Kaspersky Symphony

Безопасность как искусство

kaspersky

Ежегодно

Усложняется ландшафт угроз,
киберпреступники совершенствуют свои методы

Расширяется поверхность атаки
и количество точек входа злоумышленников

Усиливаются требования регуляторов,
особенно в отношении обеспечения защиты КИИ

+ Добавилось

Наступила эра хактивизма
и целевой киберагрессии

Больше лазеек
из-за полного ухода ИБ-вендоров или приостановки обновлений их решений

Началась активная фаза
импортонезависимости

Актуальные ИБ-задачи

Противодействие всем видам угроз в киберагрессивной среде

ИБ-замещение ушедших поставщиков в короткие сроки

Соответствие усиливающимся требованиям регуляторов

1

В первую очередь защититься от массовых угроз

2

Во-вторых выстроить защиту от сложных угроз

Самостоятельно: постепенно или сразу

Выбрать управляемую защиту

О Kaspersky Symphony

Почему Symphony?

Кибербезопасность в виртуозном исполнении:

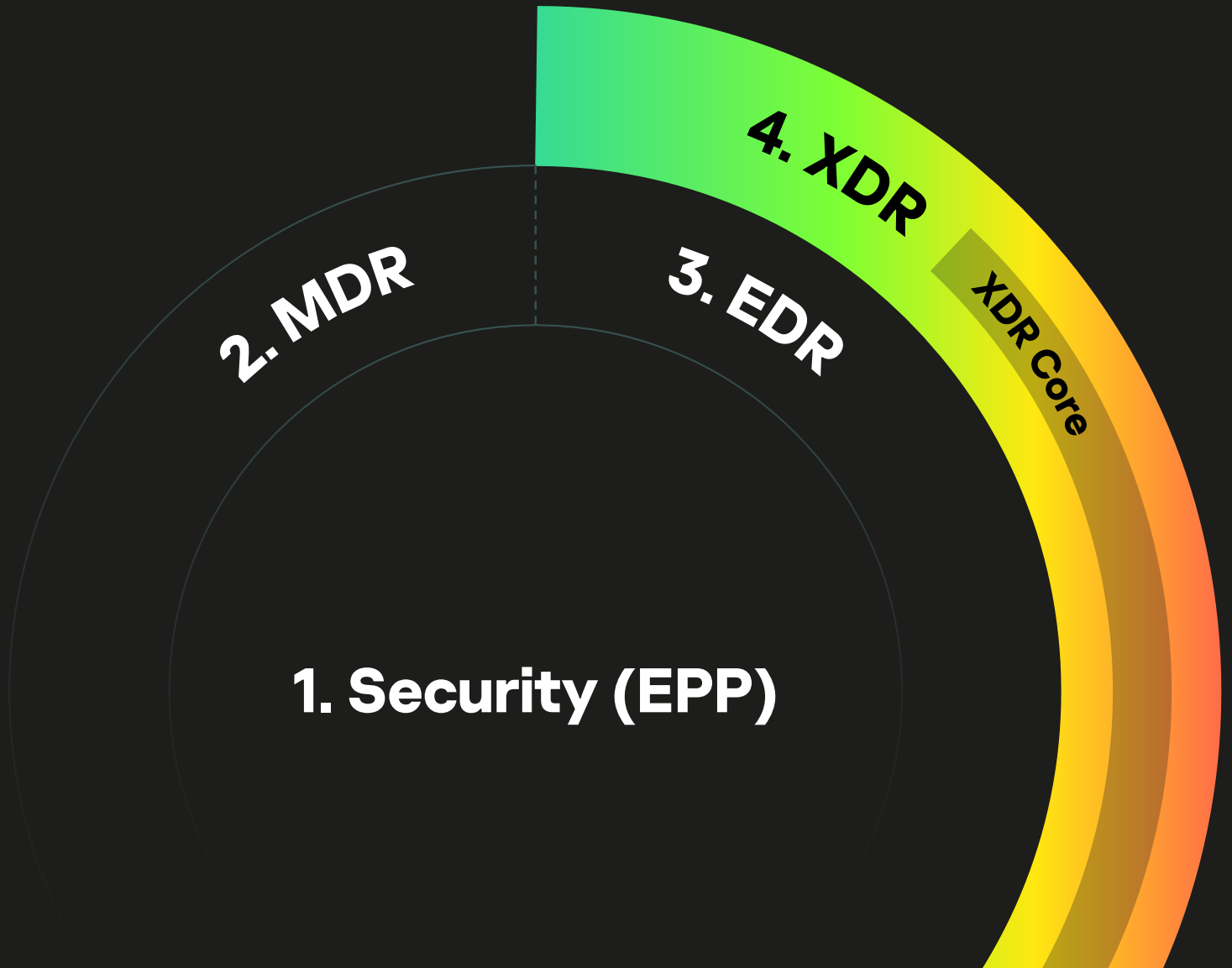
Когда все защитные решения действуют, как слаженный оркестр

Когда все инструменты идеально настроены

Когда есть всё, чтобы уверенно и просто дирижировать системой безопасности

Гибкий выбор

- Kaspersky Symphony XDR
  - XDR Core
- Kaspersky Symphony MDR
- Kaspersky Symphony EDR
- Kaspersky Symphony Security



Функциональное сравнение уровней Kaspersky Symphony

Лицензирование по устройствам

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 Security

Состав Kaspersky Symphony Security

Kaspersky Symphony Security

Kaspersky Endpoint Security для бизнеса

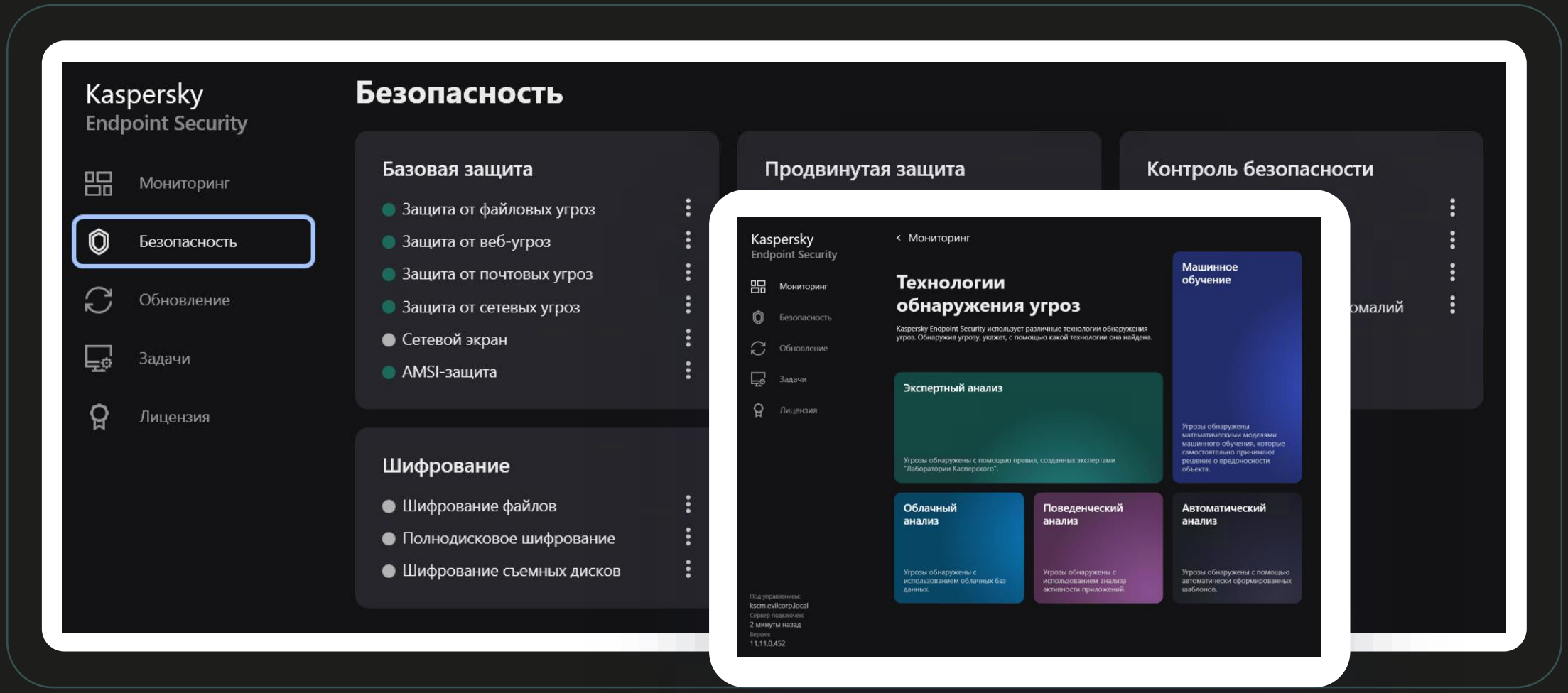
Расширенный

Kaspersky Security для виртуальных и облачных сред (LA)

Общепризнанная фундаментальная защита класса EPP (Endpoint Protection Platform) от массовых киберугроз разной степени сложности, поддерживающая все типы конечных точек: физические и виртуальные.

- Многоуровневая защита
- Гибкие инструменты контроля
- Встроенное шифрование
- Централизованное управление защитой
- Инструменты для системного администрирования
- Прозрачность и инвентаризация

Интерфейс

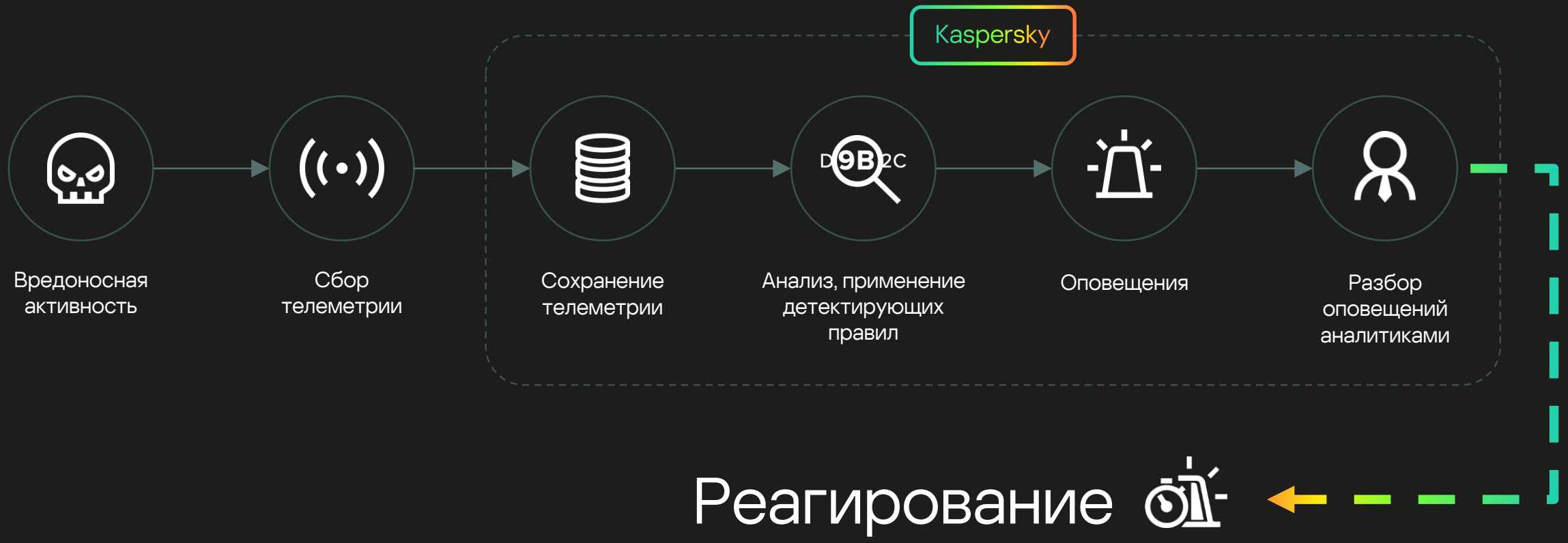

Kaspersky
Endpoint Security
Мониторинг
Безопасность
Обновление
Задачи
Лицензия
Безопасность
Базовая защита
Защита от файловых угроз
Защита от веб-угроз
Защита от почтовых угроз
Защита от сетевых угроз
Сетевой экран
AMSI-защита
Шифрование
Шифрование файлов
Полнодисковое шифрование
Шифрование съемных дисков
Продвинутая защита
Контроль безопасности
Kaspersky
Endpoint Security
Мониторинг
Безопасность
Обновление
Задачи
Лицензия
Мониторинг
Технологии обнаружения угроз
Kaspersky Endpoint Security использует различные технологии обнаружения угроз. Обнаружив угрозу, укажет, с помощью какой технологии она найдена.
Машинное обучение
Угрозы обнаружены математическими моделями машинного обучения, которые самостоятельно принимают решение о вредоносности объекта.
Экспертный анализ
Угрозы обнаружены с помощью правил, созданных экспертами "Лаборатории Касперского".
Облачный анализ
Угрозы обнаружены с использованием облачных баз данных.
Поведенческий анализ
Угрозы обнаружены с использованием анализа активности приложений.
Автоматический анализ
Угрозы обнаружены с помощью автоматически сформированных шаблонов.
Под управлением:
kscm.evilcorp.local
Сервер подключен:
2 минуты назад
Версия:
11.11.0.452

Kaspersky Symphony MDR

Kaspersky Symphony MDR

- **Kaspersky Symphony Security**
- **Kaspersky EDR для бизнеса**
  Оптимальный
- **Kaspersky Managed Detection and Response**
  Optimum

Как это работает: Kaspersky Symphony MDR



Предоставление рекомендаций по реагированию
и удаленное реагирование

Обогащение телеметрии

Телеметрия

Телеметрия обогащается аналитикой угроз из разных источников

KSN
Kaspersky Security Network

GREAT
Центр глобальных исследований и анализа угроз

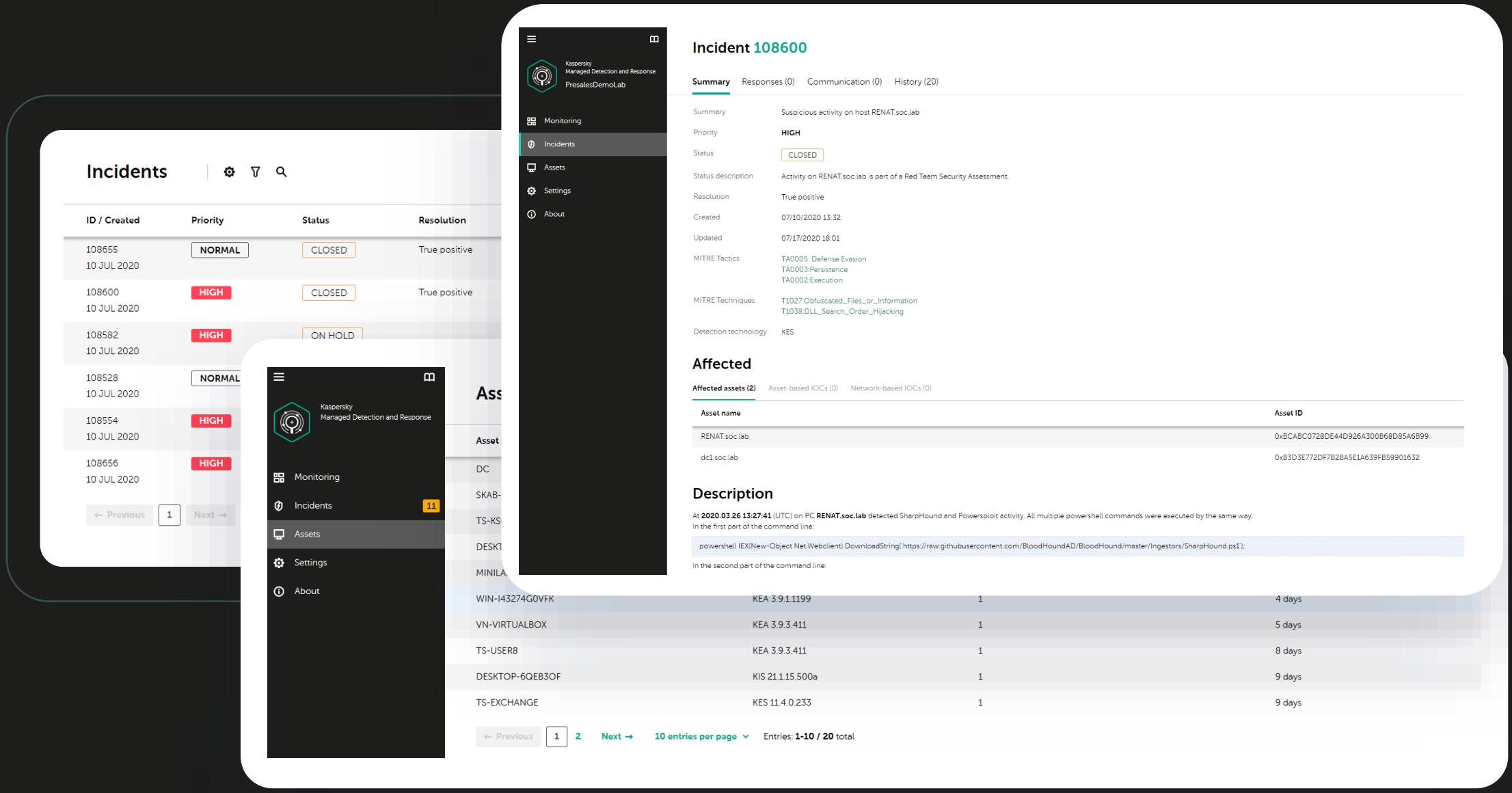
Kaspersky Threat Intelligence

GERT
Международная группа реагирования

IoA
Правила автоматического поиска угроз

Kaspersky ICS CERT

Интерфейс MDR



Преимущества использования Kaspersky Symphony MDR

Уверенность в том, что вы находитесь под постоянной защитой

Сокращение расходов из-за отсутствия необходимости нанимать ИБ-специалистов и строить свой собственный SOC центр

Возможность пользоваться преимуществами центра SOC, не имея его внутри компании

Возможность оперативно получить защиту от экспертов мирового уровня

Kaspersky Symphony EDR

Состав Kaspersky Symphony EDR

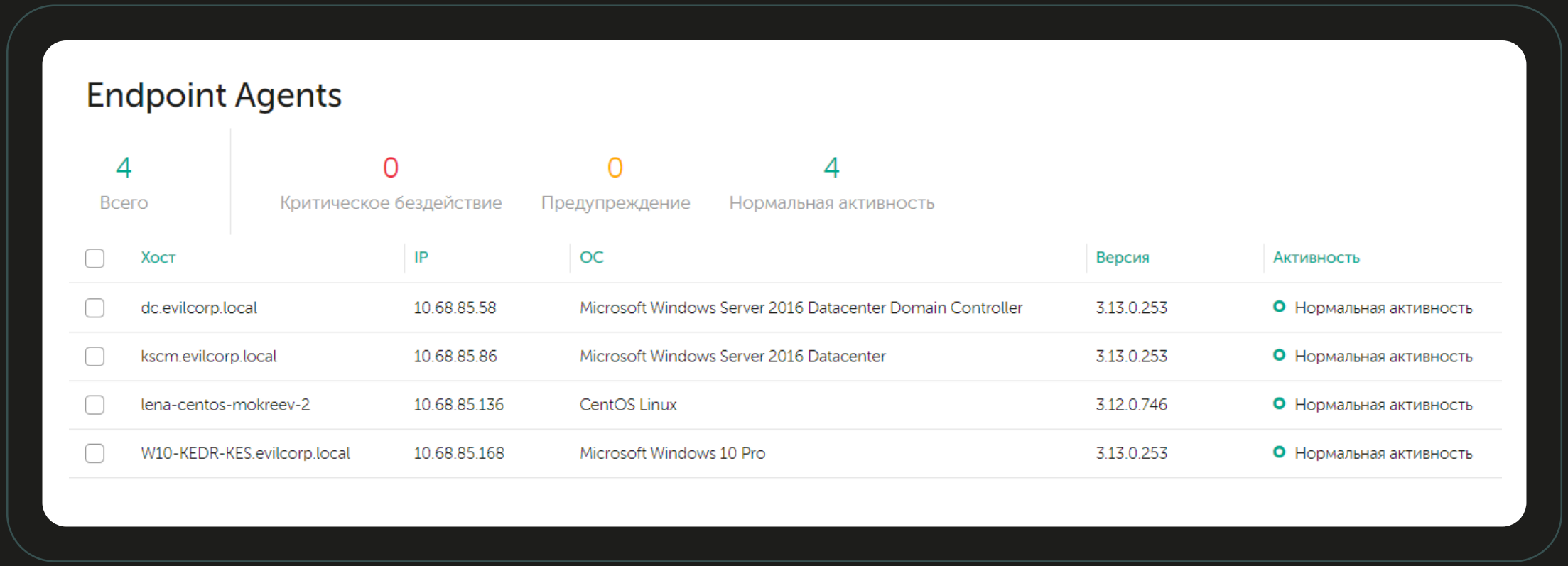
Kaspersky Symphony EDR

- Kaspersky Symphony Security
- Kaspersky EDR Expert
  Standard

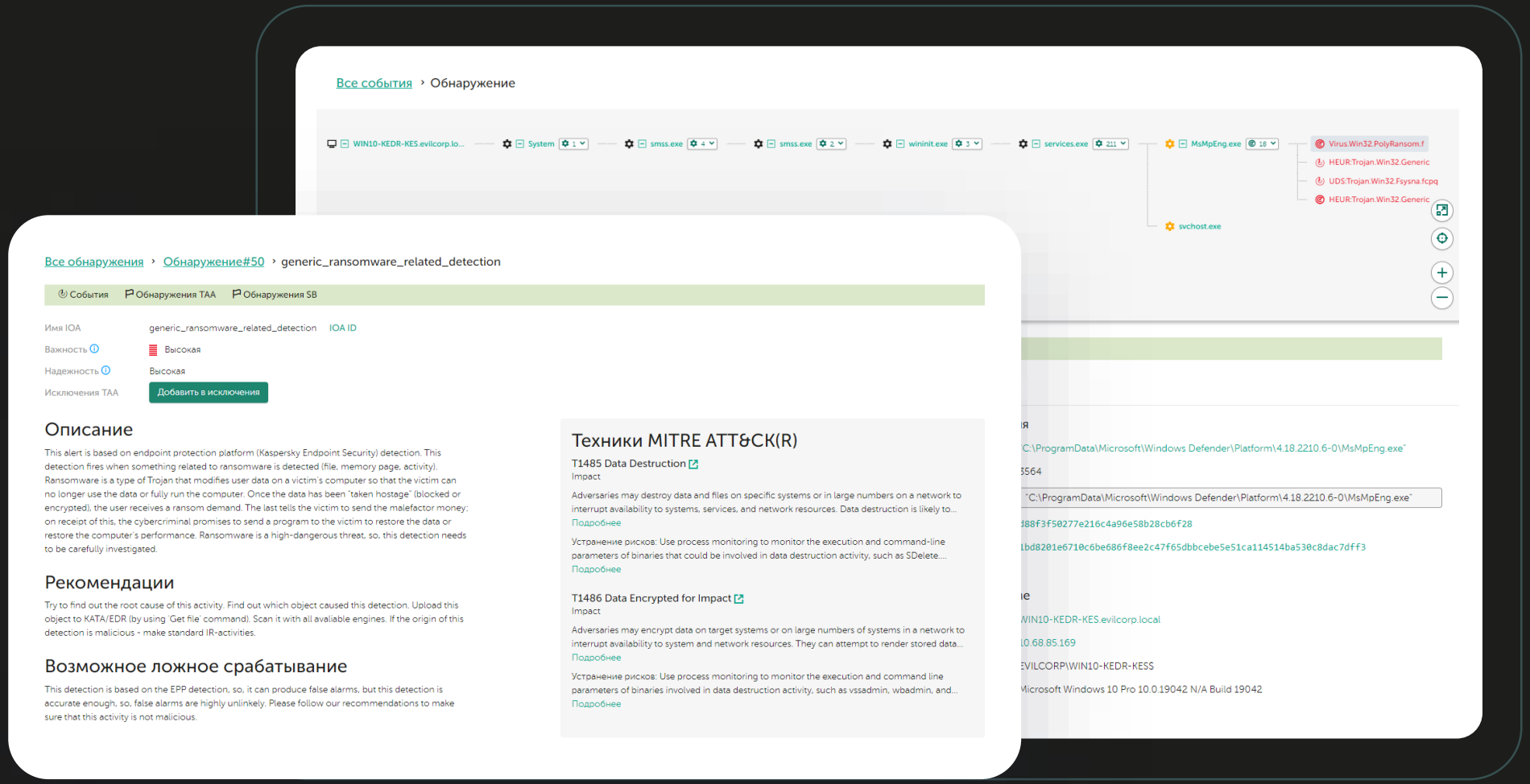
Kaspersky Symphony EDR: архитектура решения

Единый агент

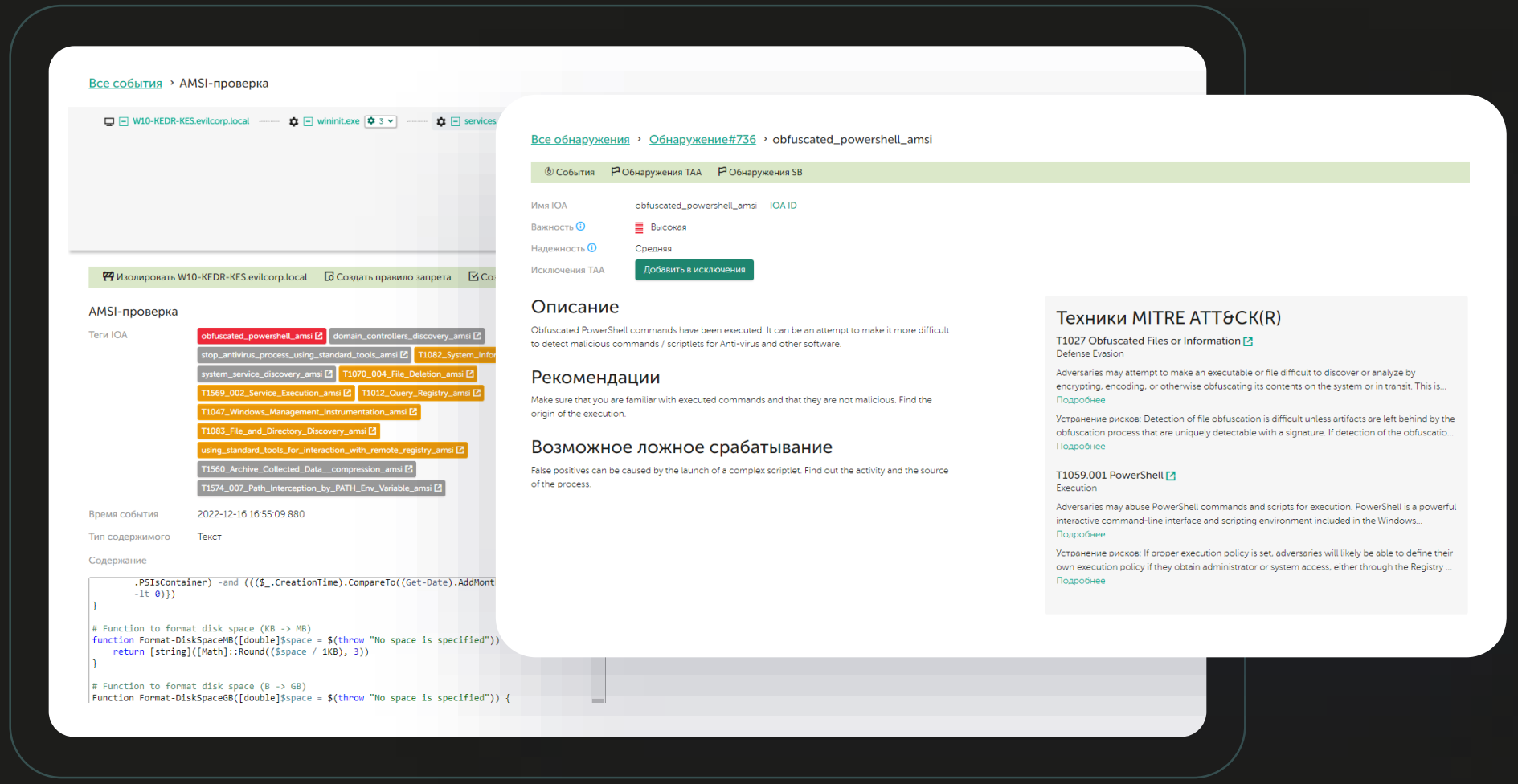
Широкое покрытие корпоративного парка защищаемых хостов



Синергия EPP и EDR на защищаемом хосте



Быстрый анализ многоэтапного вектора атаки



Основные сценарии применения Kaspersky Symphony EDR

Автоматическое предотвращение, обнаружение и расследование сложных инцидентов на уровне конечных точек

Оперативная проверка инфраструктуры на наличие IoC, получаемых от различных источников, самостоятельный проактивный поиск угроз

Помощь в соответствии требованиям / рекомендациям регуляторов

Централизованное реагирование в распределенной инфраструктуре рабочих мест и серверов (физических и виртуальных)

Получение доступа к цифровым доказательствам, в случаях недоступности скомпрометированных станций или их зашифровки

Оптимизация затрат / сокращение трудозатрат на процесс обработки сложных инцидентов на уровне конечных точек

Kaspersky Symphony XDR

Kaspersky Symphony XDR

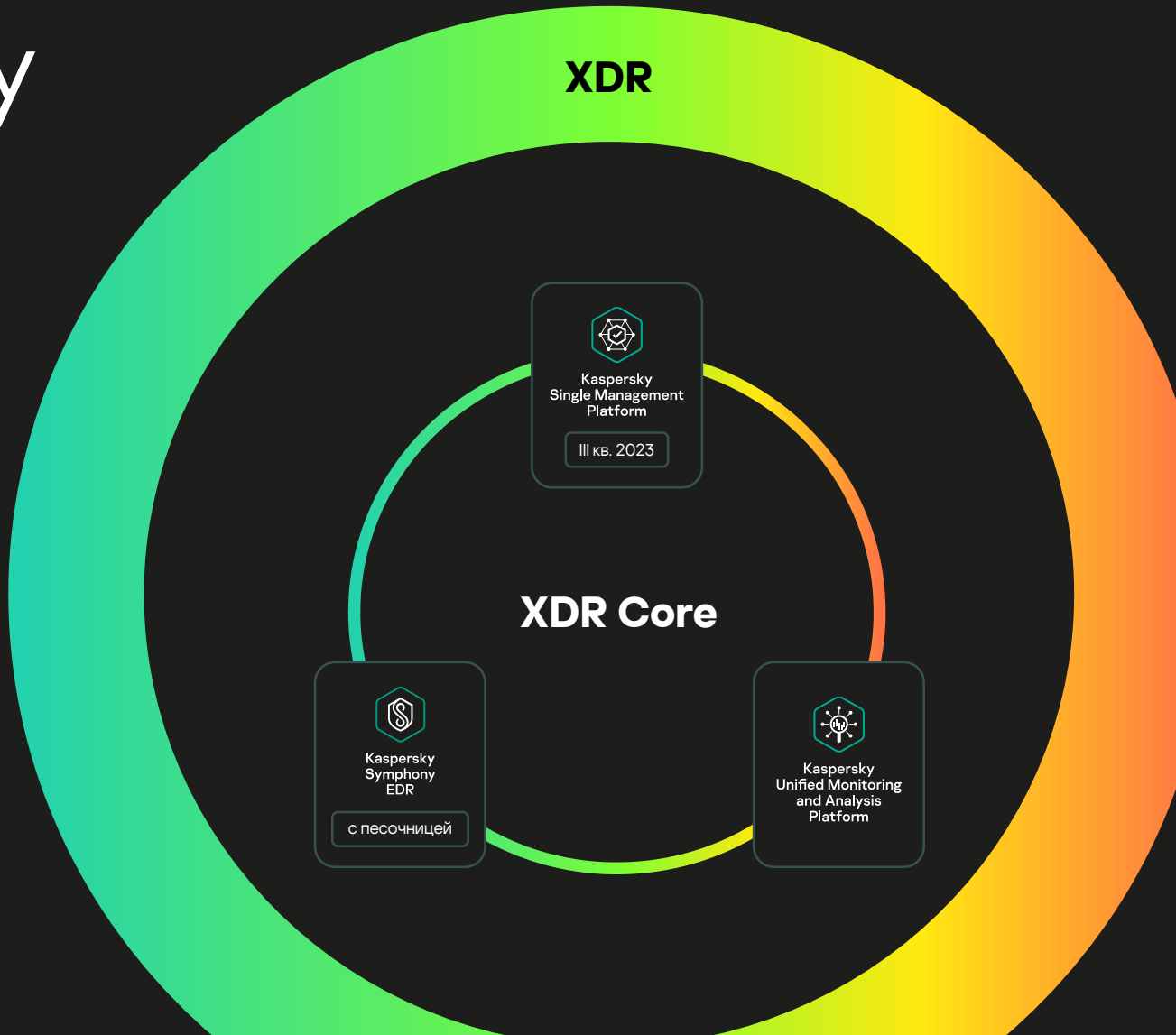
Средство мониторинга, обнаружения, проактивного поиска и реагирования

Комплексная система класса XDR для мониторинга ИБ, проактивного поиска угроз и реагирования на сложные инциденты в рамках всей инфраструктуры с соблюдением требований законодательства

Всеобъемлющий подход к защите бизнеса, адаптирующийся к существующей инфраструктуре, для компаний-новаторов среднего и крупного бизнеса любых индустрий

Kaspersky Symphony XDR Core

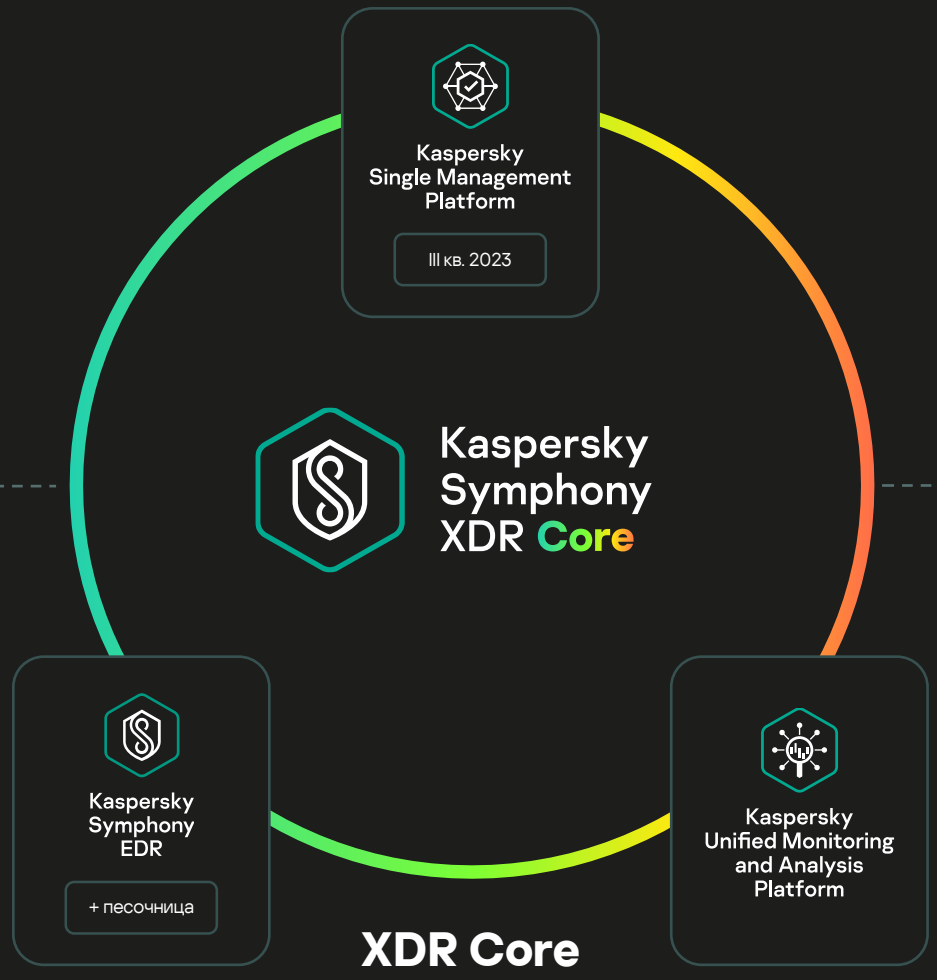
Ядро комплексной платформы XDR, которое включает в себя ключевой набор продуктов для выстраивания защиты класса XDR. Решение идеально подходит организациям, для которых важна гибкость в построении мощной XDR защиты: как на базе всех продуктов от Kaspersky, так и добавления сторонних.



Состав Kaspersky Symphony XDR Core

Интеграция со сторонними решениями

- Active Directory
- Network traffic analysis
- Next Generation Firewall
- Cloud Security
- Data Leak Prevention
- Другие



Интеграция с другими решениями Kaspersky

- Kaspersky Anti Targeted Attack
- Kaspersky Secure Mail Gateway
- Kaspersky Web Traffic Security
- Kaspersky Threat Intelligence
- Kaspersky Container Security
- Kaspersky Secure Mobility Management
- Kaspersky Automated Security Awareness Platform

Состав Kaspersky Symphony XDR

Включенные интегрированные продукты

Защита на уровне сети

- Kaspersky Anti Targeted Attack
- Kaspersky Security для почтовых серверов
- Kaspersky Security для интернет-шлюзов

Интеграции с ИБ-решениями

INFOWATCH · UserGate · Check Point · Active Directory · КОД безопасности

••• и другие

Состав XDR Core

Включенные интегрированные продукты

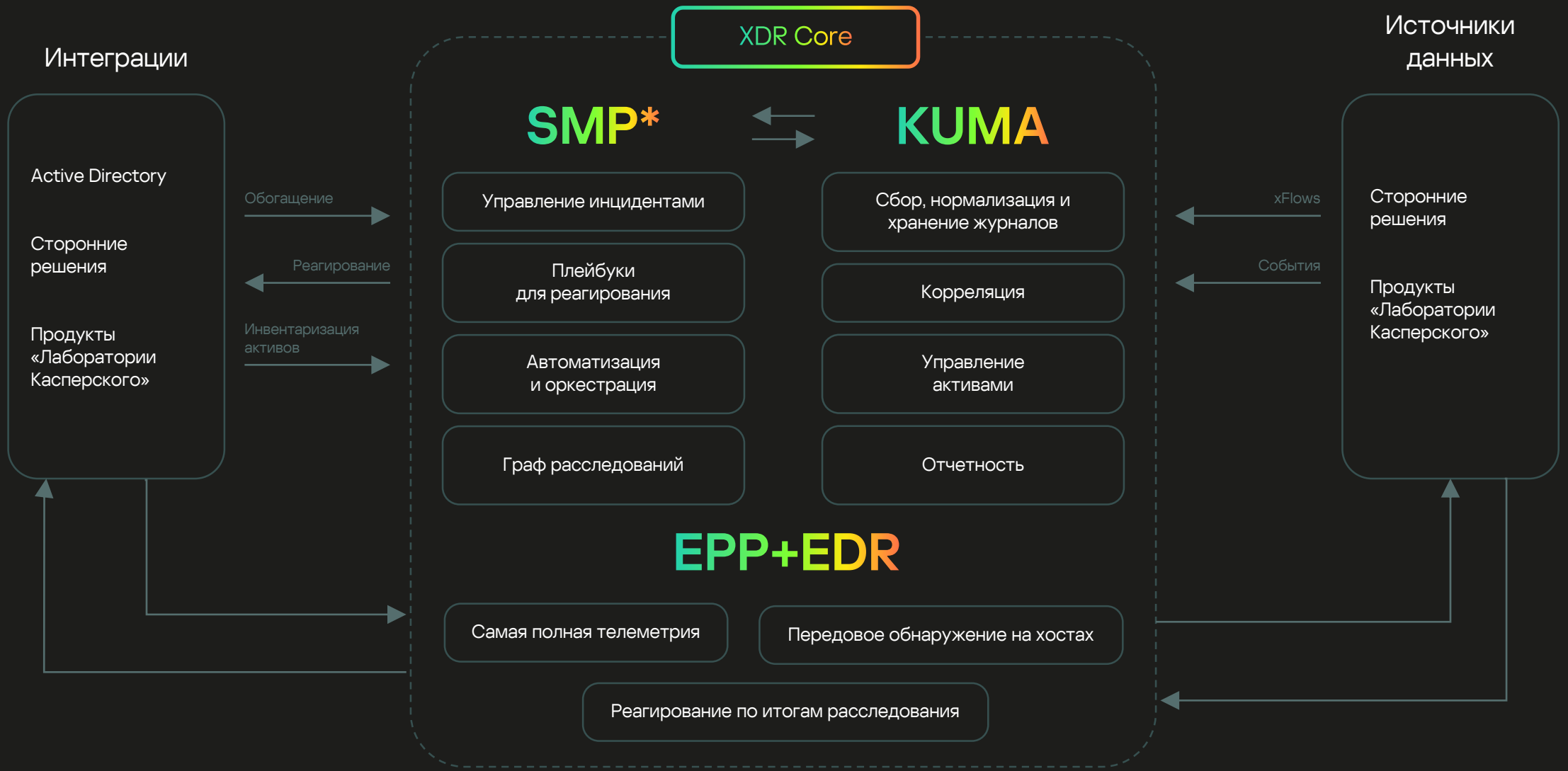
Обогащение

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

Обучение пользователей

- Kaspersky Automated Security Awareness Platform

Kaspersky Symphony XDR: архитектура



* Будет доступно в Q3 2023 году

Преимущества

Сильные стороны Kaspersky Symphony XDR

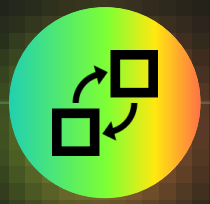
Kaspersky Symphony XDR

Фокус на конечные точки

Включен EDR в синергии с EPP – они уже защищают более чем 60 миллионов корпоративных рабочих мест по всему миру

Фокус на аналитику об угрозах

Включена признанная лучшей в мире аналитика об угрозах (по результатам Forrester Wave: External Threat Intelligence Services 2021)



Фокус на взаимодействие

Тесное взаимодействие включенных элементов, кросс-продуктовые сценарии, гибкость сетевой защиты (Netflow, движки KATA или взаимодействие с сторонними сетевыми вендорами). Взаимодействие с другими решениями сторонних поставщиков

Фокус на соответствие

Помогает обеспечить соответствие требованиям регуляторов (например, в сфере безопасности объектов КИИ), в том числе благодаря встроенному модулю ГосСОПКА

Фокус на качество

В состав входят продукты, заслужившие признание аналитиков, независимых лабораторий и клиентов по всему миру

Gartner peerinsights customers' choice 2021

FORRESTER® IDC

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

SE Labs AAA ADVANCED SECURITY ASSESSMENT

AV TEST

MITRE | ATT&CK®

Роль Kaspersky Symphony в реализации требований

Приказ ФСТЭК №239 — корпоративный сегмент

Применение экосистемы Kaspersky Symphony (совместно с орг. мерами и KDP) позволяет реализовать:

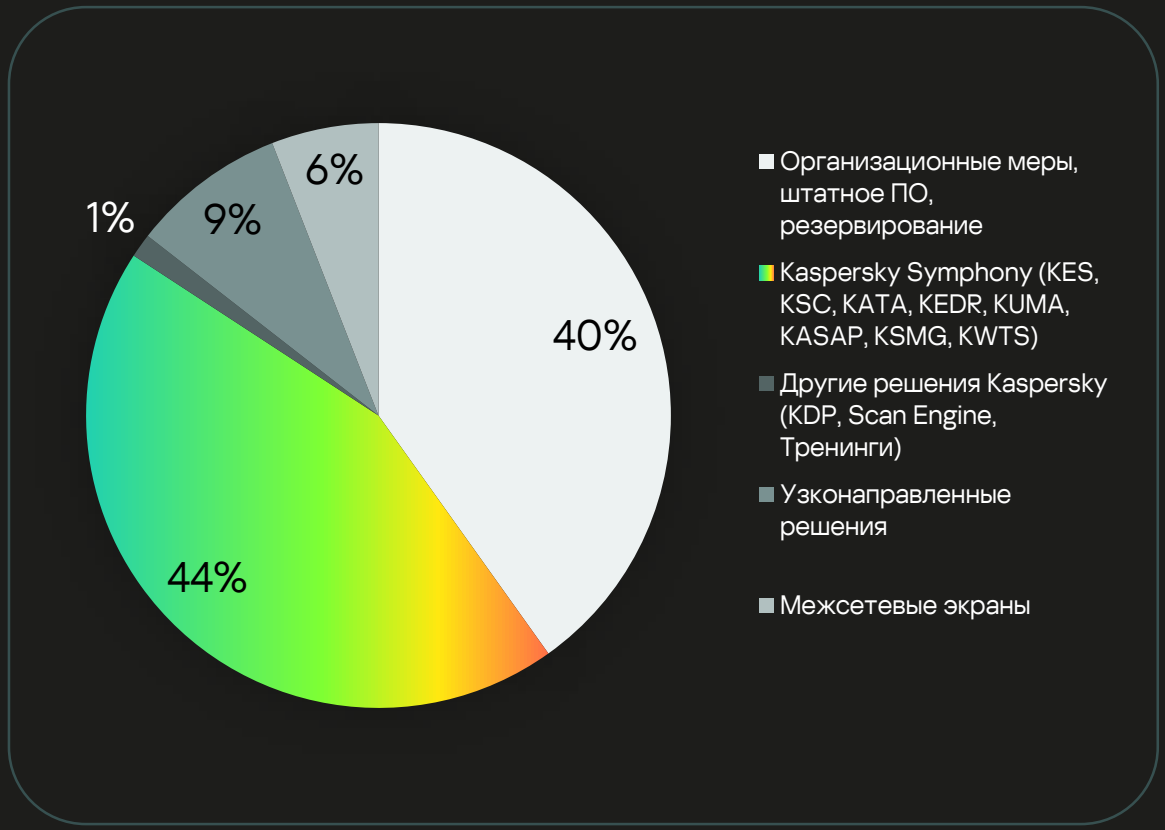
85%

всех мер приказа ФСТЭК №239

91%

базового набора мер для объектов КИИ 3-й категории

% закрытия



Приказ ФСТЭК №21 (защита перс. данных) — корпоративный сегмент

Применение Kaspersky Symphony XDR (совместно с орг. мерами и KDP) позволяет реализовать:

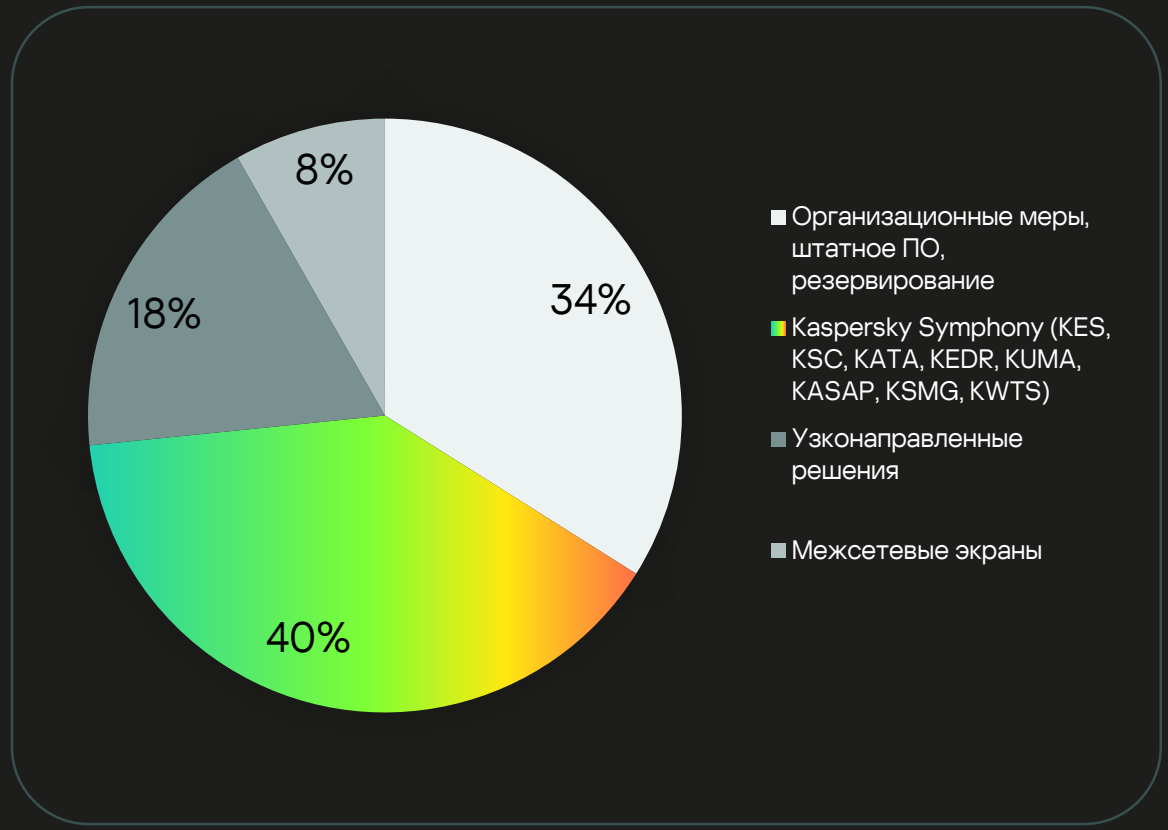
74%

всех мер приказа ФСТЭК №21

79%

базового набора мер для систем 3-го класса защищенности

% закрытия



Приказ ФСТЭК №17 (защита гос. инф. систем) — корпоративный сегмент

Применение Kaspersky Symphony XDR (совместно с орг. мерами и KDP) позволяет реализовать:

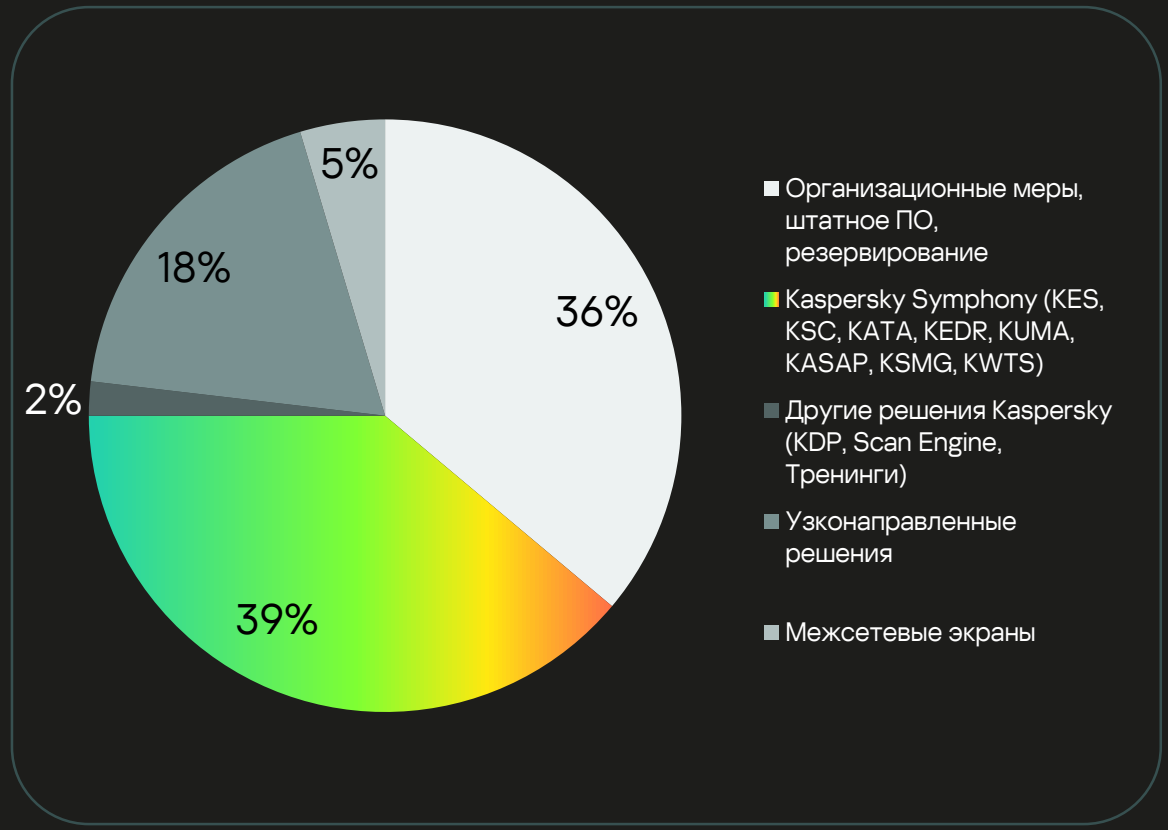
77%

всех мер приказа ФСТЭК №17

81%

базового набора мер для систем 3-го класса защищенности

% закрытия



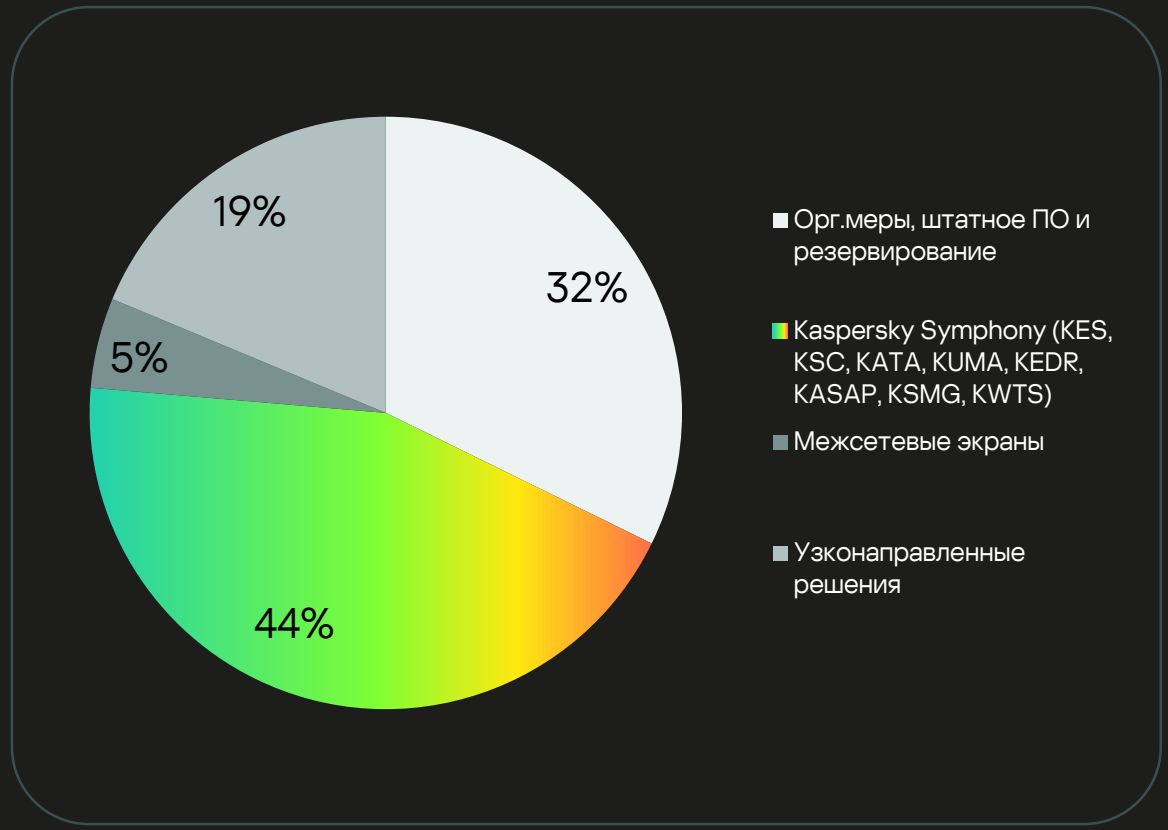
ГОСТ Р 57580.1 -2017: Защита информации финансовых организаций

Применение Kaspersky Symphony XDR (совместно с орг. мерами) позволяет реализовать:

76%

всех мер приказа ГОСТ Р 57580.1

% закрытия



Расширена интеграция с ГосСОПКА

Синхронизация статусов инцидентов

Категоризация активов в соответствии с КИИ-категориями

Возможность приложить файл к инциденту

Интерактивный чат со специалистами НКЦКИ

Сравнение актуальных значений параметров инцидентов в KUMA со значениями, переданными в ГосСОПКА

Поддержана передача инцидентов в режиме иерархии инсталляций KUMA. Родительские узлы KUMA смогут информировать НКЦКИ об инцидентах, выявленных на подчинённых системах

Сертификация решений Kaspersky

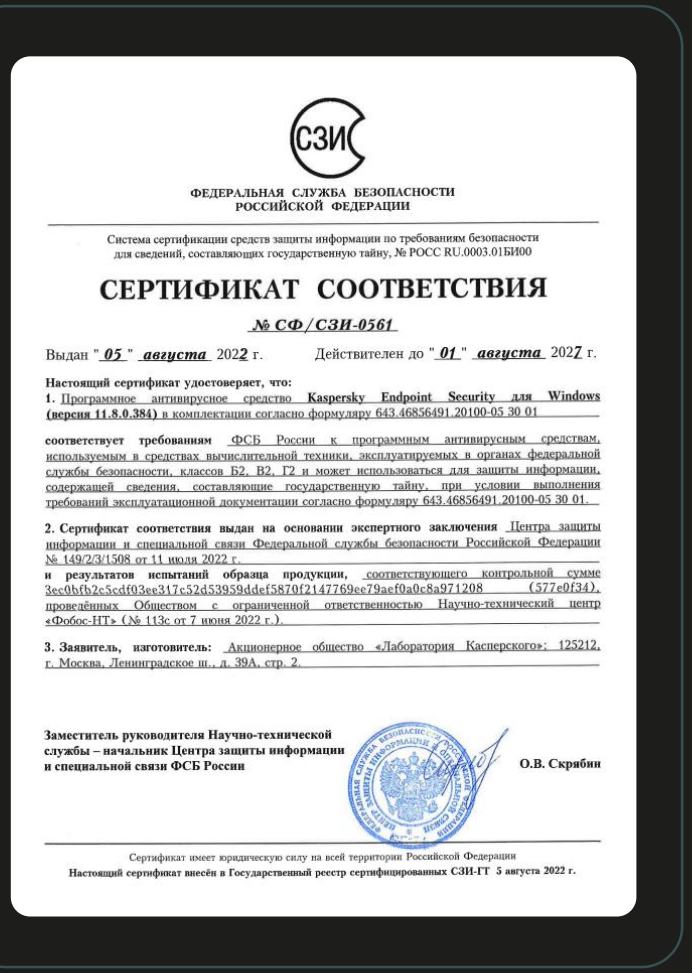
Kaspersky Endpoint Security. Сертификация ФСТЭК РФ, ФСБ

ФСТЭК:

Б2, В2, Г2

ФСБ:

Б2, В2, Г2



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, № РОСС RU.0003.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0561

Выдан "05" августа 2022 г. Действителен до "01" августа 2027 г.

Настоящий сертификат удостоверяет, что:

1. Программное антивирусное средство **Kaspersky Endpoint Security для Windows (версия 11.8.0.384)** в комплектации согласно формуляру 643.46856491.20100-05 30 01

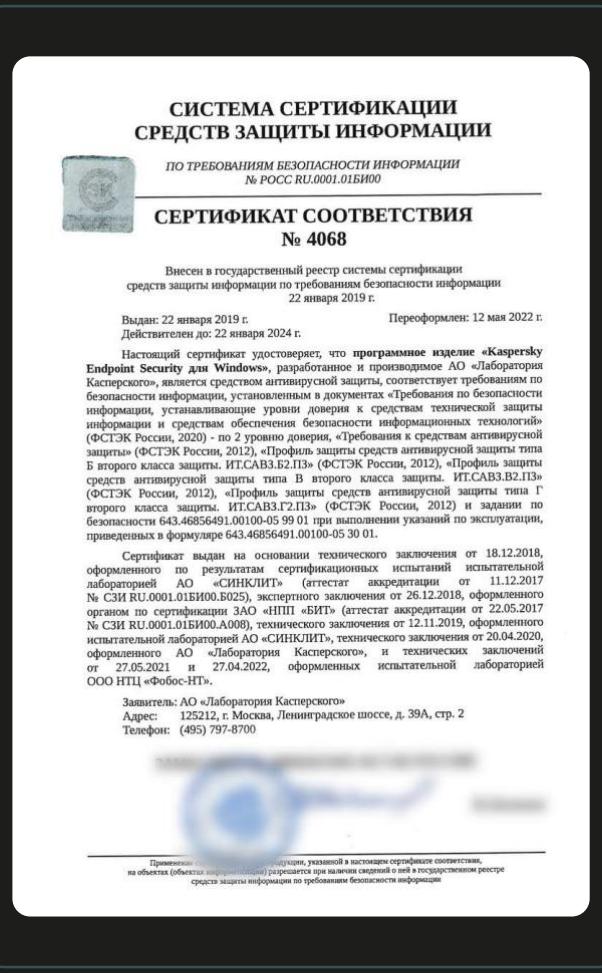
соответствует требованиям ФСБ России к программным антивирусным средствам, используемым в средствах вычислительной техники, эксплуатируемых в органах федеральной службы безопасности, классов Б2, В2, Г2 и может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну, при условии выполнения требований эксплуатационной документации согласно формуляру 643.46856491.20100-05 30 01.

2. **Сертификат соответствия выдан на основании экспертного заключения** Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации № 149/2/3/1508 от 11 июля 2022 г.
и результатов испытаний образца продукции, соответствующего контрольной сумме 3ec0bfb2c5cdf03ee317c52d53959ddef5870f2147769ee79aef0a0c8a971208 (577e0f34), проведённых Обществом с ограниченной ответственностью Научно-технический центр «Фобос-НТ» (№ 113с от 7 июня 2022 г.).

3. **Заявитель, изготовитель:** Акционерное общество «Лаборатория Касперского»; 125212, г. Москва, Ленинградское ш., д. 39А, стр. 2.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

Сертификат имеет юридическую силу на всей территории Российской Федерации
Настоящий сертификат внесён в Государственный реестр сертифицированных СЗИ-ГТ 5 августа 2022 г.



СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4068

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 22 января 2019 г.

Выдан: 22 января 2019 г. Переоформлен: 12 мая 2022 г.
Действителен до: 22 января 2024 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Endpoint Security для Windows»**, разработанное и производимое АО «Лаборатория Касперского», является средством антивирусной защиты, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 2 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 643.46856491.00100-05 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00100-05 30 01.

Сертификат выдан на основании технического заключения от 18.12.2018, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «СИНКЛИТ» (аттестат аккредитации от 11.12.2017 № СЗИ RU.0001.01БИ00.Б025), экспертного заключения от 26.12.2018, оформленного органом по сертификации ЗАО «НПП «БИТ» (аттестат аккредитации от 22.05.2017 № СЗИ RU.0001.01БИ00.А008), технического заключения от 12.11.2019, оформленного испытательной лабораторией АО «СИНКЛИТ», технического заключения от 20.04.2020, оформленного АО «Лаборатория Касперского», и технических заключений от 27.05.2021 и 27.04.2022, оформленных испытательной лабораторией ООО НТЦ «Фобос-НТ».

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

[redacted]

Применение [redacted] продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Kaspersky EDR. Сертификация ФСТЭК РФ

ФСТЭК:
САВЗ Б4, В4, СОВ У4

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4597

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
14 октября 2022 г.

Выдан: 14 октября 2022 г.
Действителен до: 14 октября 2027 г.

Настоящий сертификат удостоверяет, что **программное изделие Kaspersky Endpoint Detection and Response**, разработанное и производимое АО «Лаборатория Касперского», является программным средством, реализующим функции средства антивирусной защиты и средства обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В четвертого класса защиты. ИТ.САВЗ.В4.ПЗ» (ФСТЭК России, 2012), «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты. ИТ.СОВ.У4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 643.46856491.00120-01 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00120-01 30 01.

Сертификат выдан на основании технического заключения от 18.08.2022, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), и экспертного заключения от 02.09.2022, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

КАТА. Сертификация ФСТЭК РФ, ФСБ

ФСТЭК:

СОВ уровня сети
4 класса защиты.
По 4 уровню доверия

ФСБ:

СОА класса АП,
САВЗ Д

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, № РОСС RU.0003.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0477

Выдан "25" августа 2021 г. Действителен до "31" декабря 20

Настоящий сертификат удостоверяет, что:
1. Средство защиты информации «Программное средство обнаружения компьютерных (СОА) Kaspersky Anti Targeted Attack Platform», изготовленное в соответствии с техниче условиями ТУ 643.46856491.20099-03,

соответствует требованиям ФСБ России к средствам обнаружения компьютерных (класс АП) и может использоваться для обнаружения и предотвращения в автоматич режиме компьютерных атак (вторжений) на основе анализа сетевого трафи автоматизированных информационных системах, обрабатывающих информацию, не содерж сведений, составляющих государственную тайну, при условии выполнения требо эксплуатационной документации согласно формуляру 643.46856491.20099-03 30 01.

2. Сертификат соответствия выдан на основании экспертного заключения Центра з информации и специальной связи Федеральной службы безопасности Российской Феде № 149/2/1-1124 от 1 июля 2021 г.
и результатов испытаний образца продукции – эталонного дистри программного обеспечения на оптическом носителе DVD-R уч. № 03дсп от 1 марта 2 проведённых Акционерным обществом «СИНКЛИТ» (№ 11дсп от 23 декабря 2020 г.).

3. Заявитель, изготовитель: Акционерное общество «Лаборатория Касперского»; 1 г. Москва, Ленинградское ш., д. 39А, стр. 2.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России О.В. Ск

Сертификат имеет юридическую силу на всей территории Российской Федерации
Настоящий сертификат внесён в Государственный реестр сертифицированных СЗИ-ГТ 25 августа 202

Настоящий сертификат зарегистрирован в государственном р

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3854

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 27 декабря 2017 г.

Выдан: 27 декабря 2017 г. Переоформлен: 28 июня 2022 г.
Действителен до: 27 декабря 2020 г.
Срок действия продлён до: 27 декабря 2025 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Anti Targeted Attack Platform»**, разработанное и производимое АО «Лаборатория Касперского», является программным средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем и средств вычислительной техники, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012) и задании по безопасности 643.46856491.00086-06 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00086-06 30 01.

Сертификат выдан на основании технического заключения от 06.10.2017, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), экспертного заключения от 29.11.2017, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 12.11.2018 и 05.03.2020, оформленных испытательной лабораторией АО «СИНКЛИТ», технического заключения от 20.05.2019, оформленного АО «Лаборатория Касперского», экспертного заключения от 26.03.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России», и технических заключений от 12.04.2022 и 07.06.2022, оформленных испытательной лабораторией ООО НТЦ «Фобос-НТ».

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

ФСТЭК:
По 4 уровню доверия

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4455

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
28 сентября 2021 г.

Выдан: 28 сентября 2021 г. Переоформлен: 7 ноября 2022 г.
Действителен до: 28 сентября 2026 г.

Настоящий сертификат удостоверяет, что **программное изделие «Kaspersky Unified Monitoring and Analysis Platform»**, разработанное и производимое АО «Лаборатория Касперского», является системой управления событиями информационной безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и технических условиях ТУ 643.46856491.00116-03 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00116-03 30 01.

Сертификат выдан на основании технического заключения от 03.09.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), экспертного заключения от 17.09.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технических заключений от 19.10.2021 и 25.10.2022, оформленных испытательной лабораторией ООО НТЦ «Фобос-НТ».

Заявитель: АО «Лаборатория Касперского»
Адрес: 125212, г. Москва, Ленинградское шоссе, д. 39А, стр. 2
Телефон: (495) 797-8700

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

О компании

Наш путь в вопросе защиты бизнеса

Ваш единый партнер по защите бизнеса

От защиты рабочих мест
до стратегического партнера
по кибербезопасности

~ 5 000

высококвалифицированных специалистов

50%

наших сотрудников — R&D-специалисты

35+

ведущих мировых экспертов в области кибербезопасности

5

уникальных центров экспертизы

Ваш стратегический партнер по кибербезопасности

Глобальный охват и международное признание

Доказанная эффективность технологий

Прозрачность и соответствие стандартам

Опыт и знания мирового уровня

Высокий статус в индустрии ИБ

Более 25 лет безупречной работы

Спасибо!