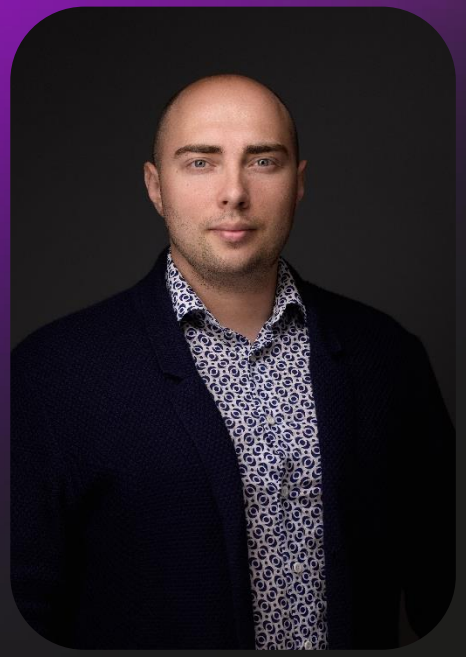
Платформа KATA и KEDR Expert

kaspersky

Спикеры



Сергей Крутских

Менеджер по развитию бизнеса, противодействия сложным и целевым атакам

«Лаборатория Касперского»

Дмитрий Мокреев

Эксперт по системам защиты от целевых атак

«Лаборатория Касперского»

Ландшафт угроз

Средний ущерб от успешной кибератаки

SMB: 105k$ Enterprise: ~1M$

Варианты атак

Эксплуатация тематики COVID-19 в 2021 году и темы частичной мобилизации – в 2022

Атаки на удаленный доступ

«Кроме Windows»: Linux, Mac, роутеры

Мобильные импланты, 0day's: iOS/Android-атаки

Атаки на цепочки поставок

Современные шифровальщики: Ransomware-as-a-Service, Big Game Hunting

Количество DDoS-атак существенно возросло

APT	0.01%
Targeted	19.9%
Crime	80%

Источники данных: Cybersecurity Ventures, Kaspersky

Масштаб современных кибератак

1	2	3	4	5
Средний ущерб от успешной кибератаки	Отношение лидеров бизнеса	Мотивация атак	Оценка активности шифровальщиков	Особенности атак
SMB: 105k$ Enterprise: от 1M$	68% лидеров бизнеса считают, что риски, связанные с кибербезопасностью растут	71% атак были финансово мотивированными (Q1 2022)	За Q3 2022 мы защитили более 72 тыс. уникальных пользователей от шифровальщиков	52% атак имели отношение к взлому, 28% были проведены с использованием вредоносов, 33% использовали фишинг и социальную инженерию (Q1 2022)

Источники данных: Kaspersky, Accenture, Verizon

Что в России?

Уход иностранных поставщиков решений для киберзащиты

Многие российские пользователи и организации оказались в одном из самых киберопасных регионов мира без защиты

Полагаться на еще работающее импортное решение опасно

Оно может быть заблокировано в любой момент

Компании лишились защиты

Иностранные продукты не обновляются или блокируются

Оставшиеся иностранные вендоры могут уйти

С теми же последствиями для заказчика

Рост числа кибератак в России в первом квартале 2022 года

Всплеск активности

- Собственная активность «хактивистов»
- Атаки, спонсируемые иными странами
- Атаки спецслужб иных стран

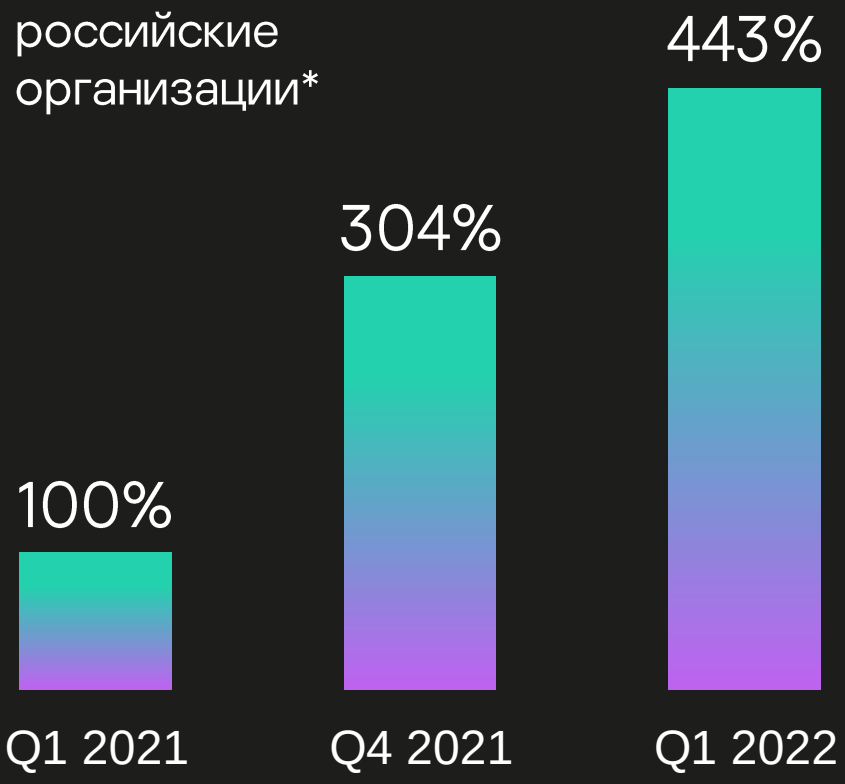
Приоритеты атакующих

- Нарушение критических процессов, с максимальным уроном
- Кибершпионаж
- Пропагандистские акции и дезинформация

Мишени атакующих

- Критические инфраструктуры и важные коммерческие поставщики
- Информационные порталы и ресурсы госслужб
- Расширенный спектр компаний-целей, участвующих в важных цепочках поставок

В 4,5 раза больше DDoS-атак на российские организации*



* В Q1 2022 по сравнению с Q1 2021, по данным сервиса Kaspersky DDoS Protection

Предсказания

Что грозит корпорациям в 2023 году

Будет еще больше утечек персональных данных, появятся комбинированные базы

Даркнет-сообщество станет еще более чутко реагировать на новостную повестку

Шантаж в медиа: компании будут узнавать о взломе из публичных постов хакеров с обратным отсчётом до публикации данных

«Потехе час»: киберпреступники будут чаще публиковать фейки о взломах

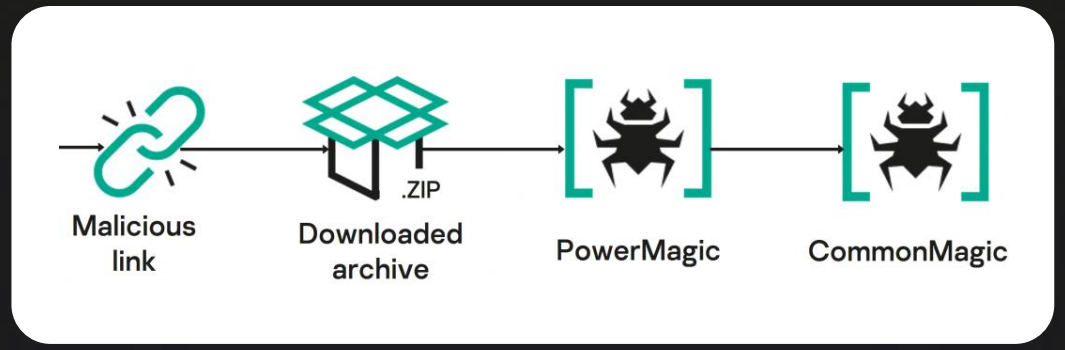
Популярными векторами станут облачные технологии и скомпрометированные данные из даркнета

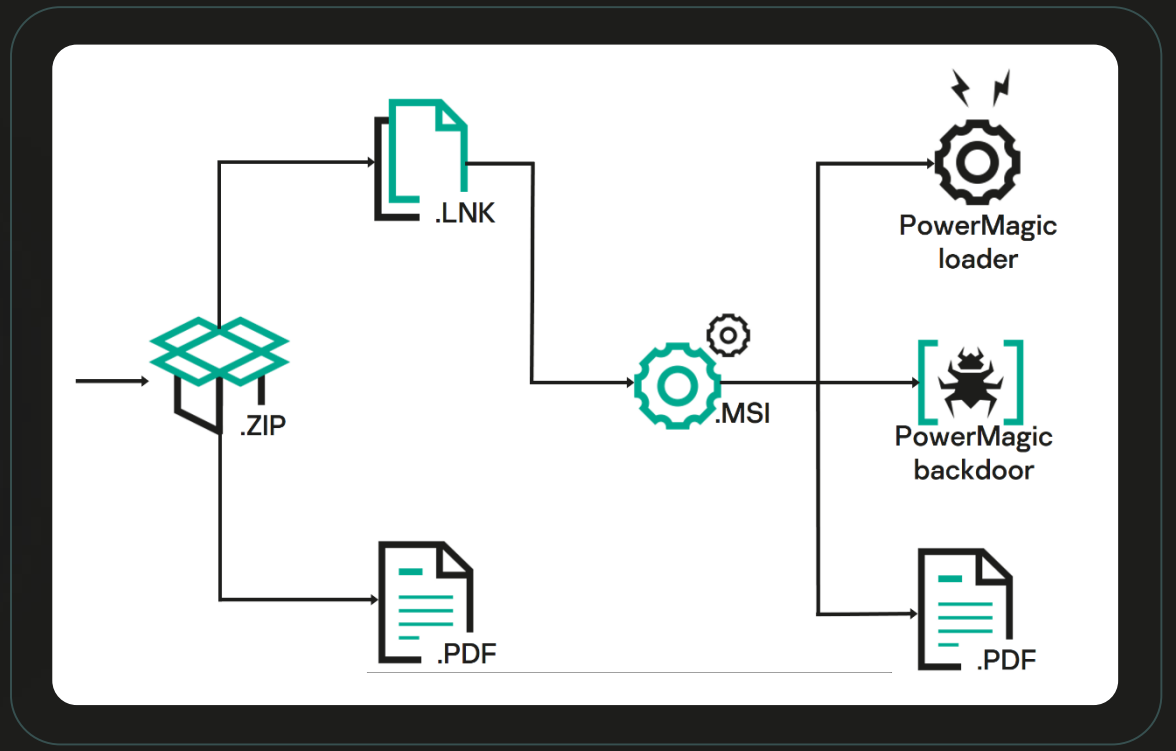
Программа-вымогатель как услуга: больше однотипных атак, сложнее инструментарий

* Security Services

Примеры атак

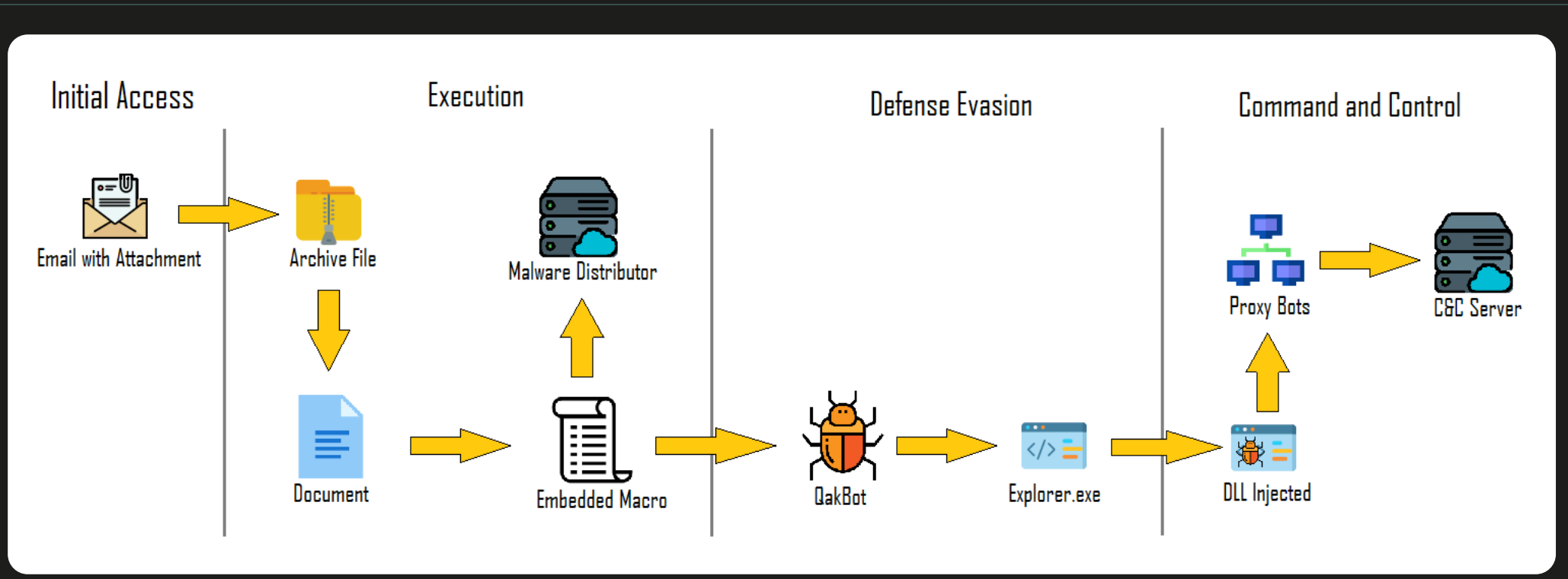
Бэкдор PowerMagic и фреймворк CommonMagic





https://securelist.ru/bad-magic-apt/107020/

Троянец QakBot, опять...



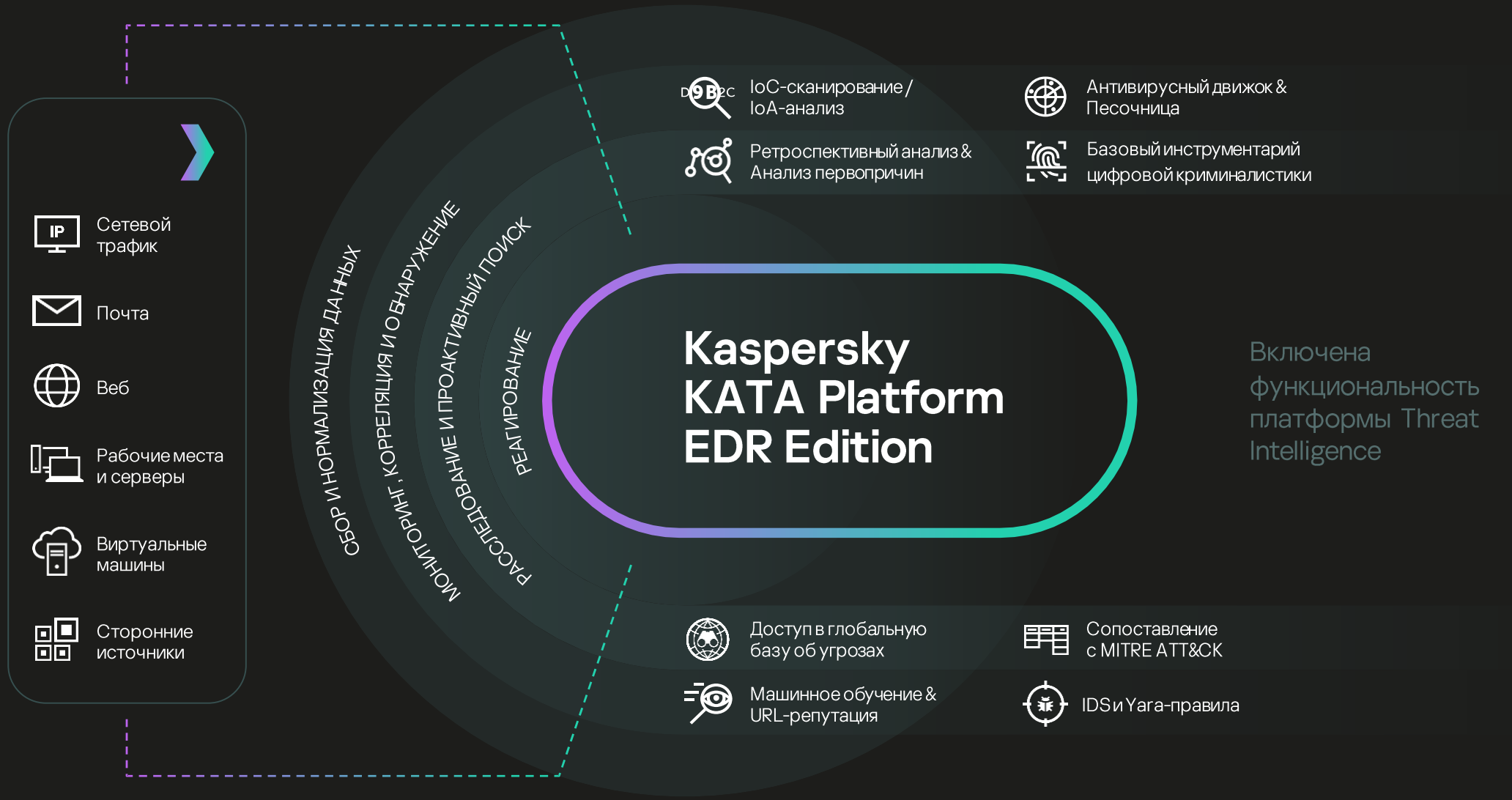
https://securelist.ru/qakbot-technical-analysis/103485/

Kaspersky
Anti Targeted
Attack

Всесторонняя платформа для защиты от продвинутых угроз и APT-атак

с широкими возможностями по детектировнаию и реагированию на сетевом уровне и на уровне рабочих станций (когда используется вместе с Kaspersky EDR)

Ключевые возможности

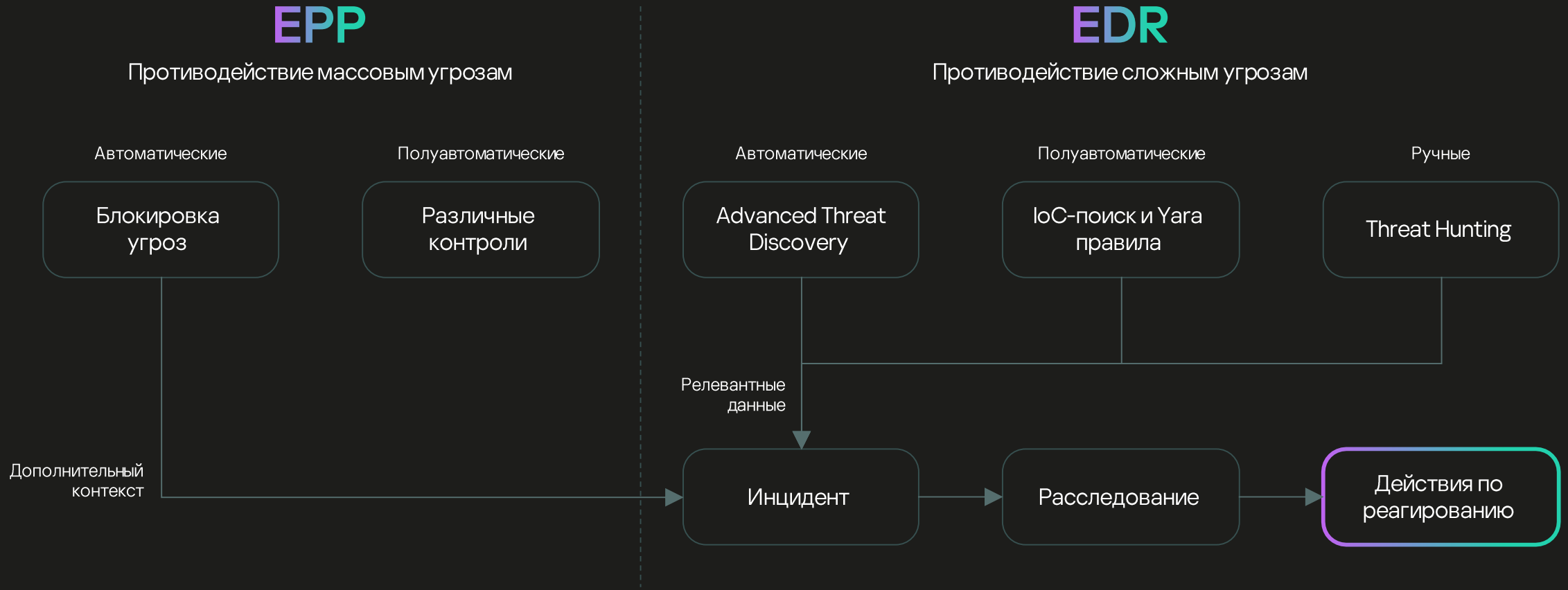


Kaspersky
EDR Expert

Мощное EDR решение, разработанное для security экспертов, SOC’ов и команд реагирования на инциденты

для продвинутого детектирования, эффективного расследования, проактивного поиска угроз и устранения последствий многоуровневых атак на инфраструктуру рабочих станций

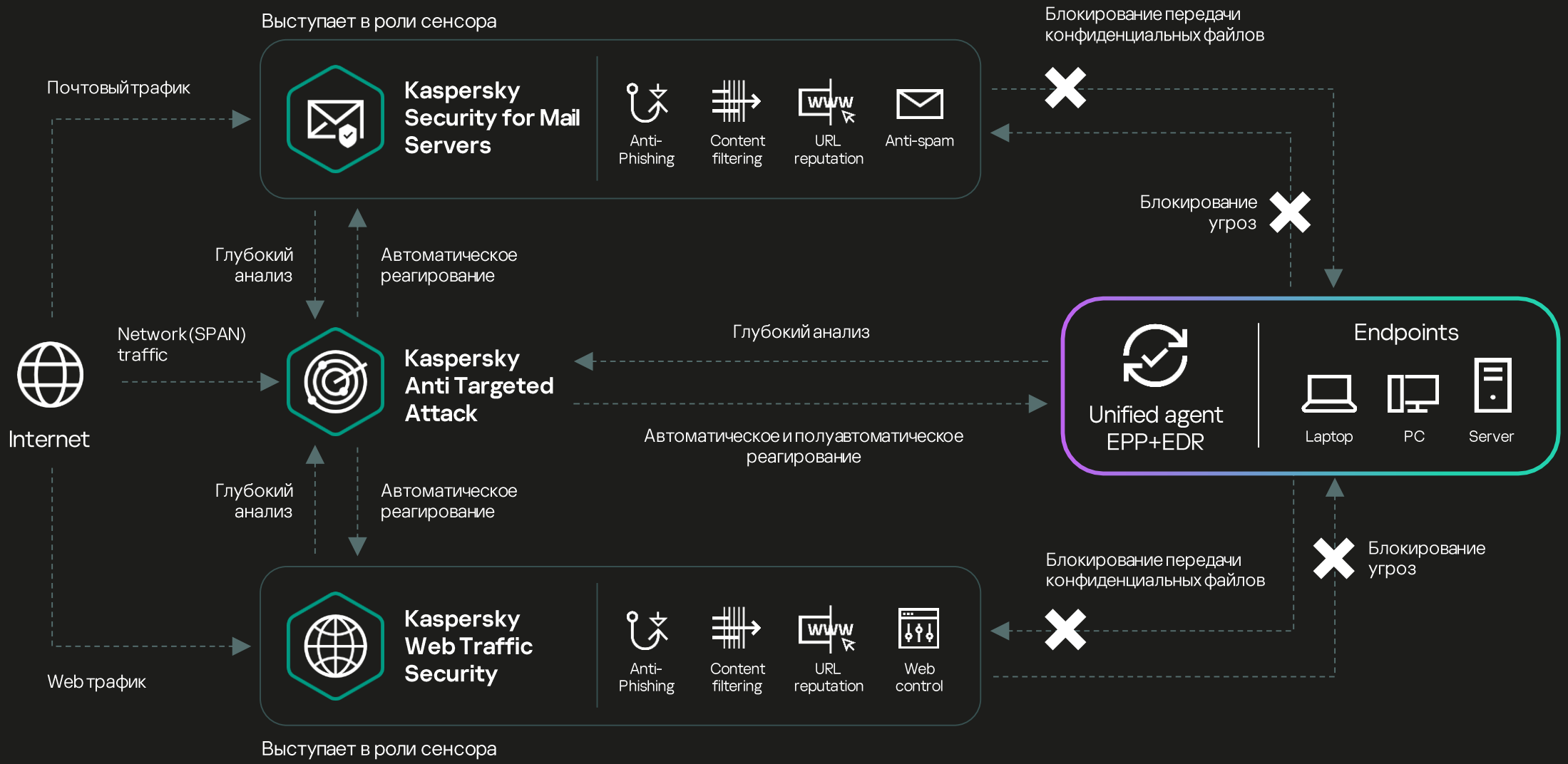
Единый агент



Технологии Kaspersky Endpoint Detection & Response

	Технология	Описание
TAA	Targeted Attack Analyzer	Обнаруживает индикаторы атак (Indicators of attack, IOA) по обновляемым и пользовательским правилам в событиях телеметрии, поступающих от компьютеров
SB	Sandbox	Анализирует исполняемые файлы и активные документы на виртуальных машинах по запросу аналитика или автоматически в результате срабатывания правила TAA. Применяет обновляемую логику обнаружения
IOC	Indicator of Compromise	Обнаруживает признаки компрометации на компьютерах сети по пользовательским правилам в формате OpenIOC
YARA	YARA Engine	Сканирует файлы (и процессы) на компьютерах, а также файлы в хранилище центрального узла по пользовательским правилам
AM	Anti-malware Engine	Сканирует файлы в хранилище центрального узла по обновляемым сигнатурам

Автоматическое реагирование с KSMG и KWTS



Сбор и анализ расширенной телеметрии

Единый агент EPP+EDR

Драйвер сети

Драйвер перехвата OS API

Драйвер мониторинга файловой системы

Драйвер мониторинга процессов и сервисов

Обогащение и фильтрация

~15k EPD

Создание, модификация файлов и т .д.

Запуск, инъекция процессов и т.д.

Сетевые соединения, DNS-запросы, скачивание файла, e-mail и т.д.

Изменение реестра, Event logs, WMI, автозапуск и т.д.

Инциденты AV, DeviceControl и т.д.

GERT
Группа реагирования

SOC Team

GREAT Центр глобальных исследований и анализа угроз

EDR Central Node

Обогащение

Визуализация

Корреляция

+ Инциденты EDR

Threat Intelligence

3rd party
Сторонние события

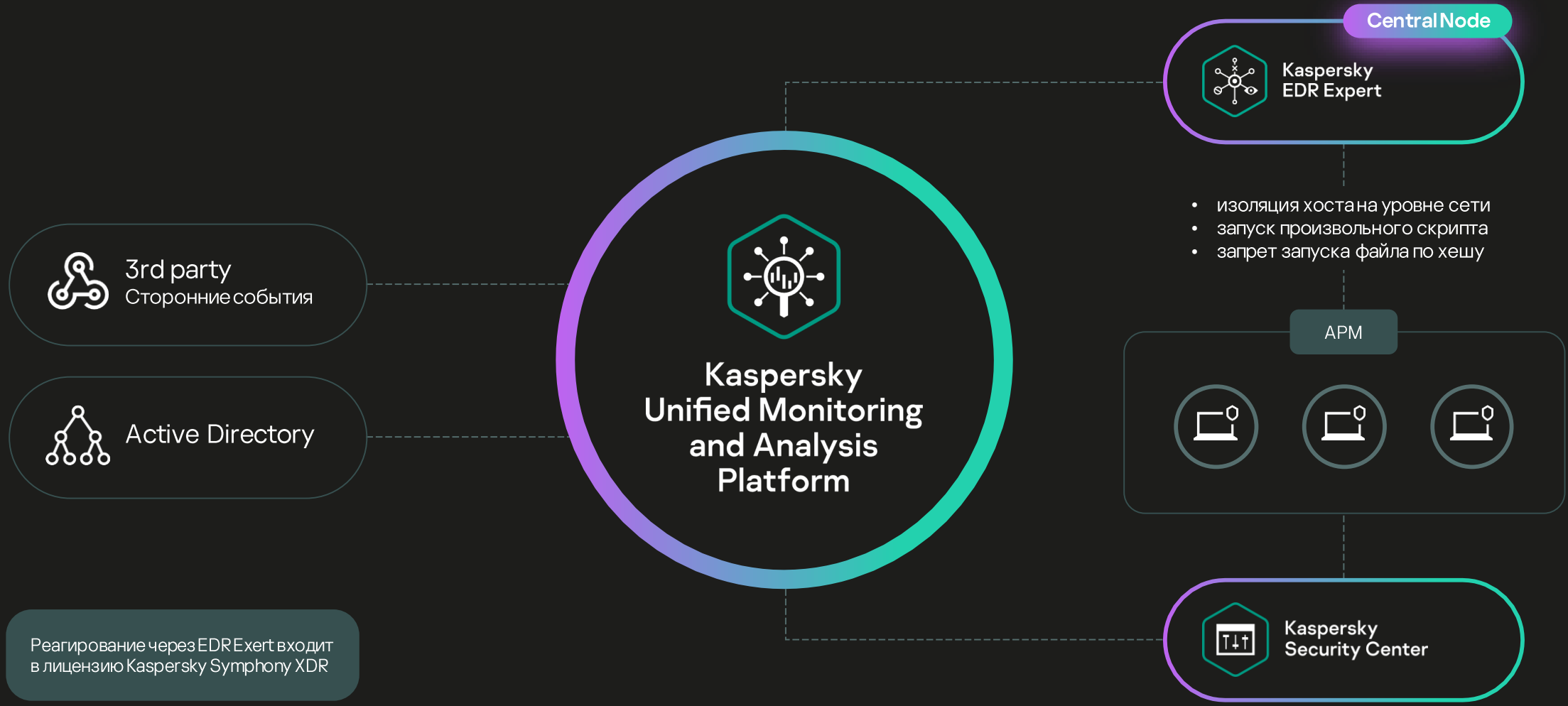
KUMA

Обогащение

Визуализация

Корреляция

Автоматизированное реагирование на инциденты KES/KEDR



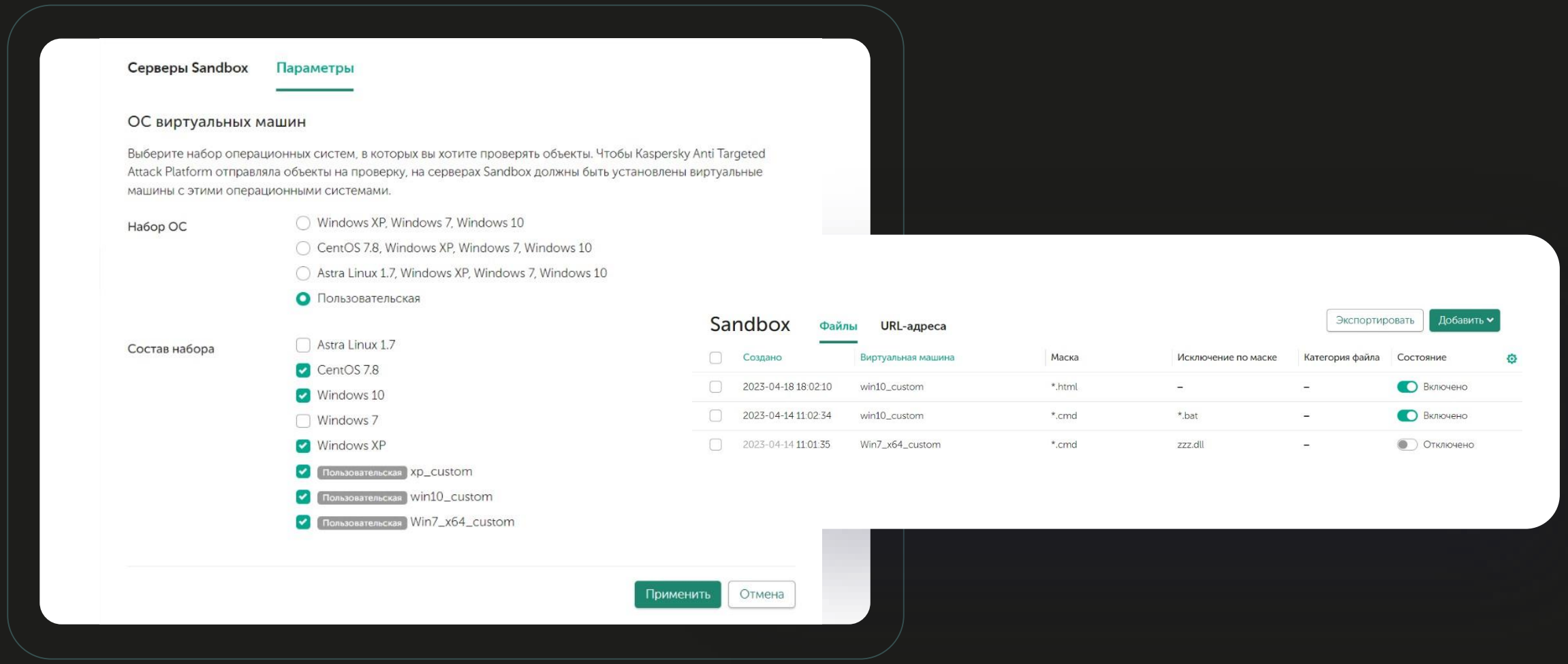
Что было сделано

На серверах с компонентом Sandbox запускаются предустановленные виртуальные образы следующих операционных систем:

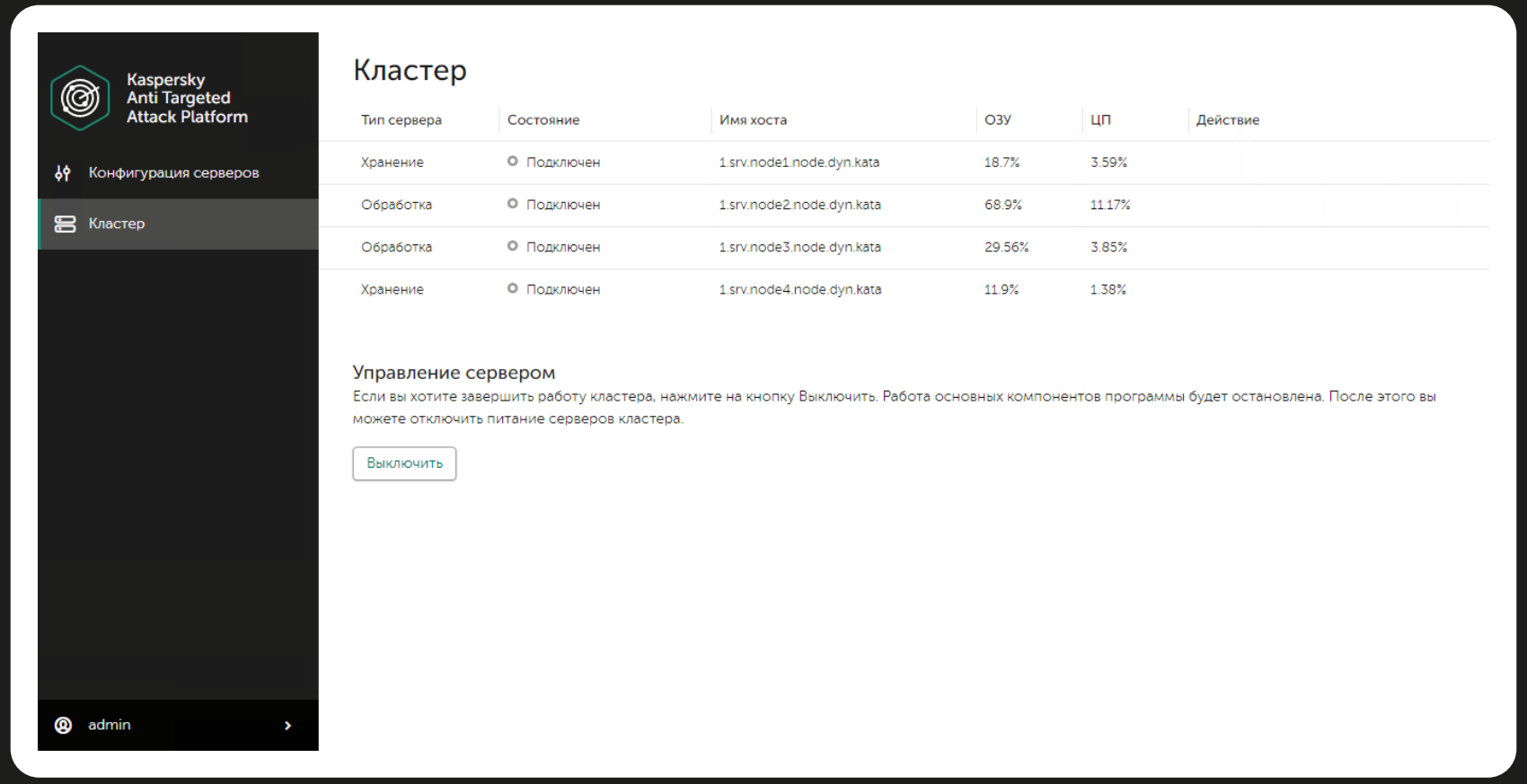
- Windows XP SP3 32-разрядная
- Windows 7 64-разрядная
- Windows 10 64-разрядная
- CentOS 7.8
- Astra Linux Special Edition 1.7

Образ CentOS и Astra Linux подключается опционально: возможен выбор набора операционных систем, на основе которого будут формироваться задачи на проверку объектов в компоненте Sandbox

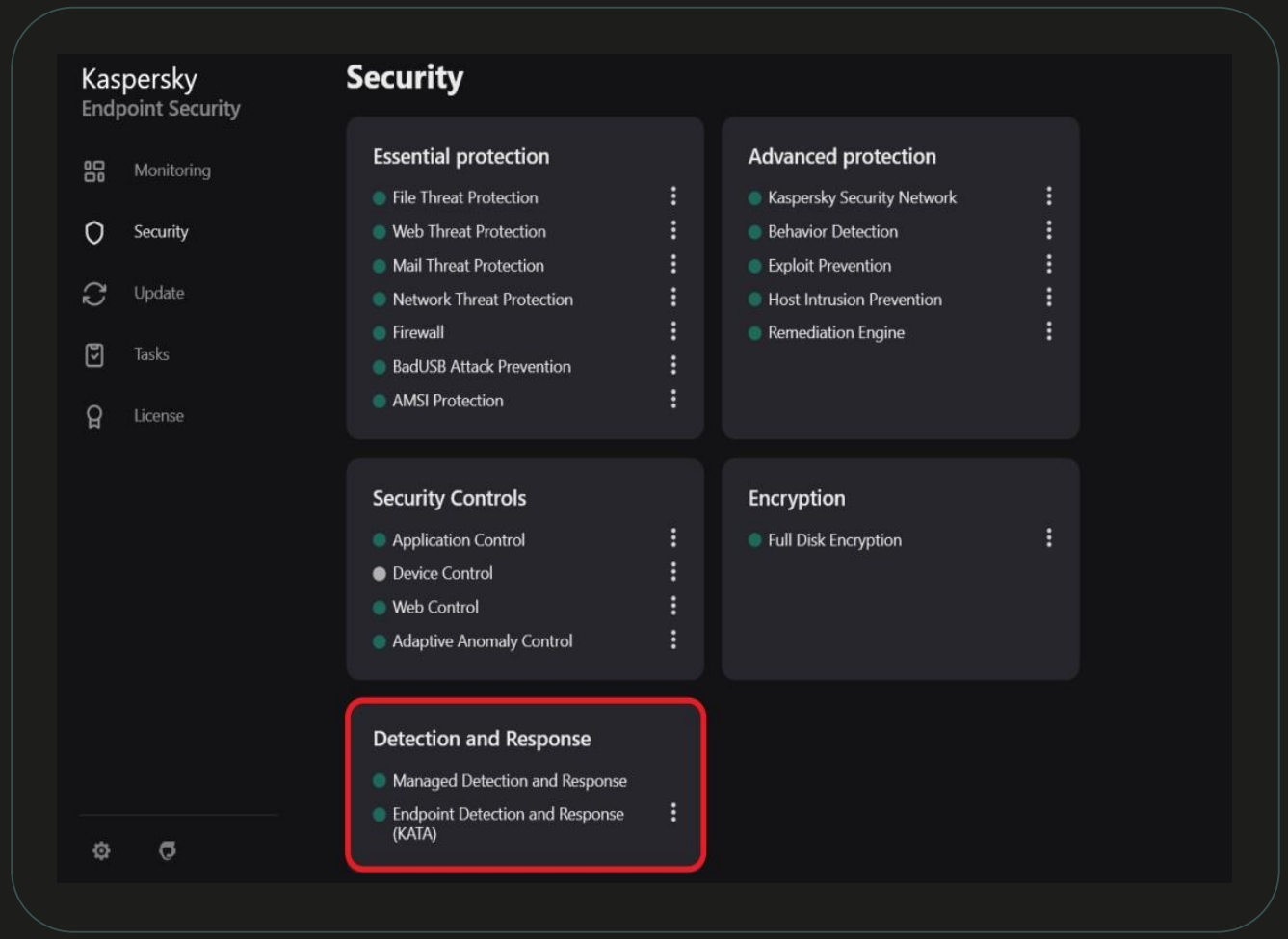
Кастомизация образов в Sandbox



Поддержка отказоустойчивого режима работы



Built-in agent (KES+EDR) для Windows и Linux

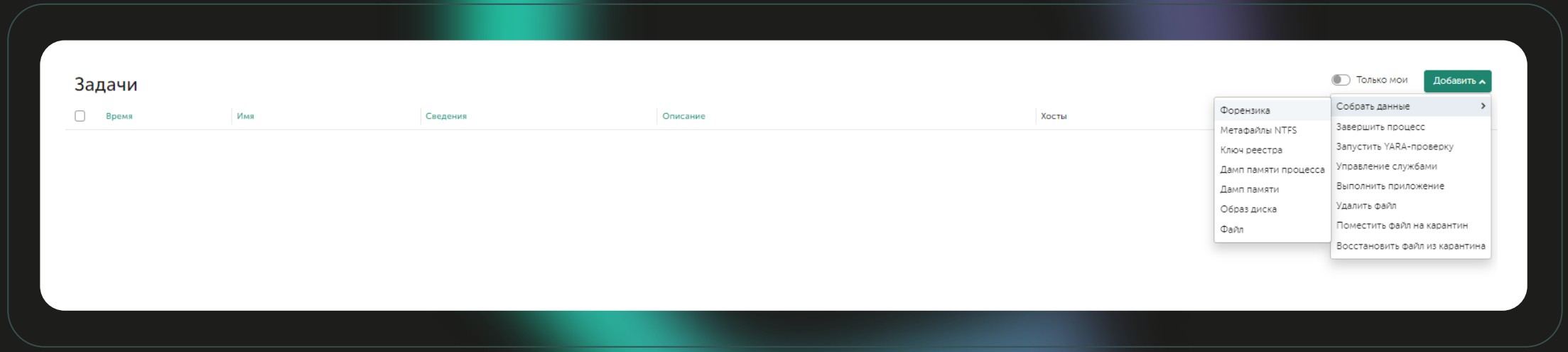


Расширение возможностей сбора данных с хоста при расследовании инцидентов

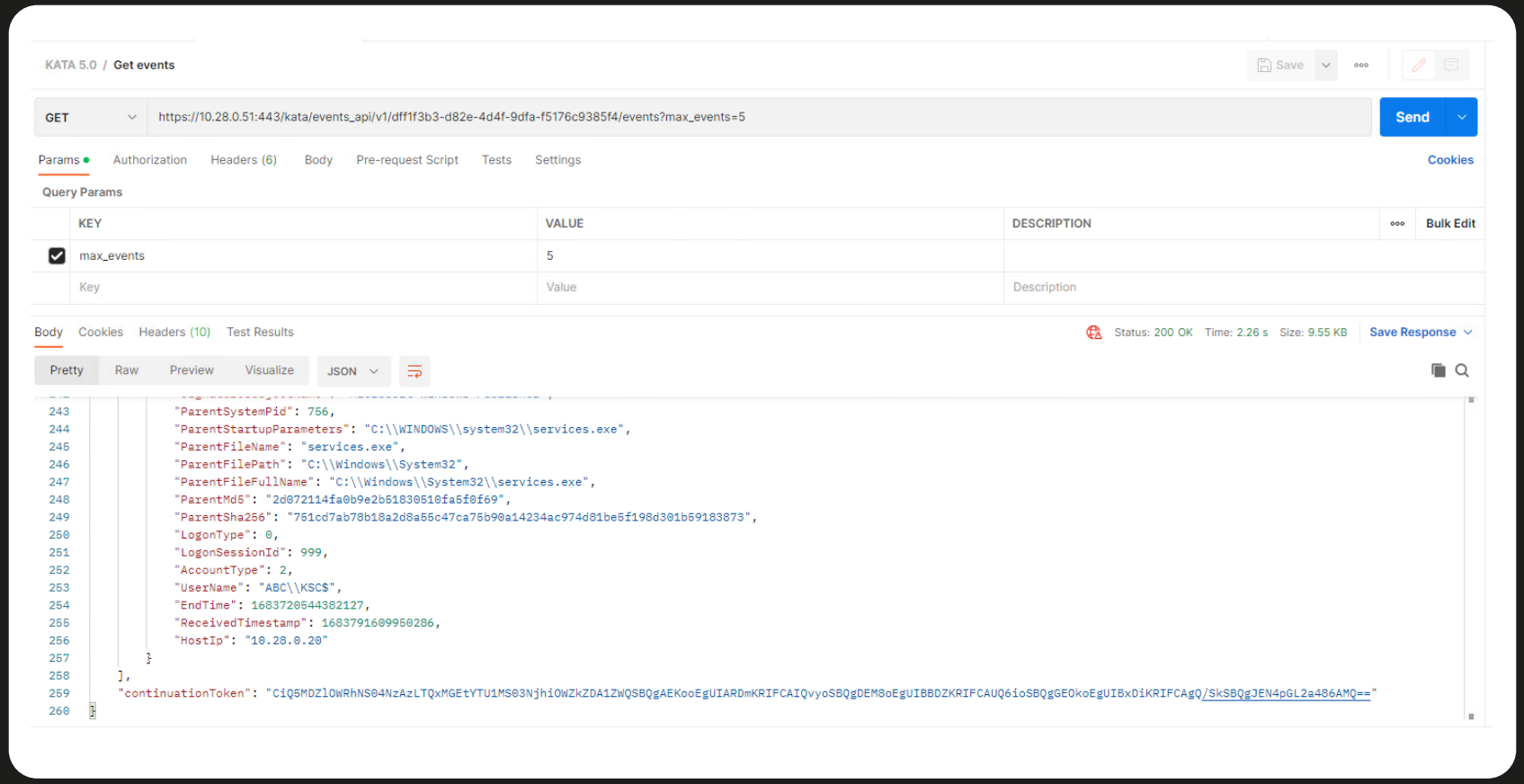
Получение с хостов ключей реестра, дампов памяти процессов, метафайлов NTFS

Сканирование YARA-правилами точек автозапуска

Получение дампов ОЗУ и диска

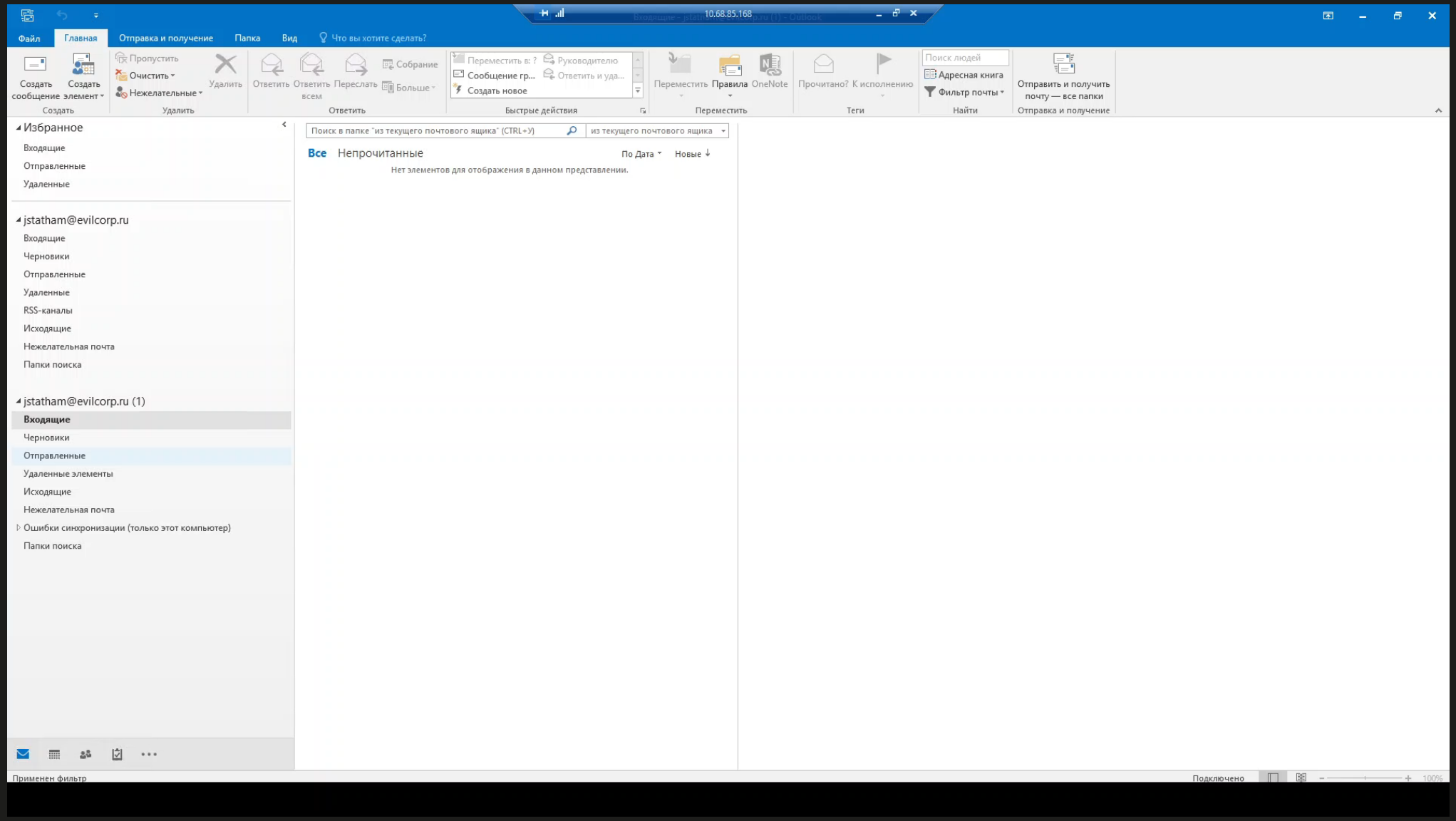


Возможность отправки телеметрии с защищаемых хостов по API



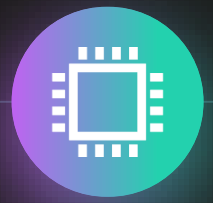
Пример расследования

Демо-видео


10.68.85.168
Файл
Главная
Отправка и получение
Папка
Вид
Что вы хотите сделать?
Создать сообщение
Создать элемент
Пропустить
Очистить
Нежелательные
Удалить
Ответить
Ответить всем
Переслать
Собрание
Больше
Переместить в: ?
Руководителю
Сообщение гр...
Ответить и уда...
Создать новое
Переместить
Правила
OneNote
Прочитано?
К исполнению
Поиск людей
Адресная книга
Фильтр почты
Отправить и получить почту — все папки
Создать
Удалить
Ответить
Быстрые действия
Переместить
Теги
Найти
Отправка и получение
Избранное
Входящие
Отправленные
Удаленные
jstatham@evilcorp.ru
Входящие
Черновики
Отправленные
Удаленные
RSS-каналы
Исходящие
Нежелательная почта
Папки поиска
jstatham@evilcorp.ru (1)
Входящие
Черновики
Отправленные
Удаленные элементы
Исходящие
Нежелательная почта
Ошибки синхронизации (только этот компьютер)
Папки поиска
Поиск в папке "из текущего почтового ящика" (CTRL+У)
из текущего почтового ящика
Все
Непрочитанные
По Дата
Новые
Нет элементов для отображения в данном представлении.
Применен фильтр
Подключено
100%

Ключевые преимущества

Ключевые преимущества



Уникальный стек технологий

Собственный Antimalware Engine

Глобальная репутационная база KSN

Интеграция с Threat Lookup

Встроенный инструментарий для написания YARA правил

Targeted Attack Analyzer

CloudML для проверки APK файлов

Низкие системные требования

Требует на 30% меньше серверных ресурсов чем аналогичные отечественные решения

Масштабируемость

Отказоустойчивость всех компонентов системы

Легкое горизонтальное и вертикальное масштабирование

Развертывание неограниченного количества песочниц в рамках одной лицензии KATA и KEDR Expert

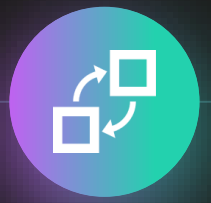
Автоматические и ручные сценарии реагирования

Автоматическое реагирование на почтовом и веб-трафике

Корреляция событий на сети и хостах

Создание правил автоматического запрета запуска исполняемых файлов по вердикту песочницы

Отправка объектов на исследование в песочницу в ручном режиме или по API



Взаимодействие с SIEM

Возможность отправки сырых событий с защищаемых хостов и готовых обнаружений в SIEM по API и Kafka

Автоматическое реагирование на инциденты с помощью EDR через API – изоляция хоста, создание правил запрета запуска файлов и процессов, а также запуск программ

Признание

Высокие рейтинги международных агентств

Соответствие требованиям регуляторов

Доверие крупных клиентов

Сертификаты

ФСТЭК:

СОВ уровня сети 4 класса защиты

ФСБ:

СОА класса АП,
САВЗ Д

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:
САВЗ Б4, В4, СОВ уровня узла 4 класса защиты

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

Истории успеха

Истории успеха

МАГНИТ

Крупнейшая розничная сеть по торговле продуктами питания на российском рынке

ФОСАГРО®

Крупнейший поставщик всех видов удобрений на российском рынке

НОВОСТАЛЬ-М

Металлургический холдинг, основными активами которого являются Абинский Электрометаллургический Завод и Металлургический Завод Балаково

МКБ

Один из крупнейших российских коммерческих банков

Крупнейший перевозчик среди пригородных пассажирских компаний России

Jet

Крупный ИТ интегратор

Banca Popolare di Sondrio

Один из крупнейших итальянских банков

ANSALDO ENERGIA

Крупнейшая итальянская энергетическая инжиниринговая компания

Что нового планируется в версии 6.0

KATA Platform EDR Edition — дальнейшее развитие

Ноябрь 2023

6.0

Переход на отечественное ПО (поддержка работы на Astra Linux)

ICAP - Интеграция с поддержкой блокирующего режима

Увеличение скорости обработки трафика

Хранение полной копии сырого трафика (PCAP) и Threat Hunting

Интеграция с модулем дешифровки трафика TLS/SSL

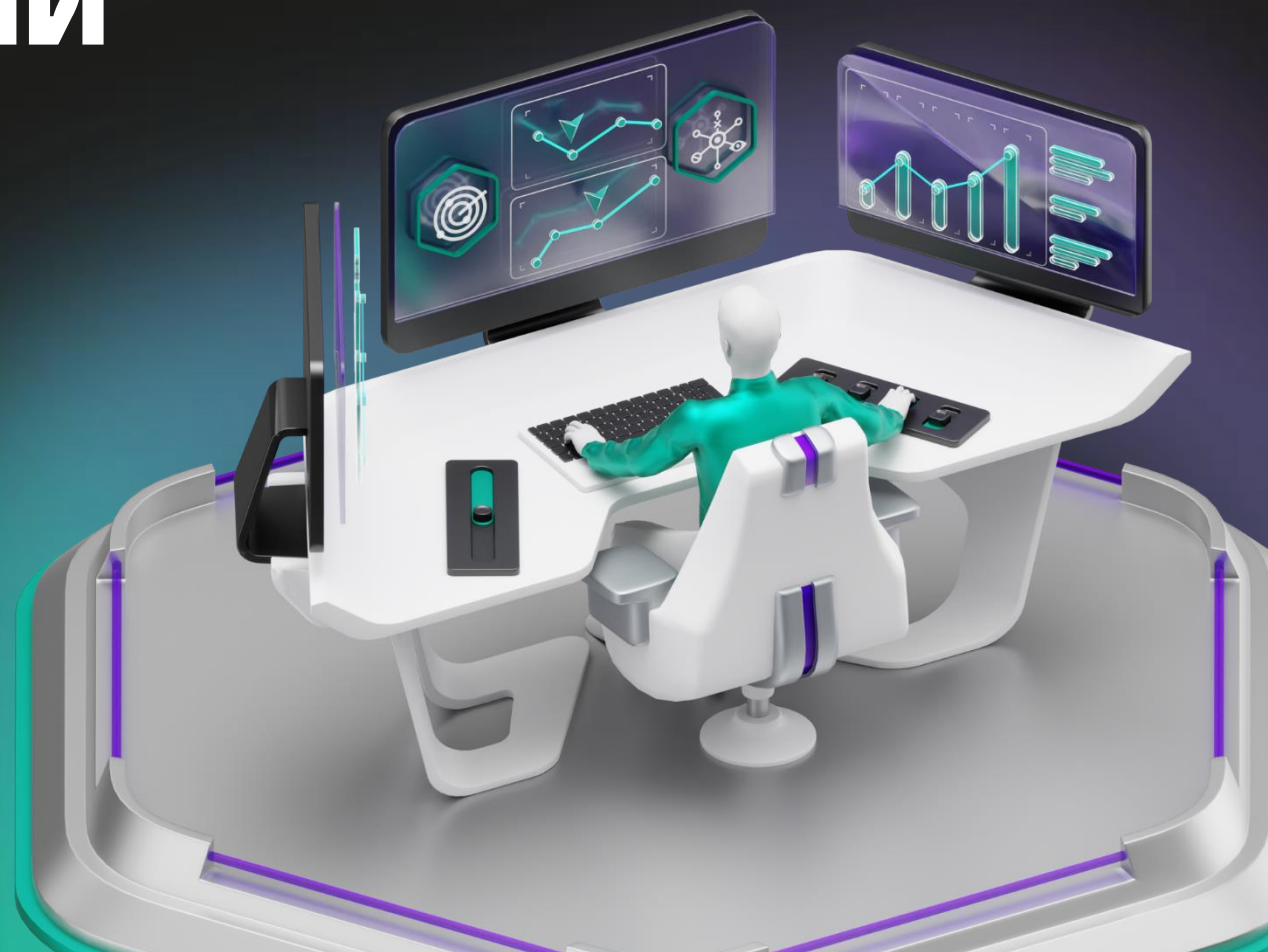
Поддержка протоколов SMB и NFS для извлечения и анализа объектов

Новые response сценарии в EDR-агенте для Linux и создание исключений по собираемой телеметрии

EDR-агент для MacOS

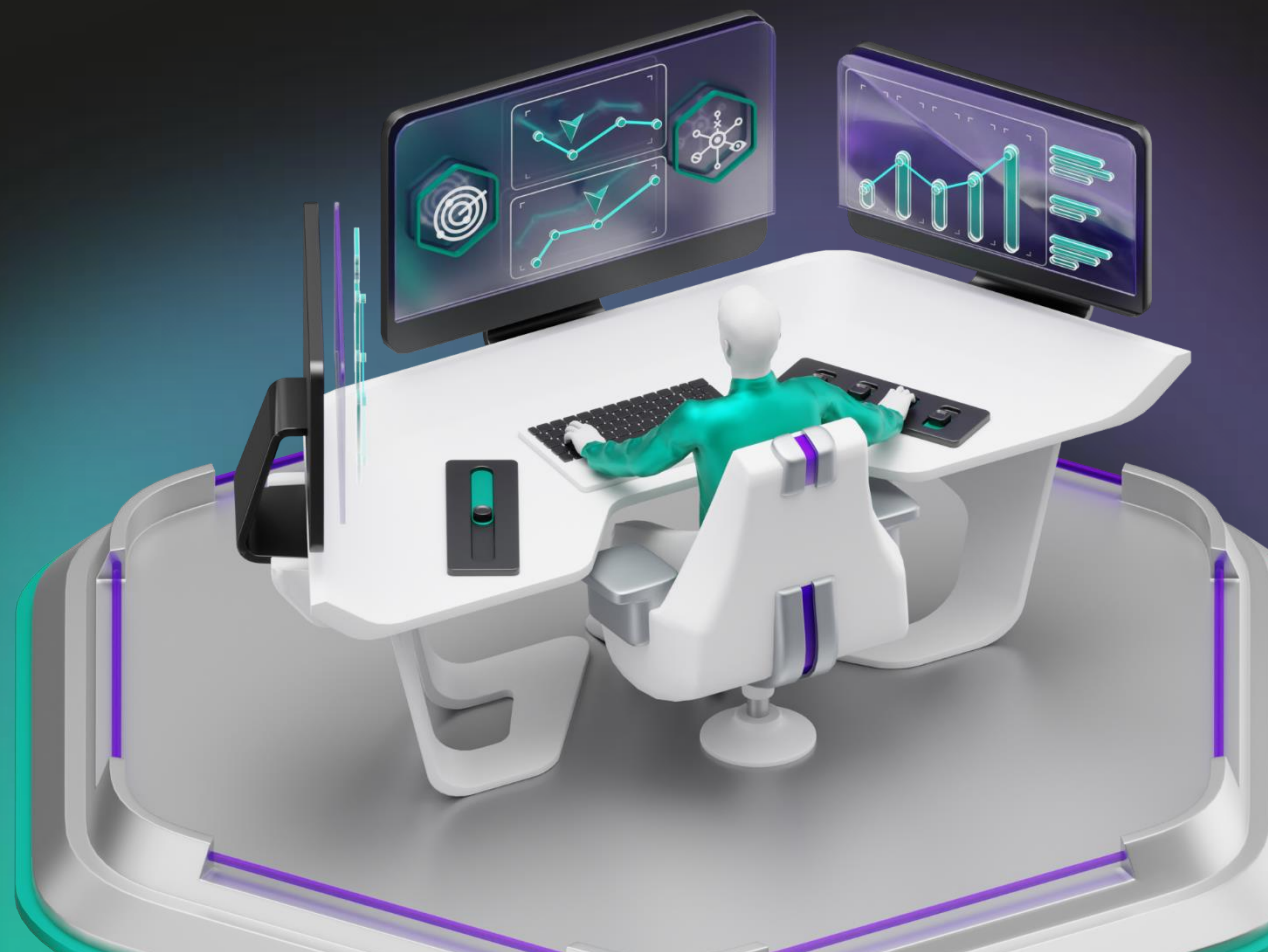
Поддержка сценариев развертывания в VDI

Мы будем рады ответить на ваши вопросы!



kaspersky

Спасибо!



kaspersky