

Киберзащита бизнеса в России

**как оптимально обеспечить
стабильность бизнеса в новых условиях**

kaspersky

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

Неопределенность. Больше рисков. Поиск решения

Интерактивная карта
киберугроз

Подробнее



Усложнение атак

Количество киберинцидентов в российских компаниях увеличилось в 4 раза (Q1 2021 vs Q1 2022)*



Киберагрессия

Россия номер 1 в мире по количеству атак



Срочное замещение

Ряд различных защитных ИБ решений становятся менее эффективными, риски пропустить сложную кибератаку значительно повышаются

* По данным центра реагирования на инциденты «Лаборатории Касперского»



Fortinet остановила работу в России

Fortinet® (NASDAQ: FTNT), мировой лидер в области комплексных, интегрированных и автоматизированных решений в области кибербезопасности, объявила сегодня о прекращении операций в России. Компания остановила все продажи, поддержку и профессиональные услуги Fortinet. Fortinet продолжает следовать всем протоколам безопасности, а также законам и рекомендациям правительства США и других стран.



Cisco ушла из России. Будущее ее устройств под угрозой

Американская корпорация Cisco прекращает поставки своей продукции в Россию и Белоруссию. Остановлена также работа сервиса Webex и Сетевой академии Cisco. Работоспособность уже приобретенных устройств, требующих подписку, под вопросом.



Из России сбежала Microsoft. Россияне остались без Windows, MS Office и Azure

Microsoft свернула все операции в России на неопределенный срок, сославшись на американские санкции против России из-за ситуации на Украине. Россияне лишатся доступа к ее облачным сервисам, а также, возможно, к игровым приставкам и обновлениям Windows и Office.



Защита от массовых угроз

В первую очередь, необходимо обратить внимание на замещение решений на базе превентивных технологий, которые стоят на передовой защиты (узлы, почта, сеть)



Защита от сложных угроз

Во вторую очередь, обратить внимание на замещение продвинутых технологий противодействия сложным атакам (EDR, SIEM, NTA, Anti-APT, Sandbox, XDR и пр.)



Управляемая защита MDR

Оперативно разворачиваемая управляемая защита от «Лаборатории Касперского» для тех, кто не располагает временем на осознанный выбор необходимых ИБ решений



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
Total 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 полnodискового шифрований, управление встроенными в операционную систему функциями шифрования
- Полная поддержка функционирования системы на отечественных ОС и базах данных

Антивирусная защита виртуальных сред и облаков

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



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

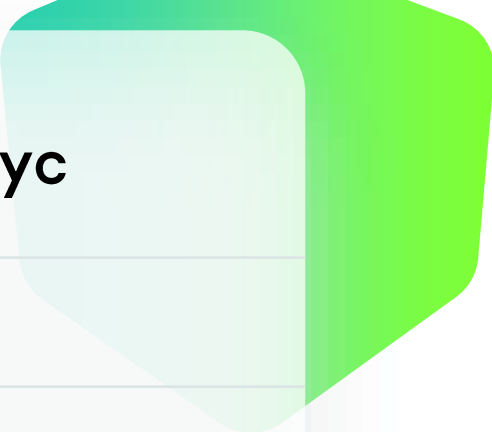
  

Agentless

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

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)

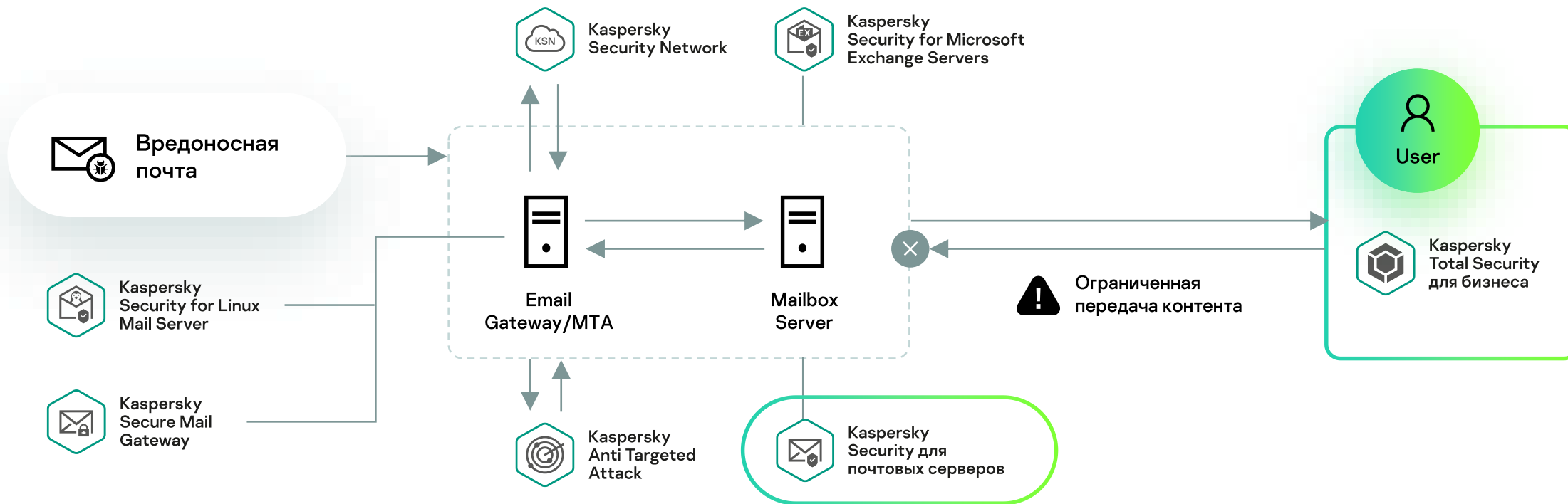
Контроль запуска приложений, Анализ логов, Мониторинг файловых операций

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

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
- Обработывает WEB-трафик, проходящий через прокси-сервер, и блокирует все, что представляет опасность с точки зрения корпоративной политики

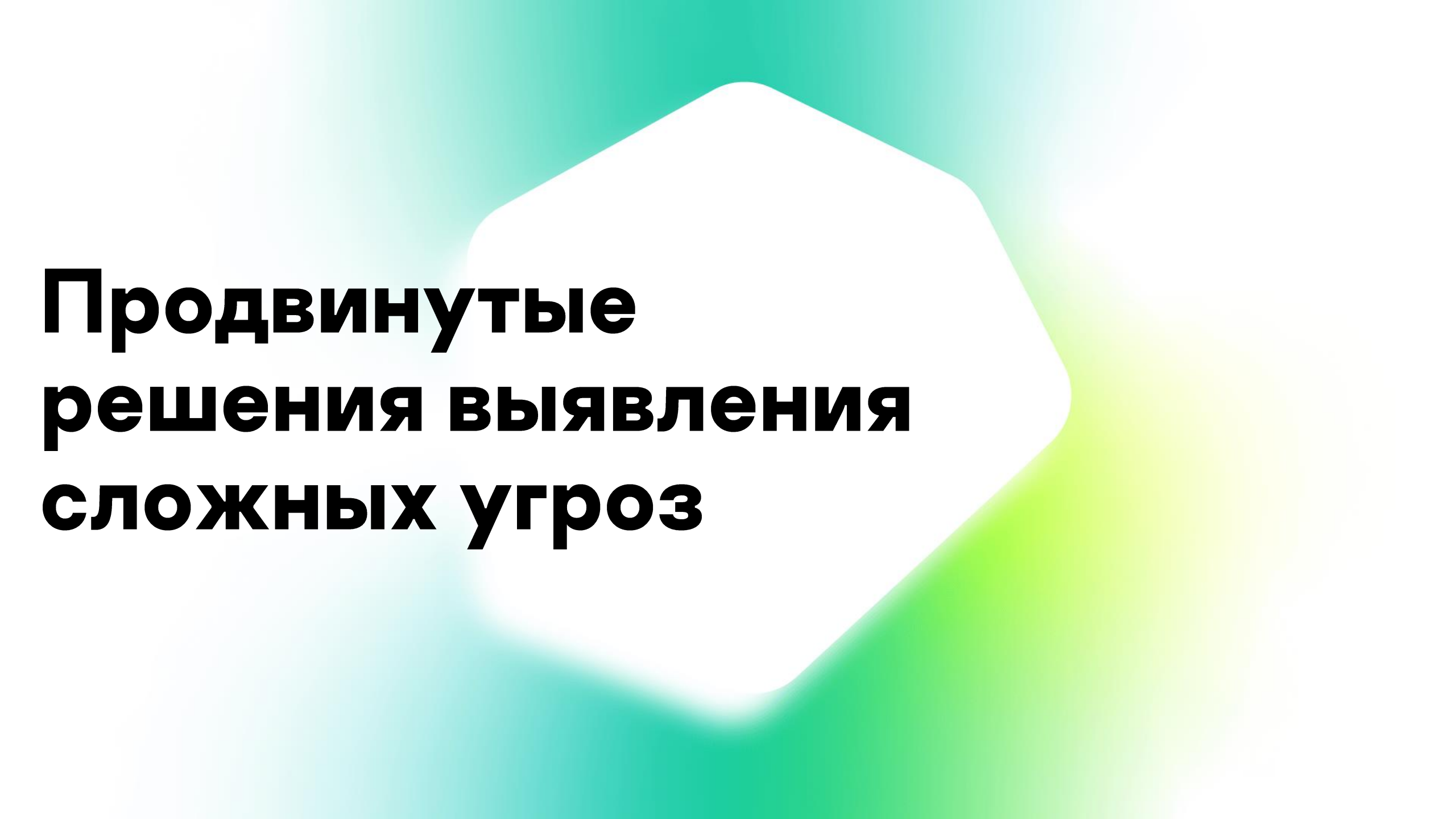
Анти-вирус

Анти-фишинг

URL-репутация

Контентная фильтрация

WEB-контроль

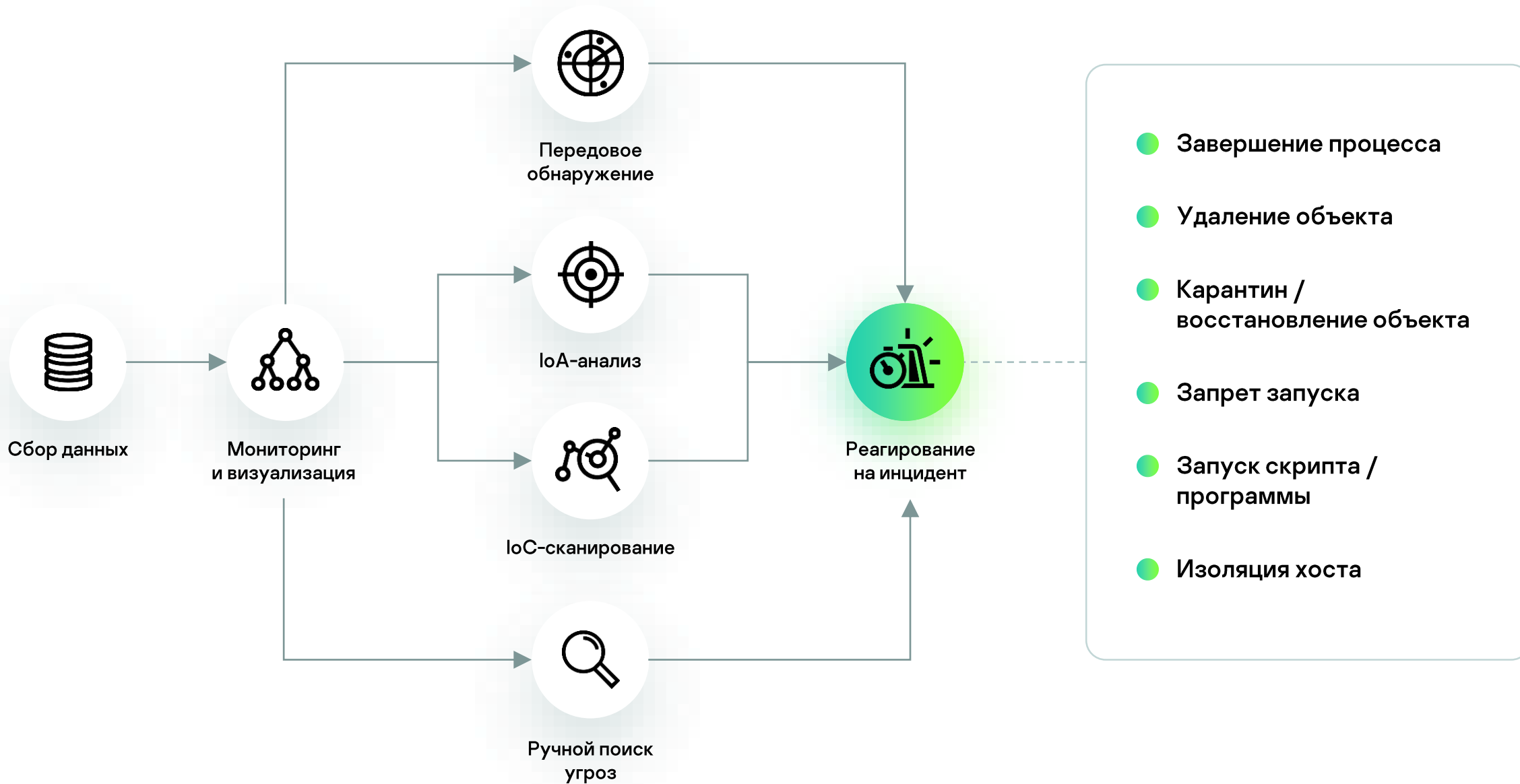


**Продвинутое
решения выявления
сложных угроз**

Endpoint Detection and Response (EDR)

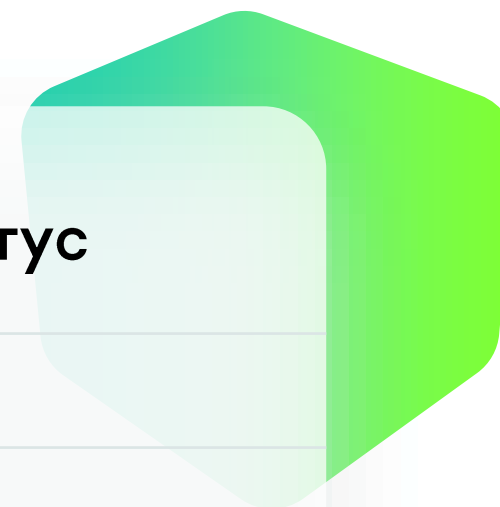
Решение	Статус
Cisco AMP (США)	●
Microsoft ATP (США)	●
PaloAlto EDR (США)	●
Fortinet FortiEDR (США)	●
TrendMicro Apex One (Япония)	●
Checkpoint Sandblast Agent (Израиль)	●





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

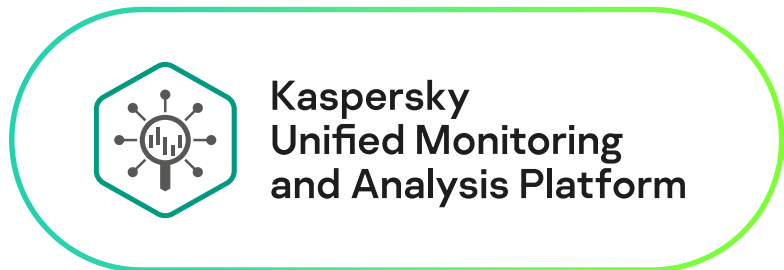


Security information and event management (SIEM)

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



Kaspersky Unified Monitoring and Analysis Platform (KUMA)



Kaspersky
Anti Targeted
Attack



Kaspersky
Sandbox



Kaspersky
Research Sandbox



Kaspersky
Endpoint Detection
and Response



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 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



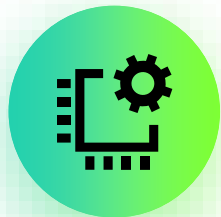
Kaspersky Automated Security Awareness Platform



Kaspersky Unified Monitoring and Analysis Platform



Интеграция с ИБ-решениями сторонних поставщиков



Автоматические

Автоматическая блокировка на хостах неизвестных вредоносных объектов при обнаружении песочниц 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 атак 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



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

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.

Если истек не более 30 дней назад, тоже приносите

3

Пользуйтесь дольше

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

Мигрируй!



[Подробнее](#)

Спасибо!