Защита устройств от массовых, сложных и целевых атак

Тренды

ВПО остается основным
инструментом злоумышленников

35%
Шифровальщики

28%
Шпионское ПО

52%
ВПО для удаленного управления

Доля применения ВПО
в атаках на организации

71%

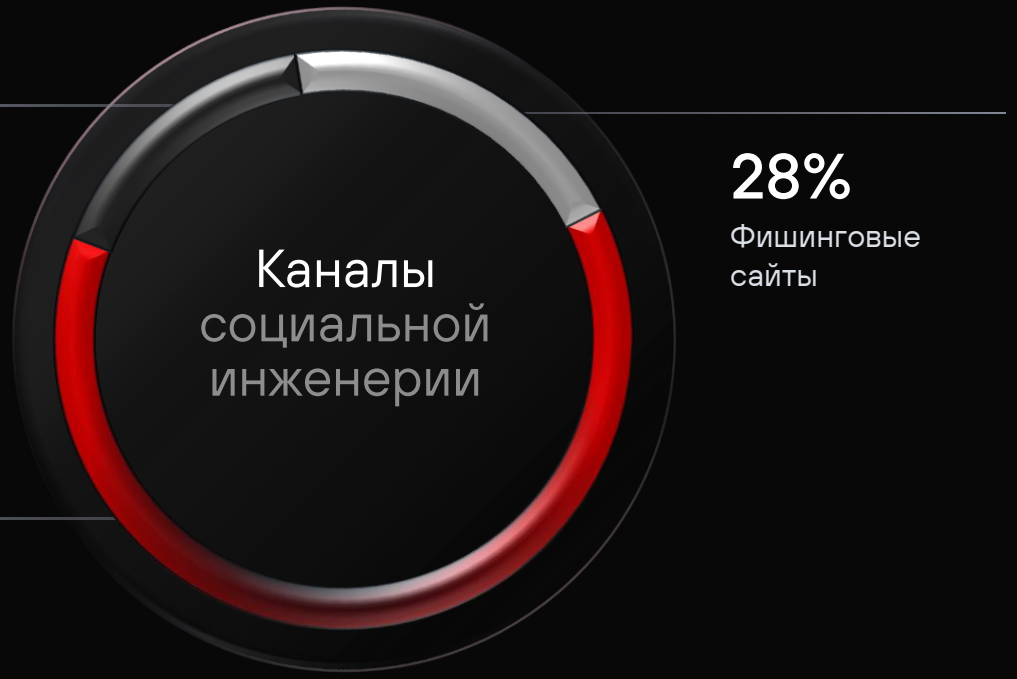
Ухищрения атакующих

- Тренд на многоэтапные схемы доставки вредоносной нагрузки
- Расширяются возможности проникновения в разные ОС за счет портирования ВПО (языки Go, Rust, Nim и др.)

* «CODE RED 2026: Актуальные киберугрозы для российских организаций».

Тактики и техники атак

Более 75% атак начинаются
с компрометации конечных устройств



23%
Мессенджеры

28%
Фишинговые сайты

88%
Электронная почта

Эксплуатация уязвимостей остается одним из самых эффективных методов атак на организации: она использовалась в 31% успешных атак

Учетные данные пользователей были скомпрометированы в 10% успешных атак

* «Актуальные киберугрозы: I–II кварталы 2025 года».

MaxPatrol Endpoint Security

Комплексное решение для
максимальной безопасности

Комплексная защита устройств от всех видов угроз

MaxPatrol Endpoint Security

Предотвращение известных угроз с MaxPatrol EPP

NEW

Обнаружение и устранение шифровальщиков и другого ВПО **благодаря антивирусным технологиям**

Контроль устройств и приложений для ограничения векторов атак (в разработке)

Автоматическое восстановление поврежденных шифровальщиком файлов (в разработке)

Выявление сложных угроз и реагирование на них с MaxPatrol EDR

1. Быстрое выявление атак, **которые могут пропустить другие средства защиты**
2. Сбор максимума данных с узлов и обнаружение киберугроз
3. Защита от злоумышленников за считанные секунды, помощь в расследовании и предотвращении атак

MaxPatrol Endpoint Protection Platform (EPP)

Необходимая защита для любых компаний

Ключевые возможности MaxPatrol EPP

1

Непрерывное обнаружение и устранение ВПО

Решение отслеживает и оперативно блокирует новые угрозы, обеспечивая постоянную защиту конечных устройств

2

Целевое реагирование

Широкий спектр методов для нейтрализации угроз:

- Блокировка запуска вредоносных файлов
- Помещение образца файла в карантин
- Удаление файлов и завершение процессов
- Сетевая изоляция узла

3

Сканирование по вашим правилам

- Проверки по расписанию или по запросу
- Оптимизация потребления ресурсов
- Возможность внесения исключений

4

Масштабируемость

Подходит как для небольших инсталляций, так и для крупных георасределенных инфраструктур

5

Гибкая настройка

Модульная структура позволяет настроить функциональность продукта с учетом поставленных задач и внутренних регламентов

6

Интеграция с другими средствами защиты

- Интеграция с SIEM-системами и песочницами для глубокого анализа угроз при минимальном расходе ресурсов
- Комбинация с MaxPatrol EDR для обнаружения инцидентов и реагирования на сложные атаки

Модули MaxPatrol EPP

ДОСТУПЕН

Антивирусный движок

Молниеносное обнаружение и блокировка угроз на основе эмуляции поведения ВПО

В РАЗРАБОТКЕ

Защита от шифровальщиков

Проактивная защита от шифровальщиков — мгновенная блокировка ВПО и восстановление данных

В РАЗРАБОТКЕ

Контроль подключаемых устройств

Ограничение доступа и предотвращение несанкционированного использования подключаемых устройств

В РАЗРАБОТКЕ

Контроль приложений

Разрешение запуска только доверенных приложений

В РАЗРАБОТКЕ

Защита от веб-угроз

Автоматическая блокировка доступа к опасным сайтам и предотвращение попытки заражения через интернет

В РАЗРАБОТКЕ

Защита от сетевых угроз

Защита узла от сетевых атак — блокировка вредоносного трафика и подозрительной активности

Преимущества MaxPatrol EPP

Мощный антивирусный движок PT AV

Статический и динамический анализ позволяют эффективно выявлять и блокировать ВПО и замаскированные угрозы

Экспертиза для бизнеса

Многолетний опыт анализа угроз и разработки средств защиты с учетом специфики российских организаций, собственная антивирусная лаборатория в PT ESC

Своевременное обновление

Ежедневные автоматические обновления баз данных позволяют всегда быть защищенными от актуальных угроз

Надежная самозащита

Предотвращает несанкционированную остановку агента даже при наличии у злоумышленников привилегированных прав доступа

Поддержка популярных ОС

Решение полностью совместимо с ОС на базе Windows и отечественными версиями Linux: Astra Linux, «РЕД ОС» и другими

Соответствие требованиям регуляторов

Приказ ФСТЭК № 239 для 1-й категории (АВ3.5), приказ ФСТЭК № 117 для обеспечения защиты информации в ГИС, ГОСТ Р 57580 «Безопасность финансовых (банковских) операций»

PT Antivirus в составе MaxPatrol EPP

Антивирусный модуль основан на 30-летнем опыте разработки компании «ВИРУСБЛОКАДА» и экспертизе антивирусной лаборатории экспертного центра Positive Technologies (PT ESC).

1 **Статический анализ**	Поиск уникальных характеристик файлов по базе сигнатур для выявления известных угроз
2 **Карантин для расследования**	Помещает файлы в изолированное хранилище для последующего анализа
3 **Эмуляционный движок**	Обеспечивает безопасный динамический анализ продвинутого ВПО
4 **Списки исключений**	Исключает из проверки доверенные файлы и процессы для минимизации ложных срабатываний и снижения нагрузки на систему
5 **Гибкие сценарии реагирования**	Предоставляет настраиваемые цепочки автоматических действий: от помещения файла в карантин до частичной блокировки узла

Ключевые преимущества

- **Устойчивость к переупаковке, шифрованию и полиморфизму:** эмулятор с динамической трансляцией кода позволяет выявлять и блокировать даже замаскированные угрозы
- **Минимальный размер баз данных:** динамические сигнатуры позволяют выявлять целые семейства вирусов по их поведению и не хранить громоздкие статические сигнатуры
- **Сбалансированная нагрузка на агент:** кэширование безопасных вердиктов до следующего обновления позволяет минимизировать количество потребляемых на узле ресурсов

Как работает эмуляция в PT AV

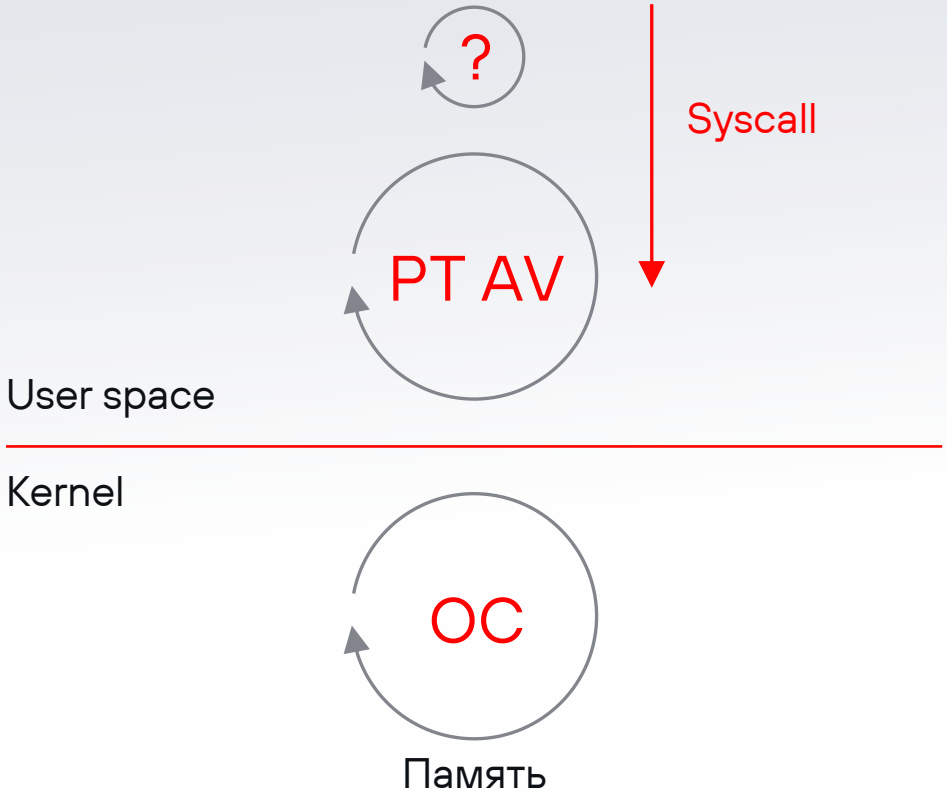
Создание контролируемого окружения

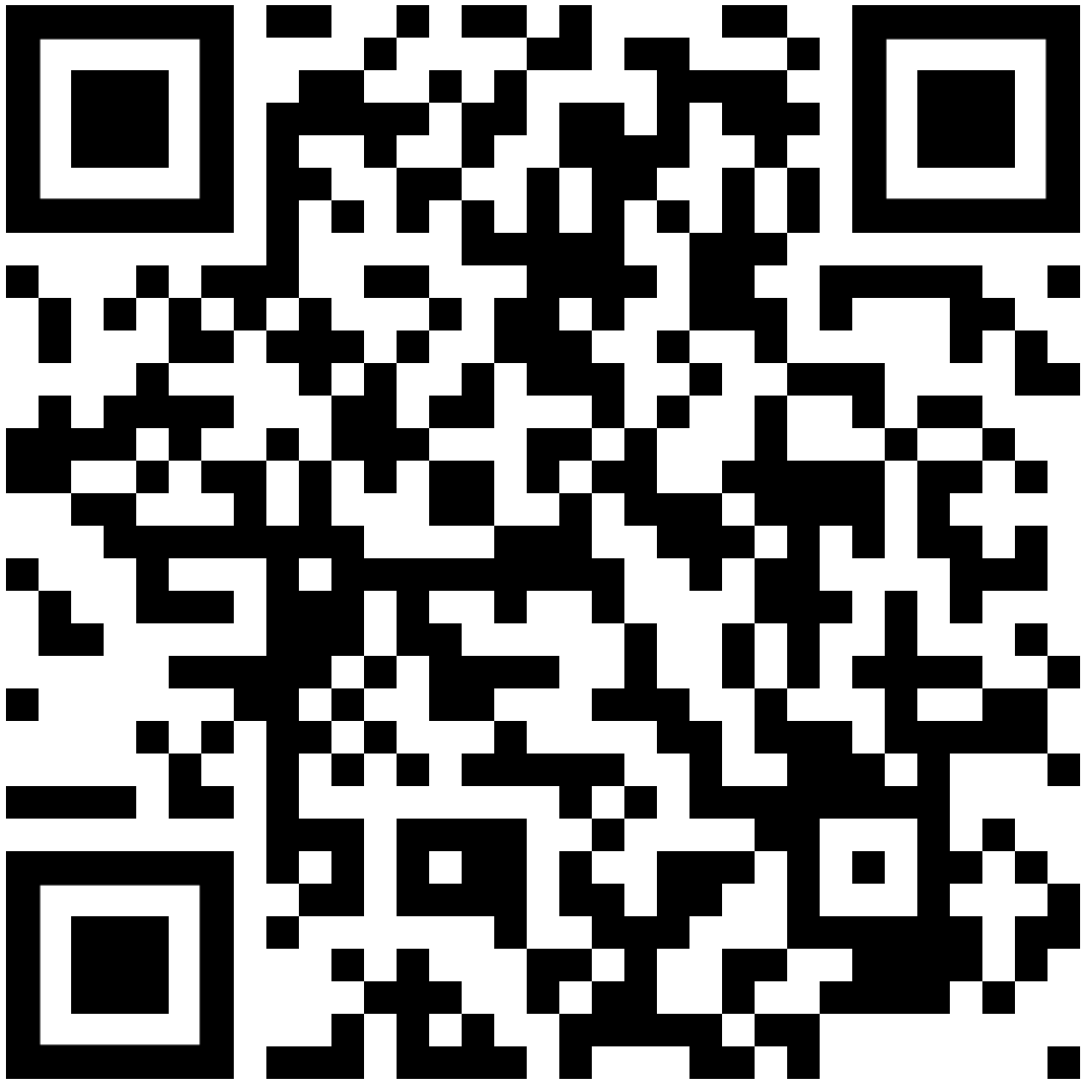
Запуск образца

Сбор трассы исполнения

Проверка наличия искомого события в трассе

Оценка состояния участков памяти





Испытайте возможности

MaxPatrol EPP — нового продукта для защиты конечных устройств

MaxPatrol EDR

Защита конечных устройств
от сложных и целевых атак

MaxPatrol EDR — безопасность конечных устройств под ключ

Эффективная защита конечных устройств от целевых атак и сложного ВПО

Глубокий мониторинг

Позволяет собрать необходимую для расследования и обнаружения информацию и управлять процессом сбора

Поведенческий анализ

Обнаруживает сложные угрозы на защищаемом устройстве благодаря корреляционному движку

Быстрое реагирование

Более 40 вариантов автоматического и ручного реагирования для оперативной защиты

Интеграция с другими решениями Positive Technologies

Отправка файлов в PT Sandbox, инвентаризация устройств для MaxPatrol VM, сбор событий для MaxPatrol SIEM

Экспертиза Positive Technologies уже на устройствах:

- Мощный корреляционный движок для поведенческого анализа угроз — более 1000 правил от PT ESC*
- Покрывает 60% техник атакующих из матрицы MITRE ATT&CK
- 6000 YARA-правил
- > 65 000 актуальных хеш-сумм в базе данных от PT ESC*

Ключевые возможности

Автономная работа

Агенты способны проводить анализ и выполнять реагирование без обращения к серверу управления или доступа в интернет

Поддержка отечественных ОС

Продукт совместим со всеми популярными ОС, включая отечественные (Astra Linux, «РЕД ОС», «Альт» и др.)

Ручное или автоматическое реагирование

Более 40 действий реагирования, которые можно полностью автоматизировать

Своевременное и непрерывное обнаружение

Поставляется с набором экспертных правил от PT ESC, обнаруживающих актуальные угрозы, включая тактики и техники атакующих из матрицы MITRE ATT&CK. Новые пакеты экспертизы поставляются непрерывно

Гибкая настройка

Позволяет гибко управлять функциональностью продукта, обеспечивая баланс между реальными задачами SOC и нагрузкой на устройство

Интеграционный потенциал

- Передает события в сторонние системы
- Сканирует узлы в режиме аудита
- Предоставляет API для реагирования на агентах
- Позволяет отправлять файлы на анализ в сторонние системы

Преимущества MaxPatrol EDR

Высокая адаптивность

Позволяет добиться баланса между уровнем защищенности и нагрузкой на узлы

Продукт можно настраивать под задачи бизнеса в зависимости от:

- размера и гетерогенности инфраструктуры
- типов устройств
- задач и угроз, с которыми предстоит бороться

Множество сценариев автоматизации

- Управление агентами
- Реагирование на инциденты и сбор контекста
- Многоэтапные проверки

Многоцелевое использование

Возможность интеграции с другими решениями Positive Technologies для расширения их возможностей:

- **PT Sandbox** (анализ файлов, передаваемых по шифрованным каналам)
- **MaxPatrol VM** (анализ уязвимостей)
- **MaxPatrol SIEM** (анализ событий и отчетность)

Синергия продуктов для полной защиты устройств

MaxPatrol EDR не заменяет решения классов AV, EPP и SIEM, а дополняет их:

- Обнаруживает сложные, таргетированные атаки, специализированные тактики, техники, процедуры (TTPs) и инструменты хакеров
- Дает большое количество инструментов для обнаружения, расследования и реагирования, в том числе автоматического
- Собирает полную телеметрию с устройств для передачи и расследования в SIEM-системах

SIEM — Расследование и визуализация

EDR — Обнаружение и реагирование

AV — Превентивная защита

Синергия продуктов для полной защиты устройств

EPP

- Контроль устройств и приложений, HIPS и др.
- Превентивная защита

AV

- Защита от массовых угроз
- Превентивная защита

РЕАГИРОВАНИЕ

EDR

- Продвинутое обнаружение и защита от целевых угроз
- Мониторинг конечных устройств
- Интеграция с решениями классов SIEM, VM, Sandbox

СБОР СОБЫТИЙ

SIEM

- Мониторинг и обнаружение
- Расследование
- Отчетность

ИНВЕНТАРИЗАЦИЯ

ИНВЕНТАРИЗАЦИЯ

VM **HCC**

- Выявление и приоритизация уязвимостей
- Контроль соответствия стандартам

Защита конечных устройств: чек-лист

Сбор данных

- События собираются со всех устройств?
- Достаточно ли этих событий для выявления атак?
- Вы можете оперативно корректировать профиль мониторинга?
- У вас есть информация о самих узлах?
- Вы контролируете устройства удаленных сотрудников?

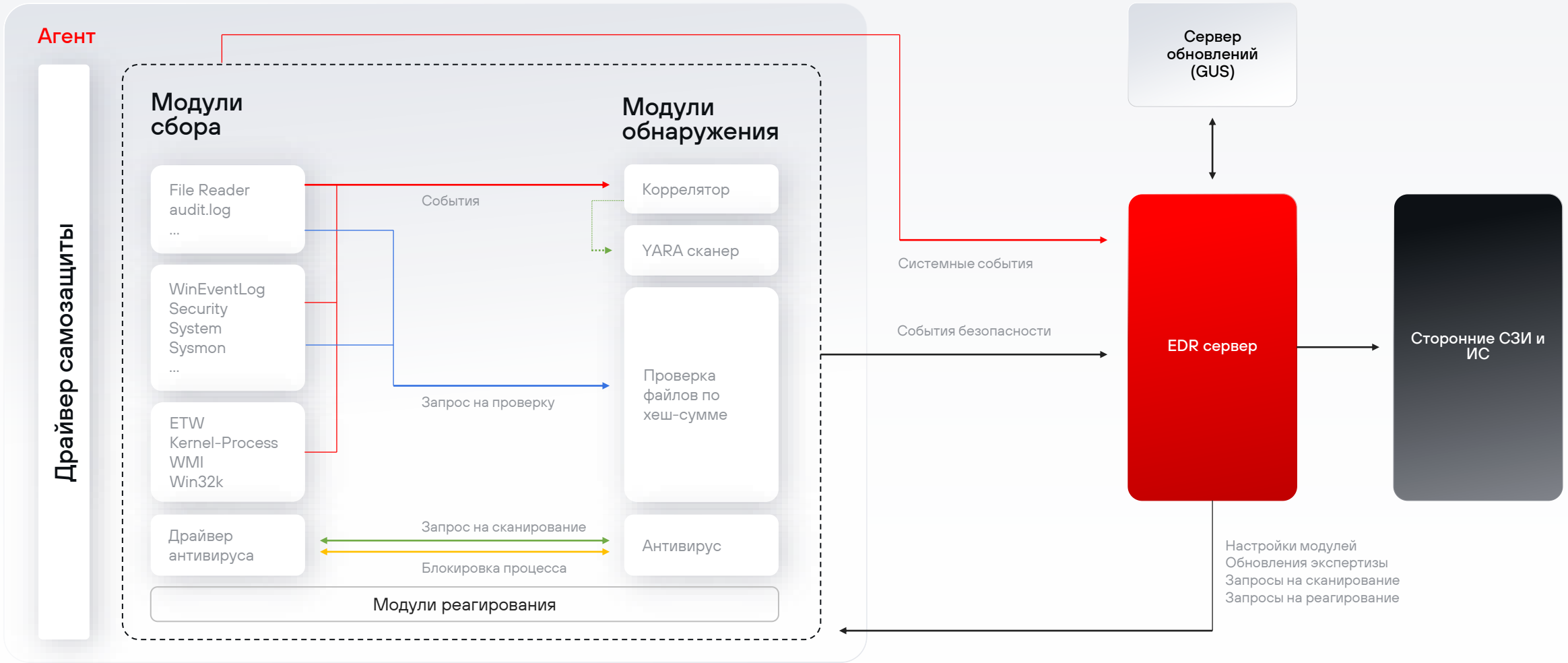
Выявление

- Есть ли у вас инструменты для оперативного выявления угроз?
- Вы уверены в качестве обнаружения?
- Можете обработать весь поток инцидентов и уведомлений?
- Достаточно ли быстро можете проанализировать ситуацию и подтвердить инцидент?

Реагирование

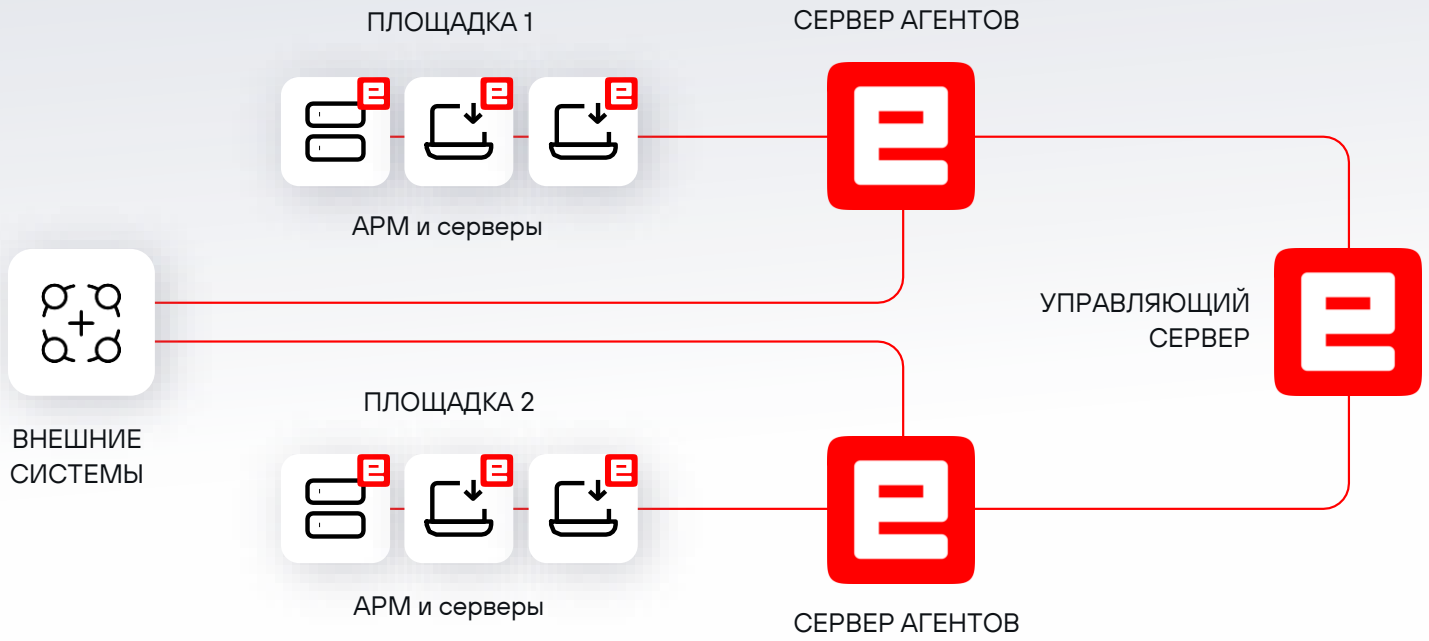
- Есть ли инструменты для реагирования? Достаточно ли вариантов действий?
- Можете ли локализовать инцидент быстро?
- Нужно ли привлекать ИТ или внешнего подрядчика?
- Можете ли автоматизировать реагирование?
- Сможете ли вы защититься, когда у агента нет связи с сервером?

Как работает MaxPatrol EDR



системные события — запрос на сканирование — запрос на проверку — блокировка процесса

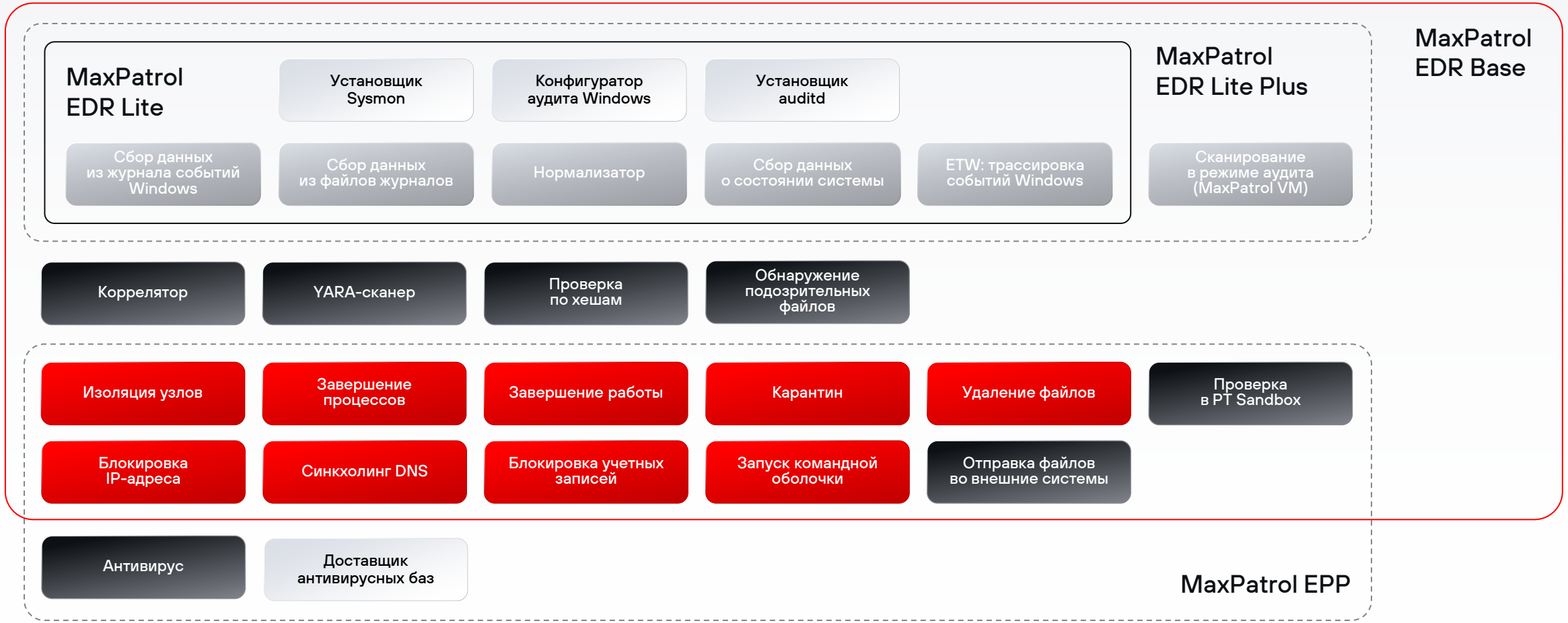
Архитектура MaxPatrol EDR



- **MaxPatrol EDR** состоит из серверной части и агентов, устанавливаемых на конечные устройства.
- **Серверная часть** состоит из управляющего сервера и сервера агентов.
- **Управляющий сервер —** основной компонент системы, который позволяет конфигурировать ее через веб-интерфейс. Поддерживается кластерная установка и резервирование.
- **Сервер агентов —** приложение для управления агентами и модулями, а также взаимодействия с внешними системами (MaxPatrol SIEM, MaxPatrol VM, PT Sandbox, сторонним syslog).
- **Агент —** приложение, которое устанавливается на конечное устройство для обеспечения работы модулей и связи с сервером агентов.

Конструктор MaxPatrol EDR

Конструктор MaxPatrol Endpoint Security



Охват инфраструктуры

Можно установить на большинство операционных систем

Windows 7	Windows 8	Windows 8.1	Windows 10	Windows Server 2016
Windows Server 2019	Windows Server 2022	Debian 10	Debian 11	Debian 12
Ubuntu 20.04	Ubuntu 22.04	Ubuntu 24.04	CentOS 9	CentOS 10
«Альт Рабочая станция» 10.4	«Альт Рабочая станция» 10.2	«Альт Сервер» 10.1	«Альт Сервер» 10.2	RHEL 8
RHEL 9	«Основа» 2.0	«РЕД ОС» 7.3	«РЕД ОС» 8.0	«МОС» 12
Oracle Linux 9	Astra Linux 2.12	Astra Linux 1.3	Astra Linux 1.7	Astra Linux 1.8

...и этот список растет с каждым релизом

Результаты MaxPatrol EDR

1

Мониторинг безопасности конечных устройств для «Газпромбанк Мобайл»

2

Построение результативной кибербезопасности для Rambler&Co

3

Сертификация ФСТЭК России

- Сертификат соответствия № 4980 от 22 сентября 2025 года
- В составе системы MaxPatrol (исполнение Endpoint Detection and Response)

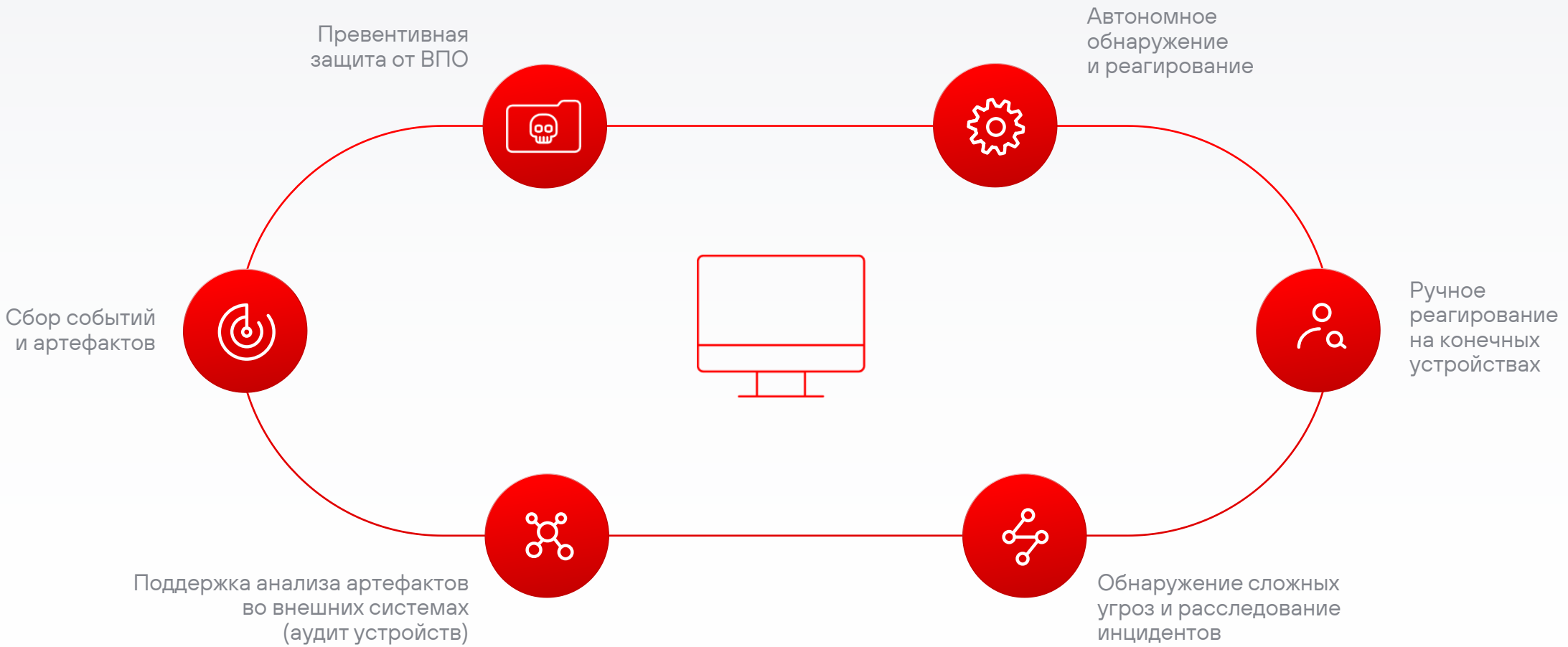
4

Защита инфраструктуры на «Играх Будущего»

5

Инструмент команды защитников в рамках кибербитв Standoff

Полная защита устройств на одном агенте



Гибкие сценарии использования

Выбирайте сценарий в зависимости
от целей и готовности инфраструктуры

Инвентаризация и сбор событий

- Простое и быстрое внедрение
- Легкая настройка
- Минимальное влияние на производительность

Сбор событий и ручное реагирование

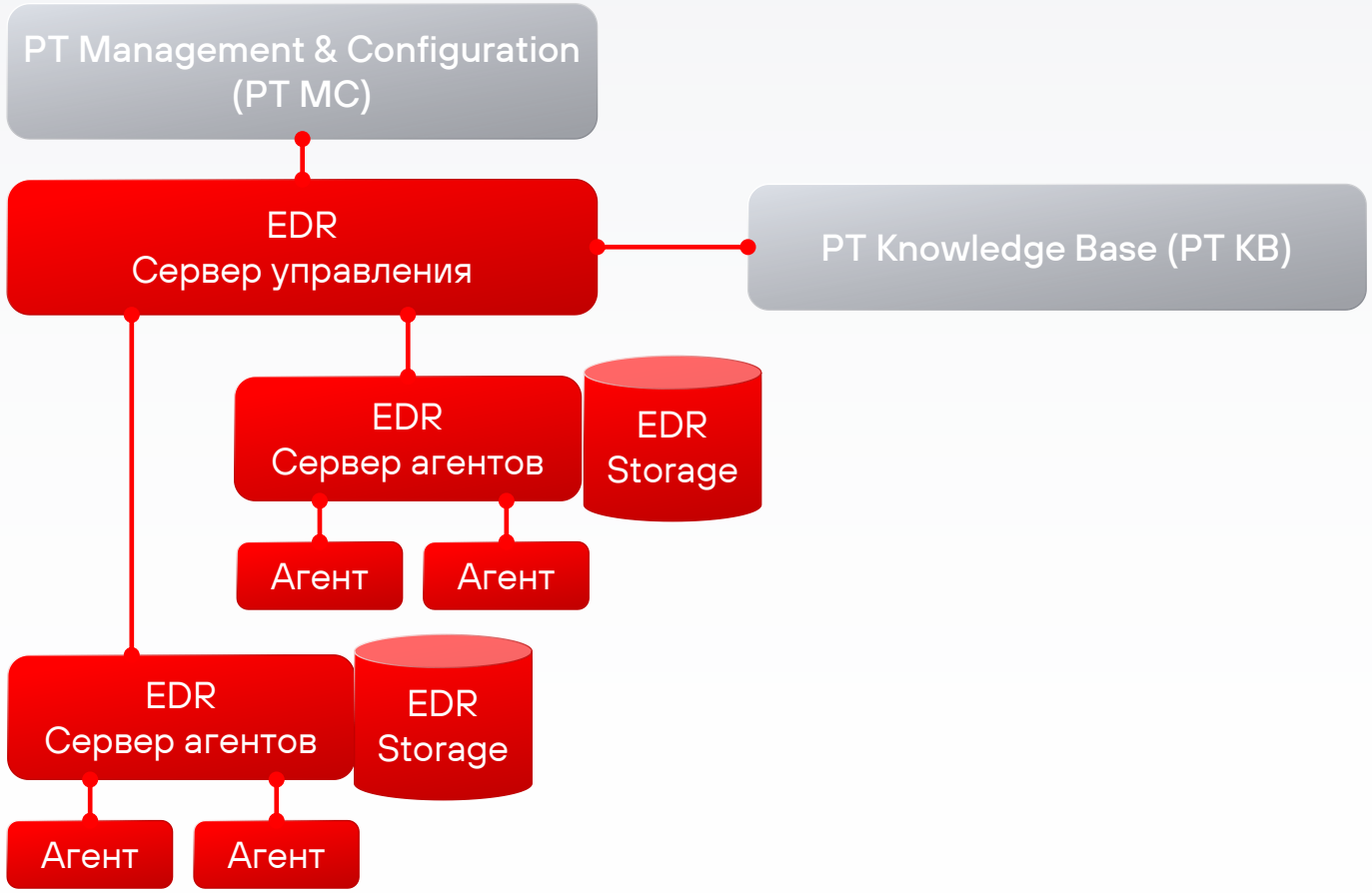
- Возможность локализации и устранения инцидентов
- Баланс между затратами на внедрение, функциональностью и нагрузкой на устройства

Сбор событий, обнаружение и автоматическое реагирование

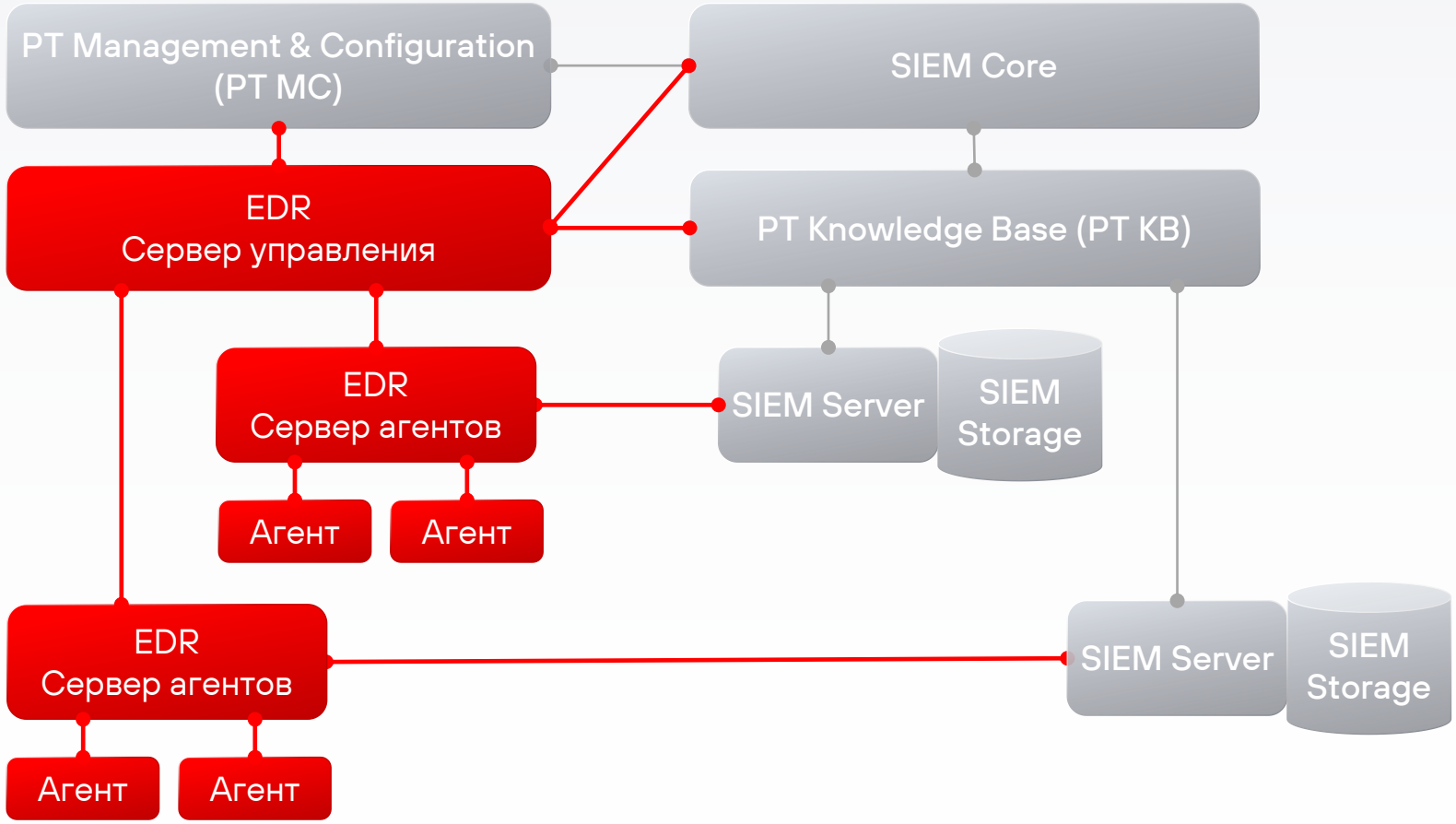
- Автономное обнаружение на агенте
- Многоэтапные проверки
- Автоматизация реагирования

Администрирование MaxPatrol EDR

Варианты развертывания: собственное хранилище



Варианты развертывания: совместно с MaxPatrol SIEM



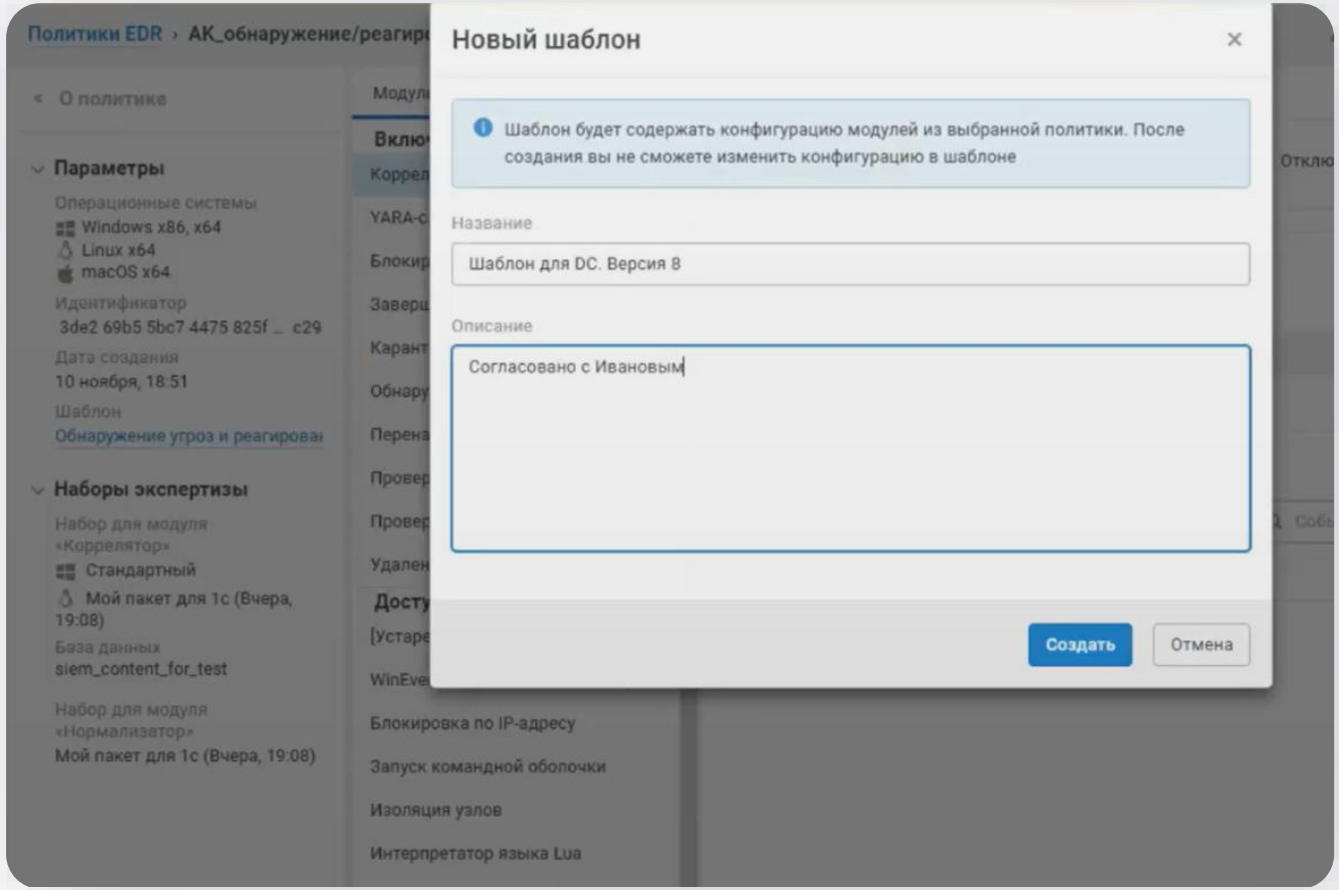
Развертывание за минуты

Конфигурировать
политики и исключения
на 30–60 серверов
долго и сложно

На это уходит время администраторов
и инженеров внедрения, усложняется
программа и методика испытаний

РЕШЕНИЕ

- Превращаем любую политику в шаблон
- Применяем шаблон на любом сервере
- Реализуем импорт и экспорт шаблонов



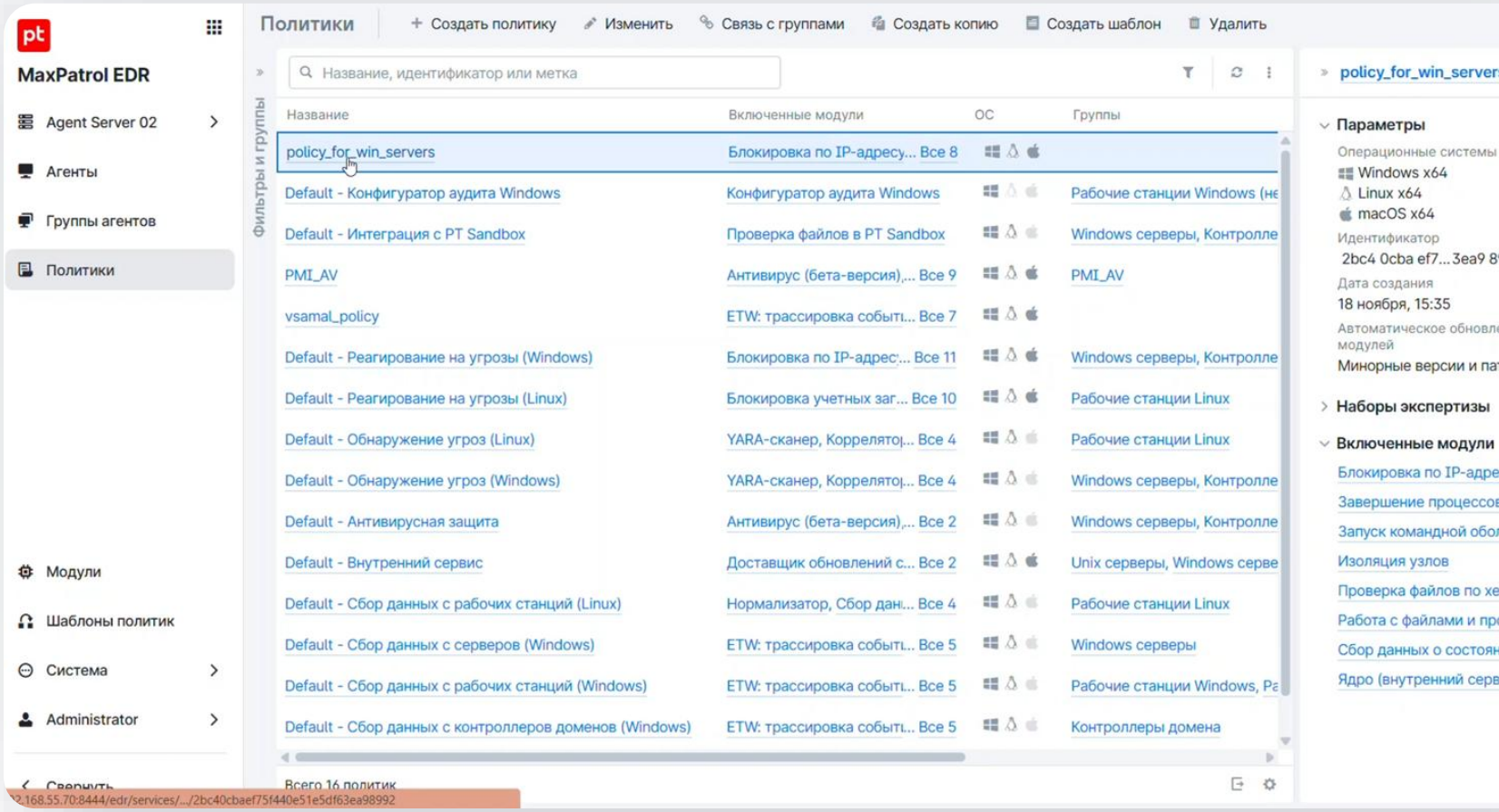
Развертывание не за часы, а за минуты

Конфигурировать политики и исключения на 30–60 серверов долго и сложно

На это уходит время администраторов и инженеров внедрения, усложняется программа и методика испытаний

РЕШЕНИЕ

- Превращаем любую политику в шаблон
- Применяем шаблон на любом сервере
- Реализуем импорт и экспорт шаблонов



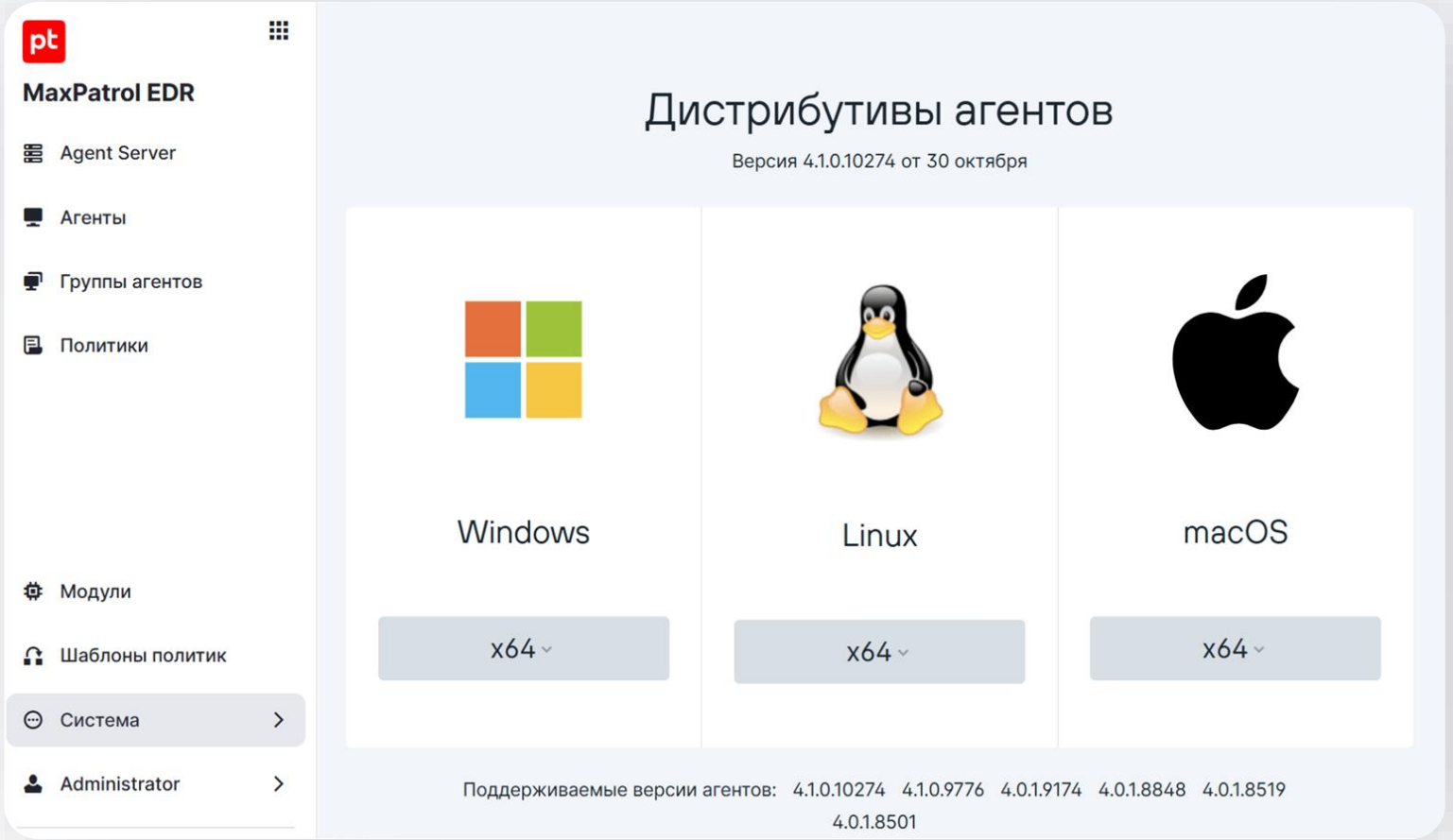
Агенты

Все необходимые дистрибутивы под рукой

- Доступны в веб-консоли, можно развернуть с помощью инструментов для группового администрирования

Быстрая масштабируемость

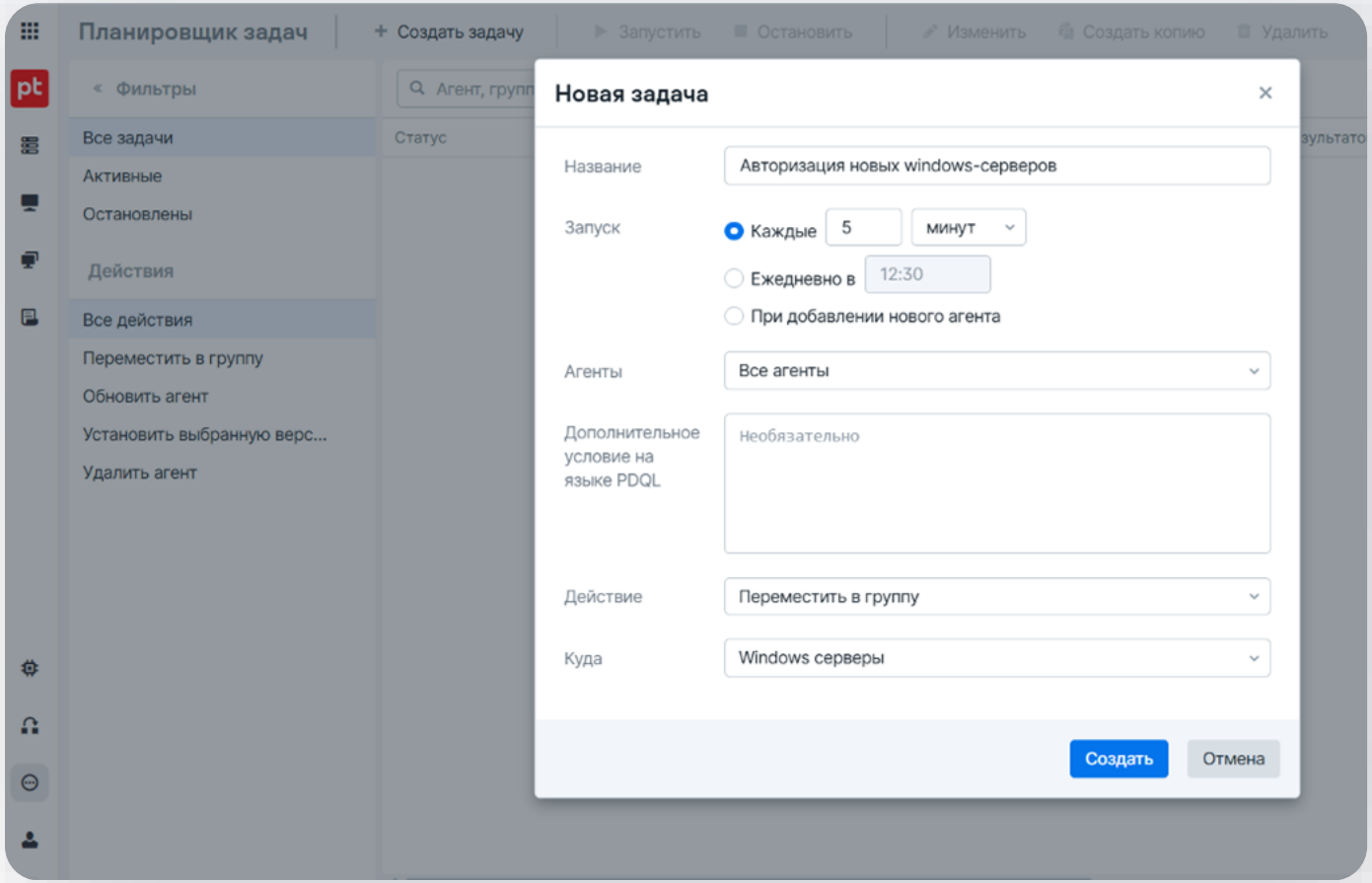
- Готовые Ansible-плейбуки для установки, обновления, удаления и переподключения к другому серверу агентов



Автоматизация работы с агентами

Планировщик
задач для быстрой
и удобной работы

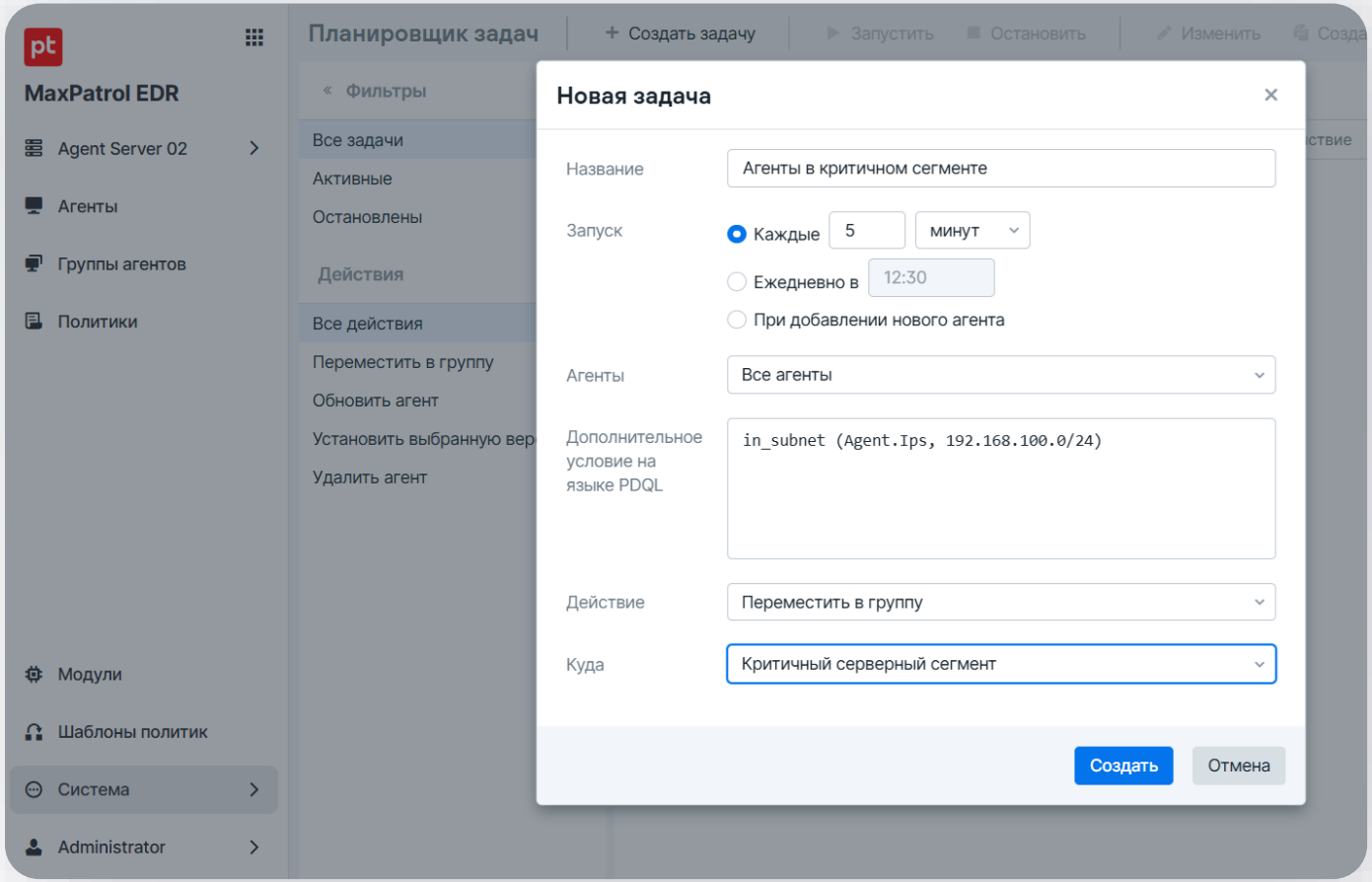
- Авторизация агентов
- Удаление агентов
- Обновление агентов
- Установка выбранной версии агента



Автоматизация работы с агентами

Защита, которая думает за вас и усиливается там, где это важно

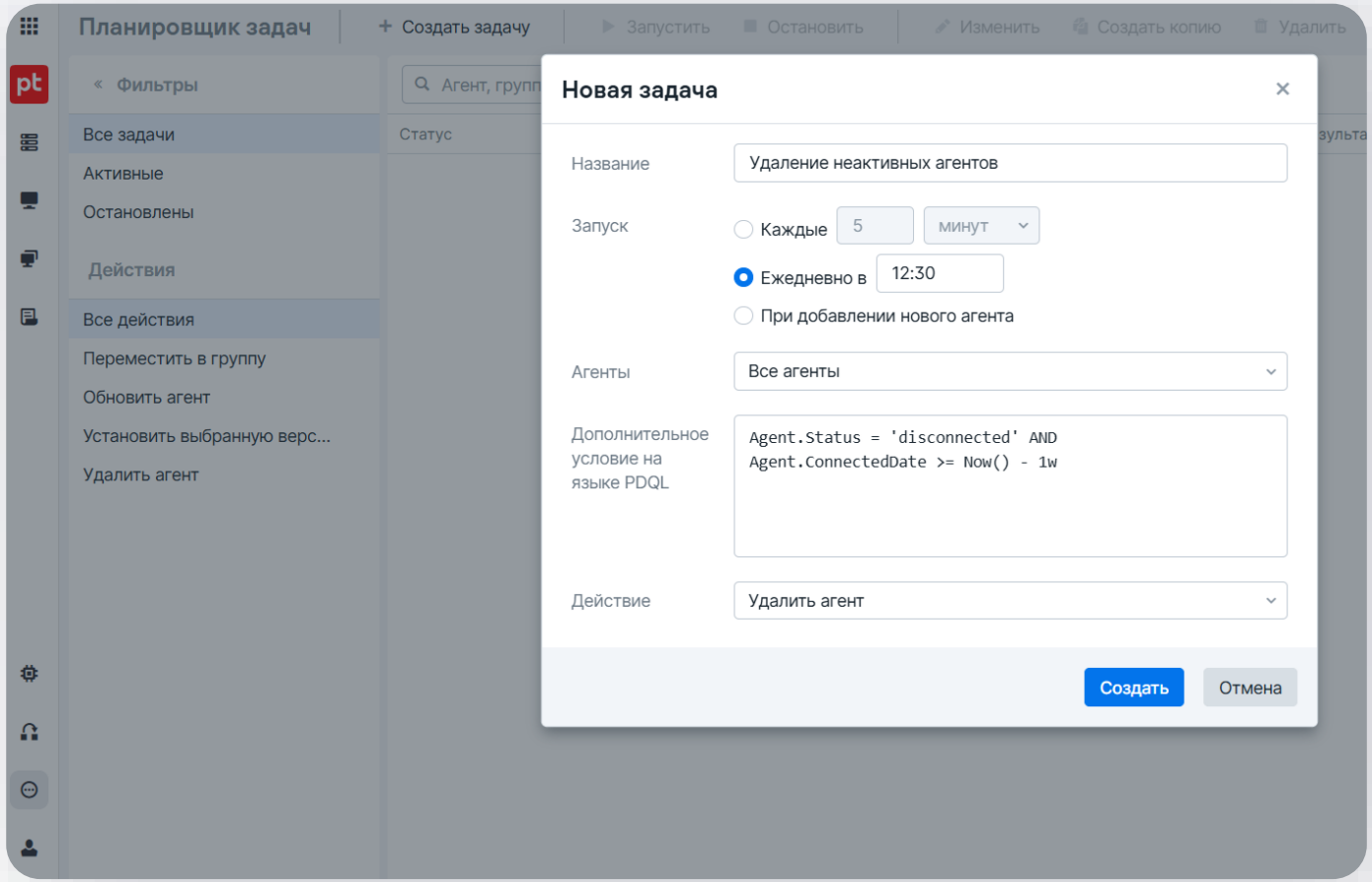
- Отслеживание перемещения агентов по подсетям
- Настройка нужного уровня защиты в зависимости от сетевого сегмента агента



Автоматизация работы с агентами

Удаление агентов

- Оптимизация использования лицензии за счет удаления неактивных агентов
- Особенно актуально для крупных компаний и тех, кто использует VDI



Сбор данных

Для обнаружения угроз
и передачи во внешние системы

ИСТОЧНИКИ

- Windows-журналы конечного устройства
- ETW-провайдеры
- Любые файлы с журналами
- Данные о состоянии системы в момент инцидента
- Дампы памяти процессов
- Инвентаризационные данные об активах

ИНСТРУМЕНТЫ

- Sysmon
- Advanced Audit Policy
- Auditd
- ETW

Управляйте сбором событий из одного окна

Обеспечиваем достаточность данных для анализа

В больших проектах затраты на настройку мониторинга составляют человеко-месяцы

- Некоторые устройства не в домене
- Есть старые Windows-серверы
- Нужно привлекать ИТ для настройки одинаковых параметров по всей инфраструктуре
- Сложно контролировать установку параметров в дочерних организациях и на удаленных площадках

Решение — централизованное управление и настройка

- Централизованное управление: Sysmon, auditd, AAP, ETW
- Гибкая настройка фильтрации собираемых событий
- Кэширование событий на агентах при отсутствии связи с сервером для минимизации потерь

Максимально точное обнаружение

Благодаря синергии механизмов обнаружения

Статический анализ

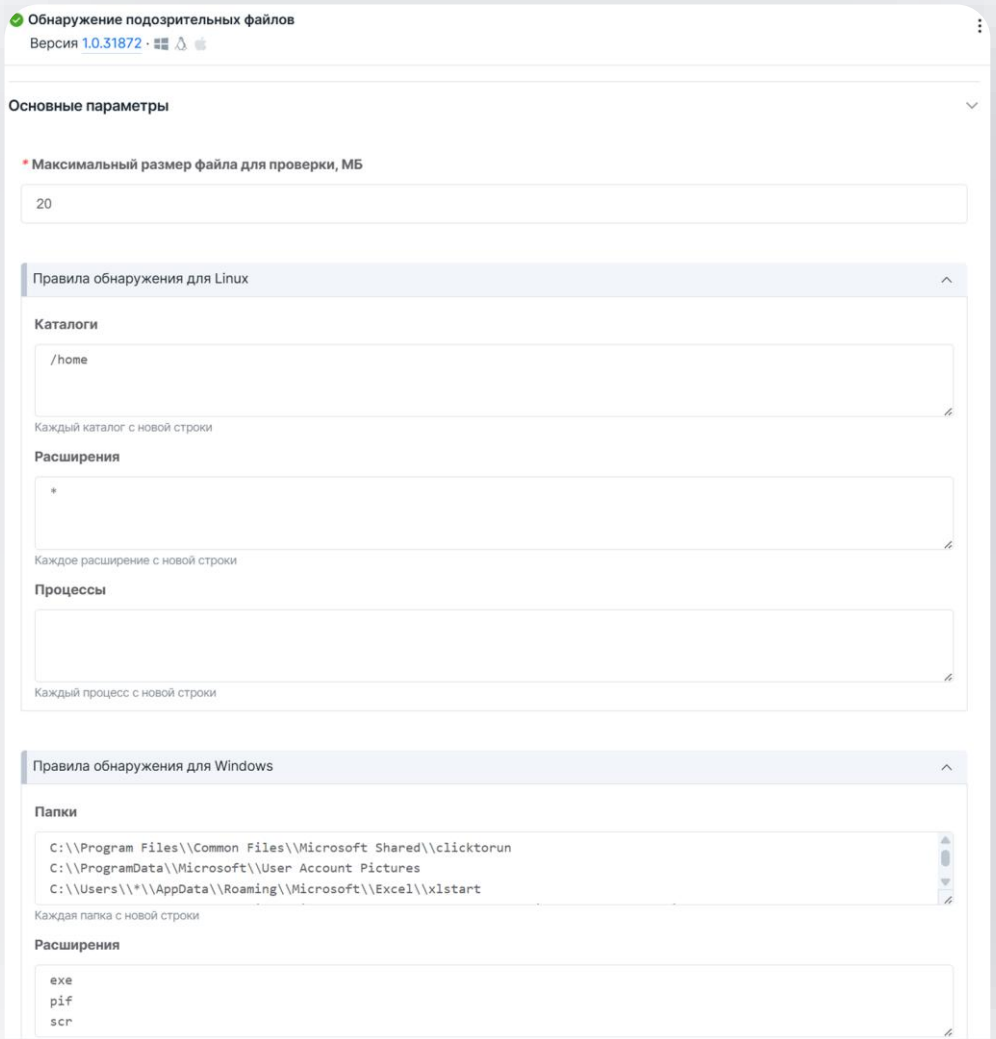
- Выявляет опасные файлы и процессы
- Проверка файлов и процессов YARA-правилами — 6000 «из коробки»
- Проверка по хешам файлов — более 65 000 (на основе перечня самых актуальных угроз от PT ESC)

Динамический анализ

- Использует богатый набор корреляционных правил — более 1000 «из коробки»
- Обнаруживает техники атакующих из матрицы MITRE ATT&CK
- Возможность кастомизации и добавления собственных правил
- Триггеры обнаружения удобно использовать для реагирования на атаки

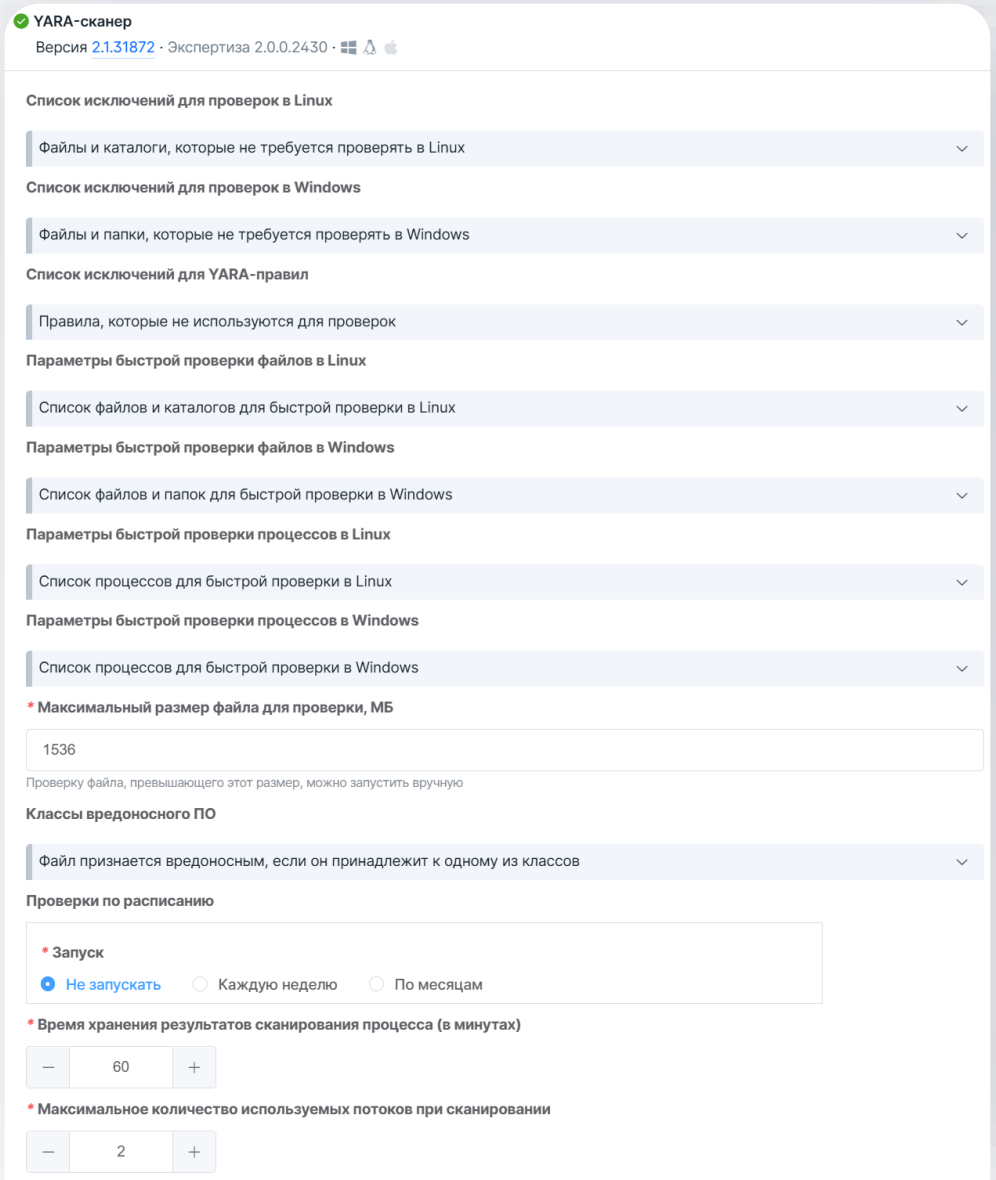
Обнаружение подозрительных файлов

- Работает автоматически на основе потока нормализованных системных событий
- Какие именно файлы считать подозрительными, определяете вы сами



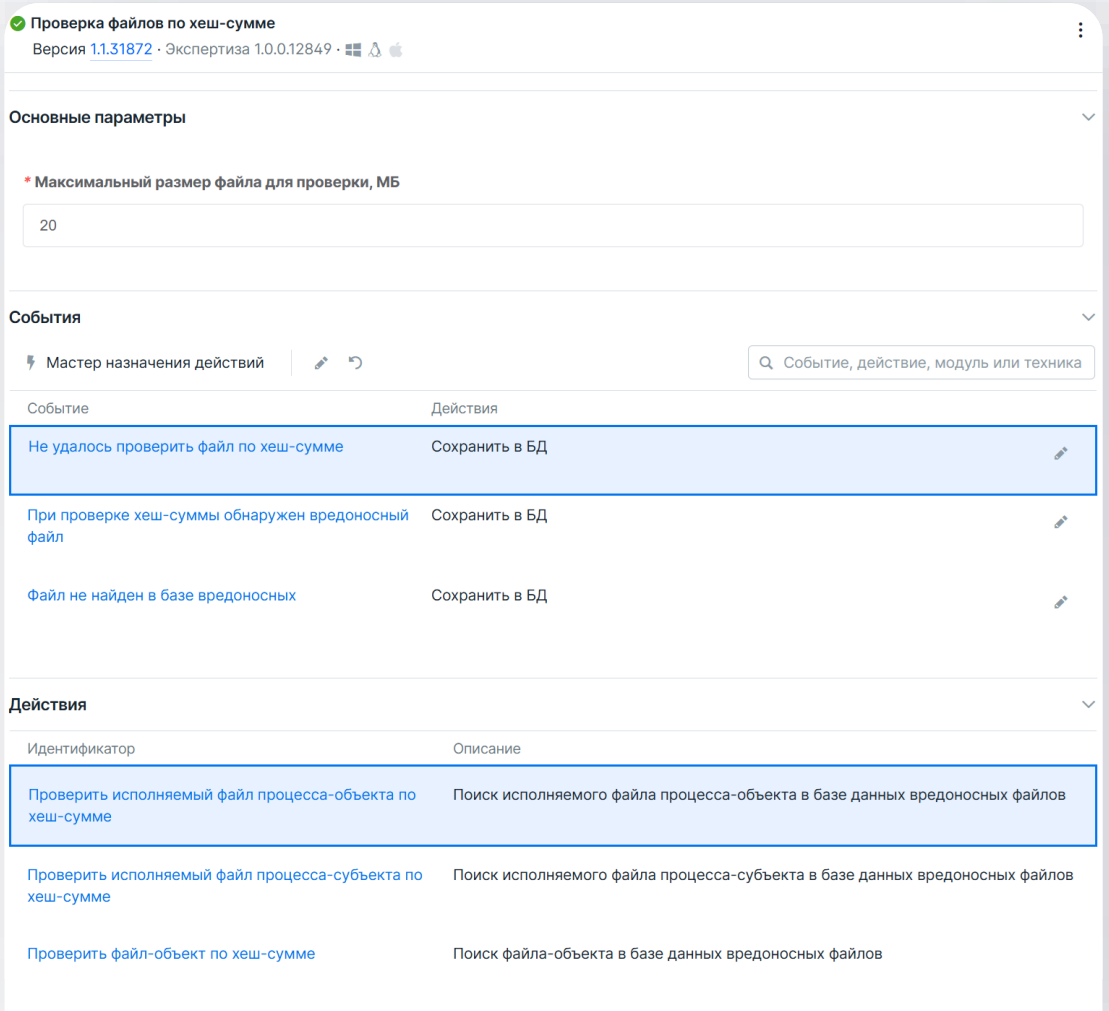
YARA-сканер

- Сигнатурный анализ файлов и процессов на основе YARA-правил
- > 6000 правил «под капотом»
- Сканирование можно запустить вручную, по расписанию и при регистрации события ИБ от другого модуля
- Можно использовать собственные YARA-правила



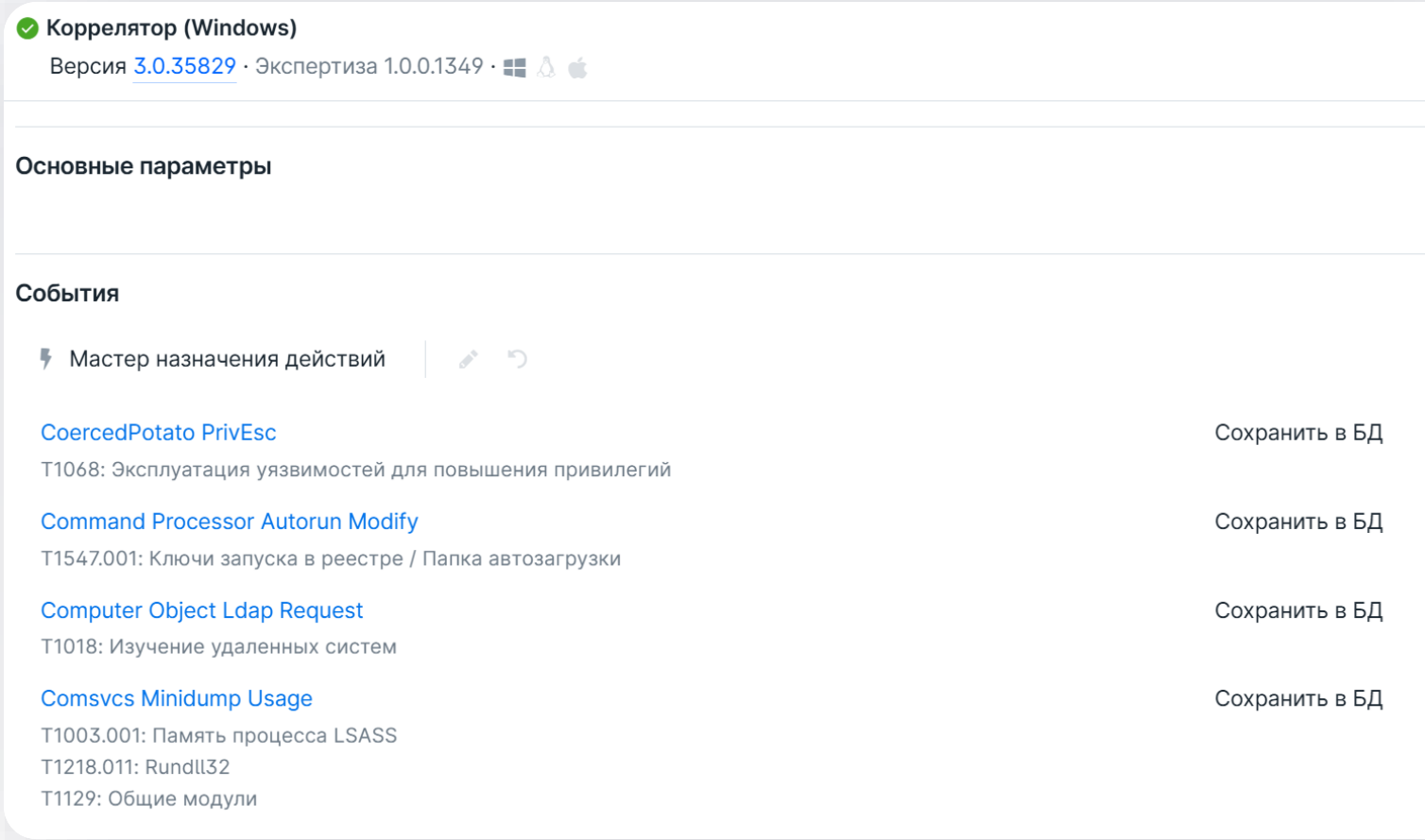
Проверка файлов по хеш-сумме

- Работает автоматически на основе потока нормализованных системных событий
- > 65 000 хешей от PT ESC
- Начиная с релиза 8.3 можно добавлять пользовательские хеши
- На большом потоке уникальных файлов модуль следует использовать осторожно



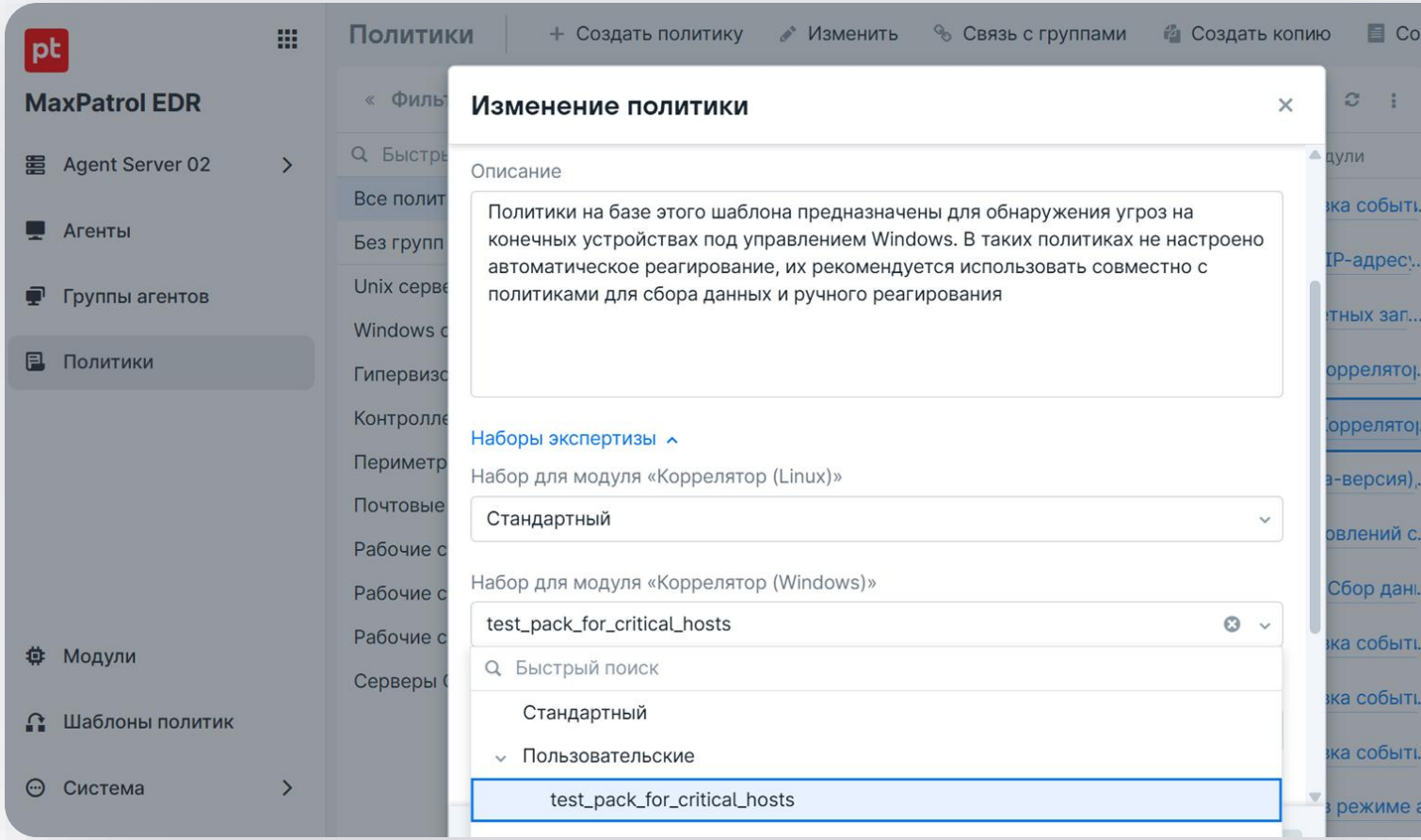
Поведенческий анализ

- Правила не перестанут работать при смене инструментария атакующих
- Работает в режиме реального времени, а значит, дает возможность автоматизировать реагирование
- Работает в автономном режиме и на устройствах вне периметра
- Создание пользовательской экспертизы — гибкая кастомизация контента «из коробки» под свои задачи и инфраструктуру



Пользовательская экспертиза

- Возможность гибкой кастомизации контента «из коробки» под свои задачи и инфраструктуру
- Возможность использовать поведенческий анализ даже на самых слабых узлах
- Возможность использовать собственные правила



Реагирование

Более 40 действий, среди которых:

- Сетевая изоляция узлов
- Завершение процессов
- Удаление и карантин файлов
- Блокировка опасных сетевых подключений
- Блокировка учетных записей
- Удаленное выполнение команд
- Сбор артефактов и дополнительный анализ

Гибкость настройки и управление нагрузкой

Настраиваемые политики реагирования

Модули реагирования в режиме ожидания потребляют минимум ресурсов

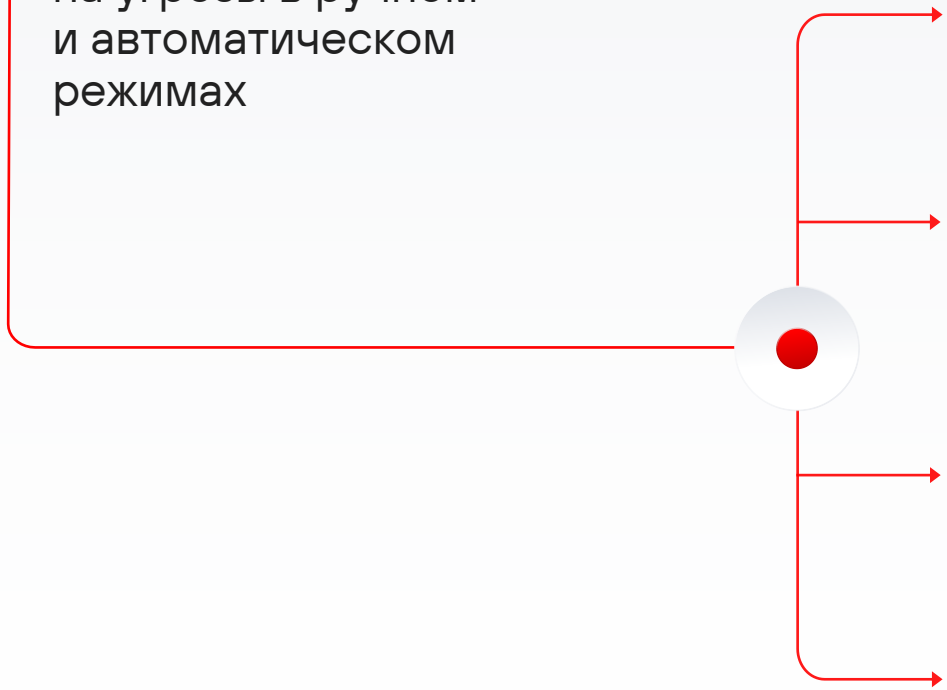
Контроль устройств, находящихся вне корпоративной сети

Реагирование на устройствах вне корпоративного периметра

Полный перечень доступных модулей на операционных системах

Реагирование

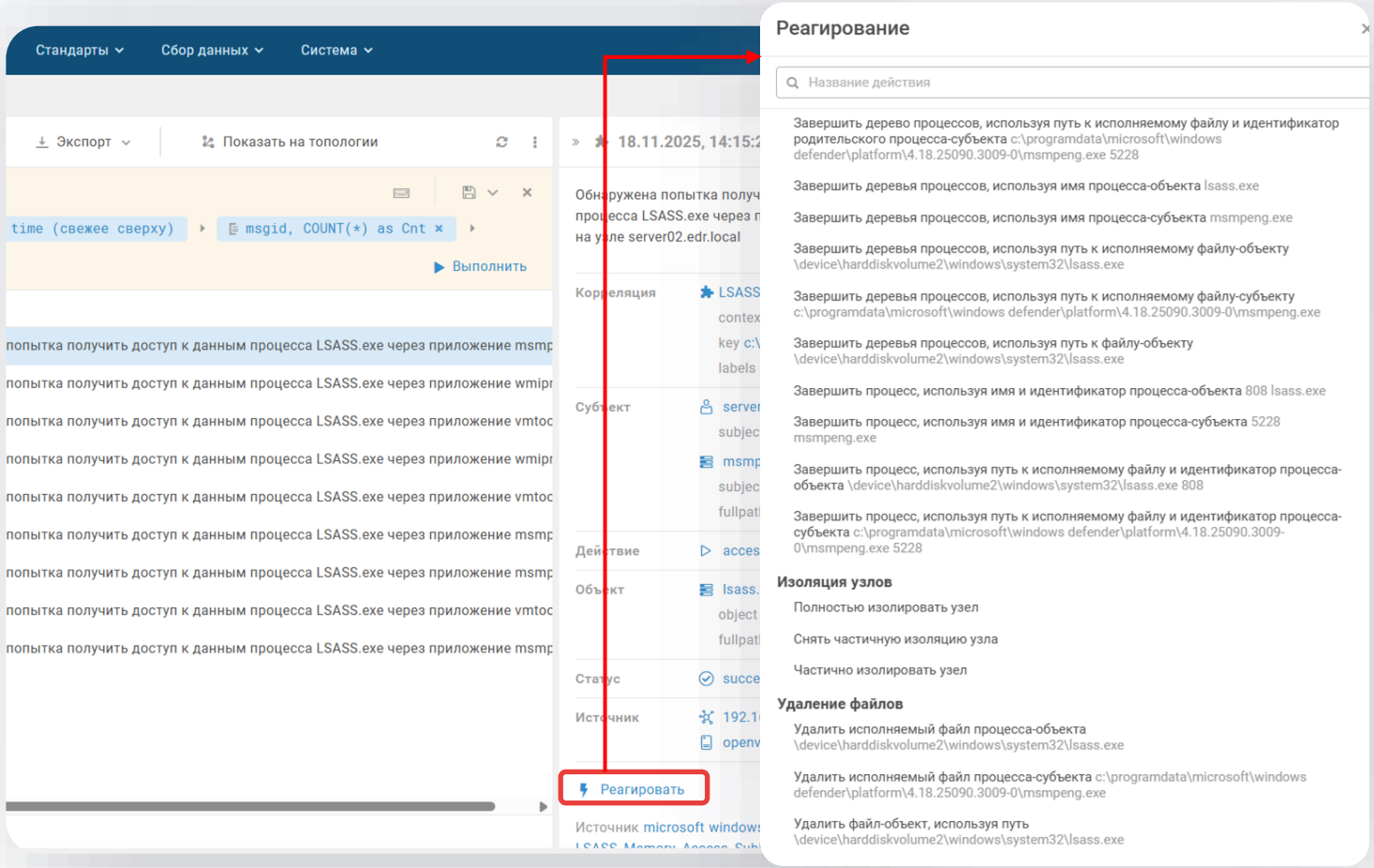
Реагирование
на угрозы в ручном
и автоматическом
режимах



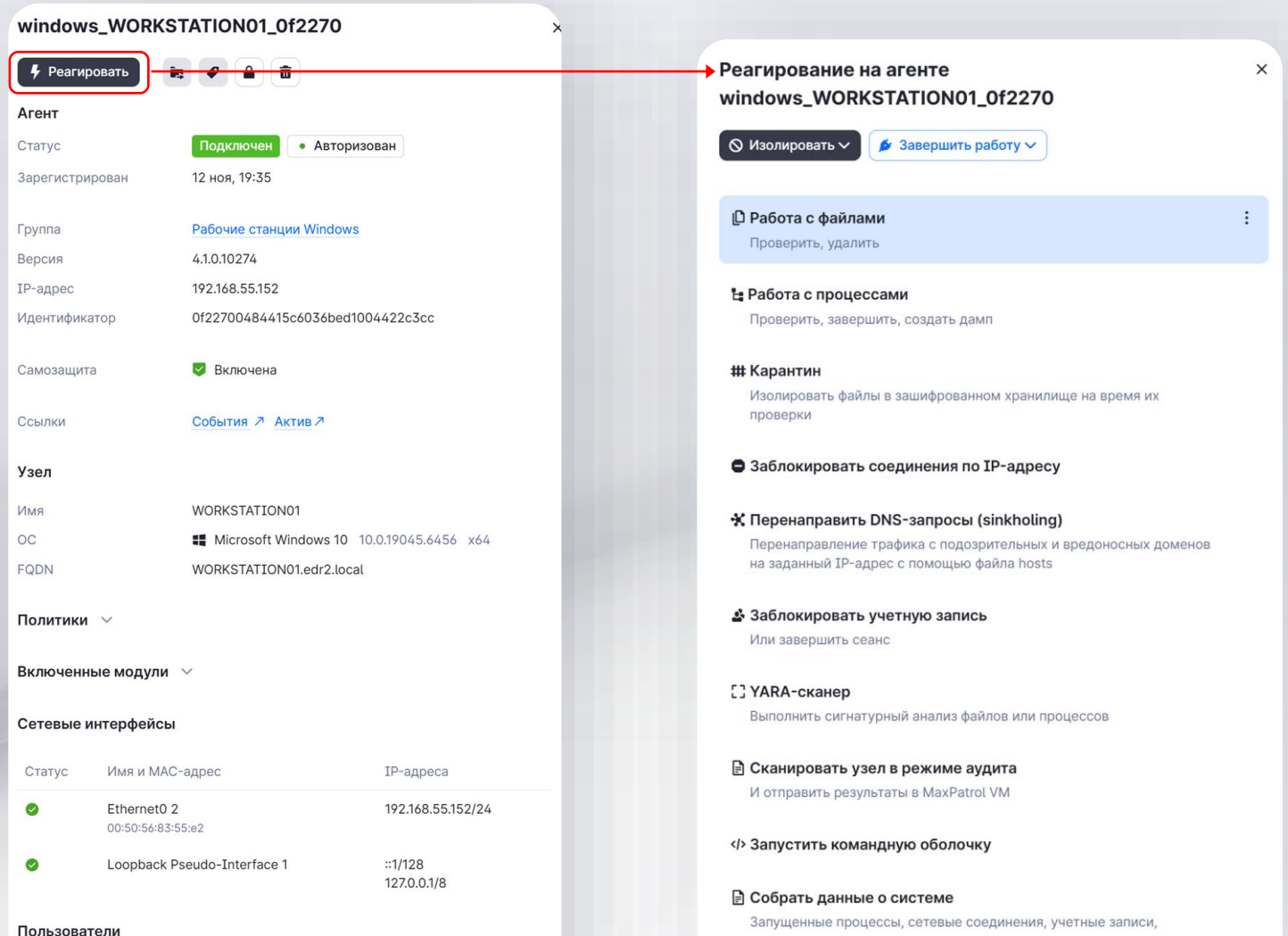
> В карточке события	При работе с событиями и инцидентами в SIEM-системе
> В отдельном модуле агента	Для точечных действий в интерактивном режиме
> В списке агентов	Для выполнения сразу на нескольких устройствах
> Через API	Для интеграции с SOAR, IRP и другими системами

Реагирование из карточки события в два клика

- Принятие защитных мер в едином интерфейсе
- Логирование выполняемых действий
- Сокращение затрат на работу с инцидентами



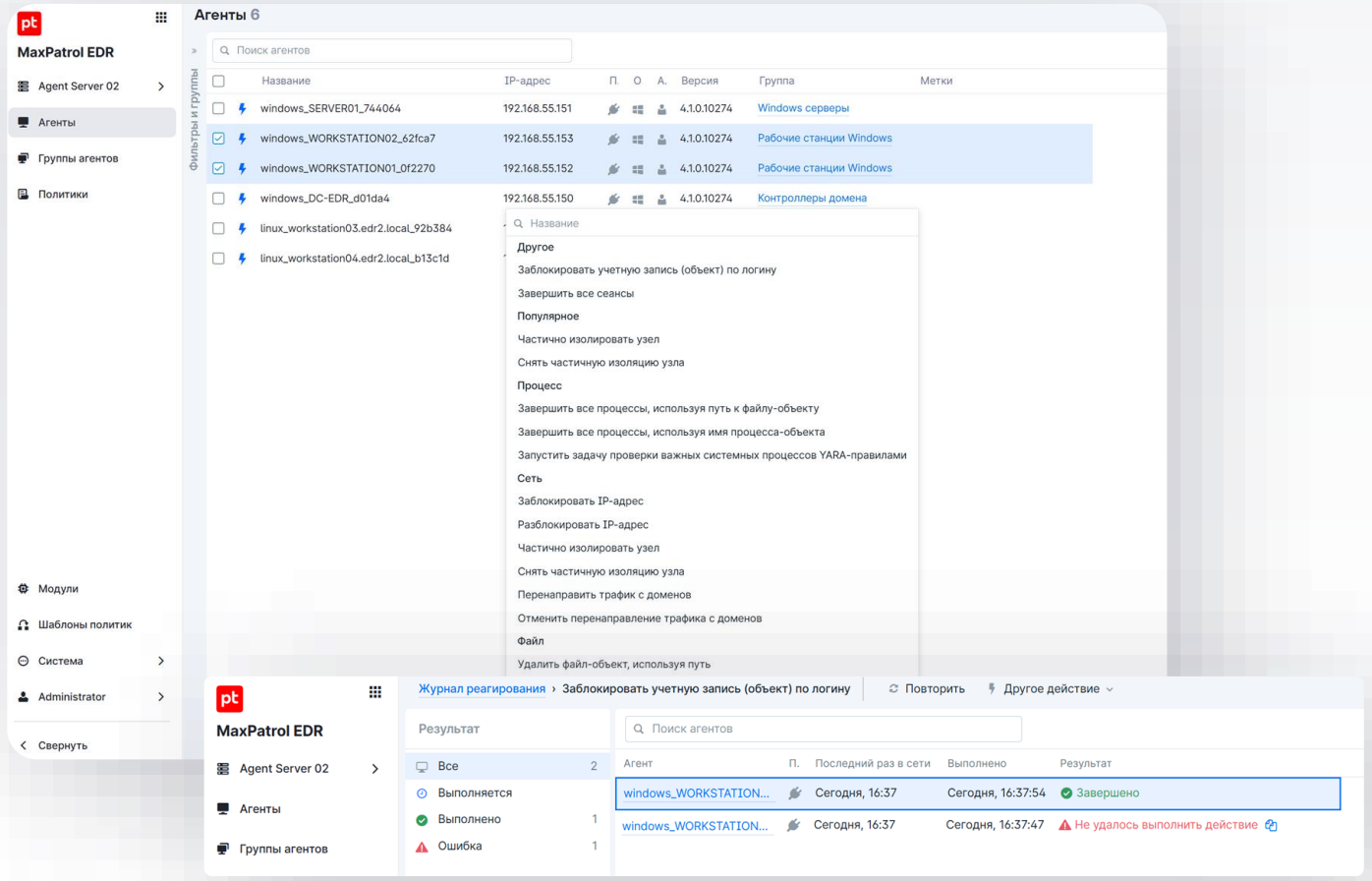
Реагирование из карточки агента в три клика



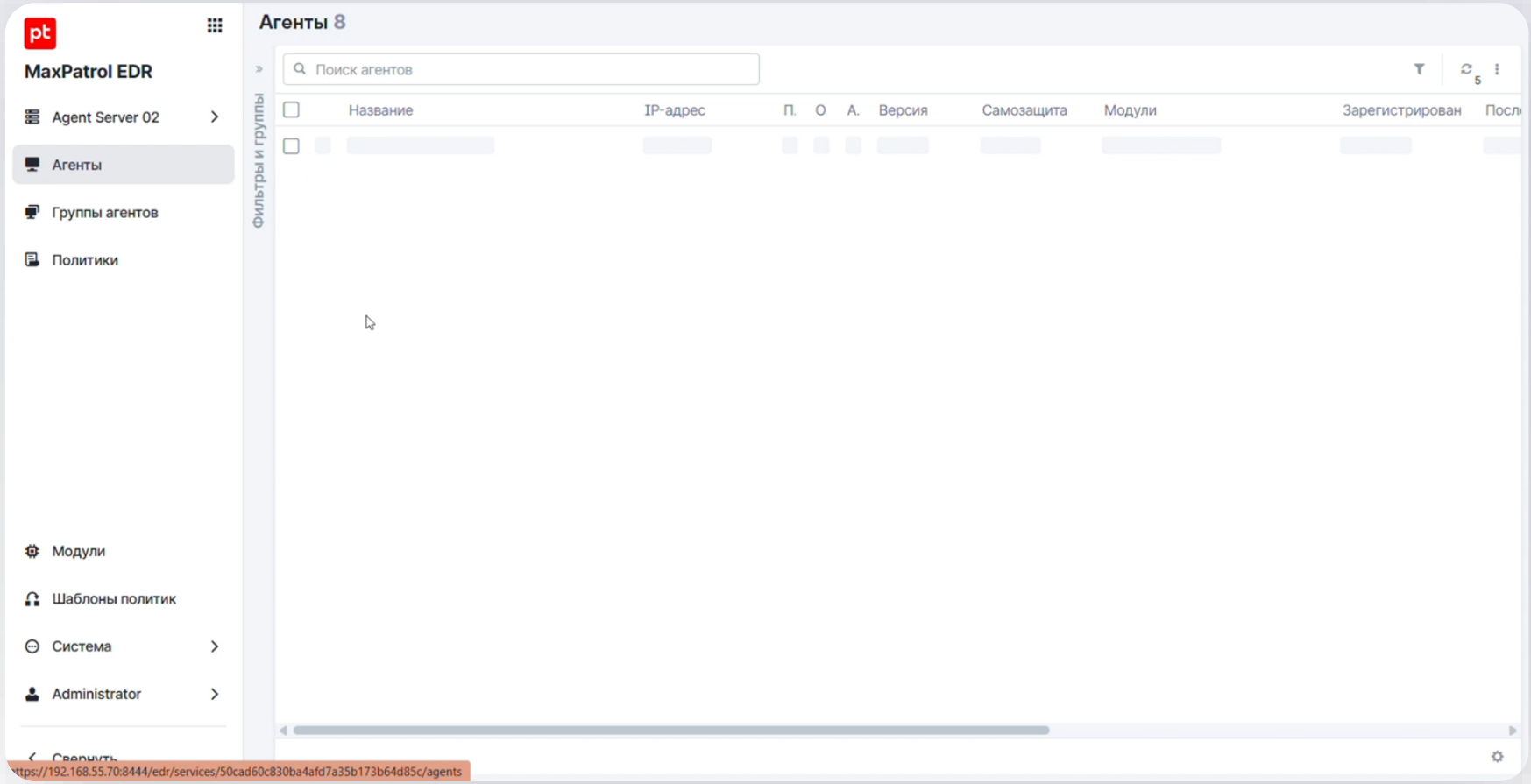
Реагирование на множестве агентов

Просто начать и удобно продолжить

- Меньше затрат на ручные операции
- Запуск любых действий реагирования на любой выборке агентов
- Отслеживание статусов задач — понятная обратная связь от всех устройств
- Возможность повтора действий
- Возможность быстро применить другое действие для выбранной группы или некоторых агентов

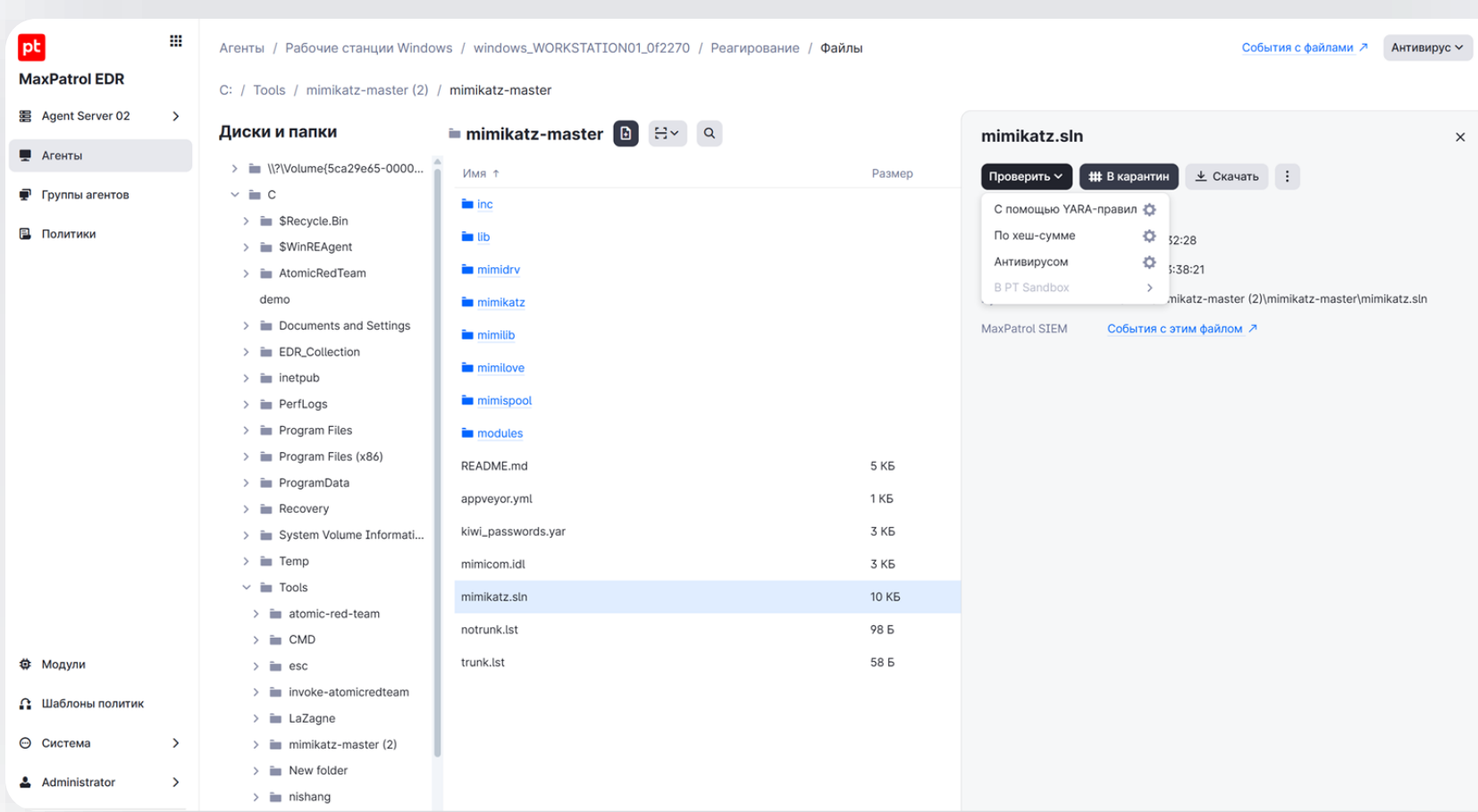


Пример реагирования на множестве агентов



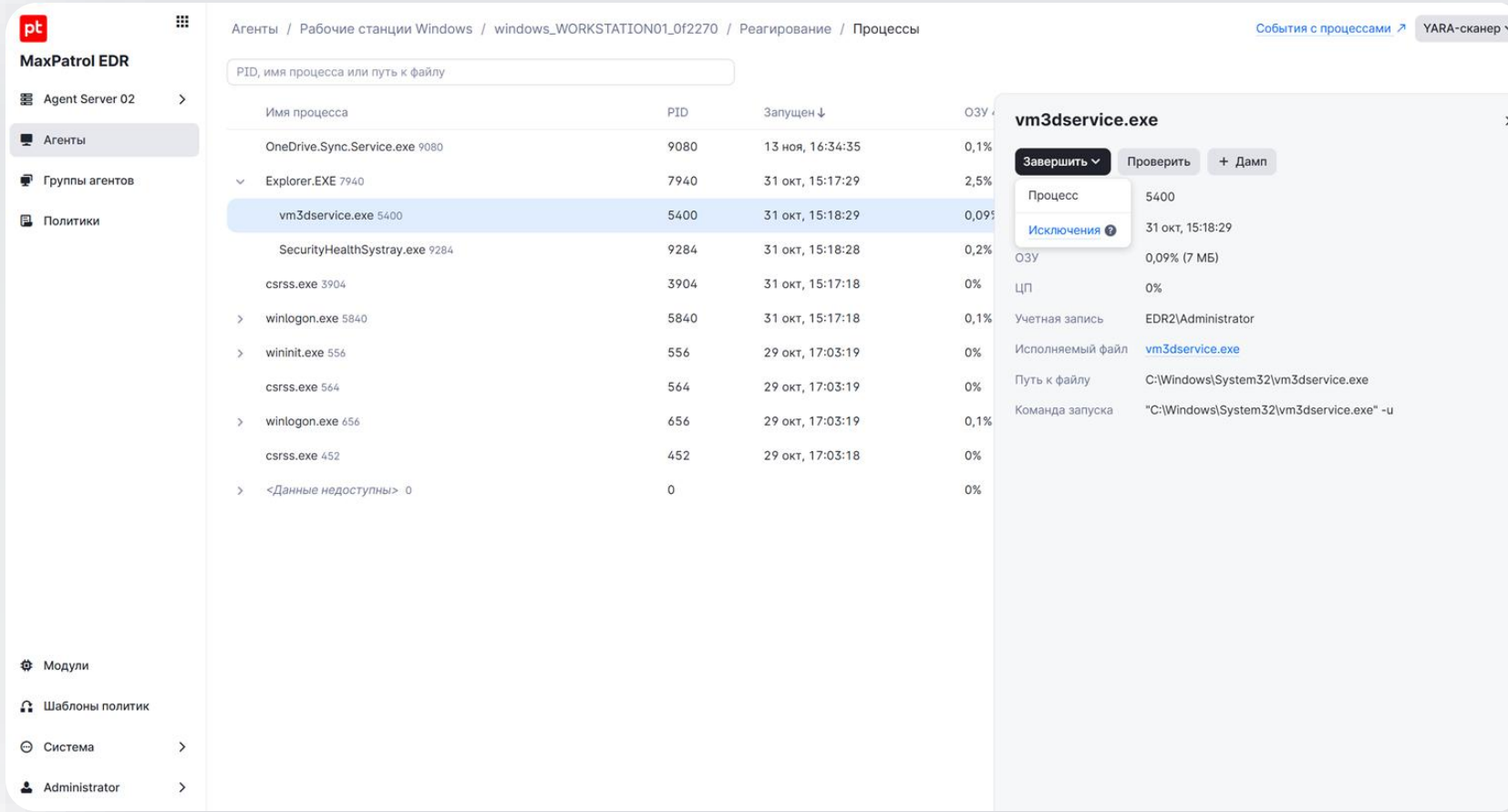
Работа с файлами

- Все операции с файловой системой — в одном окне:
  - Поиск
  - Удаление
  - Проверка (YARA, hash_checker, PT Sandbox)
  - Карантин
  - Загрузка, скачивание
  - Отправка во внешнюю систему
- Переход к запущенным процессам
- Переход к событиям с файлами в один клик



Работа с процессами

- Детальная информация обо всех запущенных процессах
- Поиск процессов по атрибутам
- Все операции с процессами в одном окне
- Быстрый переход к исполняемым файлам и операциям над ними
- Переход к событиям с процессами в один клик



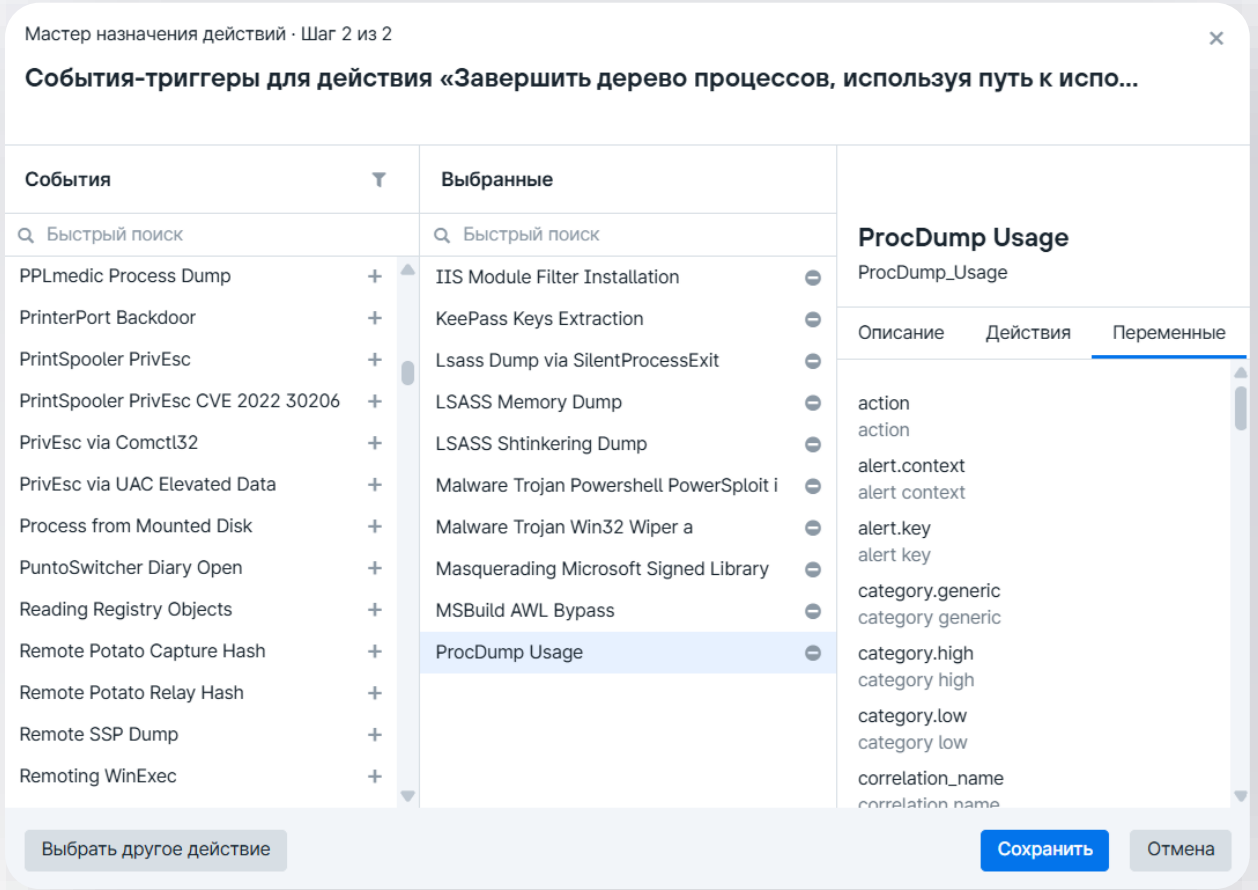
Автоматизация реагирования

Экономия времени и ресурсов

1. Можно назначить разные сценарии для разных групп агентов

2. Действия выполняются даже в автономном режиме*

3. Мгновенное выполнение действий по реагированию — минимизация ущерба от возможных атак

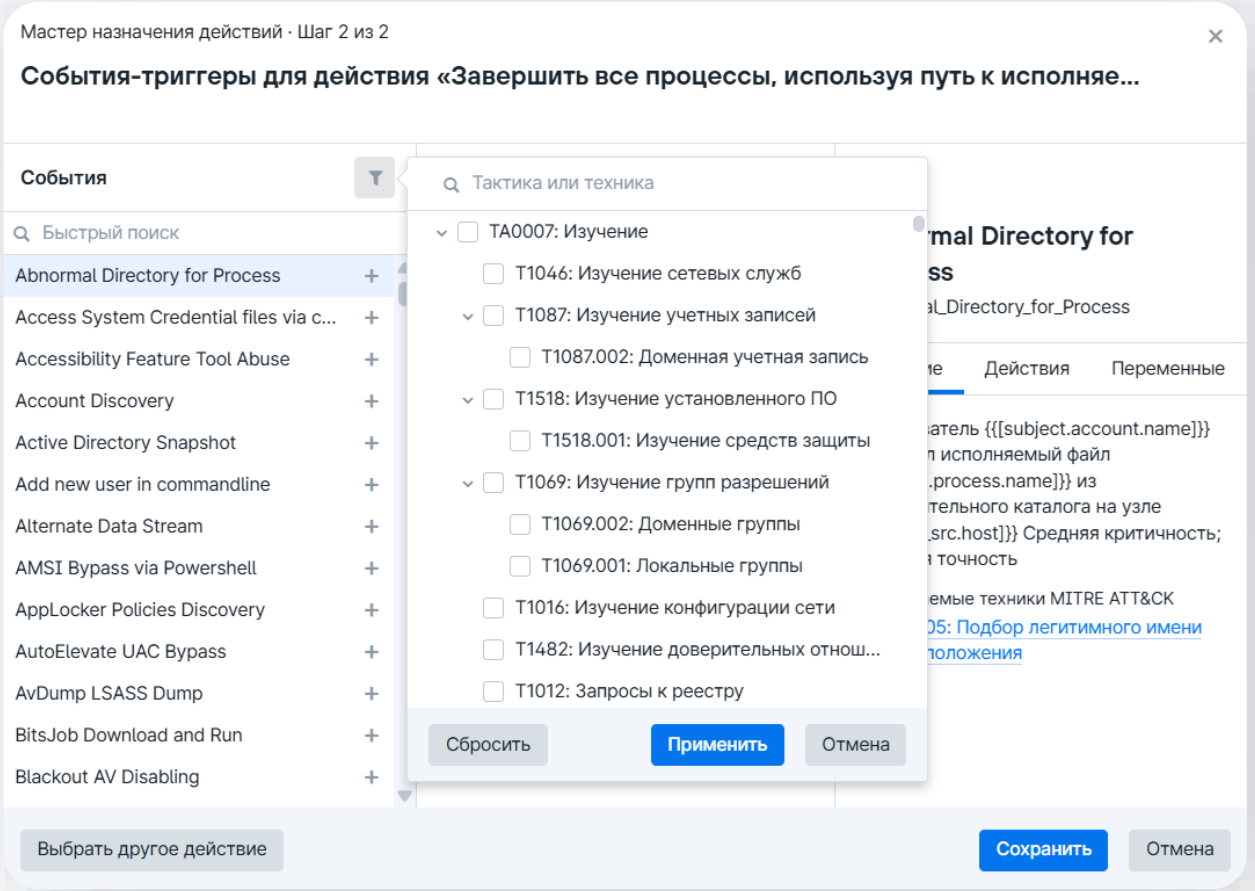


*Если не подразумевают взаимодействия с внешними системами.

Автоматизация реагирования

Фильтрация по техникам MITRE ATT&CK

При настройке политик удобно фильтровать корреляционные правила по техникам, которые они покрывают

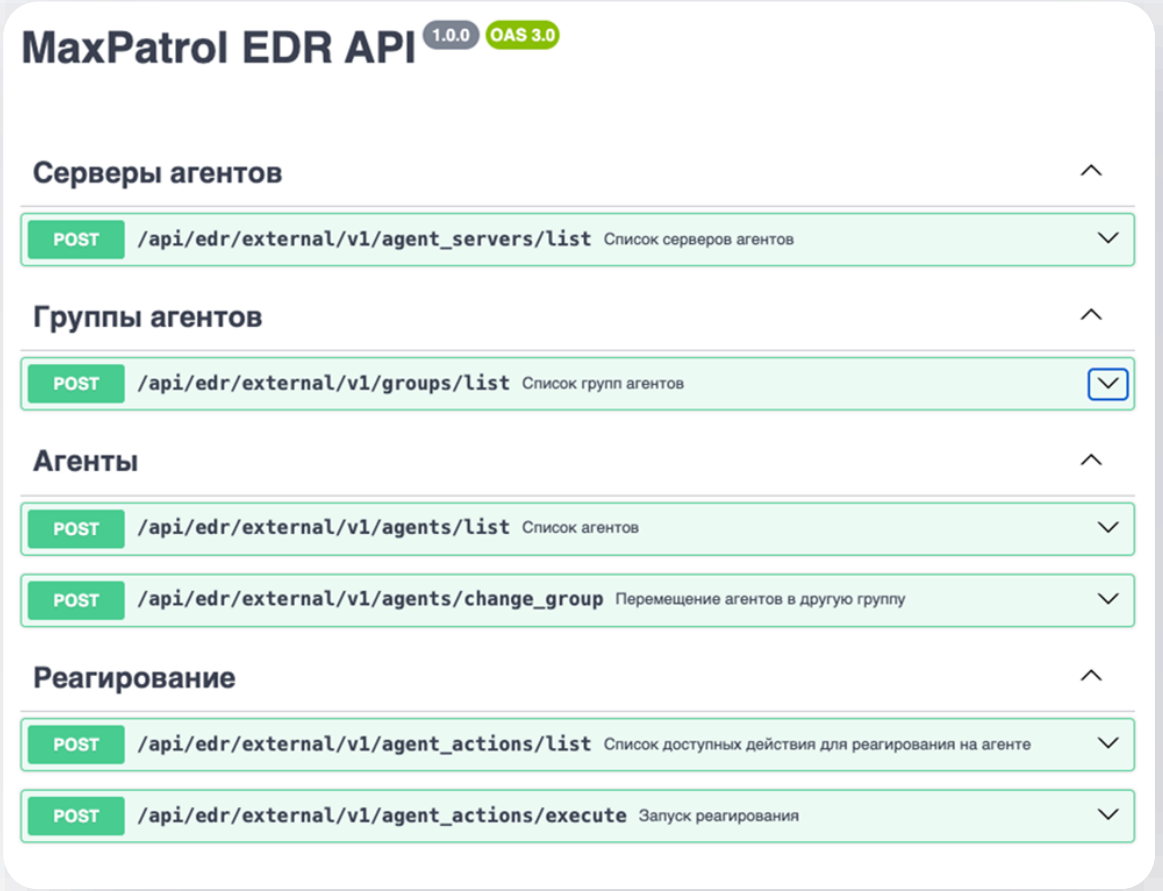


Публичный API

Расширение спектра возможностей реагирования для IRP, SOAR и других систем

Как можно взаимодействовать с агентами через API

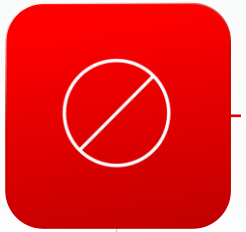
- Получить список агентов с ключевой информацией по ним
- Получить список доступных действий
- Выполнить реагирование на агенте
- Переместить агент в другую группу



Сценарий применения

Расследование инцидента

Понимаю, что атака на инфраструктуру Windows-серверов была совершена с помощью файла juicypotato.exe

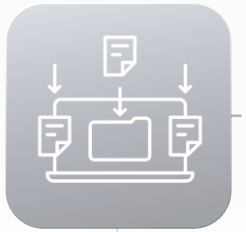


Остановка распространения

Изолирую от сети выборку устройств

Устранение

На той же группе выполняю другие операции: завершение процесса, удаление файла



Снятие ограничений

Обращаюсь к журналу изоляции. Снимаю изоляцию на тех агентах, где операция выполнена успешно

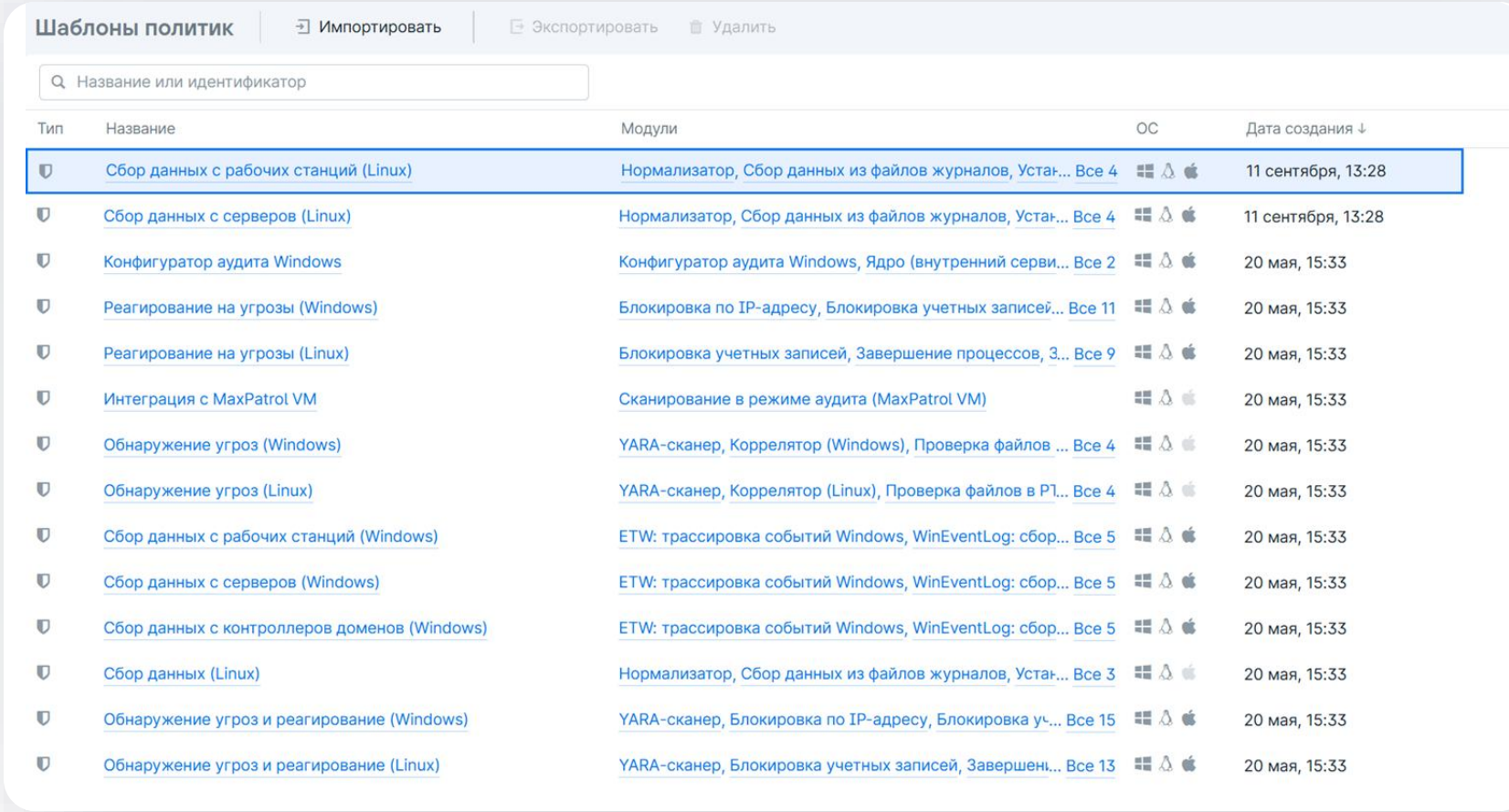
Постанализ

Анализирую инцидент и делаю выводы: обновить политики, добавить нужные модули или сделать реагирование автоматическим

Готовые шаблоны политик

Настраивайте продукт за минуты

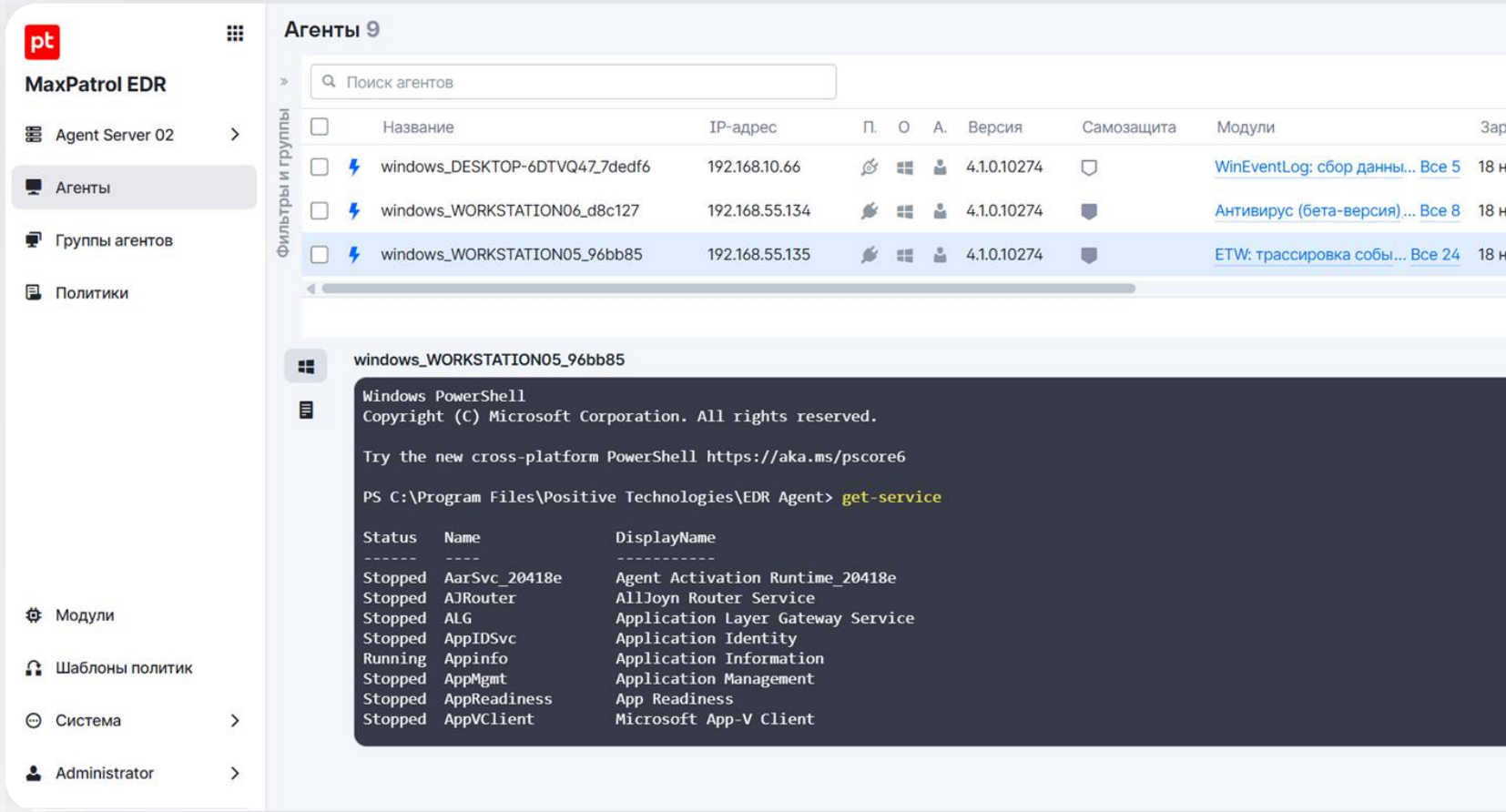
- **Отдельное окно для работы с шаблонами политик** (возможность заглянуть внутрь политики без предварительного создания)
- **Лучшие практики от вендора** по гранулярной настройке политик (сбор, обнаружение, реагирование, интеграции)
- **Шаблоны сбора под разные роли** узлов под управлением Windows
- Коррелятор в политиках **с уже настроенными исключениями**
- **Готовые плейбуки** в политиках «Обнаружение угроз и реагирование»
- Можно и нужно использовать **для быстрого старта** (аккуратно с автореагированием)



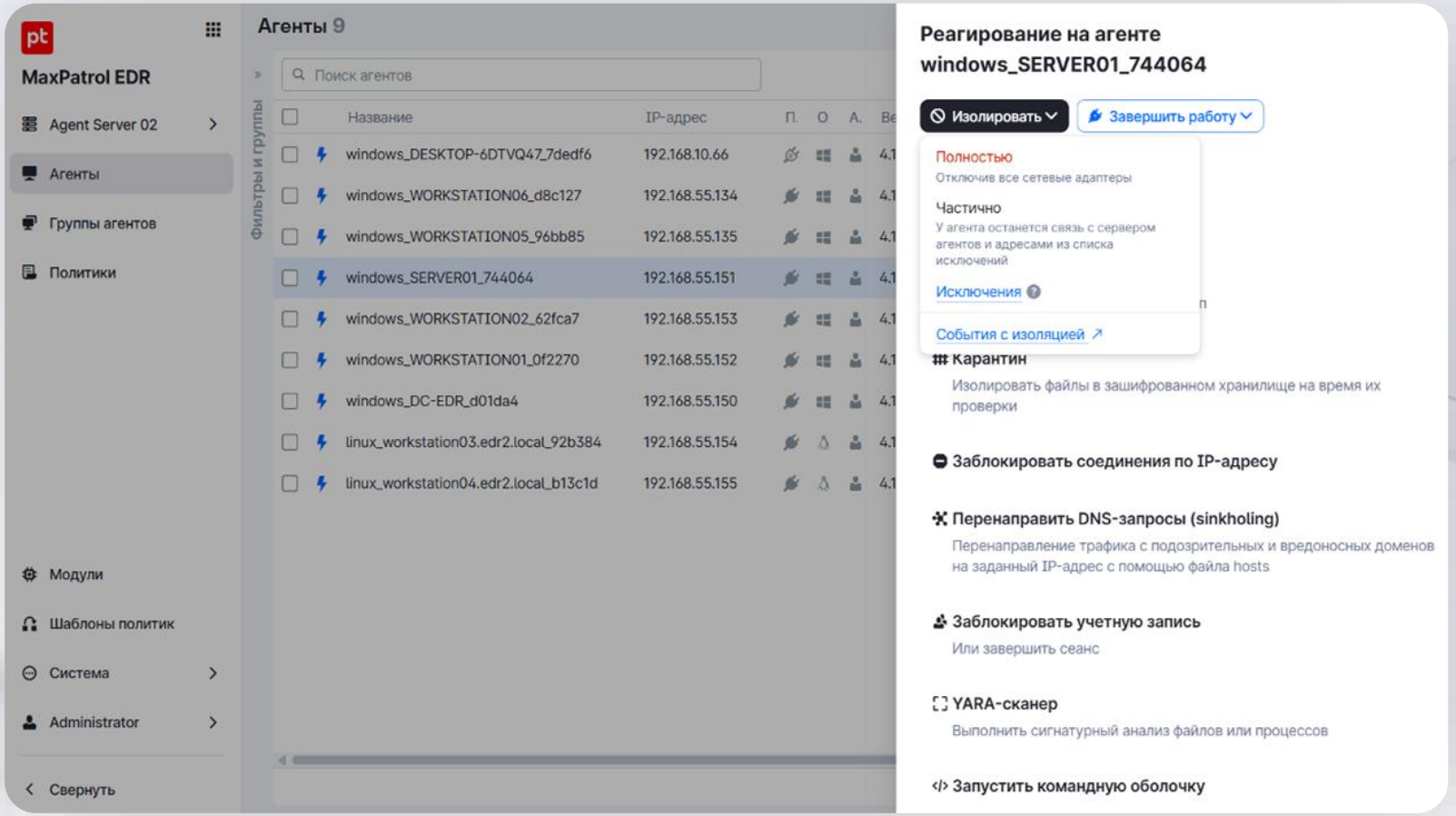
Как выглядит на практике: remote shell

Особенности модуля

- Работает на узлах под управлением Windows и Linux
- Команды выполняются в PowerShell или Bash
- Выполняет расследование инцидентов, сбор необходимых данных
- Устраняет нарушения независимо от того, где находится конечное устройство
- Все выполненные команды сохраняются в журнале
- Доступ к журналу можно ограничить паролем
- При выполнении команд создается событие ИБ



Как выглядит на практике: изоляция узлов на Windows и Linux



Уже используете решения Positive Technologies?

Усильте их за счет MaxPatrol EDR

Агент MaxPatrol EDR в экосистеме Positive Technologies

Кросс-продуктовое взаимодействие для решения задач

MaxPatrol SIEM

- Контроль сбора событий с серверов и рабочих станций (включая устройства вне домена или периметра)
- Расширенный контекст для принятия решений (агент собирает то, что не умеет SIEM-система)
- Возможность оперативного реагирования на угрозы
- Единая консоль для работы с событиями и инцидентами

MaxPatrol VM

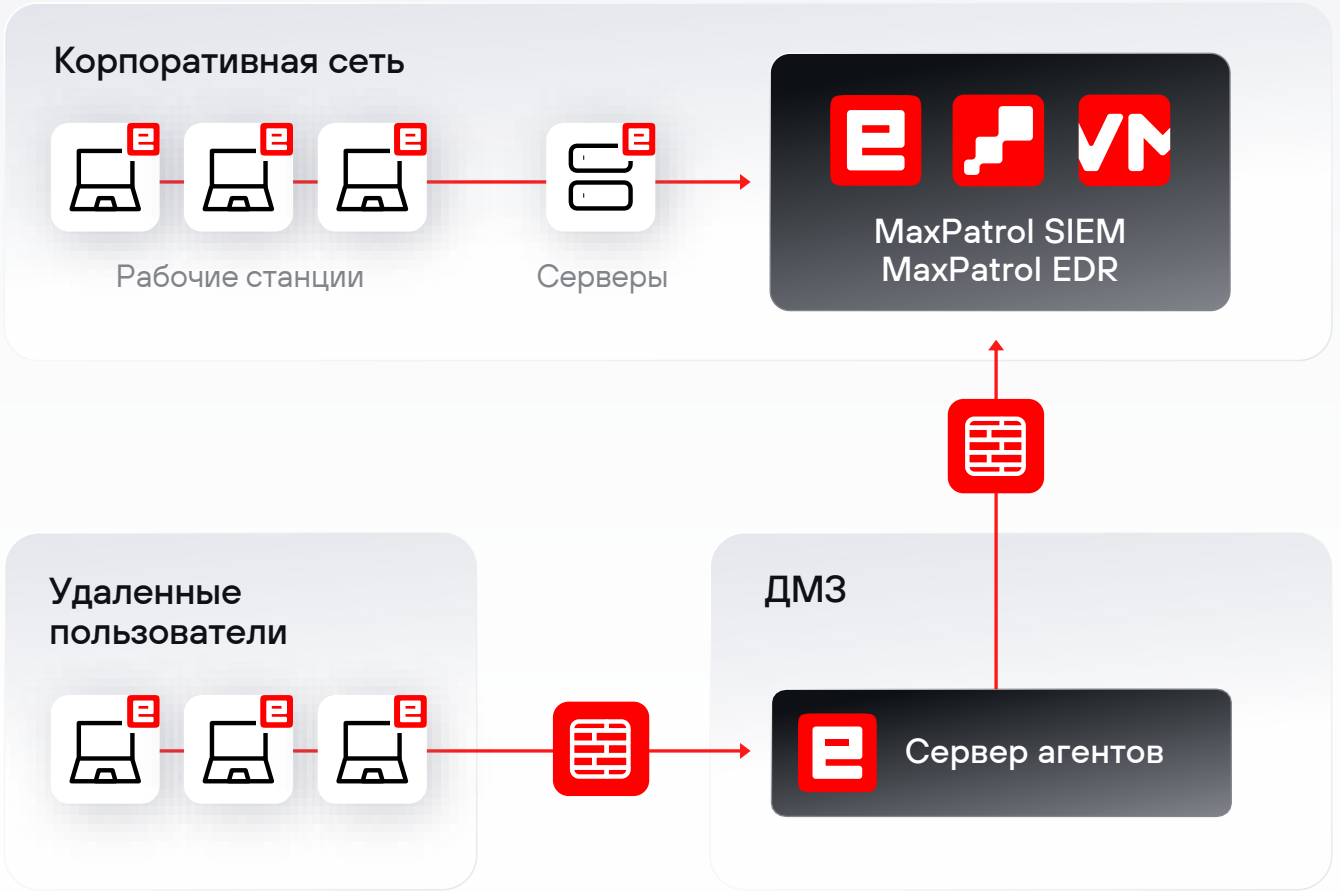
- Упрощение взаимодействия между отделами ИБ и ИТ
- Сбор данных с тех устройств, с которых не получалось собрать их средствами сетевого сканера
- Не требует сервисных учетных записей для проведения сканирования
- Более частое обновление данных об активах
- Снижение нагрузки на сканирующий сервер, каналы связи, упрощение маршрутизации

PT Sandbox

- Защита от ВПО, распространяемого через шифрованные каналы (Telegram, браузеры, P2P)
- Повышение точности обнаружения угроз
- Результат анализа PT Sandbox доступен на всех агентах, что позволяет превентивно блокировать атаки
- На вердикт песочницы можно настроить автоматическое реагирование

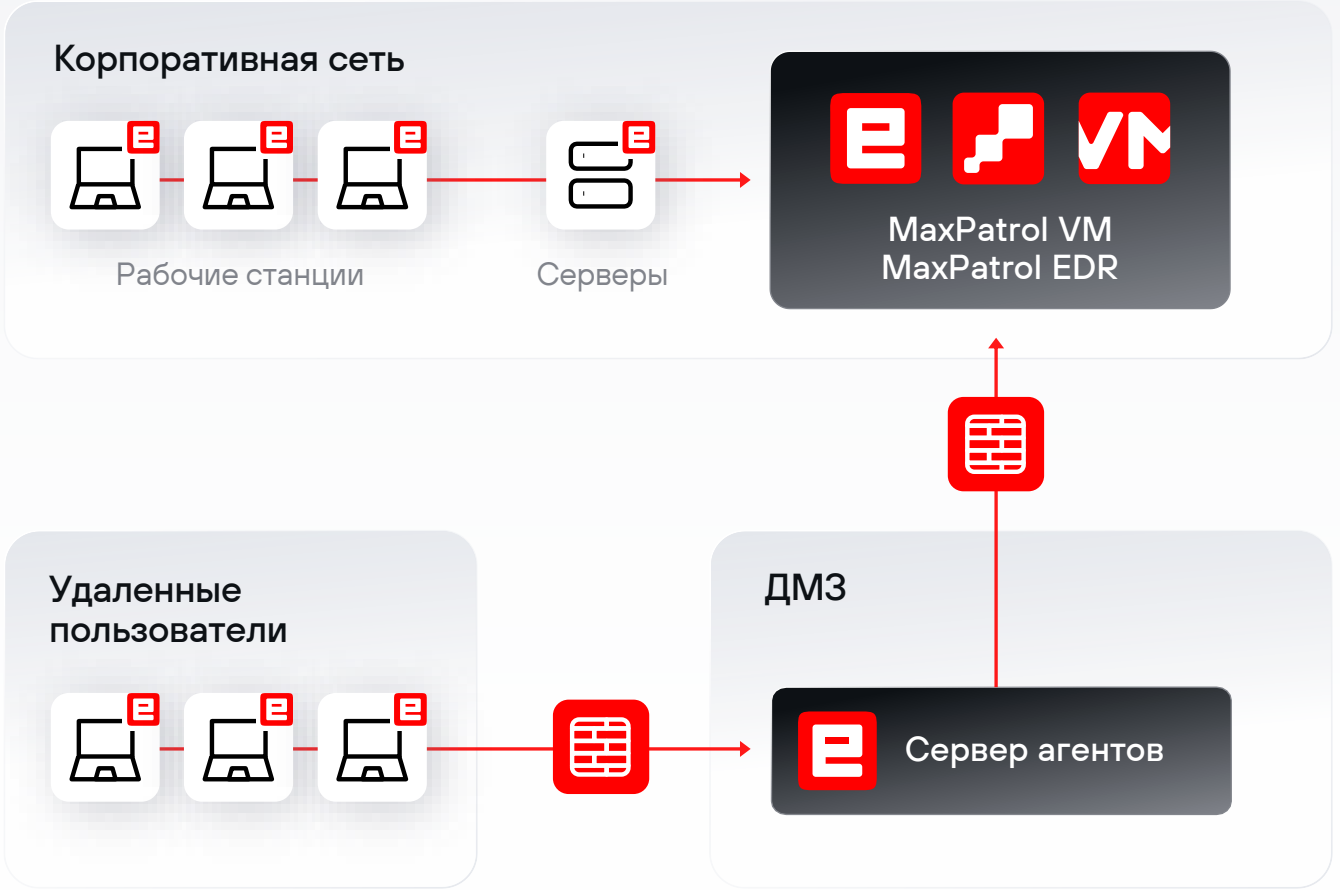
MaxPatrol EDR + MaxPatrol SIEM

- Контролируемый сбор событий (включая устройства вне домена или периметра)
- Расширенные возможности сбора данных (агент EDR собирает то, что не умеет SIEM-система)
- Оптимизация архитектуры и нагрузки на MaxPatrol SIEM
- Реагирование и работа с исключениями из карточки события
- Единая консоль для работы с событиями и инцидентами



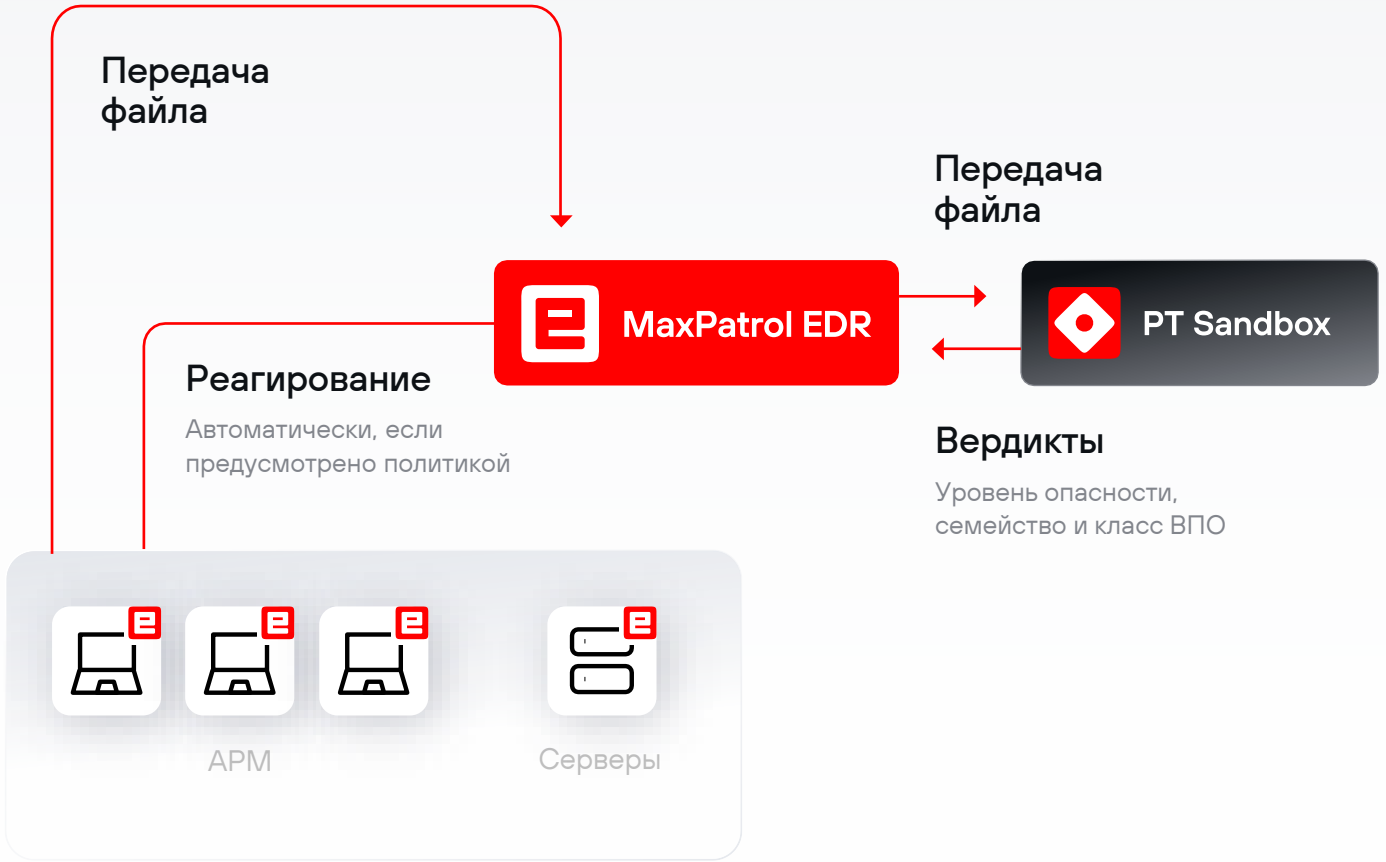
MaxPatrol EDR + MaxPatrol VM

- Нет необходимости использовать сервисные учетные записи
- Сбор данных с узлов вне домена и устройств удаленных сотрудников
- Настраиваемое расписание сканирования
- Частое обновление данных об активах
- Снижение нагрузки на сканирующий сервер и каналы связи
- Единая консоль управления



MaxPatrol EDR + PT Sandbox

- Агенты EDR обнаруживают скачиваемые файлы (в браузерах, Telegram, с помощью P2P и пр.) и передают на анализ в PT Sandbox
- PT Sandbox проводит подробный статический и поведенческий анализ и отправляет вердикт
- Можно настроить автоматическое реагирование исходя из вердикта песочницы
- Вердикт песочницы распространяется на все агенты из группы



Лицензирование

Варианты поставки и лицензирование: MaxPatrol EDR

ЛИЦЕНЗИРОВАНИЕ

Основная и единственная метрика лицензирования — количество подключаемых агентов.

ВАРИАНТЫ ПОСТАВКИ

Варианты поставки определяют набор доступных функциональных модулей, работающих на агенте:

PT-MXEDR-L-XXX, конфигурация Lite:

доступны модули для сбора и передачи журналов событий операционной системы.

PT-MXEDR-LP-XXX, конфигурация Lite Plus:

доступны модули для сбора и передачи журналов событий операционной системы и локального сбора данных в режиме аудита.

PT-MXEDR-B-XXX, базовый набор модулей:

доступны все модули поставки MaxPatrol EDR.

Варианты поставки и лицензирование: MaxPatrol EPP и MaxPatrol Endpoint Security

ЛИЦЕНЗИРОВАНИЕ

Основная и единственная метрика лицензирования — количество подключаемых агентов.

ВАРИАНТЫ ПОСТАВКИ

Варианты поставки определяют набор доступных функциональных модулей, работающих на агенте:

PT-MXEDR-EPP-XXX-YYY, конфигурация MaxPatrol Endpoint Protection Platform

(для обеспечения антивирусной защиты конечных устройств), обновления в течение года.

PT-MXEDR-ES-XXX-YYY, конфигурация MaxPatrol Endpoint Security

(базовый набор модулей и модули обеспечения антивирусной защиты конечных устройств), обновления в течение года.

Узнайте больше о Позитиве

Обзор MaxPatrol EDR

Telegram-чат пользователей

Заказать бесплатный «пилот»

Телеграм-канал Positive Technologies

Покрытие матрицы MITRE ATT&CK