Киберзащита бизнеса в России

Трансформация потребностей клиентов СМБ

kaspersky

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

Неопределенность. Больше рисков. Поиск решения

Интерактивная карта киберугроз

Подробнее

Рост количества атак и их усложнение

Количество и сложность киберинцидентов в российских компаниях растут. Рост Q1 2021 vs Q12022 составил **+300%***

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»

Новая реальность. Ландшафт киберугроз

38% Нарушение сотрудниками политик безопасности

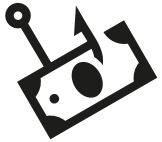
5.62 среднее количество инцидентов в одной компании за год.

26% Заражение корпоративных устройств вредоносным ПО

4.28 среднее количество инцидентов в одной компании за год.

31% DDoS-атаки

4.71 среднее количество инцидентов в одной компании за год.



19% Фишинг и социальная инженерия, нацеленные на клиентов

4.71 среднее количество инцидентов в одной компании за год.

18% Таргетированные атаки (APT, «кастомизированное» ПО)

3.21 среднее количество инцидентов в одной компании за год.

% компаний, столкнувшихся с киберинцидентами, и среднее количество таких инцидентов в России за последние 12 месяцев.

Источник: Данные опроса Kaspersky, 2022

Новая реальность бюджеты бизнеса на ИБ в России

2022

Enterprise	СМБ
$1,375 млн	$0,038 млн

2025

Enterprise	СМБ
+12%	+16%

Ключевые факторы прогнозов по росту бюджетов на ИБ

- Необходимость расширить компетенции специалистов по кибербезопасности
- Новые риски в связи с геополитическими факторами
- Растущая сложность IT-инфраструктуры компании

Источник: Данные опроса Kaspersky, 2022

Новая реальность. Импортозамещение

Уход иностранных вендоров ИБ – свершившийся факт.

Импортозамещение ПО – острая необходимость. Даже если решения ушедших с российского рынка поставщиков продолжают работать, они становятся гораздо менее эффективны. Это несёт огромные риски.

Российские производители обладают технологиями и экспертизой, чтобы заменить большинство основных решений ушедших из России вендоров.

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

migration.kaspersky.ru

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.

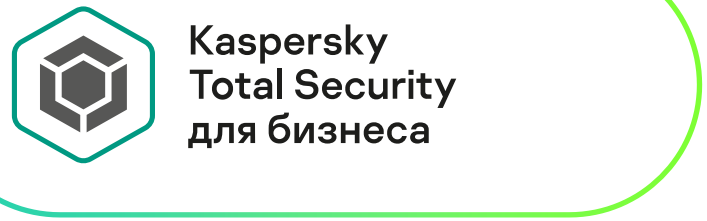
- → KESB Расширенный
- → EDR Оптимальный
- → Optimum Security
- → Kaspersky Symphony

Предварительные данные «Лаборатории Касперского»

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)	



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

CITRIX KVM vmware TIONIX openstack PROXMOX Microsoft Hyper-V

Agentless

- Тесно интегрируется с VMware NSX Vsphere и vShield
- Отсутствие дублирования, сохранение коэффициентов консолидации и высокой плотности виртуальных машин
- Простота администрирования и развертывания для мгновенной защиты и безопасности

vmware

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, for Networks)

Industrial Endpoint Protection

- 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

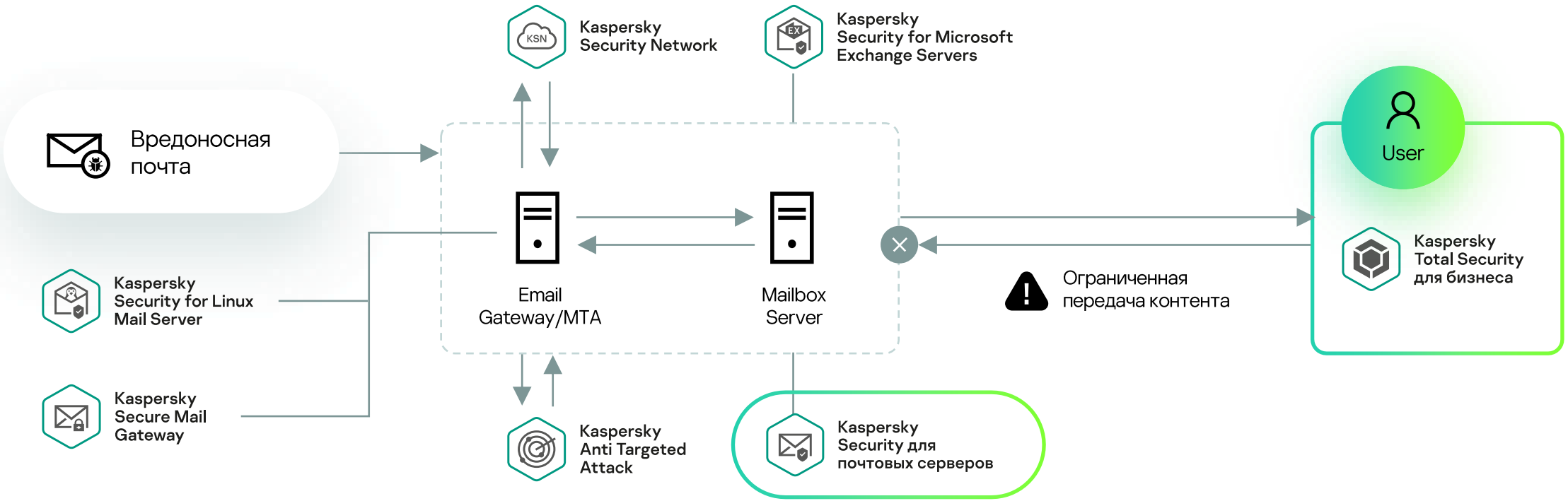
Возможность обнаружения угроз нулевого дня (в том числе в неблокирующем режиме)

Контроль запуска приложений, Анализ логов, Мониторинг файловых операций

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

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 Web Traffic Security 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

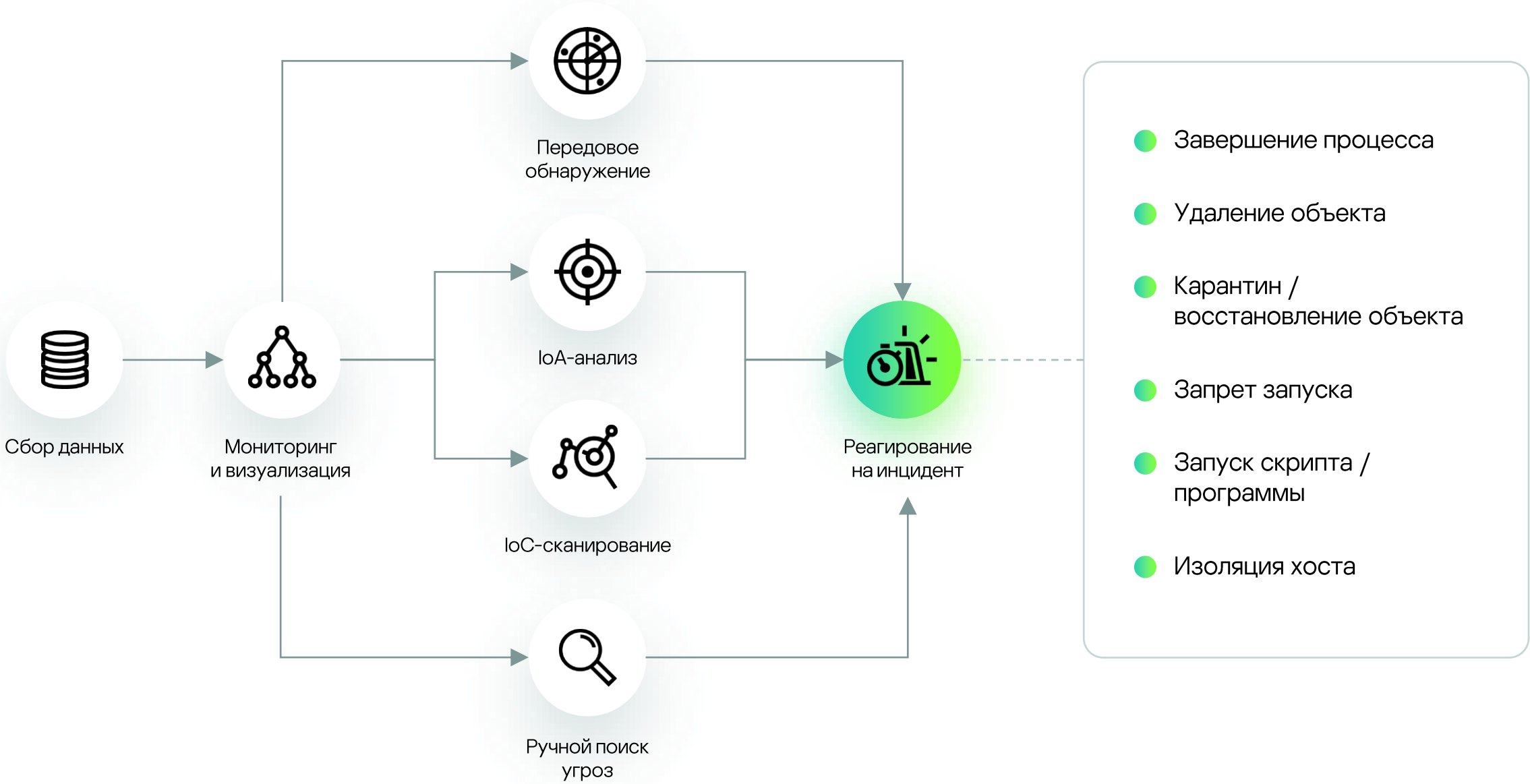
Анти-вирус | Анти-фишинг | URL-репутация | Контентная фильтрация | WEB-контроль

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



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

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)

Производительность

300k+ EPS на одну ноду

Низкие системные требования

Гибкая архитектура

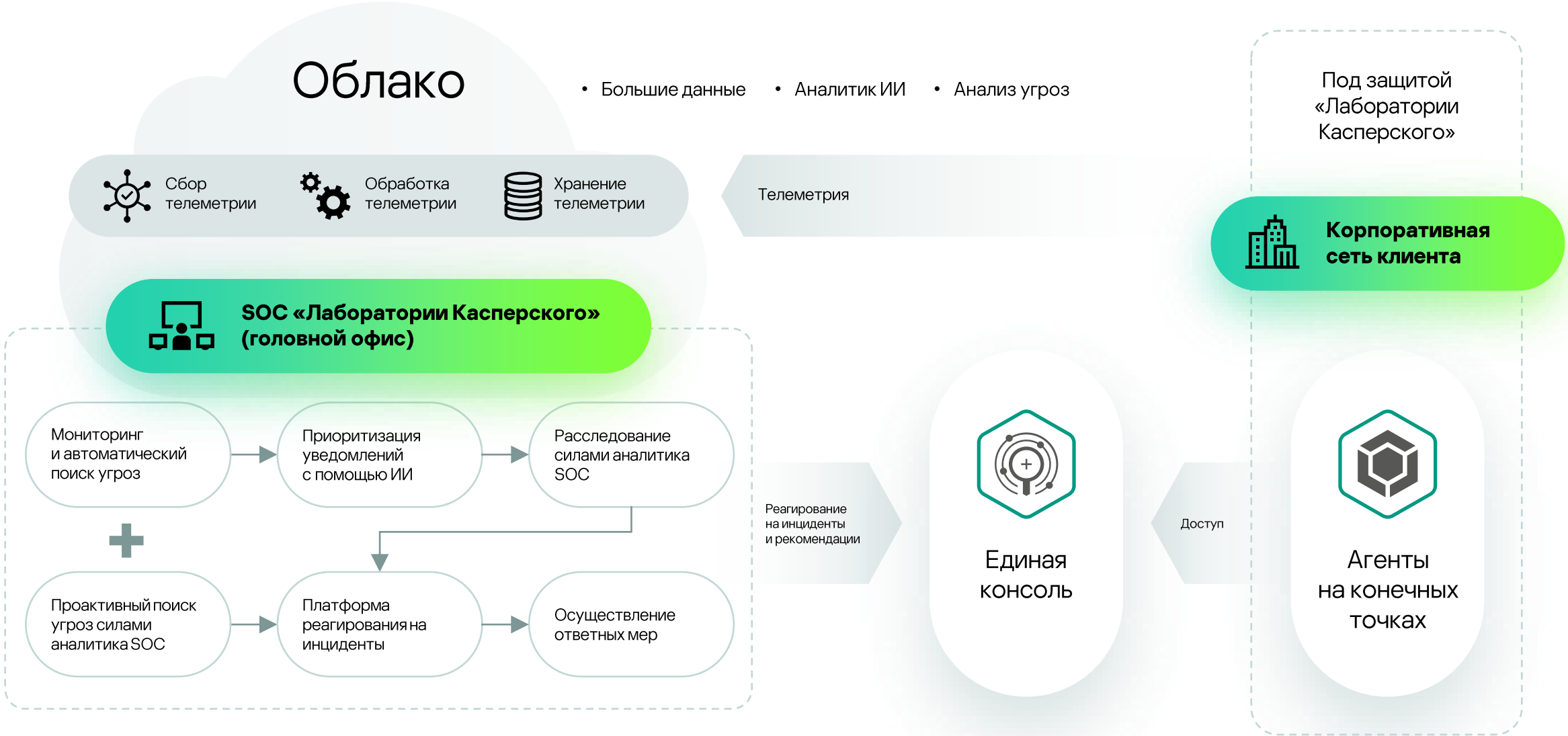
Современная микросервисная архитектура

Интеграция «из коробки»

С решениями «Лаборатории Касперского» и сторонних поставщиков

Kaspersky MDR

Kaspersky Managed Detection and Response



Kaspersky Symphony

Гибкий выбор

Подберите уровень защиты, который подходит именно для вашего бизнеса

Функциональное сравнение уровней Kaspersky Symphony

Kaspersky Symphony	Security	EDR	MDR	XDR
Уровень защиты	Базовая собственная защита	Передовая собственная защита	Передовая управляемая 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		●	●	●
Защита электронной почты и анализ сетевого трафика				●
Комплексный мониторинг и корреляция событий ИБ (+модуль ГосСОПКА)				●
Управление аналитическими данными о киберугрозах				●
Повышение киберграмотности				●

\+ Лицензирование по устройствам

Kaspersky Symphony XDR: комплексное ИБ-замещение в одной позиции

Защита конечных точек

Kaspersky Symphony **EDR**

- Kaspersky Endpoint Detection and Response

Kaspersky Symphony **Security**

- Kaspersky Endpoint Security для бизнеса
  Расширенный
- Kaspersky Security для виртуальных и облачных сред

Kaspersky Symphony XDR

Threat Intelligence

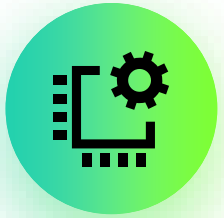
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky CyberTrace

Набор ИБ-продуктов

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов
- Kaspersky Automated Security Awareness Platform
- Kaspersky Unified Monitoring and Analysis Platform

Интеграция с ИБ-решениями сторонних поставщиков

Примеры сценариев взаимодействия элементов Kaspersky Symphony XDR

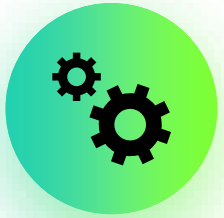


Автоматические

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочницей в сетевом и почтовом трафике	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
Потоковое обогащение событий в KUMA, предварительно обработанных в CyberTrace	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*
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

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

Спасибо!