18.02.2025

Решения «Лаборатории Касперского» для финансовых организаций

Алексей Киселев,
руководитель отдела
по работе с клиентами
среднего и малого бизнеса
«Лаборатория
Касперского»

Усложнение рисков

Технологический суверенитет

Поиск актуальных решений

Интерактивная карта киберугроз

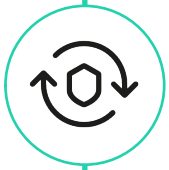
Подробнее

Напряженный киберландшафт

В последние два года 69% организаций в России пострадали минимум от одного киберинцидента.

Усложнение регулирования

Обсуждается существенное увеличение штрафов за утечки.



Технологический суверенитет

Продолжается активное замещение иностранных защитных ИБ решений, покинувших российский рынок. Повышаются требования регуляторов.

Ландшафт киберугроз

+39% рост количества критических инцидентов в организациях России и СНГ (Q1 2024 VS Q1 2023)

>2 инцидентов высокой критичности ежедневно

>19 млн паролей российских пользователей обнаружены в даркнете в Q1 2024 (x6 по сравнению с Q1 2023)

Финансовый сектор – в топ-5 отраслей по количеству утечек в 2023

Самые распространенные причины: нарушение политики безопасности, целевые кибератаки, вредоносное ПО

Основная угроза для организаций – по-прежнему шифровальщики. В 2023 году с ними был связан каждый третий инцидент

Аналитический отчет Kaspersky Managed Detection and Response за 2023 год; Отчет «О значимых утечках данных в России» от команды Kaspersky Digital Footprint Intelligence,

Утечки данных

Общие сведения о значимых[1] утечках данных в российских компаниях в 2023 году[2]:

133 факта утечек данных за 2023 год

За 2022 год	За 2023 год
141 факт утечек данных	133 факта утечек данных
>230 млн пользовательских данных	>310 млн пользовательских данных
>33 млн записей с паролями	>47 млн записей с паролями

47 976 727

Строк, содержащих парольную информацию, было скомпрометировано злоумышленниками

В каких сферах были самые крупные утечки?

- 4 Ритейл
- 2 Финансы
- 1 Интернет-сервисы
- 1 Здоровье
- 1 Карьера и образование
- 1 Производство

Подробнее

Утечки данных

Топ-5 пострадавших отраслей от утечек данных

2022	2023
Ритейл	Ритейл
↓ Рестораны и доставки еды	↑ Интернет-сервисы
Интернет-сервисы	↑ **Финансы**
Карьера и образование	Карьера и образование
↓ Транспорт	↑ IT

Топ-5 отраслей по объемам скомпрометированных данных

2022	2023
Доставка	↑ Ритейл
СМИ	↑ **Финансы**
Ритейл	↑ Интернет-сервисы
Здоровье	↑ Карьера и образование
Социальные сети	↓ Здоровье

Подробнее

Как мы можем помочь

3 СЛОЖНЫЕ
СЛОЖНЫЕ АТАКИ

Kaspersky Expert Security

Служба ИБ или SOC

- Повышение экспертизы: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky EDR Expert; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack
- Реагирование на угрозы: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

2 СКРЫТЫЕ
СКРЫТЫЕ УГРОЗЫ

Kaspersky Optimum Security

Команда ИБ

- Базовое обнаружение и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Песочница: Kaspersky Sandbox
- Обогащение данными: Kaspersky Threat Intelligence Portal
- Киберграмотность: Kaspersky Security Awarenes s
- Защита контейнеров: Kaspersky Container Security
- Умная защита для среднего бизнеса: Kaspersky Smart

1 ОБЫЧНЫЕ
МАССОВЫЕ УГРОЗЫ

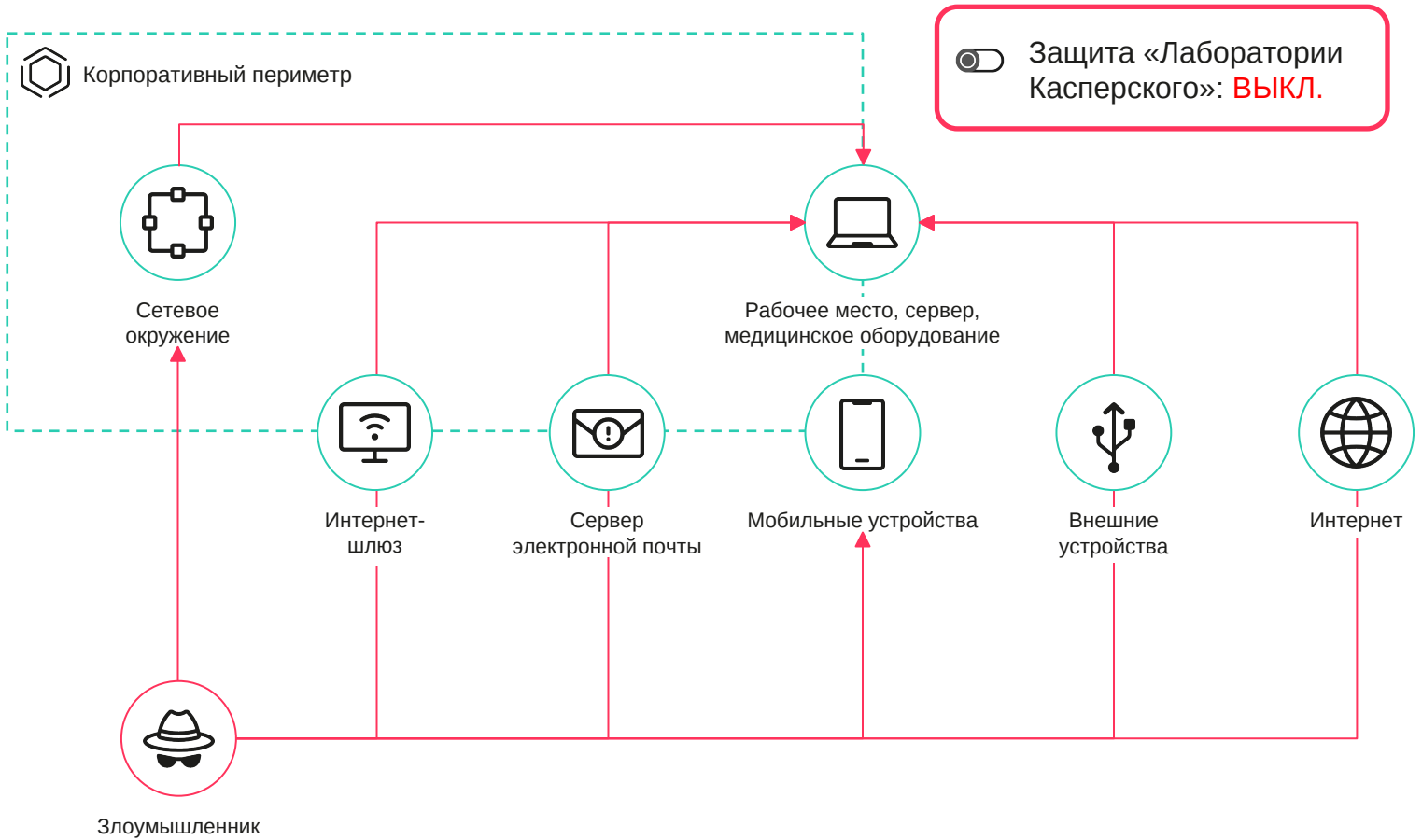
Kaspersky Security Foundations

ИТ

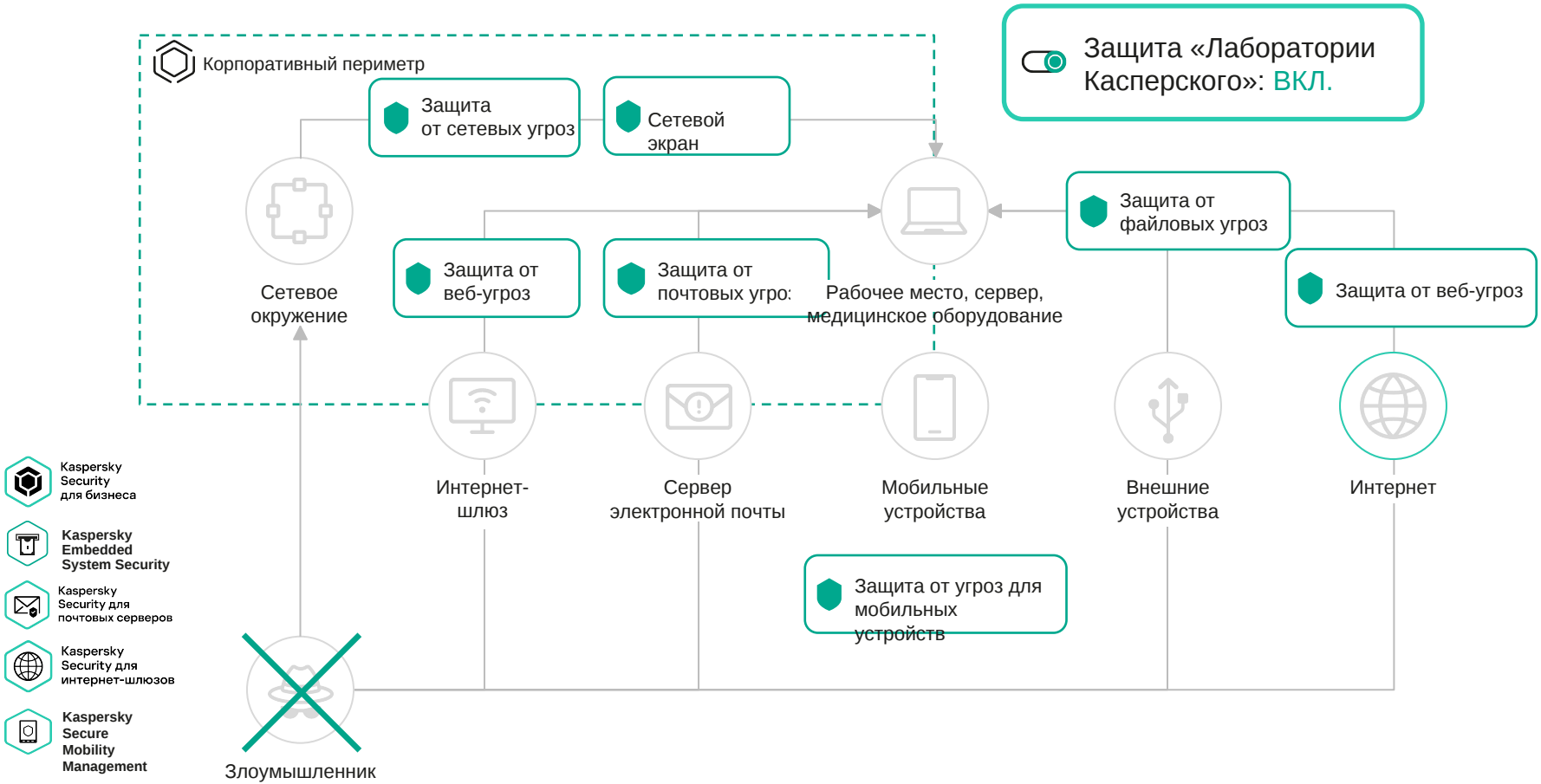
- Конечные устройства: Kaspersky Security для бизнеса; Kaspersky Embedded System Security; Kaspersky Security для виртуальных и облачных сред; Kaspersky Secure Mobility Management
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security для интернет-шлюзов
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: MSA и профессиональные сервисы

Kaspersky Managed Detection and Response

Что защищать в первую очередь



Базовая защита на всех подступах к инфраструктуре



Kaspersky Security для бизнеса

Kaspersky Security для бизнеса

О продукте

Основа любой системы ИБ для компаний любой величины и сферы деятельности для автоматического отражения массовых киберугроз

Подробнее

Ключевые возможности

- Огромное количество компонентов защиты в одном исполнении для разных платформ и операционных систем;
- Уникальные технологии по оперативному выявлению и блокированию шифровальщиков
- Инструменты контроля для управления доступом к приложениям, ресурсам сети Интернет или подключенным устройствам
- Встроенные средства по поиску и закрытию уязвимостей ОС и приложений сторон вендоров
- Инструменты системного администрирования для автоматизации развертывания приложений и операционных систем
- Поддержка частичного и полнодискового шифрований, управление встроенными в операционную систему функциями шифрования
- Полная поддержка функционирования системы на отечественных ОС и базах данных

Государственная сертификация (ФСТЭК, ФСБ) ключевых компонентов решения **для Windows и Linux**

Kaspersky Security для почтовых серверов

О продукте

Kaspersky Security для почтовых серверов защищает корпоративную почту от вредоносного ПО, программ-вымогателей, спама, фишинга и BEC-атак

Подробнее

Ключевые возможности

- Продвинутые технологии блокирования вредоносных объектов (интеграция с KATA)
- Защита от фишинга, спама и компрометации корпоративной электронной почты
- Фильтрация почтовых вложений
- Предотвращение попыток обмануть пользователей с помощью методов социальной инженерии
- Соответствие требованиям регуляторов, поддержка отечественных ОС (KLMS)

Релиз KSMG 2.0

- Кластерная архитектура для масштабирования решения
- Ролевое разграничение прав доступа, интеграция с AD
- Централизованный поиск по хранилищу событий
- Усилены технологии детектирования (IP-репутация, look-like, выявление спуфинговых атак и т.д.)

Kaspersky Security для интернет-шлюзов

О продукте

Корпоративный шлюз Web безопасности с расширенными средствами анализа и защиты, предлагает средства антивирусной защиты, динамического анализа веб страниц и мощный категоризатор веб ресурсов

Подробнее

Ключевые возможности

- Продвинутые технологии антивирусной защиты (AM-движок, интеграция с KATA)
- Инспекция SSL трафика
- URL/IP репутация
- Контроль доступа к Web-ресурсам, предопределенные списки категорий
- Анализ контента, обнаружение вредоносных скриптов
- Настройки доступа для приложений (по user агенту)
- Поддержка работы в кластере
- Несколько вариантов развертывания (готовый Virtual Appliance или интеграция с существующим Proxy)
- Ролевая модель доступа к элементам управления
- Разделение на рабочие области

О продукте

Специализированное решение для защиты встраиваемых систем (банкоматы,
POS-системы, торговые автоматы, заправочные станции, медицинское оборудование) от угроз любого типа и любой сложности

Ключевые возможности

- Укрепление системы (контроль безопасности)
- Дополнительная защита от вредоносного ПО: методы эвристического анализа и модели машинного
- Защита от эксплойтов
- Защита от сетевых угроз
- Контроль целостности и соблюдение нормативных требований
- Поддержка маломощных и устаревших систем
- Анализ журналов
- Гибкое управление – локально или в облаке
- Управление сетевым экраном
- Эффективная защита даже при нестабильном подключении к сети

О продукте

Позволяет бизнесу безопасно, гибко и удобно использовать мобильные устройства в рабочих целях. Уверенный контроль и надежная защита на каждом этапе жизненного цикла корпоративных мобильных устройств

Ключевые возможности

- Простое управление всем парком мобильных устройств и централизованное управление политиками из единой консоли
- Поддержка всех основных сценариев использования устройста (COPO, COBE, BYOD)
- Управление устройствами Android, iOS/IPadOS и жизненным циклом Windows-устройств
- Надежная защита устройств в том числе от специализированных мобильных угроз
- Корпоративный каталог приложений
- Управление и работа с сертификатами и VPN (per-app VPN)
- Полная поддержка режима supervised для iOS и возможностей в нем

Kaspersky
Secure Mobility
Management

О продукте

Позволяет бизнесу безопасно, гибко и удобно использовать мобильные устройства в рабочих целях. Уверенный контроль и надежная защита на каждом этапе жизненного цикла корпоративных мобильных устройств

Подробнее

Подготовка

- Развертывание сервисов поддержки мобильной платформы (серверная часть)
- Подготовка корпоративного каталога со списком доверенных приложений и портала для подключения BYOD-устройств
- Подготовка и конфигурирование сценариев автоматизированного развертывания корпоративных устройств

Развертывание и конфигурация

- Загрузка сертификатов безопасности, профилей email, VPN, Wi-Fi
- Установка агентской части решения, обеспечивающей защиту устройств и функции мониторинга/контроля
- Загрузка и применение корпоративных политик безопасности и ограничений использования
- Установка и автоматизированное конфигурирование бизнес-приложений

Защита и контроль

- Отслеживание событий безопасности
- Реагирование на события уровня «инцидент», включающее вмешательство администратора
- Отслеживание и реагирование на события регуляторных политик

Поддержка и выведение из обслуживания

- Обеспечение удаленной поддержки
- Аудит потерянных / украденных устройств
- Отзыв доступа к корпоративным ресурсам
- Выборочное (для BYOD-устройств) или полное обнуление устройства

Как мы можем помочь

3 СЛОЖНЫЕ СЛОЖНЫЕ АТАКИ

Kaspersky Expert Security

Служба ИБ или SOC

- Повышение экспертизы: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky EDR Expert; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack
- Реагирование на угрозы: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

2 СКРЫТЫЕ СКРЫТЫЕ УГРОЗЫ

Kaspersky Optimum Security

Команда ИБ

- Базовое обнаружение и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Песочница: Kaspersky Sandbox
- Обогащение данными: Kaspersky Threat Intelligence Portal
- Киберграмотность: Kaspersky Security Awareness
- Защита контейнеров: Kaspersky Container Security
- Умная защита для среднего бизнеса: Kaspersky Smart

1 ОБЫЧНЫЕ МАССОВЫЕ УГРОЗЫ

Kaspersky Security Foundations

ИТ

- Конечные устройства: Kaspersky Security для бизнеса; Kaspersky Embedded System Security; Kaspersky Security для виртуальных и облачных сред; Kaspersky Secure Mobility Management
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security для интернет-шлюзов
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: MSA и профессиональные сервисы

Kaspersky Managed Detection and Response

Kaspersky EDR для бизнеса Оптимальный

О продукте

Передовая защита рабочих мест, усиленная базовыми возможностями обнаружения, реагирования и расследования инцидентов.

Подробнее

Ключевые возможности

Защита рабочих мест

- Расширенная защита систем и данных от вредоносного ПО
- Быстрое обновление информации об угрозах
- Оценка уязвимостей и установка исправлений
- Поддержка рабочих станций на всех популярных платформах

Базовые инструменты EDR

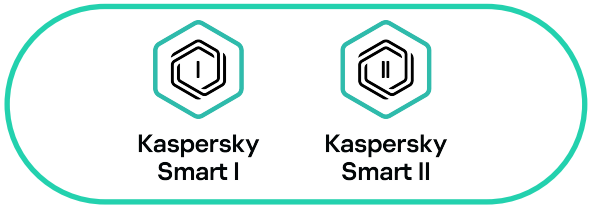
- Продвинутое обнаружение угроз на основе передовых технологий
- Предоставление детальной информации об обнаруженной угрозе
- Анализ первопричин и всей цепочки развития киберинцидента
- Автоматизация процессов

Удобное управление

- Единый агент для EPP и EDR
- Единая консоль
- Единая карточка инцидента со сценариями и инструкциями по реагированию
- Инструменты визуализации данных
- Мультитенантность

Полноценная функциональность для Windows, Linux и MacOS

Kaspersky Managed Detection and Response.
Непрерывный поиск, обнаружение и устранение угроз, направленных на ваше предприятие



О продукте

Линейка решений Kaspersky Smart делает экспертные инструменты класса SIEM и MDR доступными для организаций среднего бизнеса (250–1000 узлов) и открывает новые возможности для киберзащиты.

Подробнее

Ключевые возможности

Kaspersky Smart I

SIEM

Kaspersky Smart II

SIEM EDR

- Единая поставка самой актуальной киберзащиты для среднего размера инфраструктур
- Не только мониторинг и обнаружение, но и реагирование
- Помощь в соблюдении требований регуляторов
- Комплексная защита организаций среднего размера с минимальными требованиями к аппаратным мощностям и возможностью установки на виртуальные машины

Акция на покупку Kaspersky Smart.

Скидка на покупку

15 %

Kaspersky Smart I

30 %

Kaspersky Smart II

Kaspersky Container Security

О продукте

Kaspersky Container Security (KCS) — это решение, которое обеспечивает безопасность контейнерных приложений на всех этапах жизненного цикла: от разработки до эксплуатации.

Подробнее

Ключевые возможности

Защита оркестратора

- контроль настройки аутентификации и авторизации
- проверка конфигурации оркестратора на наличие ошибок
- отслеживание потребляемых ресурсов в кластере

Встраивание в процесс разработки

- обеспечение безопасности контейнеров в райнтайме
- контроль активности внутри контейнеров
- мониторинг потребляемых ресурсов и коммуникаций между контейнерами

Проверка на соблюдение требований регуляторов

- проверка на уровне оркестратора
- проверка на уровне отдельного контейнера
- проверка в соответствии со стандартом PCI DSS

Визуализация и инвентаризация ресурсов в кластере

- мониторинг состояния кластеров
- настраиваемые по разным уровням и разрезам виджеты
- прозрачная инвентаризация ресурсов

Kaspersky Container Security. Ценность решения

Решение проблем ИБ

Наглядность инфраструктуры

Сокращение рутинных действий

Соответствие требованиям регуляторов

Безопасность инфраструктуры

Решение проблем ИТ

Наглядность инфраструктуры

Сокращение ИТ-инцидентов

Оптимизация использования ресурсов

Повышение производительности приложений и сервисов

Решение проблем разработчиков

Ускорение релизного цикла

Защита среды рантайма

Автоматизация проверок на безопасность

Поддержка практик DevSecOps

Kaspersky
DDoS Protection

О продукте

Kaspersky DDoS Protection минимизирует влияние DDoS-атак, обеспечивая постоянную доступность всей инфраструктуры и важнейших онлайн-ресурсов.

Подробнее

Ключевые возможности

Все необходимое для защиты от любых видов DDoS-атак и уменьшения их последствий:

- **Анализ трафика в режиме 24x7x365**
  Уникальная сенсорная технология для анализа трафика в реальном времени
- **Географически распределенные центры очистки**
  Масштабируемые и отказоустойчивые центры очистки
- **Безупречная интеграция** без необходимости покупки дополнительного оборудования
- **Гибкость решения**. Постоянное перенаправление трафика или перенаправление по требованию
- **Надежная поддержка**. Эксперты «Лаборатории Касперского» круглосуточно отслеживают аномалии в трафике клиентов

О продукте

Платформе для обучения сотрудников основам кибербезопасности. Простой и эффективный онлайн-инструмент, который поможет сотрудникам овладеть навыками кибербезопасного поведения и применять их в работе

Подробнее

Ключевые преимущества

- Снижение числа инцидентов, связанных с человеческой ошибкой;
- Повышение квалификации сотрудников в области кибербезопасности;
- Соответствие требованиям регуляторов в отношении киберграмотности сотрудников;
- Автоматизация процессов, экономия времени сотрудников IT по управлению тренингом и отслеживанию прогресса;
- Простота и удобство использования;
- Контент, покрывающий все основные темы ИБ, включая ИИ и кибербезопасность промышленных систем.

Как мы можем помочь

3 СЛОЖНЫЕ
СЛОЖНЫЕ АТАКИ

Kaspersky Expert Security

Служба ИБ или SOC

- Повышение экспертизы: Kaspersky Cybersecurity Training
- Аналитика угроз: Kaspersky Threat Intelligence
- Расширенное обнаружение и реагирование: Kaspersky EDR Expert; Kaspersky Unified Monitoring and Analysis Platform; Kaspersky Anti Targeted Attack
- Реагирование на угрозы: Kaspersky Incident Response
- Анализ защищенности: Kaspersky Security Assessment

2 СКРЫТЫЕ
СКРЫТЫЕ УГРОЗЫ

Kaspersky Optimum Security

Команда ИБ

- Базовое обнаружение и реагирование: Kaspersky EDR для бизнеса Оптимальный
- Песочница: Kaspersky Sandbox
- Обогащение данными: Kaspersky Threat Intelligence Portal
- Киберграмотность: Kaspersky Security Awarenes s
- Защита контейнеров: Kaspersky Container Security
- Умная защита для среднего бизнеса: Kaspersky Smart

1 ОБЫЧНЫЕ
МАССОВЫЕ УГРОЗЫ

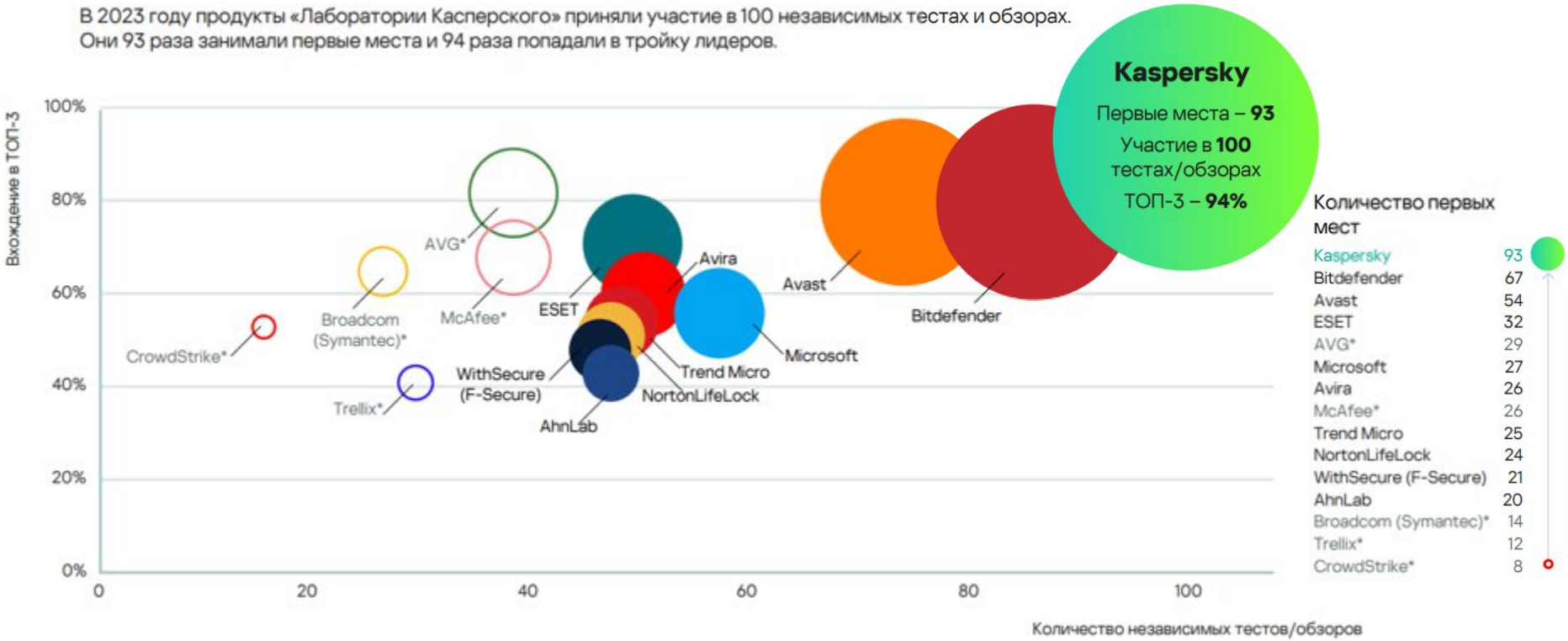
Kaspersky Security Foundations

ИТ

- Конечные устройства: Kaspersky Security для бизнеса; Kaspersky Embedded System Security; Kaspersky Security для виртуальных и облачных сред; Kaspersky Secure Mobility Management
- Сеть: Kaspersky Security для почтовых серверов; Kaspersky Security для интернет-шлюзов
- Данные: Kaspersky Security для систем хранения данных
- Поддержка: MSA и профессиональные сервисы

Kaspersky Managed Detection and Response

Подтвержденное лидерство



Переход с зарубежных решений. Программа «Мигрируй»

1

Выгода

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

2

Предоставьте лицензию

Предоставьте авторизованному партнеру Kaspersky копию лицензионного соглашения.

Мигрируй!

Подробнее

Спасибо за внимание!

Алексей Киселев
Alexey.Kiselev@Kaspersky.com

kaspersky