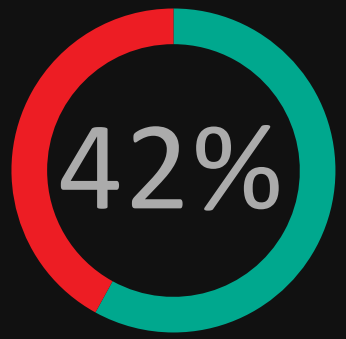
- Снижение до нуля вероятности разрушительных последствий сложных инцидентов
- Ускорение процесса обнаружения сложных угроз на ранних этапах и увеличение количества качественно обработанных инцидентов.
- Формирование полной картины, в поддержку комплексной стратегии защиты от сложных угроз
- Увеличение возможностей мониторинга и минимизация стоимости развития SOC
- Соответствие нормативным требованиям
- Стабильность бизнеса

Препятствия на пути повышения эффективности SOC



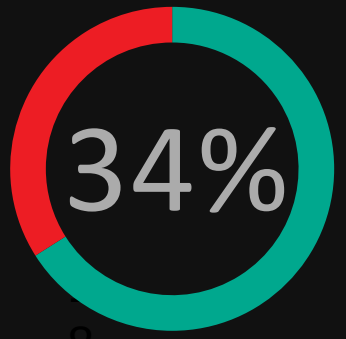
Недостаток автоматизации

- Неэффективная автоматизация по обнаружению расширенных угроз (уровень APT)
- Отсутствие автоматизации в активностях по реагированию



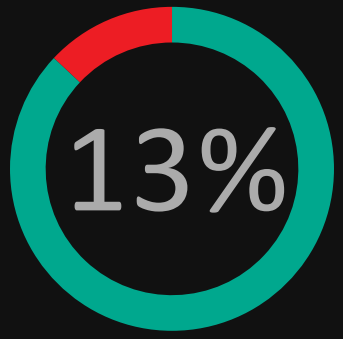
Недостаток покрытия и наглядности

- SOC фокусируется на мониторинге ограниченного круга систем
- Редко подключают конечные точки в качестве источников логов
- **Дебаты вокруг TLS 1.3**



Слишком много оповещений остаются без внимания

- 1-линия SOC тонет в оповещениях, поэтому важные предупреждения могут пропускаться
- Большой процент ложных срабатываний
- Присутствует ручное сопоставление данных



Недостаток контекста к получаемым оповещениям

- Внутренние события не всегда сопоставляются с внешними данными об угрозах
- Невозможно получить доступ к данным, необходимым для расследования, поскольку скомпрометированная конечная точка недоступна или данные зашифрованы злоумышленниками

*Source: SANS 2018 Security Operations Center Survey

SOC нуждаются в дополнительной помощи на уровне конечных точек

Конечные точки редко подключаются как источники в SOC

ПОЧЕМУ?

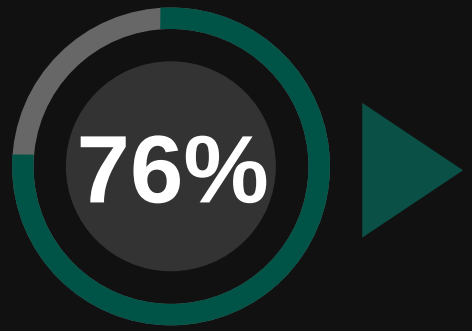
Высокая стоимость сбора и обработки журналов с конечных точек

Необходимость разбора огромного количества логов, что требует больших трудозатрат

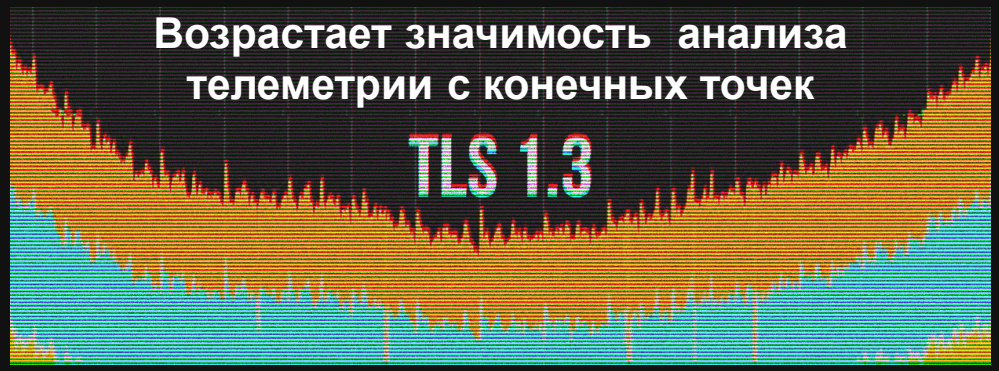
ВАЖНО

Конечные точки являются ключевой целью для киберпреступников

Конечные точки являются ключевым источником данных для расследования



Проблемы на хосте – основной сигнал к действиям по реагированию



Источник: **SANS 2018 Security Operations Center Survey**

KASPERSKY lab

ФЗ-187: драйвер перехода от защиты по остаточному принципу к построению комплексной стратегии

От продуктов защиты

• средства обнаружения и предотвращения вторжений, в том числе обнаружения целевых атак;
• специализированные решения по защите информации для индустриальных сетей, финансового сектора;
• средства выявления и устранения DDoS-атак;
• средства сбора, анализа и корреляции событий;
• средства анализа защищенности;
• средства антивирусной защиты;
• средства межсетевого экранирования;
• средства криптографической защиты информации и защищенного обмена данными.

К построению зрелых процессов

• инвентаризация информационных ресурсов;
• выявление уязвимостей ИТ ресурсов;
• анализ угроз информационной безопасности;
• повышение квалификации персонала;
• прием сообщений о возможных инцидентах от персонала и пользователей ИТ ресурсов;
• обеспечение процесса обнаружения компьютерных атак;
• анализ данных о событиях безопасности;
• регистрация инцидентов;
• реагирование на инциденты и ликвидация их последствий;
• установление причин инцидентов;
• анализ результатов устранения последствий инцидентов.

Поэтапная стратегия развития корпоративной кибербезопасности

Единая долгосрочная стратегия развития кибербезопасности с учетом уровня и темпов роста компетенций в области ИБ

Блокирование максимального количества угроз в автоматическом режиме

Автоматизация передовых средств обнаружения и защиты

Развитие передовой экспертизы для комплексной защиты

Этап 1

Оценить и максимально усилить существующие превентивные технологии

Минимизировать необходимость ручного анализа

Этап 2

Выстроить максимально эффективную и удобную защиту от передовых угроз

Автоматизировать ручные операциии службы ИБ для повышения эффективности

Этап 3

Внедрение концепции SOC, постоянного мониторинга и максимальной осведомленности о происходящем в сети

Максимальная автоматизации и удобство эксплуатации

- ✓ Максимальной автоматизации операций, связанных с процессами обнаружения, расследования и реагирования на инциденты
- ✓ Поддержки встроенной автоматической корреляции разрозненных событий
- ✓ Предоставления ИБ специалисту единого удобного инструмента с интуитивно понятным интерфейсом для действий по расследованию и реагированию
- ✓ Отображения полной картины инцидента в виде дерева событий для оперативного принятия мер
- ✓ Детальной оценки киберугроз за счет формирования максимально полного представления обо всех этапах спланированной злоумышленниками атаки

Увеличение общего числа качественно обработанных инцидентов

Повышение уровня вовлеченности существующих специалистов ИБ

Спасибо!

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212, Russian Federation
Tel: +7 (495) 797-8700
www.kaspersky.com