Kaspersky Security-новое поколение защитных решений

Александр Тищенко
инженер предпродажной поддержки в ЮФО и СКФО

kaspersky

Кто мы

Международный лидер в сфере кибербезопасности

200 стран и территорий

34 региональных офиса

Африка
Южная Африка

Азия
Китай
Гонконг
Индия
Япония
Казахстан
Малайзия
Сингапур
Южная Корея

Европа
Чехия
Франция
Германия
Израиль
Италия
Нидерланды
Португалия
Румыния
Россия
Испания
Швейцария
Великобритания

Ближний Восток
Саудовская Аравия
Турция
ОАЭ

Северная Америка
Мексика
США

Южная Америка
Бразилия

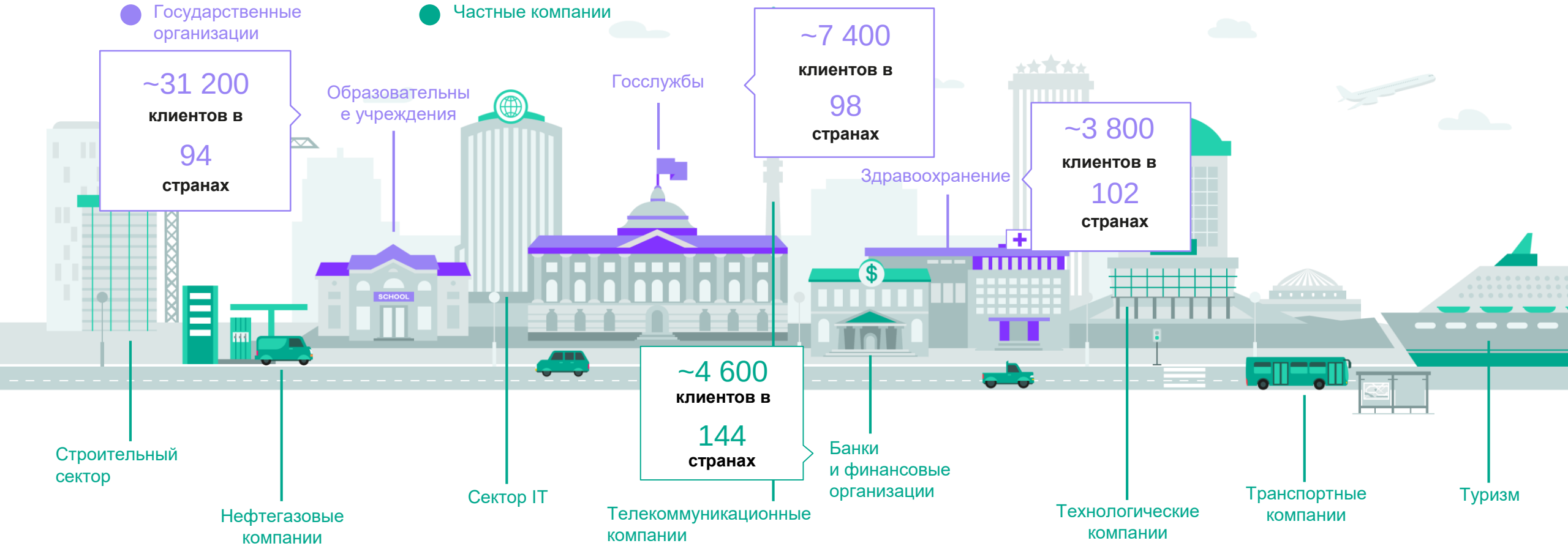
Центры прозрачности
Цюрих, Швейцария
Мадрид, Испания
Сан-Паулу, Бразилия
Куала-Лумпур, Малайзия
Вобурн, США
Сингапур, Сингапур
Токио, Япония
Рим, Италия
Утрехт, Нидерланды

Международный лидер в сфере кибербезопасности

> 240 000
корпоративных клиентов по всему миру

> 400 000 000
защищенных пользователей по всему миру

80%
наших операций – международные



Наша команда

> 4 500 высококвали-фицированных специалистов

50% наших сотрудников – профессионалы в области R&D

> 40 ведущих мировых экспертов по безопасности входят в нашу элитную группу

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.

Состояние кибербезопасности в 2023 году

Масштаб современных кибератак

1

Средний ущерб от успешной кибератаки

SMB: 105k$
Enterprise: ~1M$

2

Отношение лидеров бизнеса

68% лидеров бизнеса считают, что риски, связанные с кибербезопасностью растут

3

Мотивация атак

71% атак были финансово-мотивированными

4

Оценка активности шифровальщиков

За 2022 мы защитили от шифровальщиков более 320 тыс. уникальных пользователей (более 20 тыс. модификаций за год)

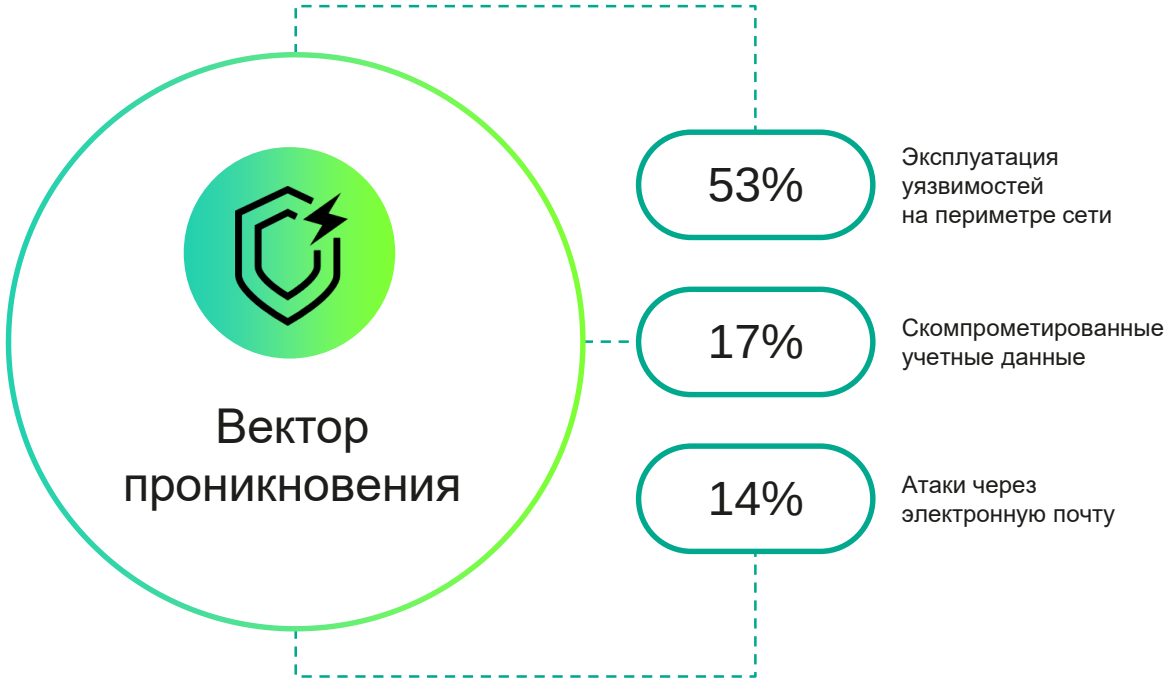
5

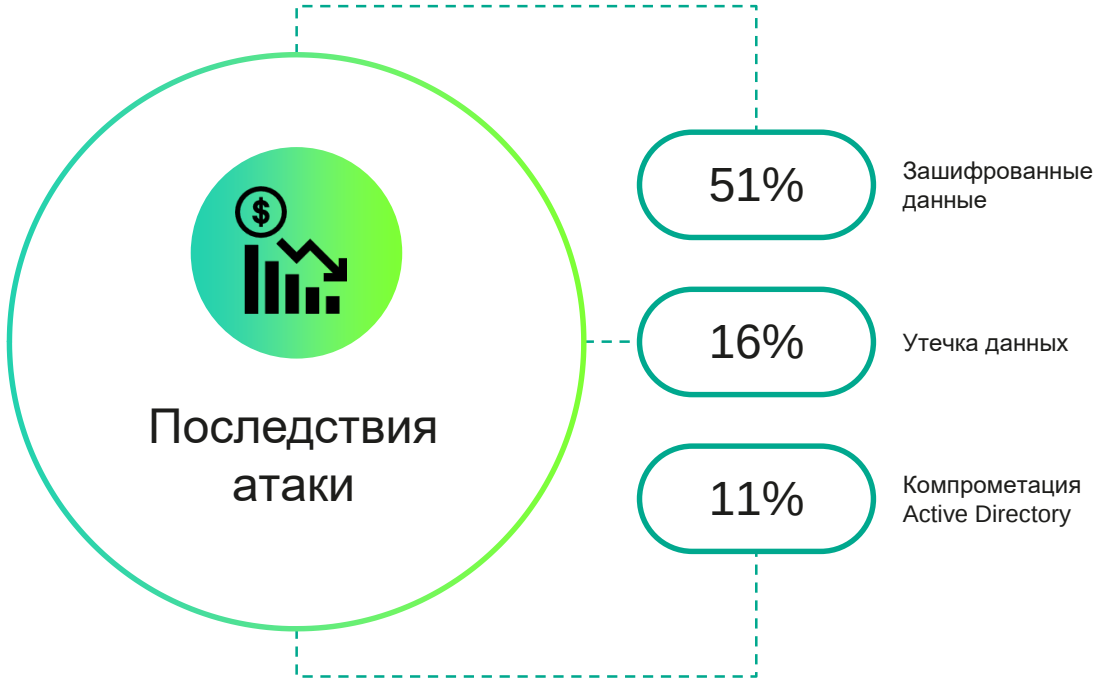
Особенности атак

52% атак имели отношение к взлому, 28% были проведены с использованием вредоносов, 33% использовали фишинг и социальную инженерию

Источники данных: Kaspersky, Accenture, Verizon

Атаки на организации в 2022





Индустрии

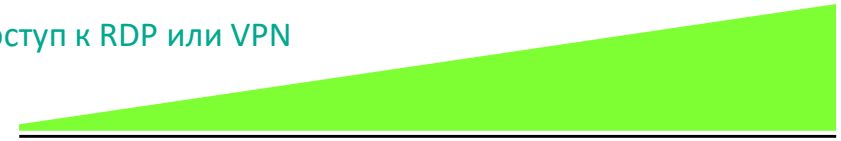
30%	19%	12%	11%
Промышленные предприятия	Государственный сектор	Финансовые организации	IT

Источник: Global Emergency Response Team, Kaspersky

Услуги по проведению атак и инструменты для кибернападений доступны широкому кругу лиц

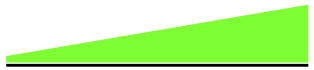
Отдельные инструменты

Доступ к RDP или VPN



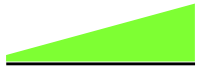
0 долл. США — 5000 долл. США

Вредоносное ПО



10 долл. США — 150 долл. США

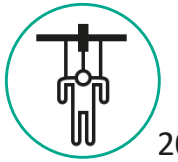
Инструкции



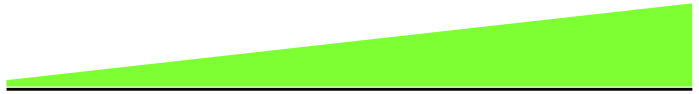
1 долл. США — 30 долл. США

от 11 долл. США

Кампания



Фишинг; программы-вымогатели; банковские троянцы



200 долл. США — 3500 долл. США

от 200 долл. США

Как мы можем помочь

Защита нового поколения для рабочих мест, которая подходит именно вам

Kaspersky Security для бизнеса

- низкий — Необходимый уровень навыков
- высокая — Персонализация и масштабируемость
- низкий — Уровень инвестиций

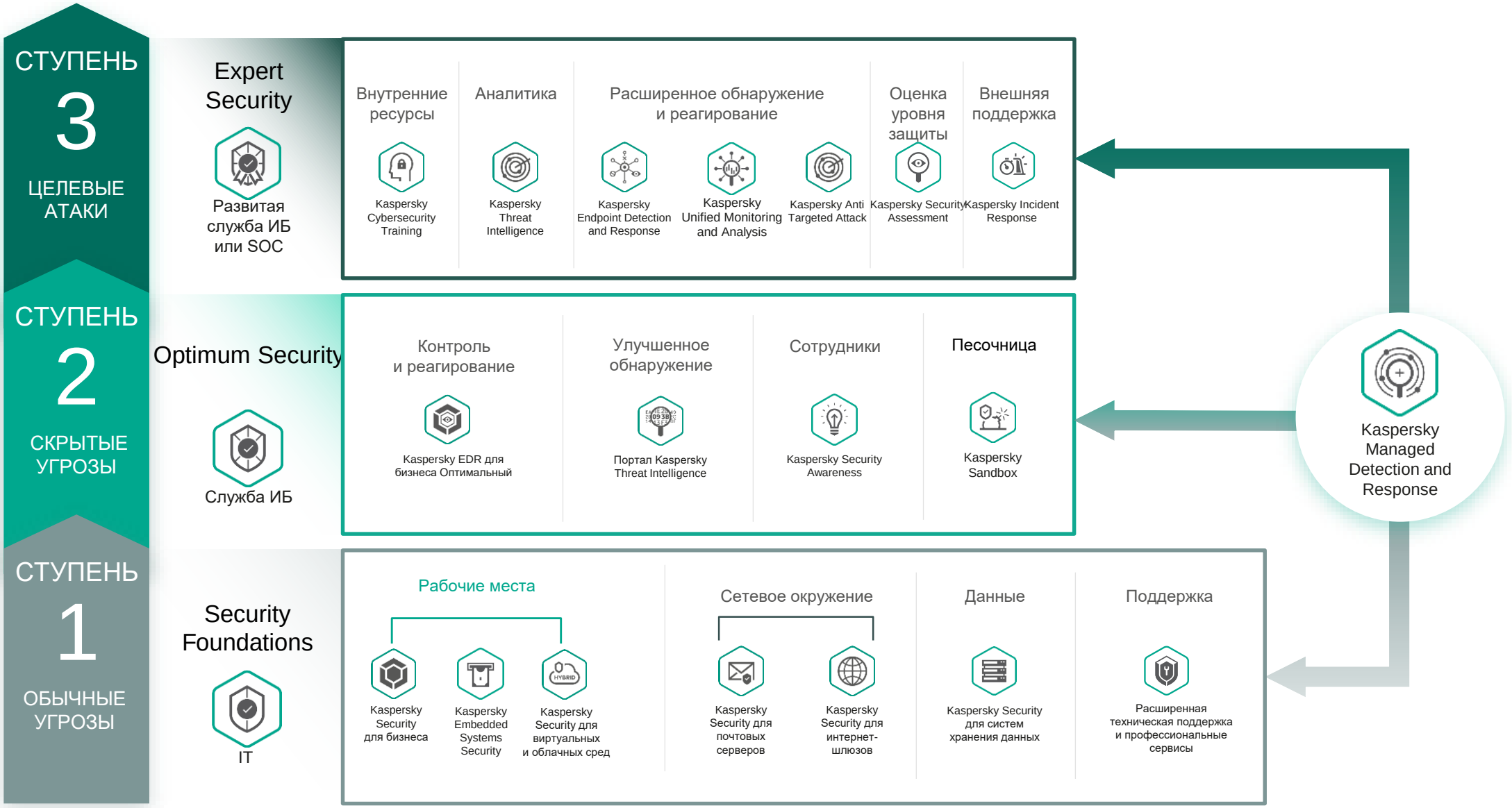
Многоуровневая защита от широкого спектра угроз

- Эксплойты
- Бесфайловые угрозы
- Сетевые угрозы
- Угрозы для мобильных устройств
- Вирусы и троянцы
- Веб-угрозы
- Руткиты
- Шифровальщики

Многоуровневая защита для всех платформ

- Windows
- macOS
- Linux
- Серверные ОС
- Android
- iOS

Kaspersky Security для бизнеса – лишь малая часть нашего портфолио



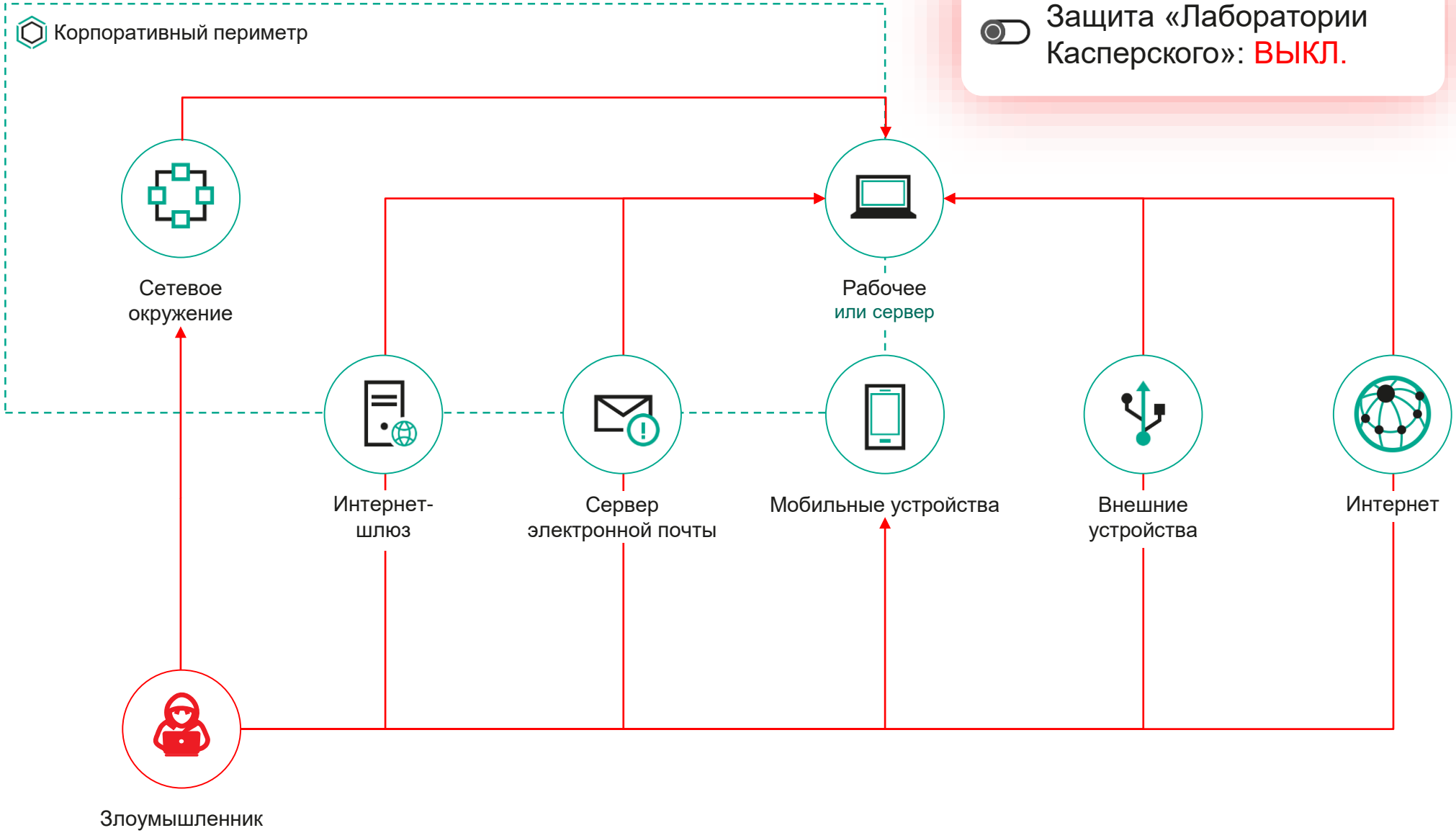
Миф: Антивирус – наш единственный продукт?

- **Защита конечных устройств и периметра**
- **Отраслевые решения** - промышленность, финансовый сектор, специализированная облачная защита
- **Решения класса EDR/XDR** - для обнаружения, реагирования и расследования
- **Kaspersky SD-WAN** - централизованное управление территориально распределенными сетями
- **Kaspersky Antidrone** - защита воздушного пространства
- **Kaspersky Thin Client** - тонкий клиент на базе KasperskyOS
- **Kaspersky Threat Data Feeds** – потоки данных об актуальных угрозах
- **Сервисы** – расследование инцидентов, анализ защищенности, поиск уязвимостей, расширенная ТП…
- **Kaspersky Scan Engine** – технологическое решение
- **Kaspersky Security Awareness** - обучение
- **Kaspersky Unified Monitoring and Analysis Platform -** SIEM

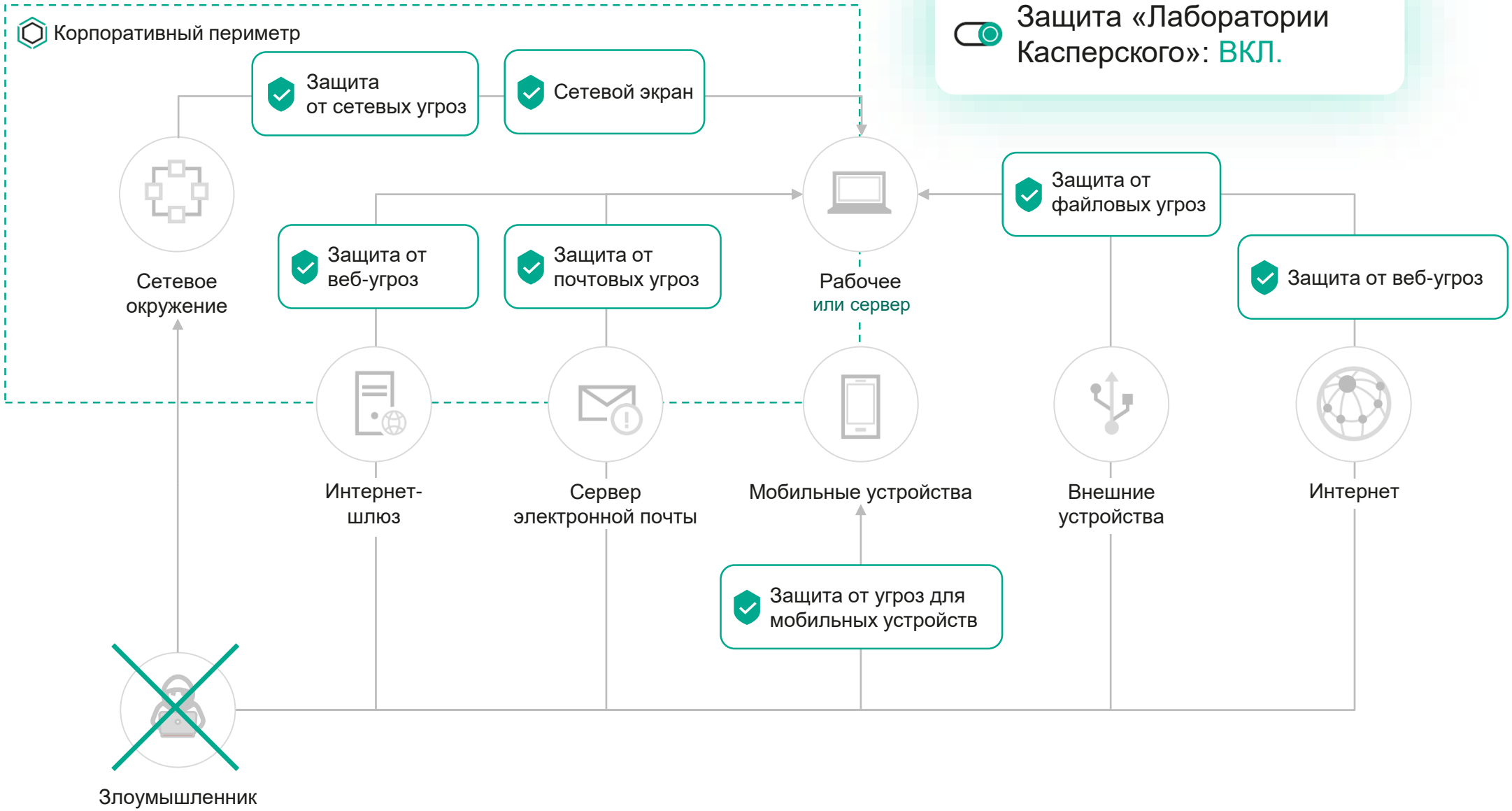
Как это работает

У злоумышленников есть разные пути проникновения в вашу инфраструктуру

Защита «Лаборатории Касперского»: ВЫКЛ.



Защита на подступах к инфраструктуре



Технологии машинного обучения в решениях «Лаборатории Касперского»

Выявление аномалий:

- Обнаружение отклонений от заданных параметров
- Поиск подозрительных признаков в обычных операциях
- Сопоставление шаблонов поведения с вердиктами, вынесенными модулями безопасности
- Сопоставление событий с внешними аналитическими данными об угрозах

Адаптивный контроль аномалий:

- Определение базовых параметров
- Распознавание шаблонов типичного поведения
- Постепенная адаптация шаблонов

2020 — Адаптивное обнаружение аномалий на основе регулярно обновляемой информации о поведении пользователей и систем

2018 — В решениях «Лаборатории Касперского» появляется технология машинного обучения, которая работает на основе анализа поведения

2016–2017 — В решениях «Лаборатории Касперского» появляются модели обнаружения на основе машинного обучения и технологии PeForest

2015 — Модуль автоматического анализа собственной разработки начинает использовать журналы поведенческого анализа (мониторинг системы), выполненного в песочнице

2014 — SmartHash: создание Умных записей на основе машинного обучения с использованием локально-чувствительных хешей для обнаружения семейств вредоносного ПО

2013 — TrueForest: создание умных записей на основе машинного обучения с помощью дерева принятия решений

2011 — Система определения сходств на основе шаблонов с обработкой журналов эмулятора на стороне пользователя, которые затем используются в качестве шаблонов выполнения при запуске моделей машинного обучения в лабораторных условиях

2010 — Собственный эвристический автоматический анализ с автоматической кластеризацией образцов на основе журналов эмулятора и технологии машинного обучения

2008 — Собственный классический автоматический анализ на основе характеристик файлов

Машинное обучение используется для извлечения данных о характеристиках файлов из потока образцов

2006 — Начало разработки облачной технологии автоматизированной обработки угроз

Ключевые выводы

Широкий набор инструментов для IT- и ИБ-специалистов

Сокращение

поверхности атаки,
времени реагирования

Отрежьте злоумышленникам все пути к вашей инфраструктуре, автоматизация рутинных задач

Защита

рабочих мест и не только

Блокируйте атаки, устраняйте последствия инцидентов и защищайте рабочие места – автоматически.

Фундамент

для EDR/XDR

Когда будете готовы сделать следующий шаг в развитии стратегии кибербезопасности и расширить возможности обнаружения и реагирования, просто выберите подходящее вам решение.

Спасибо за внимание

kaspersky