kaspersky
Platinum Partner

Обнаружение и реагирование на сложные атаки

Kaspersky Anti Targeted Attack

Kaspersky Endpoint Detection and Response

Руководитель направления решений «Лаборатории Касперского»
Константин Никитин

ПОЛИКОМ про

Kaspersky Symphony XDR

Защита конечных точек

Kaspersky Symphony EDR

- Kaspersky Endpoint Detection and Response
- \+
- Endpoint Security для бизнеса РАСШИРЕННЫЙ
- Kaspersky Security для виртуальных и облачных сред

Обучение пользователей

- Kaspersky Automated Security Awareness Platform (ASAP)

Kaspersky

Unified Monitoring and Analysis Platform

\+

Интеграция с решениями сторонних поставщиков

Защита на уровне сети

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Threat Intelligence

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

www.polikom.ru

Kaspersky
Anti Targeted
Attack

&

Kaspersky
Endpoint Detection
and Response

ПОЛИКОМ про

Kaspersky Anti Targeted Attack

Комплексное решение для защиты
от сложных угроз и APT-атак с расширенным
функционалом обнаружения и реагирования
на уровне сети и конечных устройств
(при взаимодействии с Kaspersky EDR Expert)

ПОЛИКОМ про

Архитектура решения – компоненты

KATA и KEDR Expert построены на единой технологической платформе

Central Node (Центр анализа)

Основной серверный компонент платформы. Выполняет проверку данных, их анализ, а также публикацию результатов исследования в веб-интерфейс программы

Sandbox (Песочница)

Запускает виртуальные образы операционных систем и отслеживает поведение файлов в них с целью обнаружения вредоносной активности и признаков целевых атак на IT-инфраструктуру организации

ПОЛИКОМ про

Архитектура решения – компоненты

Для автоматического сбора и последующей передачи информации для анализа, KATA и KEDR Expert используют:

Sensor
(Сетевой сенсор)
Выполняет прием данных из сетевого, веб-трафика и почтового трафика, а также данных с хостов, защищаемых компонентом Endpoint Agent или Kaspersky Endpoint Security для передачи их на сервер с компонентом Central Node

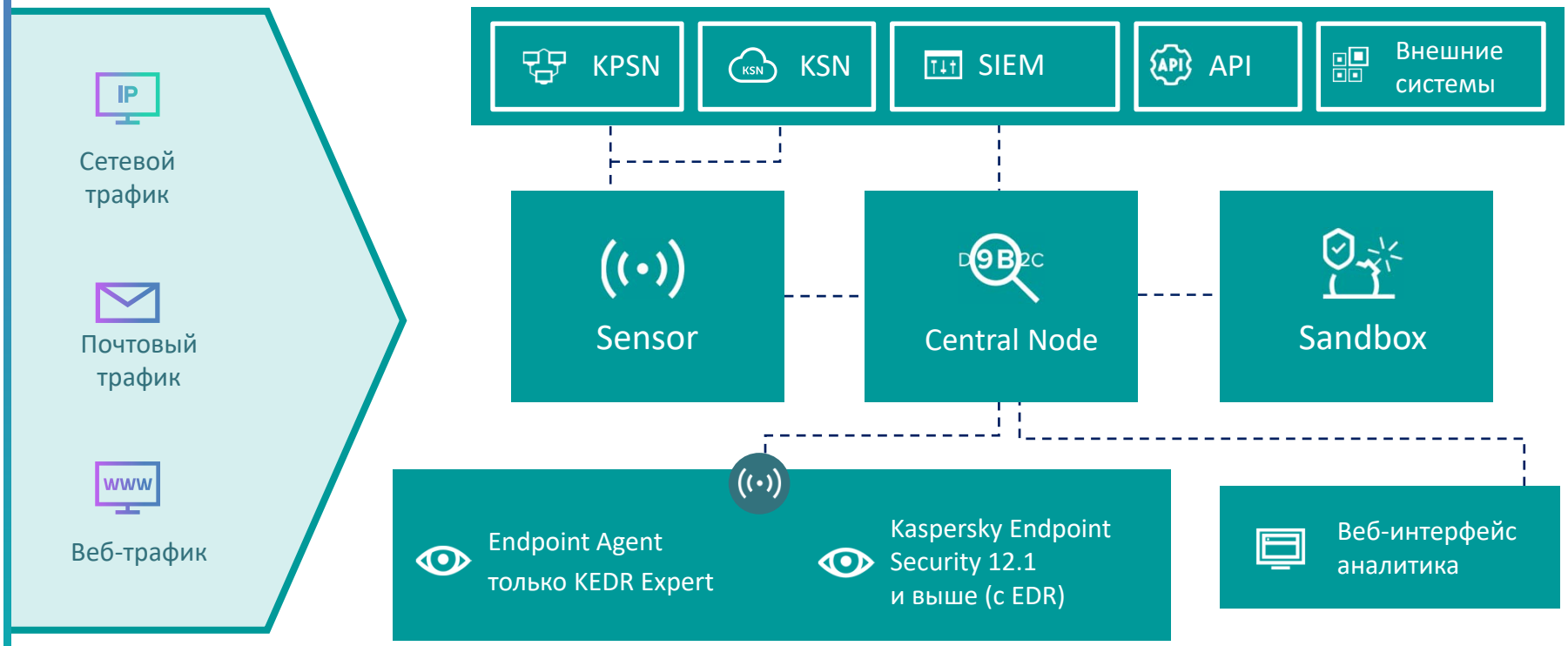
Endpoint Agent
(Агенты на конечных точках)
Устанавливается на рабочие станции и серверы, входящие в IT-инфраструктуру организации и работающие под управлением операционных систем семейств Microsoft Windows, GNU/Linux.
Осуществляет постоянное наблюдение за процессами, запущенными на этих компьютерах, открытыми сетевыми соединениями и изменяемыми файлами

ПОЛИКОМ про

Платформа KATA с EDR: расширенные возможности защиты (XDR)

ПОЛИКОМ про

Архитектура решения: типовое развертывание на 3 сервера



ПОЛИКОМ про

Sensor: поддерживаемые источники данных

Компонент Sensor может получать и обрабатывать данные следующими способами:

Интегрироваться в локальную сеть

получать и обрабатывать зеркалированный SPAN-, ERSPAN- и RSPAN-трафик и извлекать объекты и метаинформацию HTTP-, FTP-, MTP- и DNS-протоколов

Подключаться к почтовому серверу

по протоколам POP3(S) и SMTP, получать и обрабатывать копии сообщений электронной почты

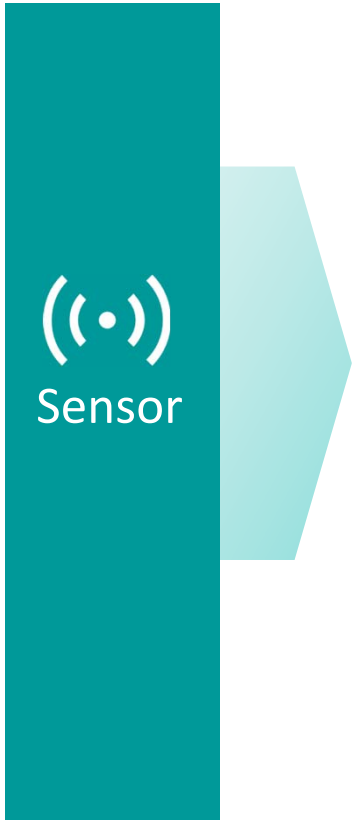
Подключаться к прокси-серверу

по протоколу ICAP, получать и обрабатывать данные HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на собственном прокси-сервере

Прокси-сервер для соединений

Компонент Sensor может использоваться в качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent

Шлюзы в роли компонента Sensor



Kaspersky Security для почтовых серверов

В качестве компонента Sensor может использоваться почтовый шлюз – Kaspersky Security для почтовых серверов, отправляющий сообщения электронной почты на обработку в KATA.
По результатам обработки в решении KATA продукт может блокировать пересылку сообщений конечным пользователям.

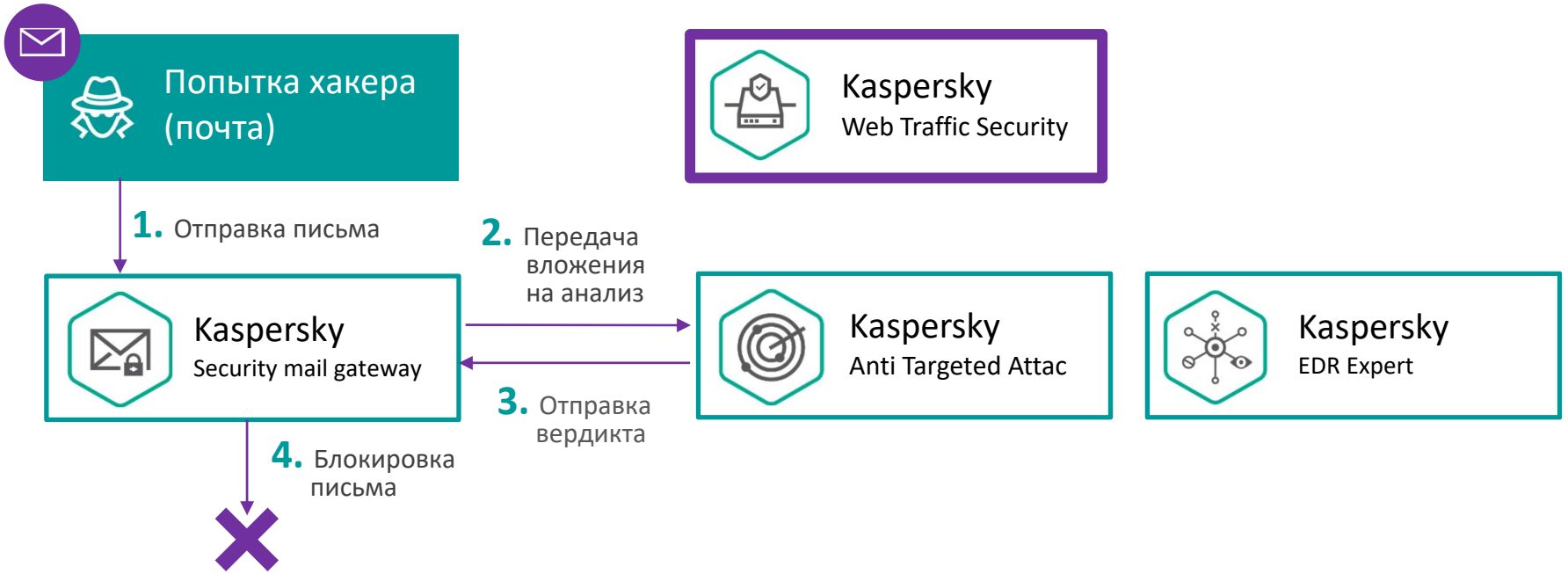
Endpoint Agent

Компонент Sensor может выступать в качестве прокси-сервера для соединений, исходящих от компонента Endpoint Agent.

Kaspersky Security для интернет-шлюзов

В качестве компонента Sensor может использоваться веб-шлюз Kaspersky Security для интернет-шлюзов, отправляющий веб-ссылки и файлы на обработку в KATA Platform.
По результатам обработки в решении KATA, веб-шлюз будет блокировать корпоративным пользователям доступ к ссылкам и файлам для скачивания.

Интеграции с KSMG



Интеграции с KWTS

Компонент Endpoint Agent

Агенты на уровне конечных точек собирают Все необходимые данные с конечных устройств в инфраструктуре организации

Установленный на рабочем месте агент выполняет непрерывный мониторинг процессов, обмена данными, открытых сетевых подключений, состояния операционной системы, изменений в файлах и т. п.
Собранные данные и информацию, связанную с обнаружением подозрительных событий, агент отправляет в KATA для дополнительного исследования, анализа и сравнения с событиями, обнаруженными в других информационных потоках.

Компонент Endpoint Agent

Компонент Endpoint Agent может работать следующими способами:

Компонент **Endpoint Agent** устанавливается на отдельных компьютерах, входящих в IT-инфраструктуру организации и работающих под управлением операционных систем семейств Microsoft Windows и GNU/Linux

Endpoint Agent может использоваться совместно в составе продукта Kaspersky Endpoint Security for Business, а также совместно с Endpoint-решениями других производителей

На этих компьютерах компонент постоянно наблюдает за процессами, открытыми сетевыми соединениями и изменяемыми файлами и отправляет данные наблюдения на сервер с компонентом Central Node либо на Sensor, выступающий промежуточным звеном между Endpoint Agent и Central Node

Реагирование на угрозы

В решении **KATA Platform** в рамках реагирования на инциденты доступны следующие возможности:

Изоляция скомпрометированного хоста от корпоративной сети

Завершение подозрительного процесса

Удаление вредоносного объекта или перемещение его в карантин

Автоматическое создание правил блокировки запуска подозрительных объектов в результате обнаружения Sandbox

Система рекомендаций, помогающая аналитику выстроить правильную цепочку ответных действий

Выполнение команд и управление службами на защищаемом хосте

Запуск YARA-проверки

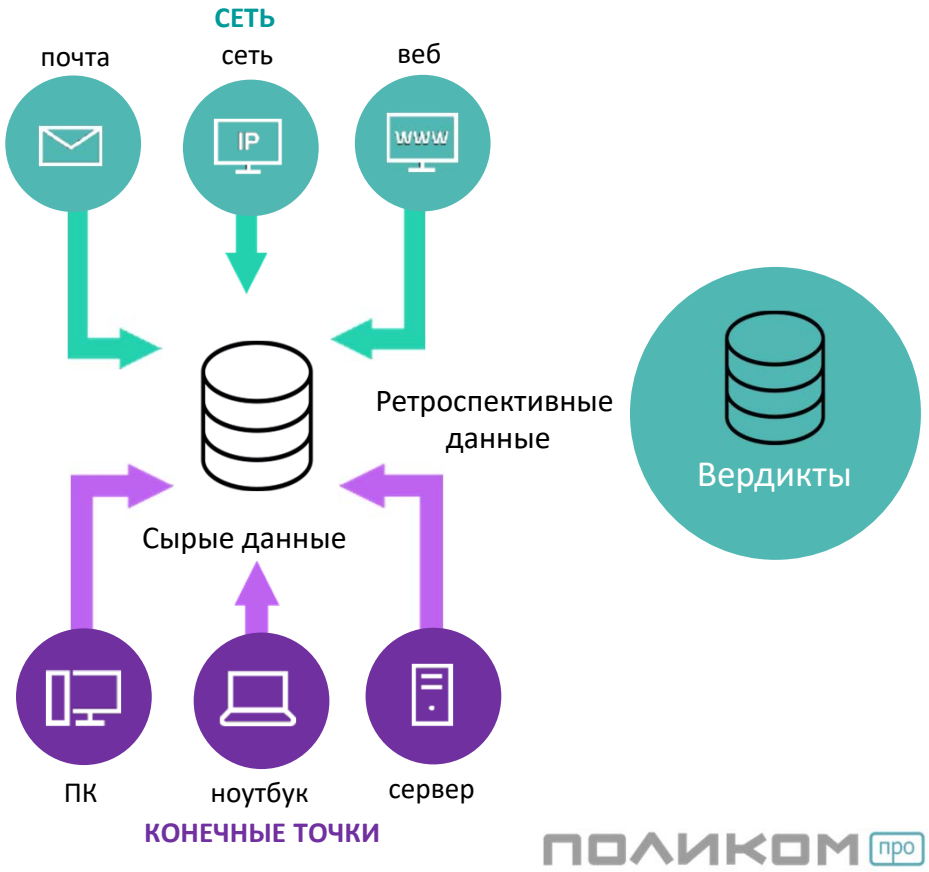
ПОЛИКОМ про

Автоматический сбор и централизованное хранение данных

Сбор и хранение

Автоматический сбор, запись и хранение телеметрии/объектов/вердиктов:

- Предоставляет необходимую информацию об обнаруженных угрозах, облегчая работу ИБ специалистов
- Предоставляет доступ к ретроспективным данным, необходимым для проведения расследования при недоступности или заражении рабочих станций или шифровании данных злоумышленниками
- Проактивный поиск угроз
- Позволяет расследовать продолжительные атаки и предоставляет группе реагирования и регулирующим органам своевременную информацию об обнаруженных инцидентах

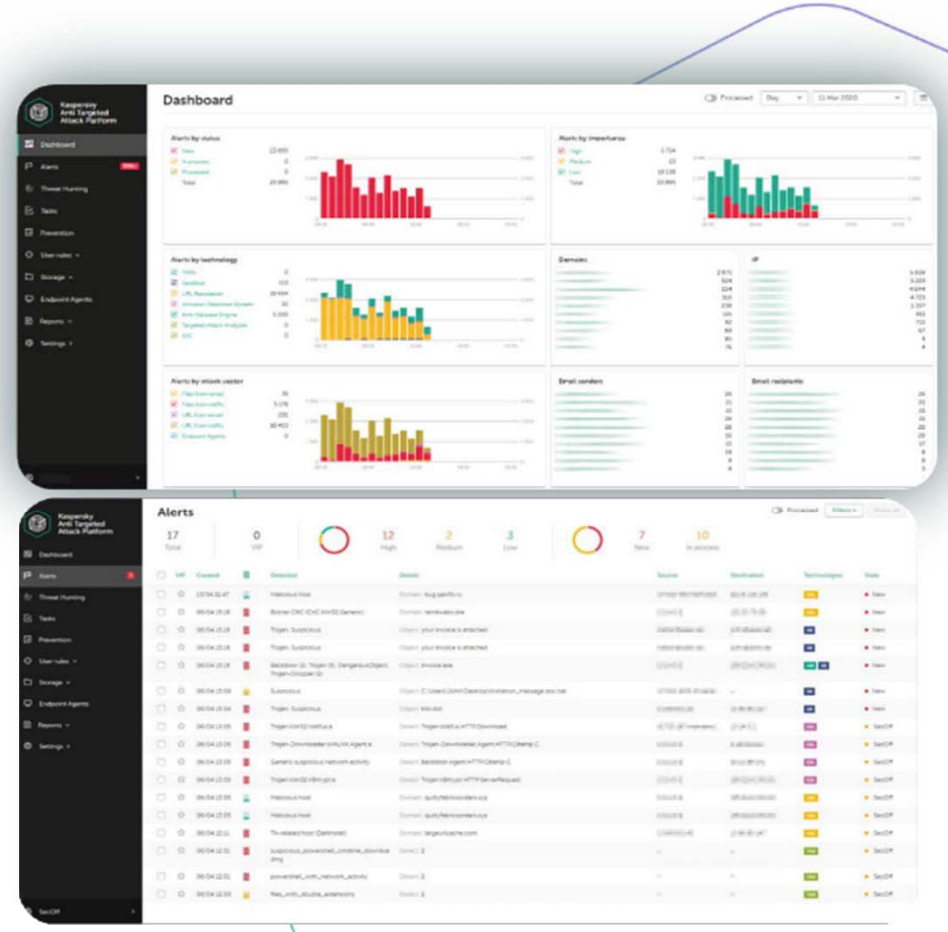


ПОЛИКОМ про

Обнаружение угроз и информирование об угрозах

Обнаружение

- Большое количество детектирующих движков как для сети, так и для конечных точек
- Сканирование инфраструктуры на наличие индикаторов атак и сопоставление с MITREATT & CK
- Передовая песочница
- Рекомендации по расследованию и реагированию



ПОЛИКОМ про

Основные преимущества Платформы KATA с EDR

Один программный продукт с единой веб-консолью

Автоматизация рутинных операций и наглядное представление

Быстрый поиск IoC, анализ IoA и сопоставление с матрицей MITRE ATT&CK, доступ в TI

Автоматический сбор и централизованное хранение данных

Инструментарий для проактивного поиска угроз

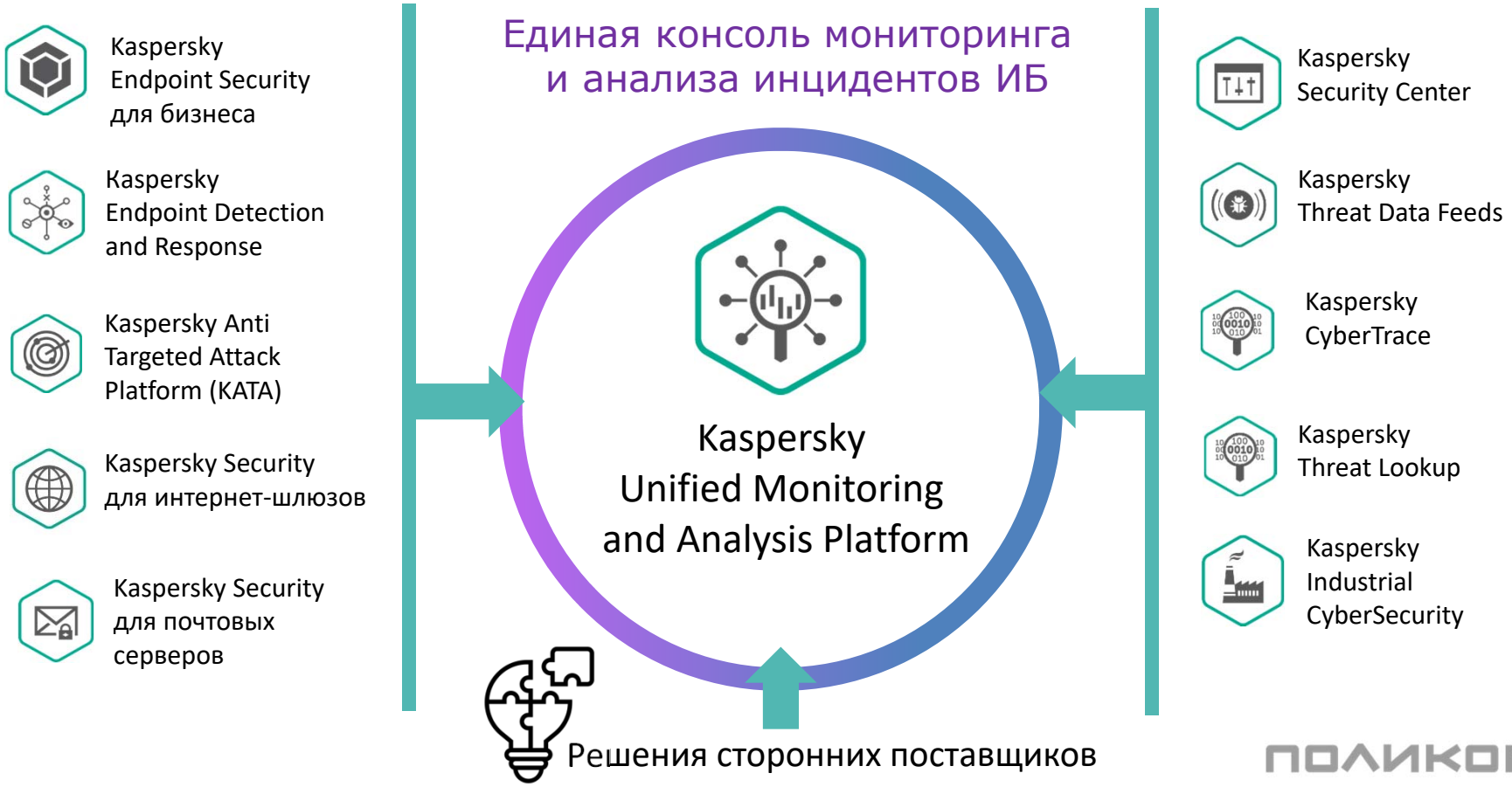
Взаимодействие с превентивными технологиями и обогащение SIEM/SOC

Централизованный процесс реагирования

- Предоставляет комплексный единый инструментарий защиты
- Защищает множество точек входа потенциальной атаки
- Создает целостную картину происходящего
- Автоматизирует рутинную ручную работу
- Оптимизирует рабочую нагрузку экспертов
- Уменьшает количество ложных срабатываний и время для анализа
- Сокращает среднее время обнаружения и реагирования на инциденты (MTTD/MTTR)
- Повышает эффективность процесса реагирования на инциденты

ПОЛИКОМ про

Kaspersky Unified Monitoring and Analysis Platform (SIEM)



ПОЛИКОМ про

kaspersky
Platinum Partner

ПОЛИКОМ про

Руководитель направления решений
«Лаборатории Касперского»
Константин Никитин

тел: + 7 (812) 325 84 00
e-mail: KNikitin@polikom.ru