Переход на российское ПО: решения, результаты, перспективы

16.08.2023

Алексей Киселев
Руководитель отдела по работе с клиентами среднего и малого бизнеса

kaspersky

Постоянное давление. Эволюция угроз. Импортозамещение

Интерактивная карта киберугроз

Подробнее

Рост количества атак и их усложнение

Частые всплески различных киберугроз в российских компаниях

Киберагрессия

Россия номер 1 в мире по количеству атак

Киберугрозы для всех

Атакам сегодня подвержены компании любого размера из любой отрасли

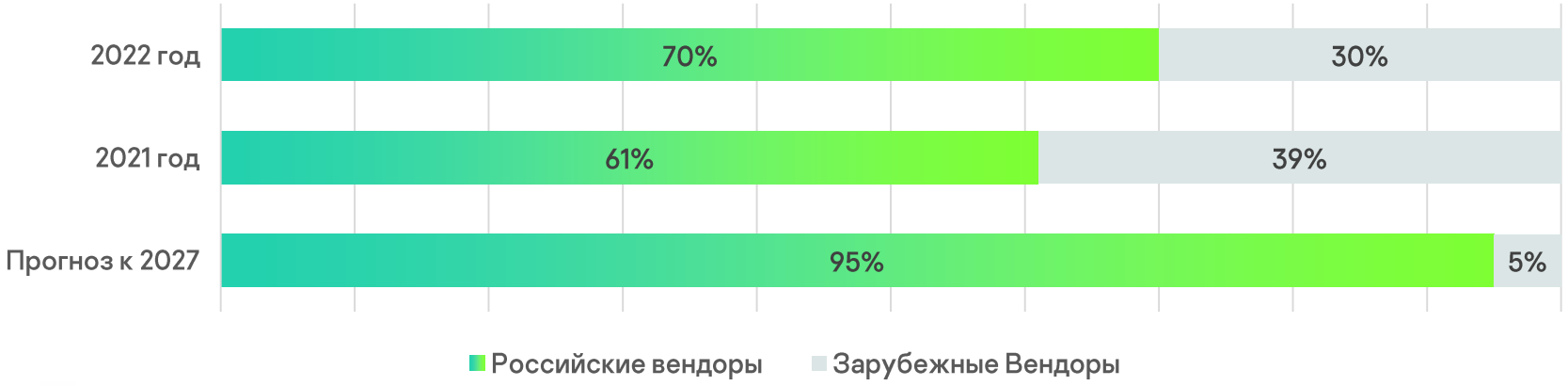
* По данным центра реагирования на инциденты «Лаборатории Касперского»

Промежуточные результаты импортозамещения

К лету 2023 года российский рынок покинули (прекратили продажи и/или поддержку) почти все ведущие иностранные вендоры ИБ, в том числе Fortinet, Palo Alto Networks, Trend Micro, Cisco, IBM, ESET, Broadcom (Symantec), Imperva, F5, CyberArk и др.

Продолжают свою деятельность из числа ведущих компаний отрасли только Check Point Software Technologies (Израиль) и Checkmarx (США)

Рисунок 2. Доля российских и зарубежных вендоров средств защиты



Источник: ЦСР

migration.kaspersky.ru

+300% спрос на программу по миграции на решения «Лаборатории Касперского»

Новая реальность. Стимулирование импортозамещения

Ответственность первых лиц организаций за обеспечение их информационной безопасности

Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»

Запрет закупка иностранного ПО для использования **на значимых объектах КИИ.** С 1 января 2025 года будет запрещено использование иностранного ПО **на всех объектах, определенных Указом Президента № 250**

Указ Президента от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры РФ»

Ужесточение **требования отраслевых регуляторов**, предъявляемые к заказчикам решений ИБ

Государственное **стимулирование развития отрасли ИБ** (субсидии, гранты, налоговые и прочие льготы и послабления)

Решения «Лаборатории Касперского» для реализации требований

Регуляторные акты	Решения Kaspersky	Закрытие требований	
Приказ ФСТЭК России №239 – промышленный сегмент	Kaspersky Symphony совместно с орг. мерами и KDP	**80%** **всех мер приказа ФСТЭК №239**	**84%** базового набора мер для объектов КИИ 3-й категории
Приказ ФСТЭК №239 – корпоративный сегмент	KICS совместно с орг. мерами	**85%** всех мер приказа ФСТЭК №239	**91%** базового набора мер для объектов КИИ 3-й категории
Приказ ФСБ России №196	KUMA + KATA + KICS + CyberTrace	**81%** всех мер приказа ФСБ №196	
Приказ ФСТЭК №21 (защита перс. данных) – корпоративный сегмент	Kaspersky Symphony совместно с орг. мерами и KDP	**74%** всех мер приказа ФСТЭК №21	**79%** базового набора мер для систем 3-го класса защищенности
Приказ ФСТЭК России №31 (защита АСУ ТП) – промышленный сегмент	KICS совместно с орг. мерами	**80%** всех мер приказа ФСТЭК №31	**85%** базового набора мер для АСУ ТП 3-й категорий

Актуальные потребности компаний в ИБ

Рост спроса на все основные решения экосистемы «Лаборатории Касперского» в 2022

Защита от массовых угроз

В первую очередь, компании нацелены на замещение решений на базе превентивных технологий, которые стоят на передовой защиты (узлы, почта, сеть)

до **+300%**

Защита от сложных угроз

Во вторую очередь, обращают внимание на замещение продвинутых технологий противодействия сложным атакам

до **+450%**

Управляемая защита MDR

Оперативно разворачиваемая управляемая защита для тех, кто не располагает временем на осознанный выбор необходимых ИБ решений.

Для компаний СМБ без выделенных служб ИБ передача функций кибербезопасности на аутсорс — зачастую единственный способ защититься от актуальных сложных киберугроз.

Продвинутая комплексная защита

Комплексный подход к ИБ позволит обезопасить компанию и её активы от многовекторных киберугроз за счет сокращения поверхности потенциальных атак.

- → KESB Расширенный
- → EDR Оптимальный
- → Optimum Security
- → Kaspersky Symphony

Предварительные данные «Лаборатории Касперского»

- Расширение продуктового портфолио
- Windows → Linux
- Поддержка наиболее востребованных платформ на базе отечественных ОС и российских платформ виртуализации

ASTRA LINUX®
РЕД Операционная система
alt linux
СКАЛА-Р
ТИОНИКС
Альт Сервер Виртуализации
БРЕСТ
ROSA VIRTUALIZATION
РЕД ВИРТУАЛИЗАЦИЯ
и другие

Развитие российских решений

Kaspersky Security для почтовых серверов

Защита корпоративной почты

Обновление 12.2022

Kaspersky SD-WAN

Построение безопасных сетей

Обновление 04.2023

Kaspersky Secure Mobility Management

Управление мобильностью

Запуск 04.2023

Kaspersky Container Security

Защита контейнерных сред

Запуск 07.2023

Kaspersky Embedded Systems Security for Linux

Защита встраиваемых систем на базе Linux

Расширение 07.2023

Превентивные средства защиты

Антивирус для корпоративной сети

Решение	Статус
TrendMicro Apex One (Япония)	
ESET Protect (Словакия)	
Symantec Endpoint Protection (США)	
Microsoft Defender (США)	
McAfee Endpoint Security (США)	

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 сторонних 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**

Антивирусная защита виртуальных сред и облаков

Решение	Статус
Trend Micro Hybrid Cloud Security (Япония)	
McAfee MOVE AntiVirus (США)	
Eset Virtualization Security (Словакия)	

Kaspersky Security для виртуальных сред

Light Agent

- Поддержка всех самых популярных гипервизоров
- Облегченный агент добавляет критичные возможности безопасности, сохраняя высокую плотность виртуальных машин
- Веб-контроль, Контроль устройств и приложений на основе политик
- Анализ поведения и защита от эксплойтов

Agentless

- Тесно интегрируется с основными платформами виртуализации
- Отсутствие дублирования, сохранение коэффициентов консолидации и высокой плотности виртуальных машин
- Простота администрирования и развертывания для мгновенной защиты и безопасности

Kaspersky Security для виртуальных сред

Kaspersky
Security для виртуальных
и облачных сред

О продукте

Помогает эффективно защищать виртуальные и облачные среды, позволяет управлять IT-инфраструктурой и обеспечивает ее прозрачность, не влияя на производительность системы и не мешая работе пользователей

Подробнее

Ключевые возможности

- Несколько вариантов исполнения, включая как безагентную защиту, так и на базе сверхлегкого агента
- Поддержка большого количества производителей сред виртуализация, включая платформы отечественного рынка
- Поддержка защиты гостевых систем на базе Windows, Linux, а также отечественных ОС
- Высокий уровень оптимизации затрат ресурсов гипервизоров в пользу работы бизнес-задач клиента
- Гибкая схема лицензирования решения по CPU, ядрам или защищаемым ОС
- Наличие государственных сертификации

Решения для управления корпоративной мобильностью

Решение	Статус
AirWatch by VMWare (США)	
XenMobile by Citrix (США)	
Ivanti (США)	

Kaspersky Secure Mobility Management

Kaspersky
Secure Mobility
Management

О продукте

Позволяет бизнесу безопасно, гибко и удобно использовать мобильные устройства в рабочих целях.

Подробнее

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

Решения для безопасной разработки и защиты контейнеров

Решение	Статус
Aqua Security (Израиль)	
Palo Alto (США)	
TrendMicro (Япония)	

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

Антивирусная защита промышленных сетей

Решение	Статус
Trend Micro Industrial Endpoint Security (Япония)	
McAfee Endpoint Security (США)	
Symantec endpoint Protection (США)	

Kaspersky Industrial CyberSecurity

for Nodes

Kaspersky Industrial CyberSecurity

Специализированная защита конечных точек для промышленности

- Позволяет не допустить ложных срабатываний и перерасхода системных ресурсов
- Значительно снижает затраты на обслуживание в сравнении с корпоративными решениями

Уменьшено потребление ресурсов

256-512 MB Оперативной памяти для Windows XP SP2 / XP Embedded

Установка / Обновление / Удаление без перезагрузки

Возможность работы в полностью неблокирующем режиме

Возможность обнаружения угроз нулевого дня (в том числе в неблокирующем режиме)

Контроль запуска приложений, Анализ логов, Мониторинг файловых операций

Kaspersky Industrial CyberSecurity for Nodes

for Nodes

Kaspersky Industrial CyberSecurity

О продукте

Создано специально для защиты промышленной инфраструктуры организации от киберугроз, предназначено для защиты промышленных панелей оператора, рабочих станций и серверов

Подробнее

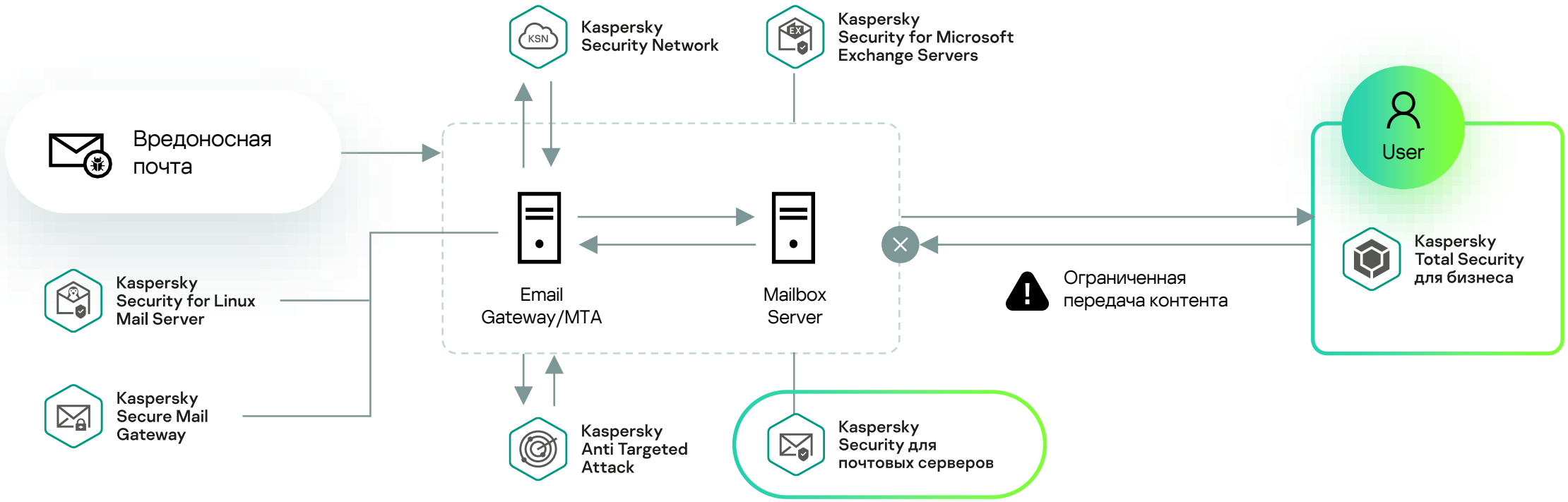
Ключевые возможности

- Незначительное влияние на защищаемое устройство за счет минимального потребления ресурсов и модульной архитектуры решения
- Контроли целостности ПЛК и файлов SCADA
- Расширенная защита от вредоносного ПО: шифровальщиков, эксплойтов, руткитов и т.д. Встроенные средства анализа журналов и управления сетевым экраном.
- Инструменты контроля для управления доступом к приложениям, подключенным устройствам и Wi-Fi сетям
- Высокий уровень совместимости с решениями вендоров АСУ-ТП, подтвержденный наличием сертификатов совместимости после совместных испытаний
- Поддержка Windows, Linux, включая устаревшие ОС на низкопроизводительном оборудовании.
- Наличие государственной сертификации

Защита почтового трафика

Решение	Статус
Fortinet FortiMail (США)	
Cisco IronPort (США)	
Barracuda Email Security Gateway (США)	
TrendMicro Email Security (Япония)	

Kaspersky Security для почтовых серверов



- Многоуровневая защита от ВПО и фишинга на основе ML
- Контентная фильтрация для защиты снижения риска заражения
- Автоматический анти-спам с репутацией
- Универсальное, готовое к использованию решение Secure Mail Gateway
- Обнаружение вредоносных скриптов
- Поддержка облачной инсталляции
- Поддержка Linux and MS Exchange почтовых серверов
- Углубленный анализ угроз с помощью Kaspersky Anti Targeted Attack

Kaspersky Security для почтовых серверов

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.)

Защита веб-трафика

Решение	Статус
Checkpoint Secure Web Gateway (Израиль)	
Fortinet FortiGate (США)	
Cisco WSA (США)	
ForcePoint Web Security - Websense (США)	
Kerio Control (США)	
TrendMicro Web Security (Япония)	

Kaspersky Security для интернет-шлюзов поставляется в виде виртуального устройства безопасности, которое включает прокси-сервер и средства его защиты

- Защищает корпоративную сеть от интернет-угроз, снижает риск утечки данных и повышает производительность труда за счет управления доступом к WEB-ресурсам
- Обрабатывает WEB-трафик, проходящий через прокси-сервер, и блокирует все, что представляет опасность с точки зрения корпоративной политики

Анти-вирус | Анти-фишинг | URL-репутация | Контентная фильтрация | WEB-контроль

Kaspersky Security для интернет-шлюзов

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

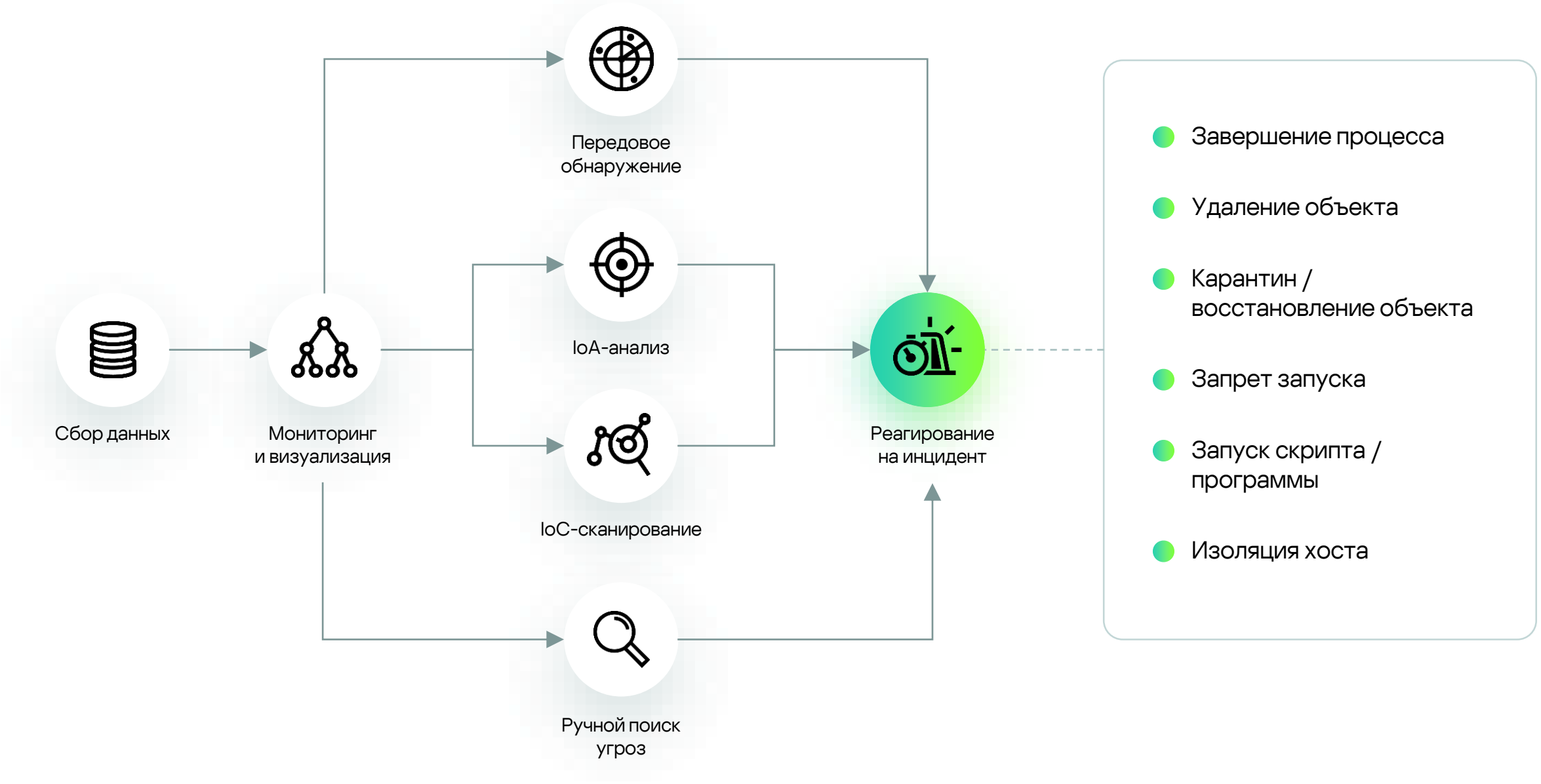
- Продвинутые технологии антивирусной защиты (AM-движок, интеграция с KATA)
- Инспекция SSL трафика
- URL/IP репутация
- Контроль доступа к Web-ресурсам, предопределенные списки категорий
- Анализ контента, обнаружение вредоносных скриптов
- Настройки доступа для приложений (по user агенту)
- Поддержка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

Продвинутые решения выявления сложных угроз

Endpoint Detection and Response (EDR)

Решение	Статус
Cisco AMP (США)	
Microsoft ATP (США)	
PaloAlto EDR (США)	
Fortinet FortiEDR (США)	
TrendMicro Apex One (Япония)	
Checkpoint Sandblast Agent (Израиль)	

Kaspersky EDR



Kaspersky
EDR Expert

О продукте

Решение класса EDR экспертного уровня для обнаружения, расследования и реагирования на сложные угрозы и целевые атаки на уровне конечных точек (защищаемых устройств)

Подробнее

Ключевые возможности

- Продвинутые технологии обнаружения (AM-движок, Sandbox, IoC, IoA)
- Обновляемые правила автоматического детектирования на основе MITRE
- Автоматизированный и ручной поиск угроз (Threat hunting)
- Автоматическое и ручное реагирование (Response) на защищаемых устройствах (изоляция устройств, остановка процессов, изъятие объекта и др)
- API для реагирования из сторонних систем
- Дополнение NDR-решений до класса XDR (защитой уровня конечных точек (EDR))
- Поддержка Windows и Linux систем, включая отечественные ОС
- Интеграция с антивирусным решением для обмена информацией и кросс-сценариев

Защита от целенаправленных атак (NTA, Sandbox, AntiAPT)

Решение	Статус
Checkpoint Sandblast (Израиль)	
Cisco Sandbox (США)	
FireEye NX, EX, FX (США)	
PaloAlto WeldFire (США)	
TrendMicro Deep Discovery Inspector (Япония)	
Fortinet FortiSandbox (США)	

Kaspersky Anti Targeted Attack (KATA)

- Sandbox
- Anti-Malware Engine
- Intrusion Detection System
- YARA
- GOSHA engine (Cloud APK sandbox)
- KSN / KPSN

* Threat Intelligence | ** MITRE Framework

Kaspersky Anti Targeted Attack (KATA)

Kaspersky
Anti Targeted
Attack

О продукте

Решение класса NTA/NDR
для обнаружения, расследования
и реагирования на сложные угрозы
и целевые атаки на уровне сети

Подробнее

Ключевые возможности

- Различные варианты интеграции в инфраструктуру (inline, mirror)
- Быстрое масштабирование, поддержка различных схем развертывания
- Продвинутые технологии обнаружения на уровне сети (AM-движок, IDS Sandbox)
- Встроенный инструментарий для написания своих собственных правил обнаружения(Yara, IDS)
- Получение по API объектов на проверку из сторонних систем
- Автоматическое и ручное реагирование (Response) на веб и почтовых шлюзах (интеграция с KSMG и KWTS)
- Дополнение EDR-решений до класса XDR (защитой уровня сети (NDR))

Security information and event management (SIEM)

Решение	Статус
IBM Qradar (США)	
Fortinet FortiSIEM (США)	
MicroFocus ArcSight ESM (США)	
ELK	

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Kaspersky
Unified Monitoring
and Analysis Platform

- Kaspersky Anti Targeted Attack
- Kaspersky Sandbox
- Kaspersky Research Sandbox
- Kaspersky EDR Expert
- Kaspersky Threat Lookup
- Kaspersky Security Center
- Kaspersky Threat Data Feeds
- Kaspersky Secure Mail Gateway
- Kaspersky Threat Intelligence
- Endpoint Security

Производительность

300k+ EPS на одну ноду

Низкие системные требования

Гибкая архитектура

Современная микросервисная архитектура

Интеграция «из коробки»

С решениями «Лаборатории Касперского» и сторонних поставщиков

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Kaspersky
Unified Monitoring
and Analysis Platform

О продукте

KUMA SIEM - это центральный элемент единой платформы безопасности от «Лаборатории Касперского», который взаимодействует как с решениями ЛК, так и с разработками сторонних поставщиков

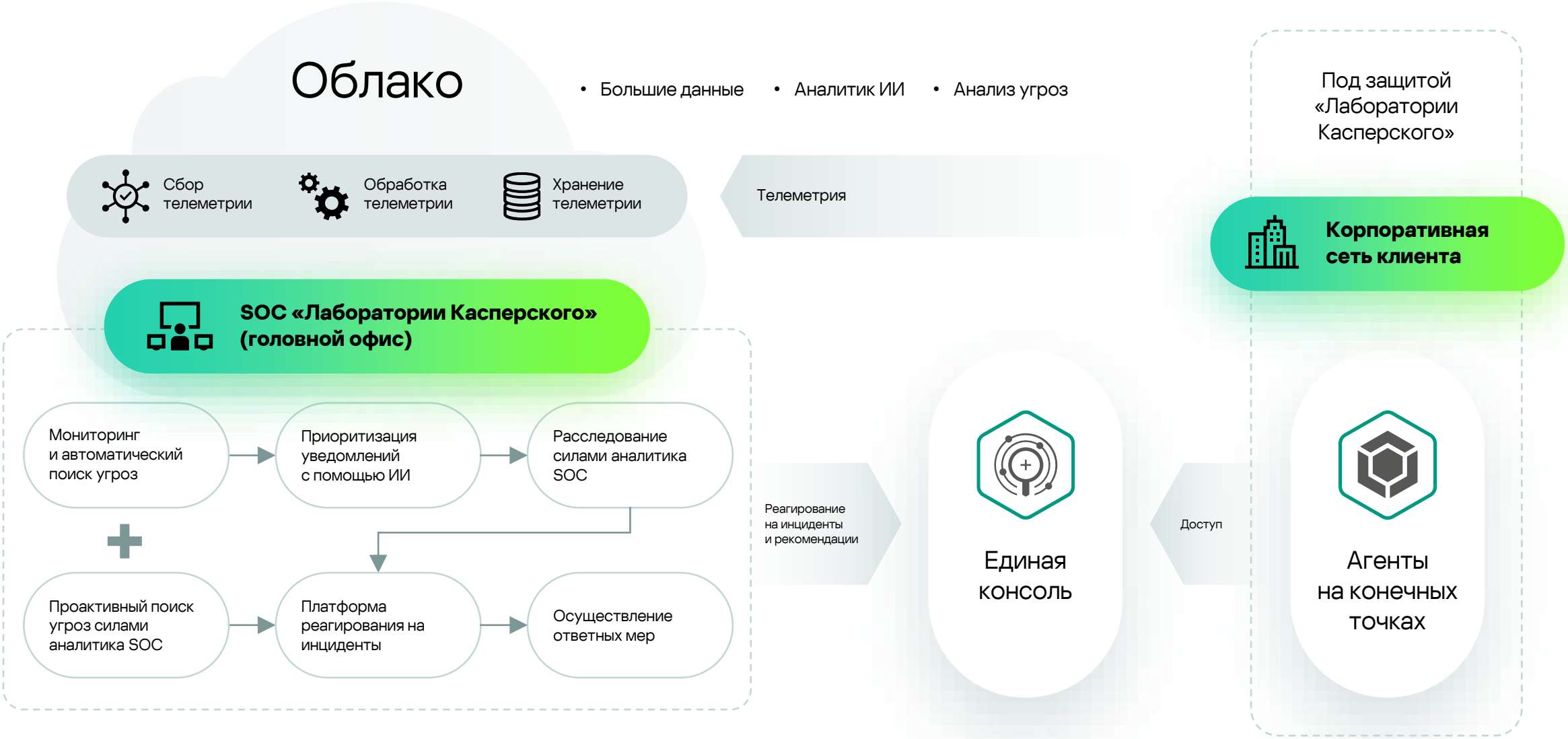
Подробнее

Ключевые возможности

- Ситуационная осведомлённость и аналитика - дашборды и отчёты по актуальному состоянию ИБ для отслеживания трендов (C-level) и операционной работы по поиску аномалий
- Мониторинг безопасности - непрерывная корреляция потока событий от источников для выявления инцидентов ИБ
- Реагирование на инциденты - единая консоль позволяет обогатить карточки инцидентов дополнительной информацией (по индикаторам компрометации, активам, пользователям) и запустить задачи реагирования через KES, EDR, ASAP и другие решения
- Проактивный поиск угроз - быстрый поиск ClickHouse по всей собранной информации с использованием возможностей SQL-запросов или применение ретроспективной корреляции для выявления подозрительных цепочек событий
- Соответствие требованиям - KUMA имеет сертификат ФСТЭК, свидетельство о регистрации, включена в реестр отечественного ПО и позволяет выполнять требования 187-ФЗ, приказа ФСТЭК России № 239, рекомендаций ЦБ и других НПА.
- Поддержка отечественной ОС (Astra Linux)

Kaspersky MDR

Kaspersky Managed Detection and Response



Ключевые преимущества сервиса по круглосуточной управляемой защите

Быстрый старт предоставления сервиса

Сервис оказывается на ресурсах расположенных в России

Уверенность в том, что вы находитесь под постоянной защитой даже от самых сложных угроз

Возможность направить внутренние ИБ-ресурсы компании на решение по-настоящему важных задач

Сокращение расходов на безопасность из-за отсутствия необходимости нанимать новых ИБ-специалистов

Возможность пользоваться ключевыми преимуществами центра SOC, не имея его внутри компании

Kaspersky Symphony

Гибкий выбор

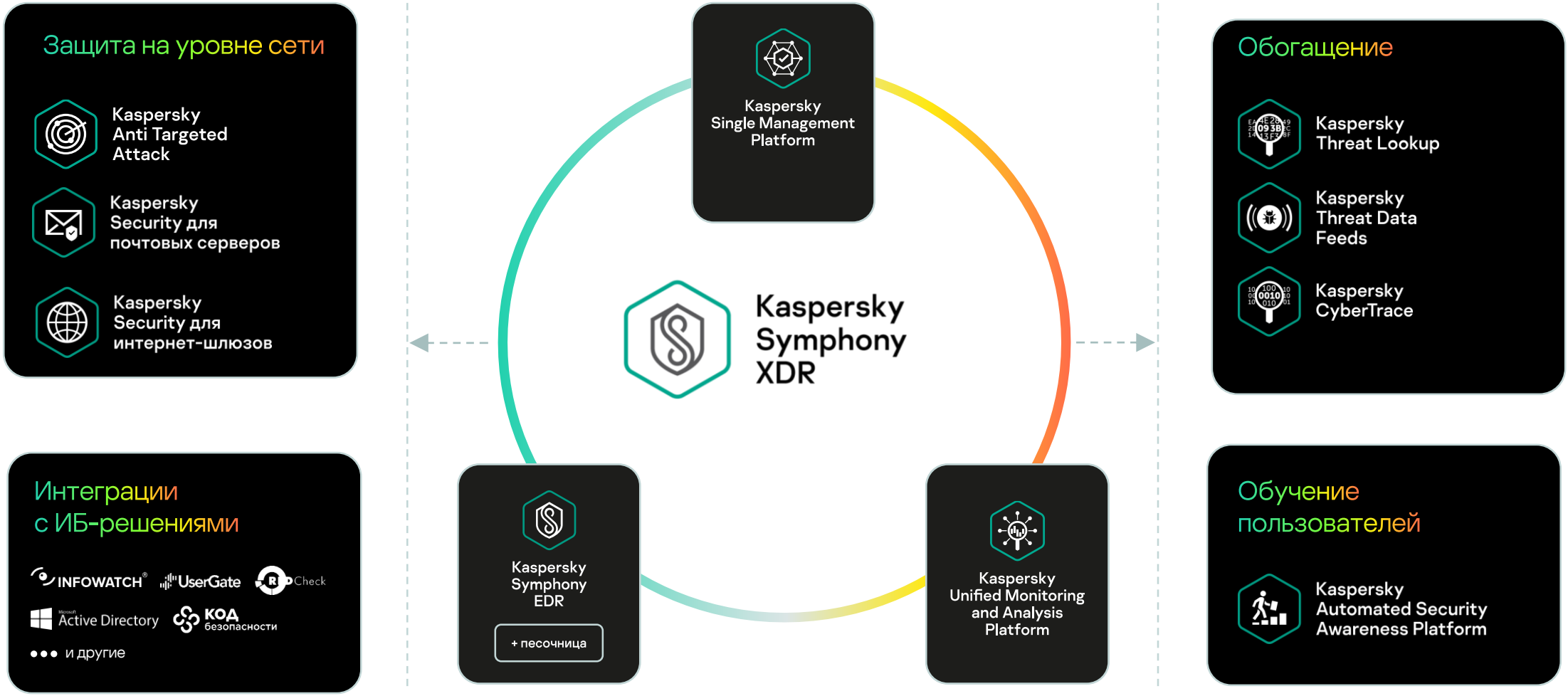
Подберите уровень защиты, который подходит именно для вашего бизнеса

Функциональное сравнение уровней Kaspersky Symphony

Kaspersky Symphony	Security	MDR	EDR	XDR
Уровень защиты	Базовая собственная защита	Передовая управляемая защита	Передовая собственная защита	Расширенная собственная защита
Автоматическая защита конечных точек (физических, мобильных и виртуальных) от массовых угроз	●	●	●	●
Передовое обнаружение сложных угроз на уровне конечных точек и реагирование на них		●	●	●
Детектирование с помощью передовой песочницы и реагирование на обнаружения				●
Комплексный мониторинг и корреляция событий ИБ (SIEM), встроенный модуль ГосСОПКА, интеграция с различными ИБ- системами				●
Управление аналитическими данными о киберугрозах (TI Platform) и встроенные потоки данных (data feeds)				●
Защита электронной почты (SEG), и веб-трафика (SWG)				●
Глубокий анализ сетевого трафика (NTA) и реагирование на уровне шлюзов				●
Повышение киберграмотности				●

XDR Core

Kaspersky Symphony XDR: комплексное ИБ-замещение в одной позиции



Состав XDR Core

Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Автоматические

Автоматическая блокировка на уровне почтового шлюза неизвестных вредоносных объектов, обнаруженных детектирующими механизмами KATA (до доставки получателю)

Взаимодействие веб-шлюза и KATA через API для передачи объектов из веб-трафика на проверку в песочницу и последующей их автоматической блокировки в случае выявленной вредоносной нагрузки

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике

Автоматическое отслеживание и реагирование на изменения состояния активов в том числе статусов компонентов защиты, наличия уязвимостей и тд.

Передача релевантных сложных атакам событий с KATA, KES, KEDR, KSMG, KWTS в KUMA для корреляции с данными от сторонних источников

Автоматическое обогащение карточки инцидента в KUMA информацией об уровне осведомленности атакованного пользователя

Реагирование через EDR на найденные угрозы в KUMA:

- Изоляция хоста и снятие с изоляции
- Блокировка хеша по md5 и sha256 на хосте
- Запуск исполняемого файла на хосте по полному пути
- Логирование реагирования в системном журнале

Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace:

- Централизованная блокировка доступа пользователей к вредоносному домену
- Запрет скачивания вредоносных файлов из сети Интернет при получении вердикта от KATA Sandbox

Автоматическое создание и обновление карточек активов на основании информации от KSC

Автоматическое реагирование на найденные угрозы в KUMA средствами сторонних решений через запуск различных сценариев

Сбор данных и реагирование на инциденты из KWTS

Передача сырой телеметрии с EDR в KUMA

* В ближайшем Roadmap

Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

Полуавтоматические

Доступ в Threat Lookup для получения дополнительного контекста для эффективного расследования

Построение и обогащение модели активов в KUMA на основании данных из KSC

Принудительный запуск обновления баз, антивирусной проверки, установки патча и других задач через KSC с карточки инцидента в KUMA

Запуск действий по реагированию через EDR с карточки инцидента в KUMA*

Возможность назначить обучение по повышению киберграмотности из карточки инцидента в KUMA*

Передача информации о произошедших инцидентах в НКЦКИ, благодаря встроенному в решение модулю ГосСОПКА

* В ближайшем Roadmap

Предварительные выводы и прогнозы

Решения российских вендоров уже сейчас позволяют заменить защитные продукты ушедших с рынка иностранных вендоров в основных категориях

Продолжение активного перехода на российское ПО в течение ближайших 5 лет

Продолжение роста рынка кибербезопасности в России

Ожидается существенный рост объема рынка услуг по кибербезопасности (внедрение, сопровождение, консалтинг, аутсорс, оценка защищенности, расследование инцидентов и т.д.)

Развитие российских решений во всё новых нишах

Мигрируй

1

Скидка 40%

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.

3

Пользуйтесь дольше

Пользуйтесь нашими продуктами дольше, если срок действия старой лицензии еще не истек

Мигрируй!

Подробнее