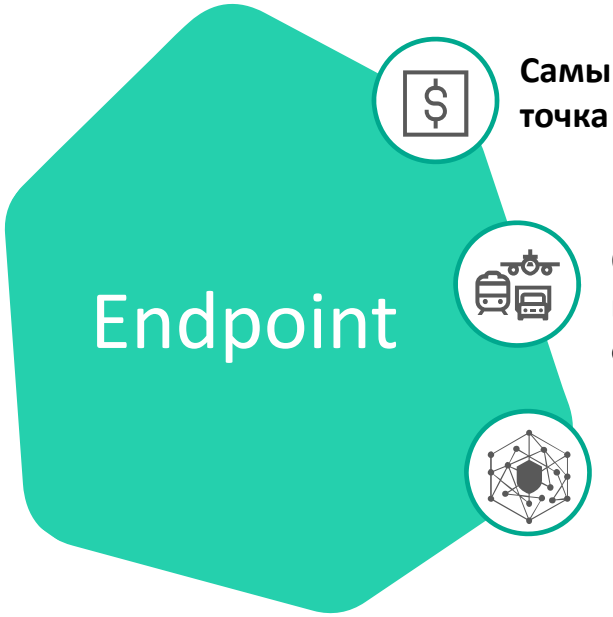
Kaspersky Security для бизнеса

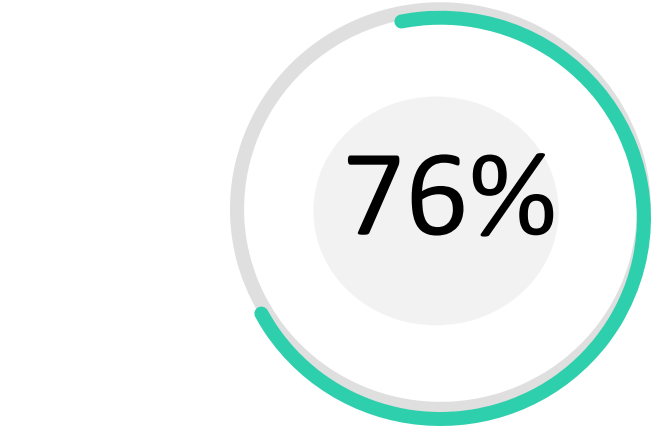
Защита конечных устройств



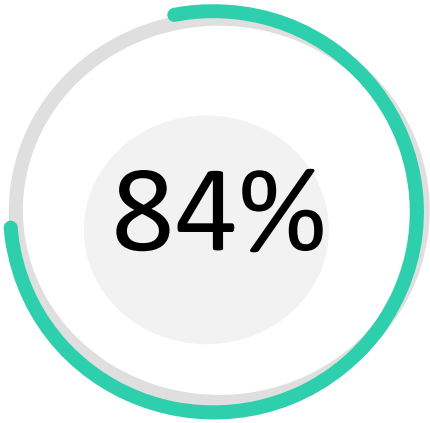
Самый уязвимый элемент и общая точка входа в ИТ-инфраструктуру

Ограниченные ресурсы для анализа подозрительных файлов и активностей

Больше внимания на endpoint с введением TLS 1.3 (сложнее расшифровать трафик)



всех зарегистрированных событий безопасности генерируются на endpoint



более 1 сервера/рабочей станции вовлечены в инцидент

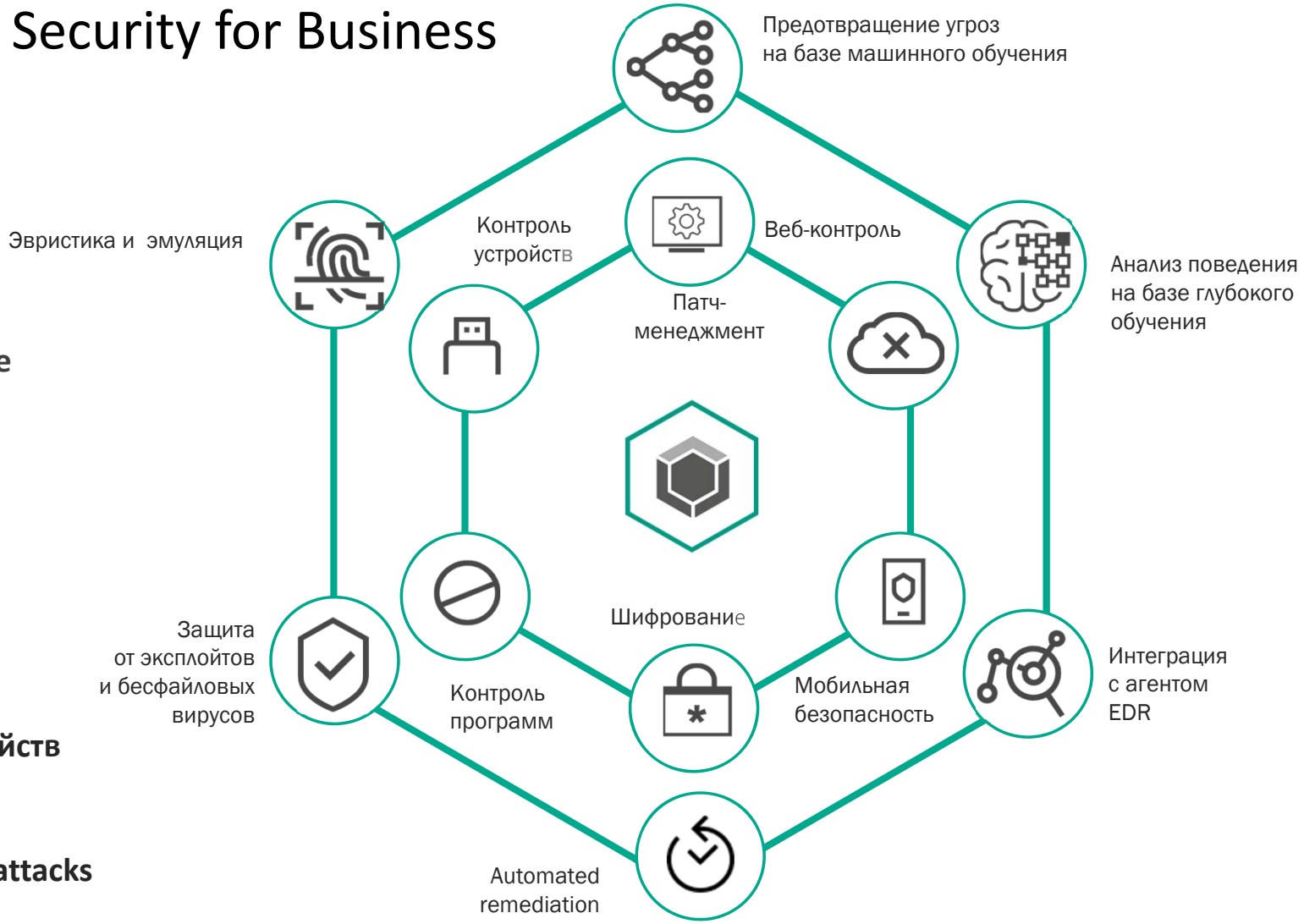
Kaspersky Endpoint Security for Business

Многоуровневая защита для:

— **Windows, Linux и Mac**
— **Windows и Linux Servers**
— **Android и другие мобильные устройства**
— **Съемных носителей**

Высокое качество защиты от:

— **Эксплойтов**
— **Шифровальщиков**
— **Угроз для мобильных устройств**
— **Передовых угроз**
— **Бесфайловых вирусов**
— **PowerShell and script-based attacks**
— **Веб-угроз**



Семейство Kaspersky Endpoint Security for Business

Kaspersky Endpoint Security для бизнеса Стандартный

базовая защита рабочих станций и серверов, защита мобильных устройств, контроль программ, устройств и использования интернета

Kaspersky Endpoint Security для бизнеса Расширенный

патч-менеджмент, расширенные средств администрирования, адаптивный контроль аномалий, шифрование, интеграция с системами SIEM

Kaspersky Endpoint Security для бизнеса Универсальный

состоит из двух продуктов, Kaspersky Endpoint Security для бизнеса Расширенный и Kaspersky Security для виртуальных сред. Легкий агент.

Kaspersky Endpoint Security Cloud

контроль использования облачных ресурсов, защита Microsoft Office 365, контроль устройств, защита мобильных устройств, шифрование

Универсального решения не существует

Линейка решений Kaspersky Security для бизнеса содержит несколько уровней с нарастающим функционалом. Для перехода на новый уровень не требуется переустановка защитного ПО, а для управления используется одна и та же консоль.

Стандартный
Endpoint Security для бизнеса

Защита и контроль каждого рабочего места

Расширенный
Endpoint Security для бизнеса

Уникальная адаптивная система безопасности

Включает все возможности Kaspersky Endpoint Security для бизнеса Стандартный

Total
Security для бизнеса

Максимальная защита каждого аспекта вашего бизнеса

Включает все возможности Kaspersky Endpoint Security для бизнеса Расширенный

Сравнение возможностей

Total
Security для бизнеса

Расширенный
Endpoint Security для бизнеса

Стандартный
Endpoint Security для бизнеса

- Контроль программ для компьютеров
- Контроль веб и устройств
- Защита от угроз для мобильных устройств
- Защита от программ-вымогателей
- Аналитика на основе облака
- Единая консоль управления
- Защита для Windows, Linux и Mac
- Защита серверов
- Базовая поддержка SIEM (Syslog)
- Управление доступом на основе ролей (базовое)

- Развертывание ОС и стороннего ПО
- Поиск уязвимостей и установка патчей
- Расширенная поддержка SIEM (проприетарная технология)
- Управление шифрованием
- Адаптивный контроль аномалий
- Управление доступом на основе ролей (расширенное)

- **Защита интернет-шлюзов**
- **Защита почтовых серверов**
- **Управление доступом на основе ролей (расширенное)**

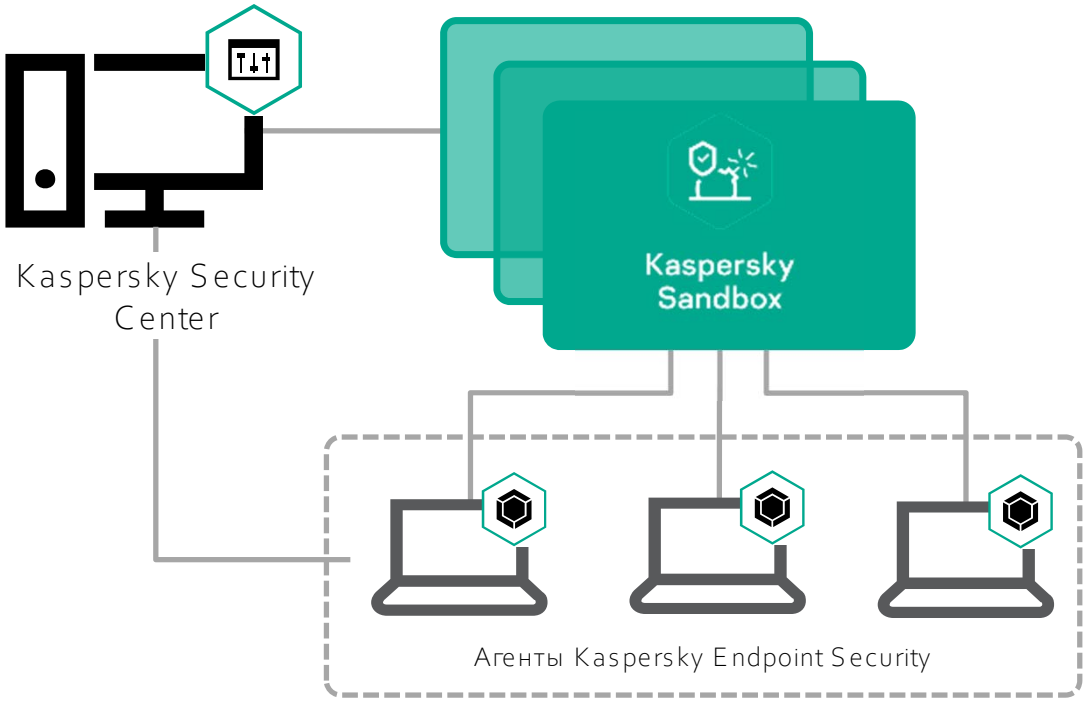
Интегрированное решения для всех

Kaspersky Sandbox

Kaspersky Sandbox

Основной функционал

- Выявление новых угроз
- Сценарии реагирования
- Выявление IOC на endpoint сети

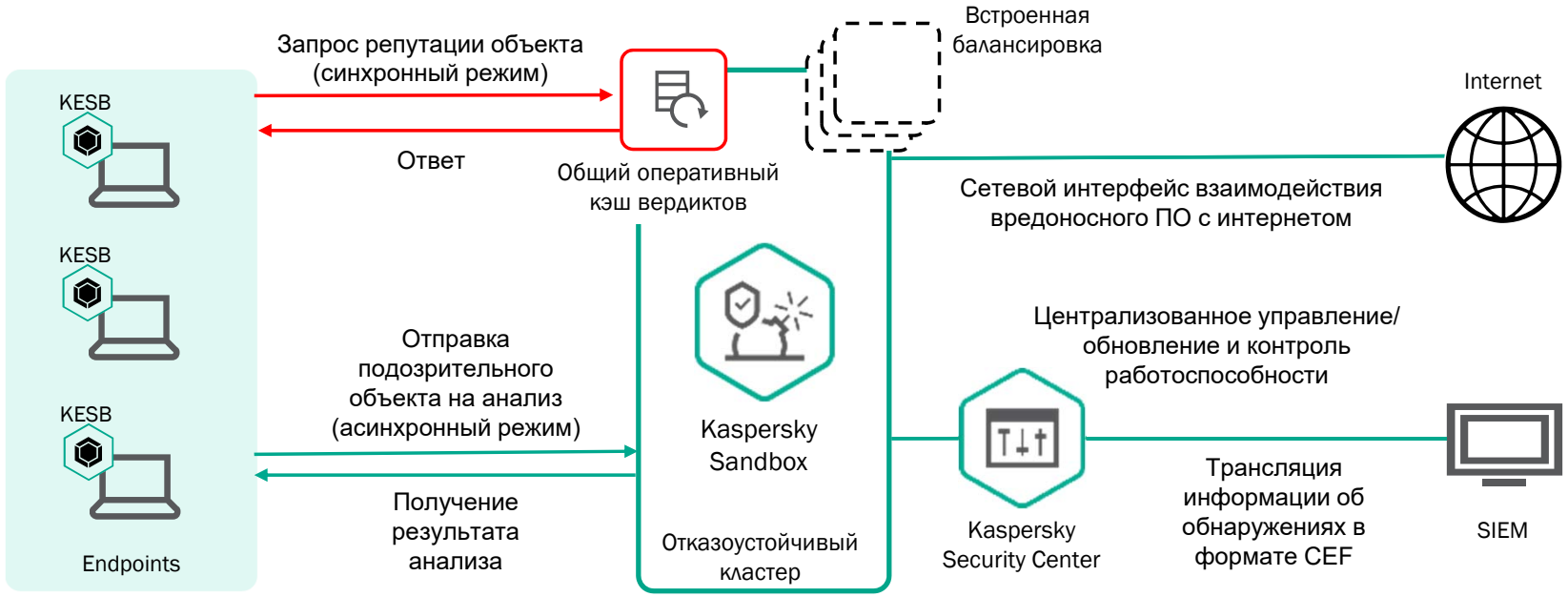


Сценарии

- Поддержка автоматических сценариев противодействия неизвестным угрозам без необходимости привлечения специалистов
- Защита высоконагруженных терминальных серверов, в том числе с выключенным модулем поведенческого анализа в Kaspersky Security для бизнеса
- Защита рабочих станций при отключенном взаимодействии с глобальной базой данных об угрозах KSN\KPSN
- Наличие API для интеграции со сторонними приложениями в инфраструктуре заказчика

Архитектура решения

- Дополняет Kaspersky Endpoint Security новыми сценариями обнаружения новых и целевых угроз без ущерба для производительности рабочих станций
- Улучшенная защита и автоматическое реагирование на передовые угрозы для сложных распределенных сетей с удаленными офисами
- Решение не требует дополнительных инвестиций в экспертизу персонала
- Возможность интеграции со сторонними решениями через RESTful API позволит достичь максимальной эффективности решения в комплексных системах ИБ клиентов



Лицензирование

1 лицензия = 1 Endpoint
* от 250 Endpoints

Лицензии Microsoft предоставляются в сборке Kaspersky Sandbox.
Предустановленные и предактивированные образы виртуальных машин позволяют избежать необходимости добавления заказчиком/партнером собственных лицензий Microsoft для работы песочницы

Необходимые для Kaspersky Sandbox физические и виртуальные серверы НЕ входят в поставку и приобретаются отдельно.

Рекомендованные конфигурации оборудования:

250 Endpoints	500 Endpoints	750 Endpoints	1000 Endpoints	5000 Endpoints
4 core CPU / 32 Gb RAM	8 core CPU / 48 Gb RAM	12 core CPU / 64 Gb RAM	16 core CPU / 64 Gb RAM	32 core CPU / 196 Gb RAM

Результат от инвестиций в решение Kaspersky Sandbox


Снижение рисков ИБ


Оптимизация затрат


Повышение продуктивности


Сокращение трудозатрат

- **Повышение уровня защищенности инфраструктуры** рабочих мест и серверов от сложных угроз без необходимости расширения штата
- **Предотвращение прямых потерь и последующих трат** связанных со сложными угрозами за счет максимальной автоматизации в вопросе противодействия им
- **Экономия трудозатрат** высокооплачиваемых штатных ИБ-аналитиков для решения тех задач, которые действительно требуют их внимания и **увеличение их продуктивности** за счет уменьшения количества ручных операций
- **Повышение общего уровня информационной безопасности**, с сохранением ранее вложенных инвестиций

Kaspersky Endpoint Detection and Response Optimum

Kaspersky Endpoint Detection and Response Optimum

Основные возможности

Сокращение накладных расходов, связанных с развертыванием решения

Быстрое реагирование на сложные и скрытые угрозы, предотвращение их дальнейшего развития

Предоставление больше полезной информации по инцидентам

Простой инструмент для расследования инцидентов

Возможности анализа и визуализации

Визуализация пути атаки
построение всех событий*
связанных с инцидентом

- Обнаружение угрозы на конечном устройстве
- Извлечение кода
- Процесс, порождающий другие процессы
- Создание файла
- Сетевые соединения
- Модификация реестра

Подробное описание артефактов
в информационной карточке инцидента для Анализа Первопричин

Возможность **выявления всех затронутых** серверов и рабочих станций

* EDR агент передает детальную информацию требуемую для Анализа Первопричин

Упрощение процедуры реагирования

Возможные способы реакции

- Изоляция хоста
- Запуск антивирусного сканирования на хосте
- Удалить, поместить в карантин файл
- Остановить процесс
- Получить файл
- Предотвратить запуск файла
- Добавить файл в KESB Whitelist, отправить в Kaspersky для анализа

- Внешний импорт индикаторов (доверенные источники/регулирующие органы)
- Сканирование инфраструктуры в реальном времени и запланированное на основе индикаторов с возможностью реакции в «один клик»

Автоматическое создание индикаторов угроз с возможностью применения их на всех хостах сразу

При обнаружении подозрительной активности на хосте, EDR Optimum может выполнять поиск аналогичных событий на других хостах

Преимущества для пользователей KESB

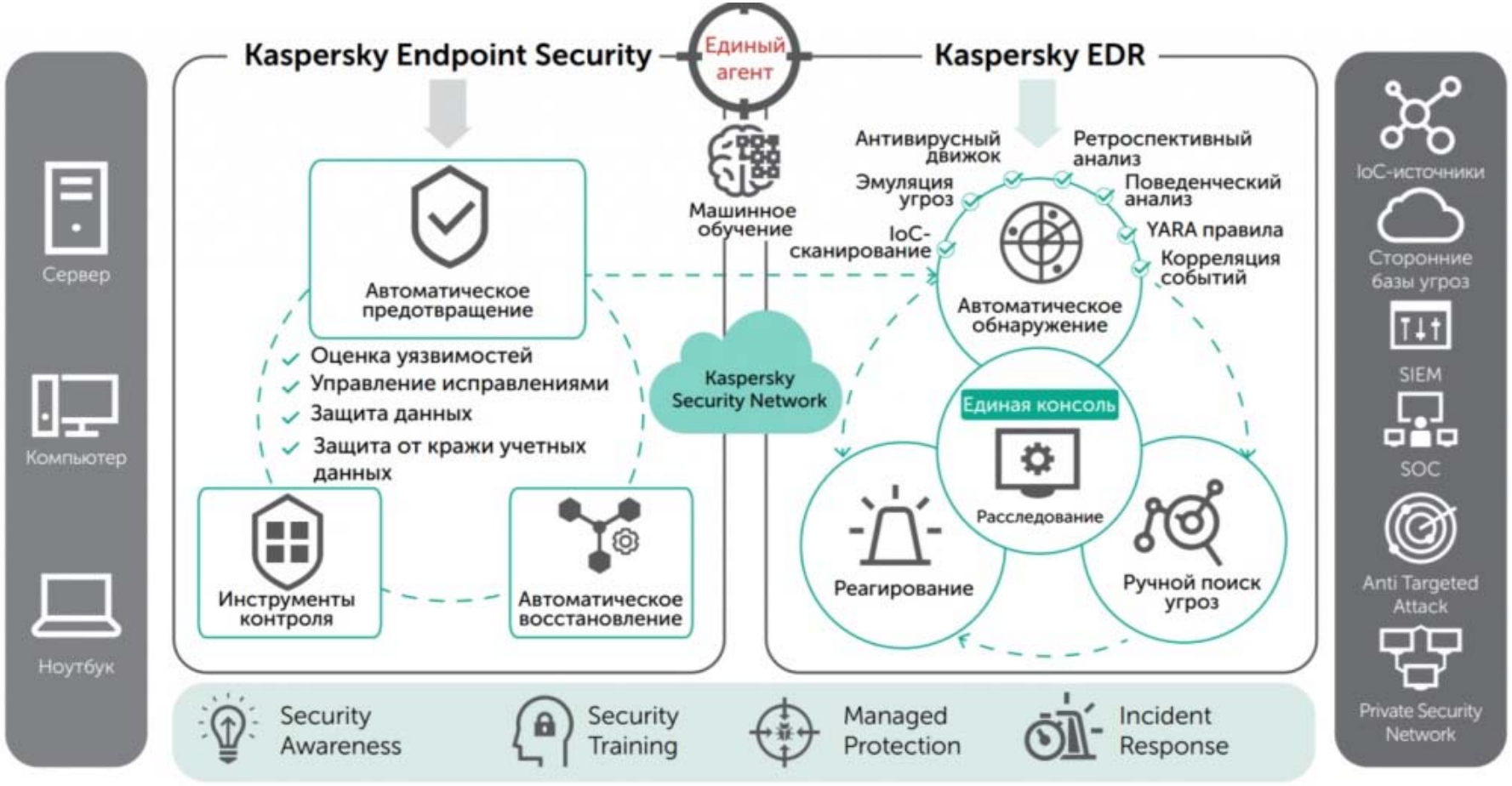
Использование функционала EDR в уже **установленном продукте**

Универсальная Консоль:
KSC Web как централизованная консоль управления (локальная и облачная)

Снижение TCO

(совокупной стоимости владения)
за счет упрощения обработки инцидентов, минимизации затрат на обслуживание и минимального вовлечения персонала

Итог активации EDR Optimum



Лицензирование Kaspersky EDR Optimum

- Лицензируется по количеству установленных KESB
- Включает в себя Kaspersky Security для Бизнеса Расширенный
- При наличии KESB есть возможность закупки по цене продления
- Вместе с Kaspersky Sandbox входит в лицензию Kaspersky Total Security Plus