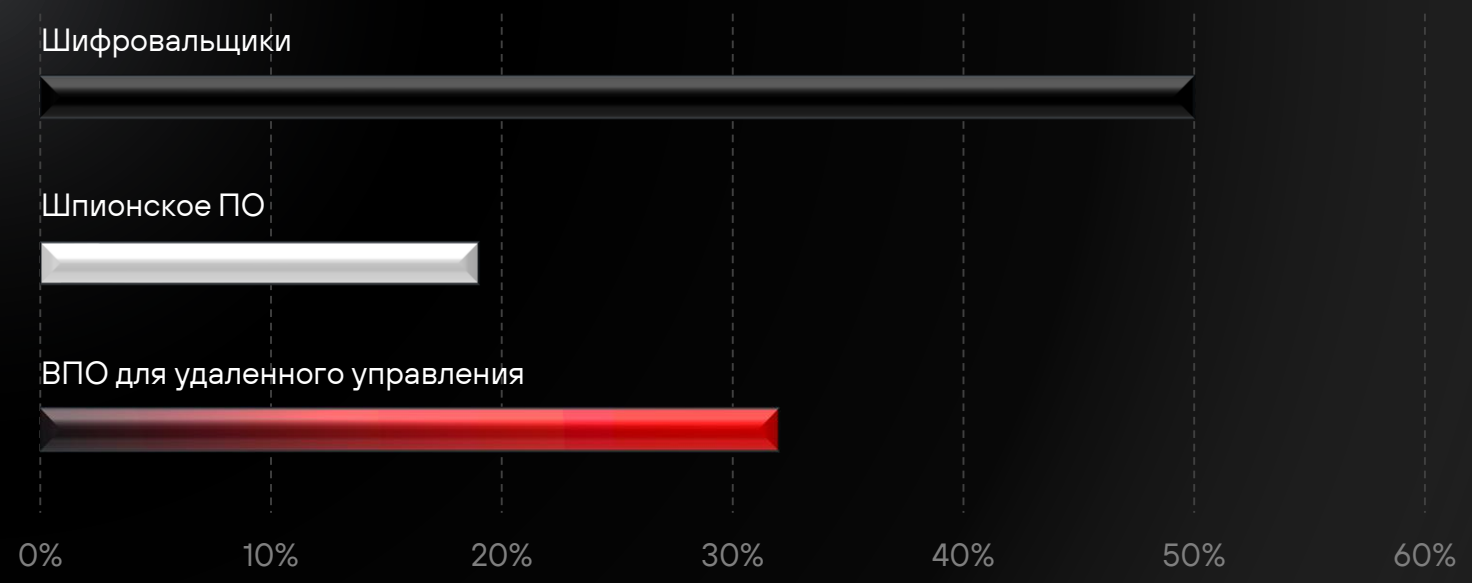
Непрерывная работа бизнеса начинается с непробиваемой защиты конечных устройств

Тренды

ВПО остается основным инструментом злоумышленников



Типы ВПО, чаще всего применяемые в успешных атаках на организации

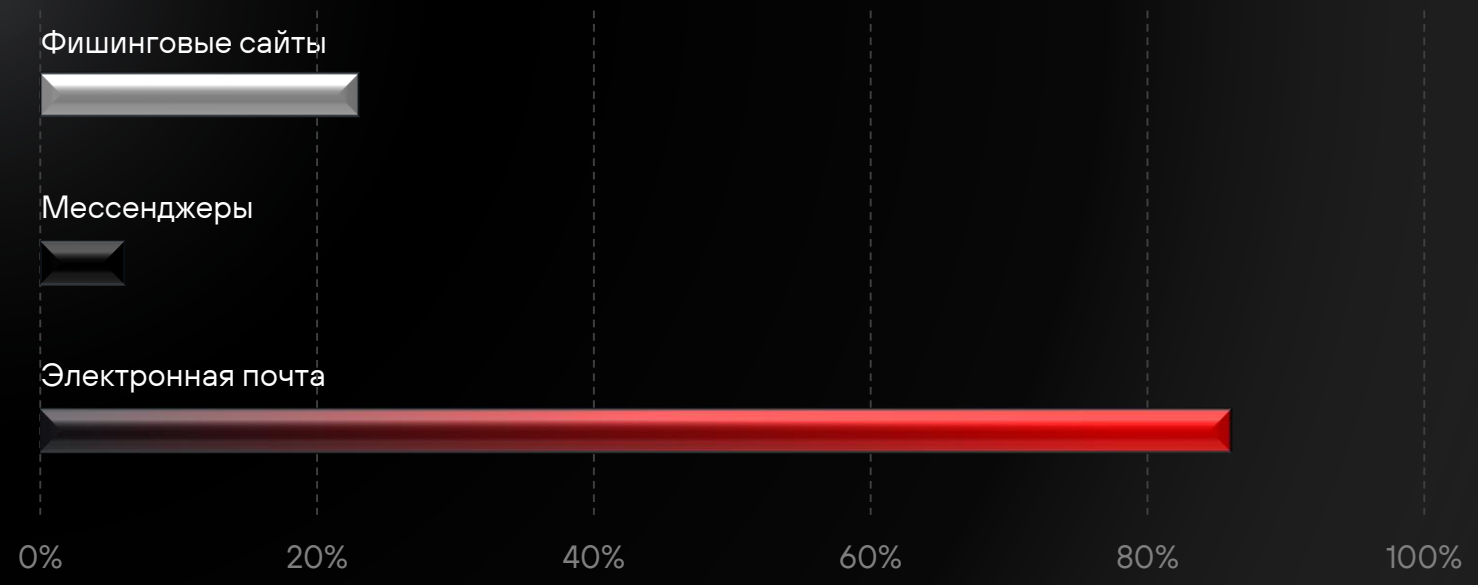
Доля применения ВПО в атаках на организации

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.)

Тактики и техники атак



Каналы социальной инженерии, которые чаще всего используют в успешных атаках на организации

Эксплуатация уязвимостей остается одним из самых эффективных методов атак на организации: она использовалась в 35% успешных атак

Учетные данные пользователей были скомпрометированы в 18% успешных атак

MaxPatrol Endpoint Security

Комплексное решение для максимальной безопасности

Комплексная защита конечных устройств от всех видов угроз

MaxPatrol Endpoint Security

Предотвращение известных угроз с MaxPatrol EPP

NEW

1. Обнаружение и устранение шифровальщиков и другого ВПО **благодаря антивирусным технологиям**
2. Контроль устройств и приложений для ограничения векторов атак
3. Автоматическое восстановление поврежденных шифровальщиком файлов

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 с гибкой конфигурацией и настройкой глубины кэширования данных
3. Защита от злоумышленников за считаные секунды, помощь в расследовании и предотвращении атак

MaxPatrol Endpoint Security экспертный уровень защиты

Автономная работа

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

Поддержка 90% актуальных 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

Превентивная защита

Мощный антивирусный движок обеспечивает эффективное обнаружение ВПО с помощью сигнатурного и эмуляционного анализа. Инструменты для управления перечнем разрешенных устройств и приложений

Ультимативная самозащита

Встроенные системы и параметры защиты не позволят вывести агент из строя — злоумышленники не обойдут защиту конечного устройства, а агент гарантирует непрерывный сбор событий и реагирование

Соответствие требованиям регуляторов

MaxPatrol Endpoint Security соответствует требованиям:

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

MaxPatrol EPP

Сертифицирован ФСТЭК как средство антивирусной защиты (класс САВЗ)

Может использоваться в качестве второго антивируса для финансовых организаций и значимых объектов КИИ

MaxPatrol EDR

Сертифицирован ФСТЭК как средство обнаружения и реагирования (класс СОР)

Может использоваться для анализа и комплексного реагирования на события безопасности, мониторинга процессов и состояния устройств

MaxPatrol Endpoint Protection Platform (MaxPatrol 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

ДОСТУПЕН

Защита от шифровальщиков

Проактивная защита от шифровальщиков — мгновенная блокировка ВПО и восстановление данных

ДОСТУПЕН

Контроль подключаемых устройств

Ограничение доступа и предотвращение несанкционированного использования подключаемых устройств

ДОСТУПЕН

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

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	Позволяет проводить динамический анализ для выявления продвинутого и неизвестного 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
6	Собственная экспертиза	Многолетний опыт анализа угроз и разработки средств защиты с учетом специфики российских организаций, собственная антивирусная лаборатория в PT ESC

Ключевые преимущества

- **Устойчивость к переупаковке, шифрованию и полиморфизму:** эмулятор с динамической трансляцией 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

▼

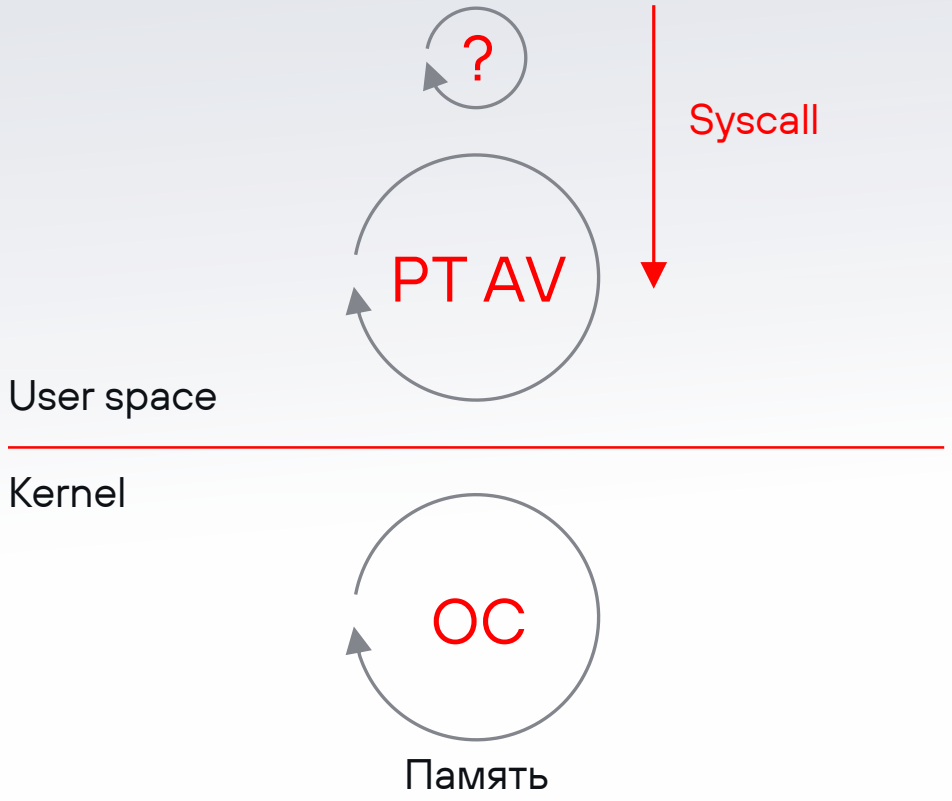
Сбор трассы исполнения

▼

Проверка наличия искомого события в трассе

▼

Оценка состояния участков памяти



Испытайте возможности MaxPatrol EPP

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)
- PT NAD (реагирование на сетевые угрозы)

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

- Антивирусная защита
- Контроль подключаемых устройств
- Контроль приложений
- Защита от шифровальщиков и вайперов, восстановление поврежденных файлов

РЕАГИРОВАНИЕ

EDR

- Продвинутое обнаружение и защита от целевых угроз
- Мониторинг конечных устройств
- Сценарии реагирования для всех случаев обнаружения
- Расследование инцидентов безопасности
- Инструменты администрирования и оперативного подключения к конечному устройству

СБОР СОБЫТИЙ

SIEM

- Мониторинг и обнаружение
- Расследование
- Отчетность

ИНВЕНТАРИЗАЦИЯ

VM HCC

- Выявление и приоритизация уязвимостей
- Контроль соответствия стандартам

АНАЛИЗ СЕТИ

NAD

- Глубокий анализ (DPI)
- Обнаружение аномалий и угроз
- Контроль политик ИБ

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?

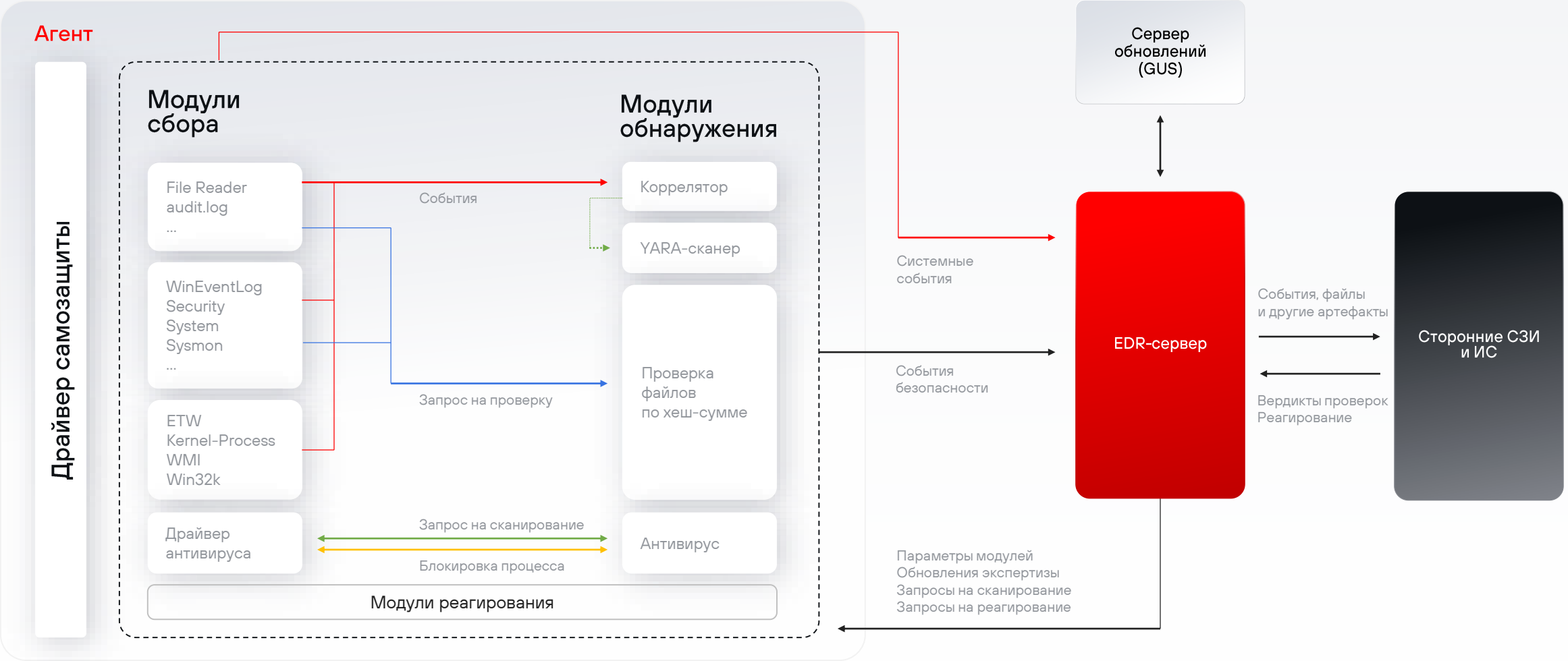
Выявление

- 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?

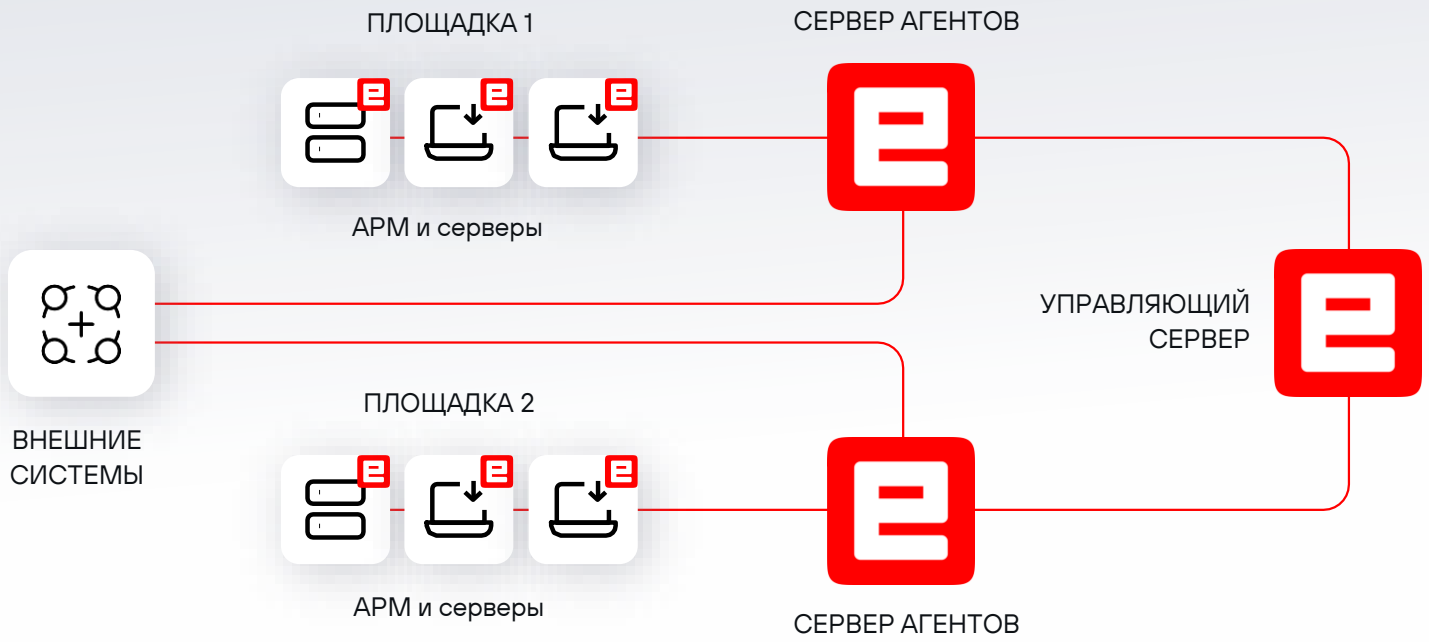
Реагирование

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

Как работает MaxPatrol EDR



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 11
Windows Server 2016, 2019	Windows Server 2022, 2025	Debian 10, 11	Debian 12,13	Ubuntu 20.04
Ubuntu 22.04	Ubuntu 24.04	Ubuntu 25.04	CentOS 9	CentOS 10
«Альт Рабочая станция» 10.2	«Альт Рабочая станция» 10.4	«Альт Сервер» 10.1	«Альт Сервер» 10.2	RHEL 9
RHEL 10	«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 Endpoint Security

1

Мониторинг безопасности конечных устройств для «Газпромбанк Мобайл»

2

Построение результативной кибербезопасности для Rambler&Co

3

Защита конечных устройств в Positive Technologies

4

Защита инфраструктуры на «Играх будущего»

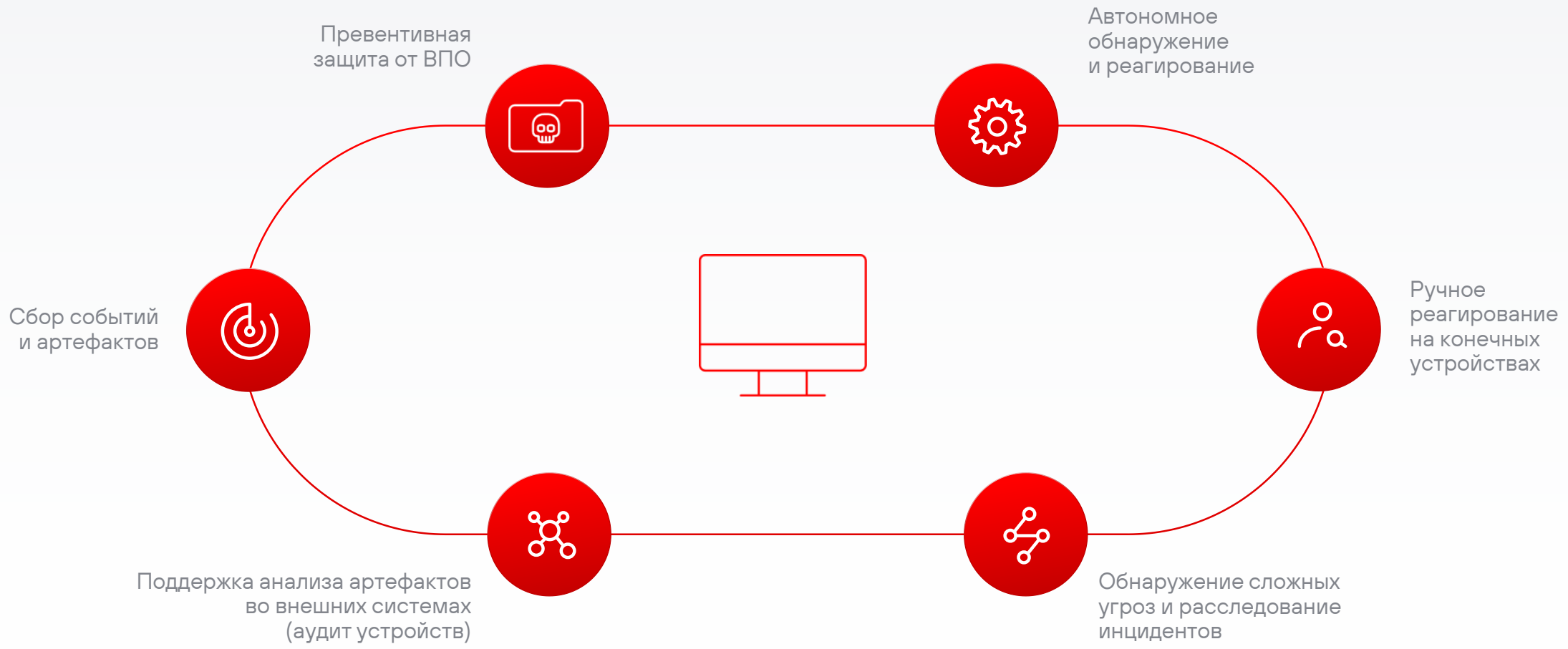
5

Инструмент команды защитников в рамках кибербитв Standoff

6

Проверен белыми хакерами в рамках Endpoint Hack Zone и Standoff Bug Bounty

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

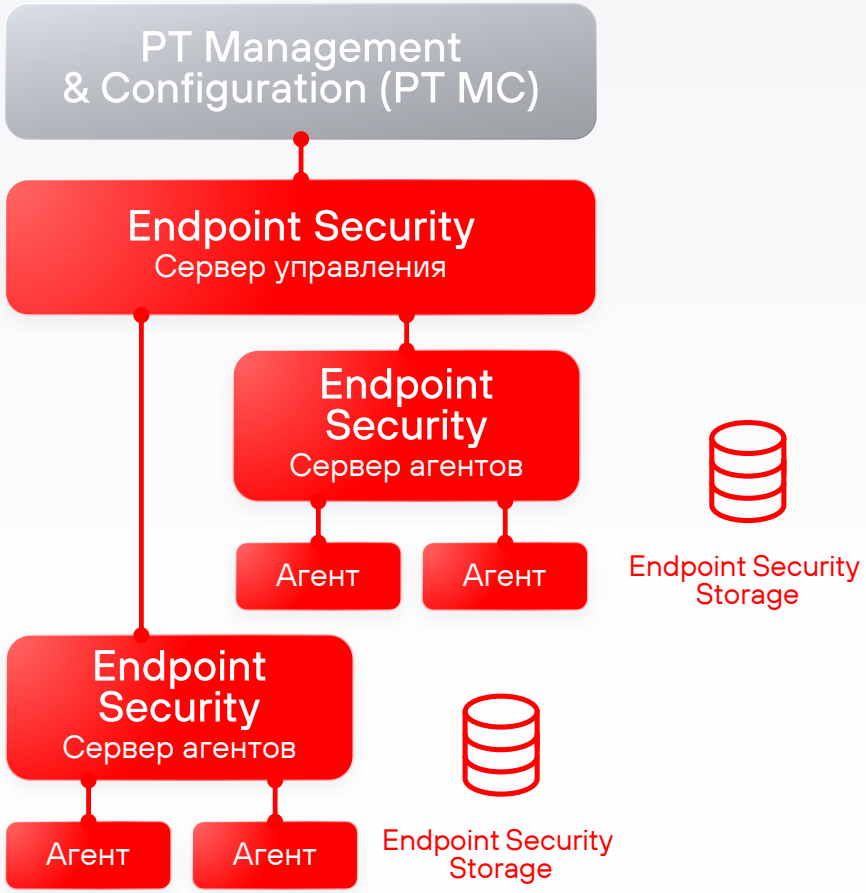
- Возможность локализации и устранения инцидентов
- Баланс между затратами на внедрение, функциональностью и нагрузкой на устройства

Сбор событий, обнаружение и автоматическое реагирование

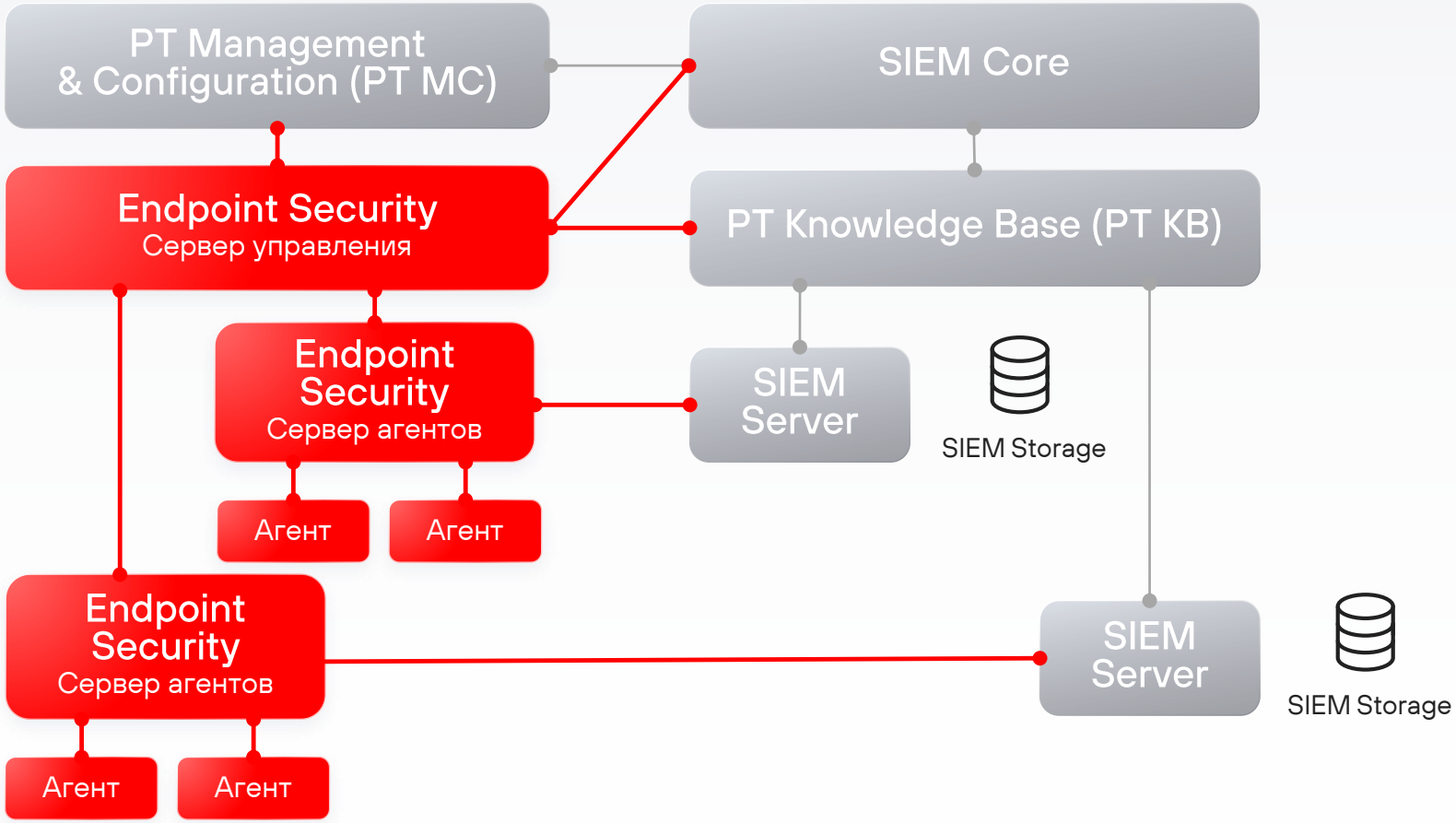
- Автономное обнаружение на агенте
- Многоэтапные проверки
- Автоматизация реагирования

Установка и настройка MaxPatrol Endpoint Security

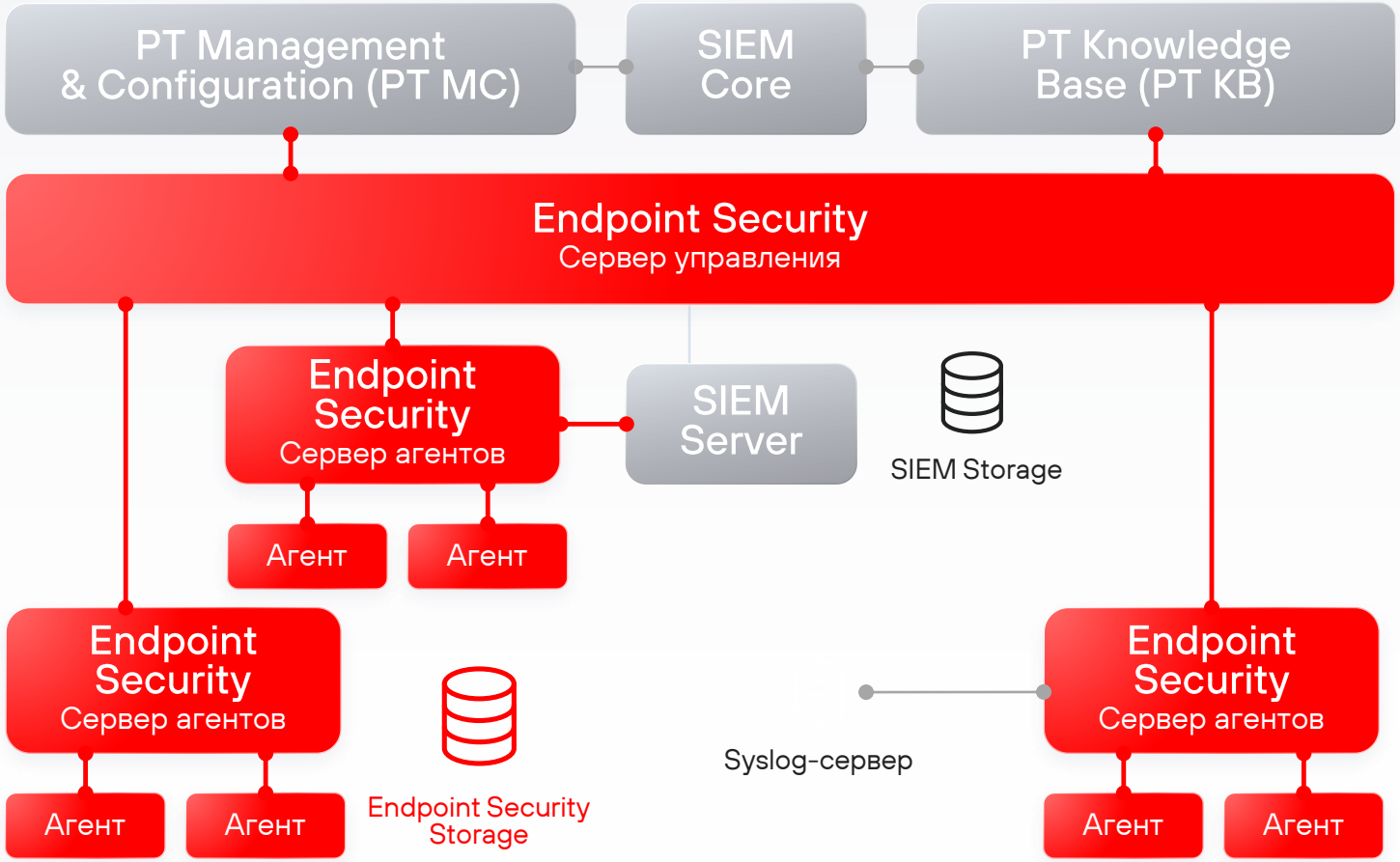
Варианты развертывания: собственное хранилище



Варианты развертывания: совместно с MaxPatrol SIEM



Варианты развертывания: гибридная установка



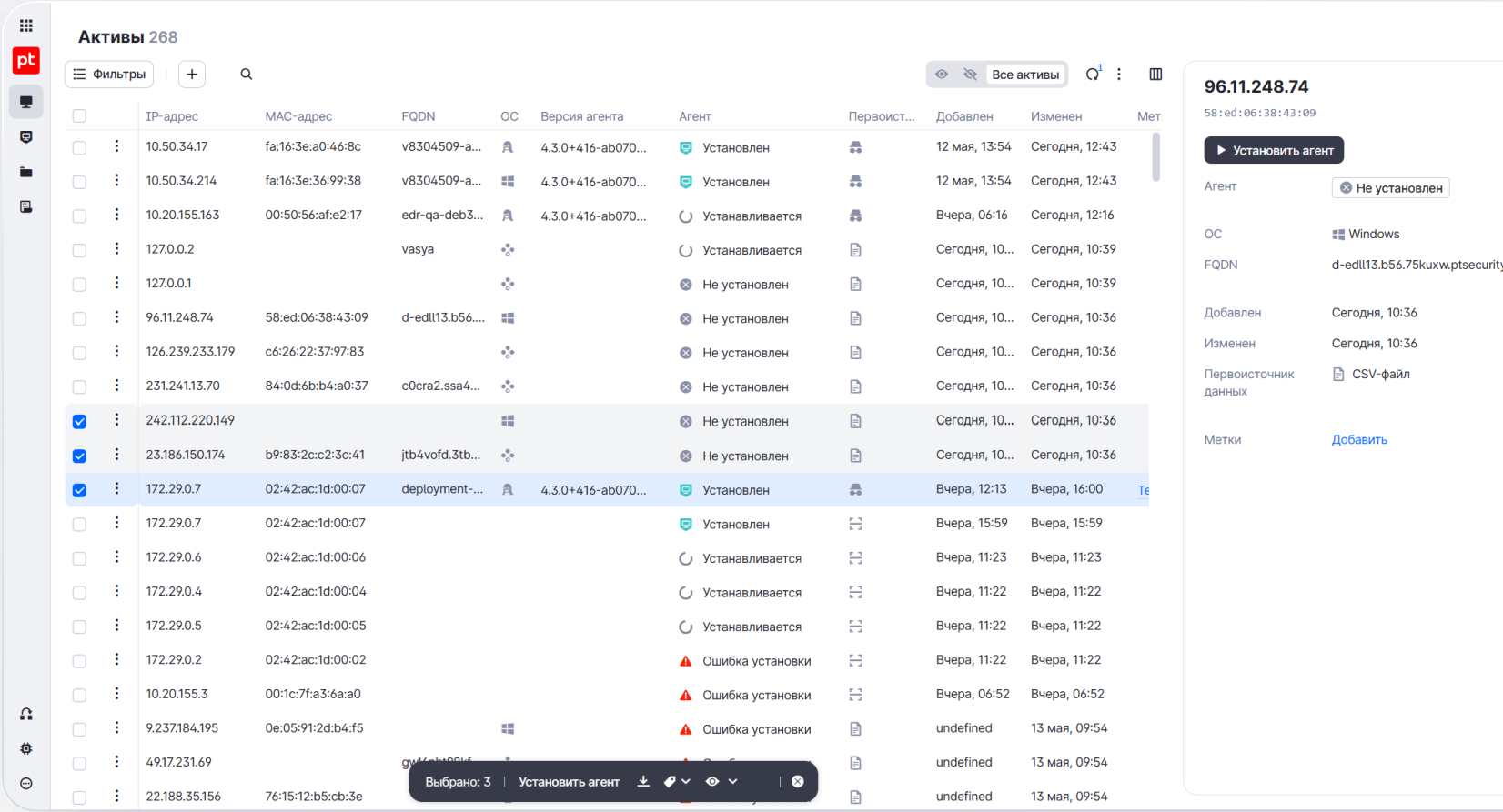
Выбираем тип инсталляции

	Самостоятельная (неинтегрированная)	Совместная с MaxPatrol SIEM (интегрированная)
Хранение событий из журналов ОС	Хранятся только события обнаружения и реагирования	Хранятся все события ОС, которые собрал агент
Наличие нескольких серверов агентов, централизованное хранение событий	Для каждого сервера агентов выделяется собственное хранилище	Для каждого сервера агентов указывается целевой конвейер MaxPatrol SIEM, он может быть один для всех
Единая консоль для работы с инцидентами		
Дашборды и отчеты		Функциональность виджетов, дашбордов и отчетов из MaxPatrol SIEM
Возможность использовать собственные правила корреляции и нормализации	Только экспертиза «из коробки»	Единая база правил в PT Knowledge Base
Интеграция с MaxPatrol VM		
Интеграция с PT Sandbox		
Интеграция с PT NAD		
Возможность реагирования из SOAR/IRP-систем		

— функциональность будет добавлена в ближайших версиях продукта

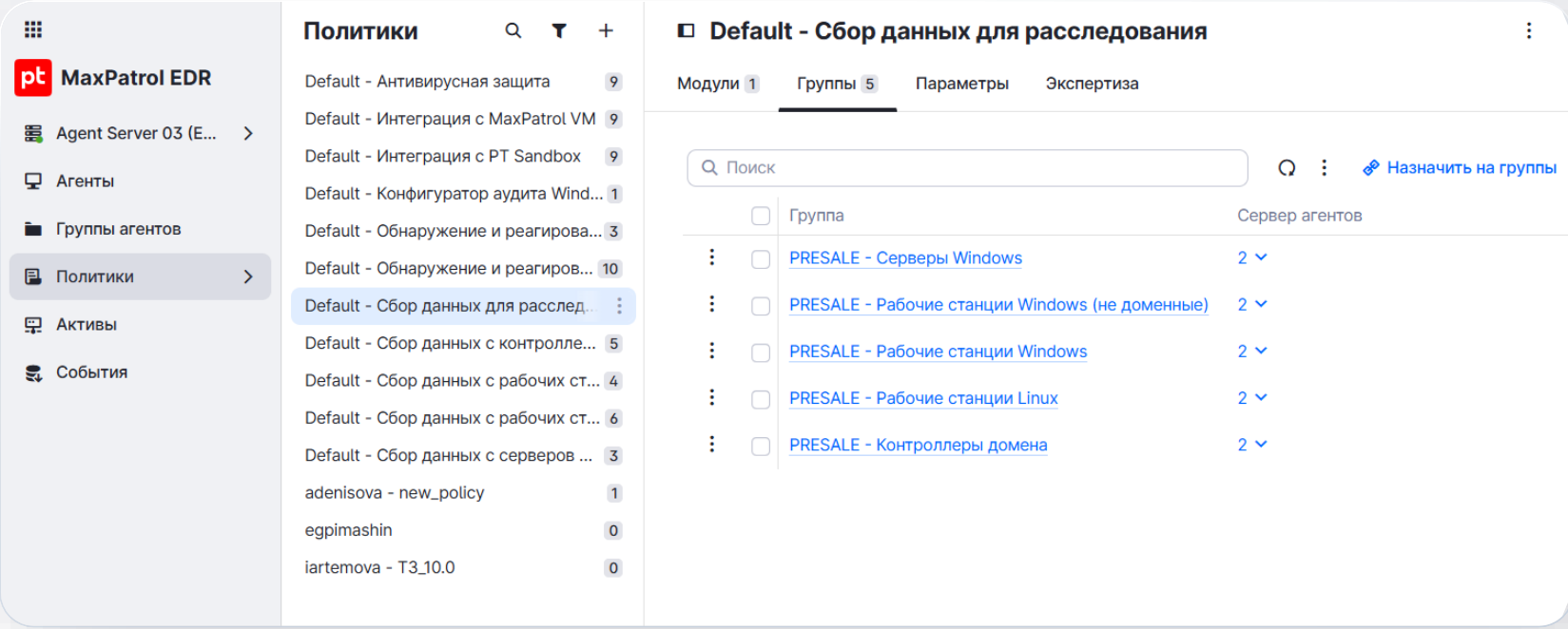
Обнаружение хостов и установка агентов

- Поиск новых хостов в инфраструктуре
- Карта покрытия инфраструктуры агентами
- Возможность установить агенты из интерфейса продукта
- Можно загрузить свой CSV-файл со списком активов



Централизация политик и групп

- Централизованное управление группами и политиками в продукте
- Автоматическое применение изменений политик сразу на всех серверах агентов



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)

Шаблоны политик | Импортировать | Экспортировать | Удалить

Название или идентификатор

Тип	Название	Модули	ОС	Дата создания ↓
	Сбор данных с рабочих станций (Linux)	Нормализатор, Сбор данных из файлов журналов, Устан... Все 4		11 сентября, 13:28
	Сбор данных с серверов (Linux)	Нормализатор, Сбор данных из файлов журналов, Устан... Все 4		11 сентября, 13:28
	Конфигуратор аудита Windows	Конфигуратор аудита Windows, Ядро (внутренний серви... Все 2		20 мая, 15:33
	Реагирование на угрозы (Windows)	Блокировка по IP-адресу, Блокировка учетных записей... Все 11		20 мая, 15:33
	Реагирование на угрозы (Linux)	Блокировка учетных записей, Завершение процессов, З... Все 9		20 мая, 15:33
	Интеграция с MaxPatrol VM	Сканирование в режиме аудита (MaxPatrol VM)		20 мая, 15:33
	Обнаружение угроз (Windows)	YARA-сканер, Коррелятор (Windows), Проверка файлов ... Все 4		20 мая, 15:33
	Обнаружение угроз (Linux)	YARA-сканер, Коррелятор (Linux), Проверка файлов в РП... Все 4		20 мая, 15:33
	Сбор данных с рабочих станций (Windows)	ETW: трассировка событий Windows, WinEventLog: сбор... Все 5		20 мая, 15:33
	Сбор данных с серверов (Windows)	ETW: трассировка событий Windows, WinEventLog: сбор... Все 5		20 мая, 15:33
	Сбор данных с контроллеров доменов (Windows)	ETW: трассировка событий Windows, WinEventLog: сбор... Все 5		20 мая, 15:33
	Сбор данных (Linux)	Нормализатор, Сбор данных из файлов журналов, Устан... Все 3		20 мая, 15:33
	Обнаружение угроз и реагирование (Windows)	YARA-сканер, Блокировка по IP-адресу, Блокировка уч... Все 15		20 мая, 15:33
	Обнаружение угроз и реагирование (Linux)	YARA-сканер, Блокировка учетных записей, Завершени... Все 13		20 мая, 15:33

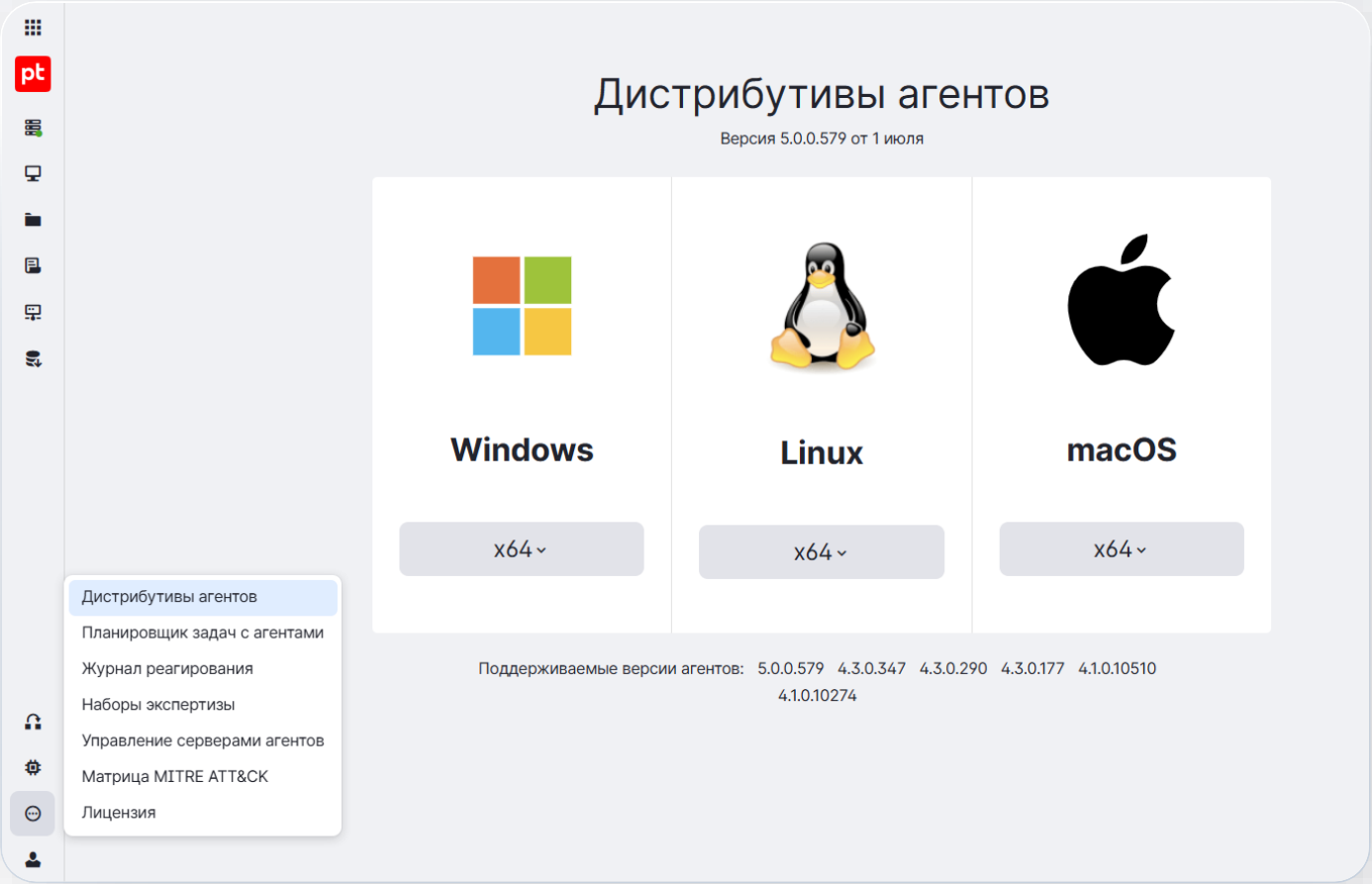
Агенты

Все необходимые дистрибутивы под рукой

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

Быстрая масштабируемость

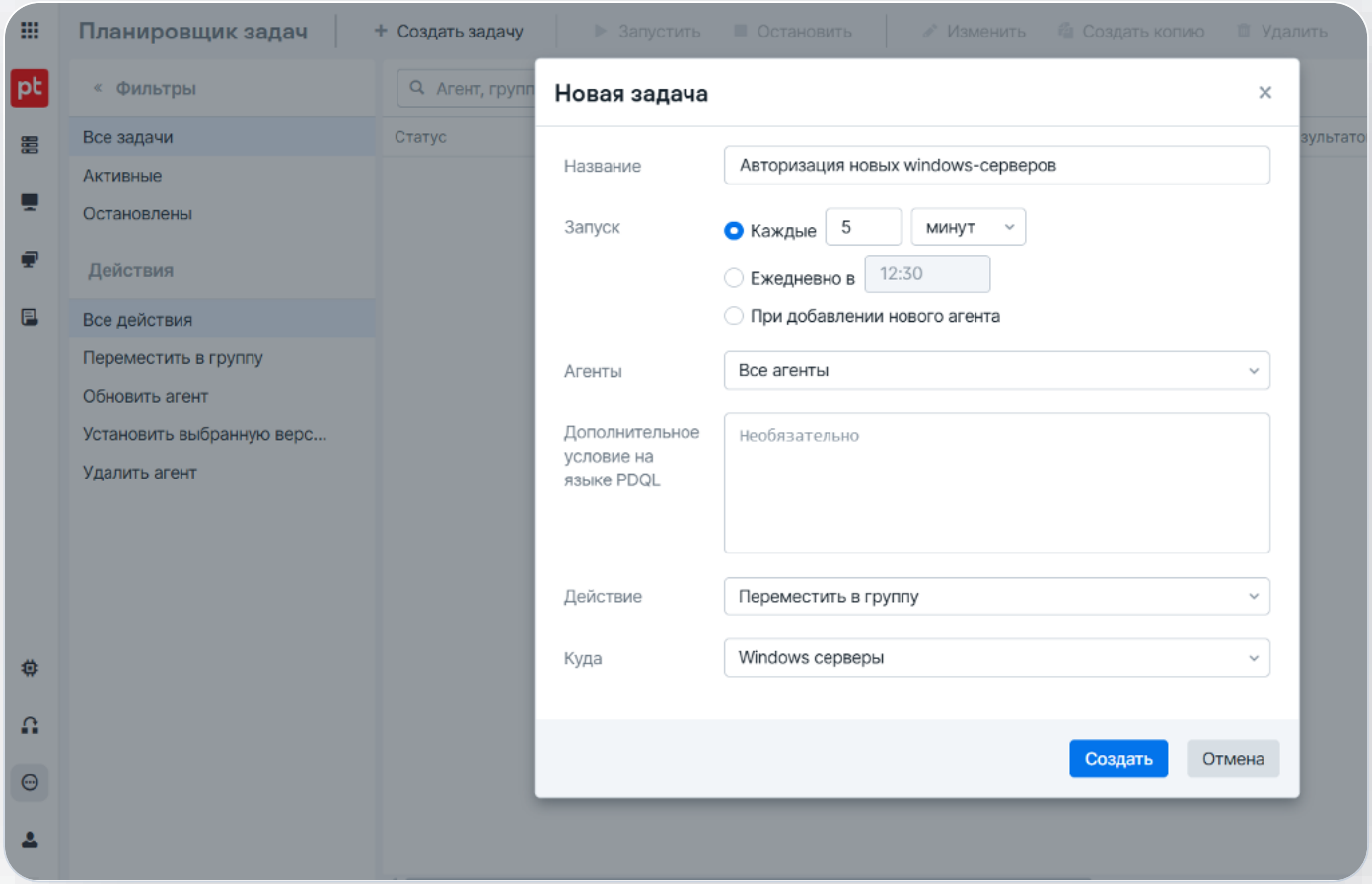
- Установка агентов из интерфейса продукта
- Готовые Ansible-плейбуки для установки, обновления, удаления и переподключения к другому серверу агентов



Автоматизация работы с агентами

Планировщик задач для быстрой и удобной работы

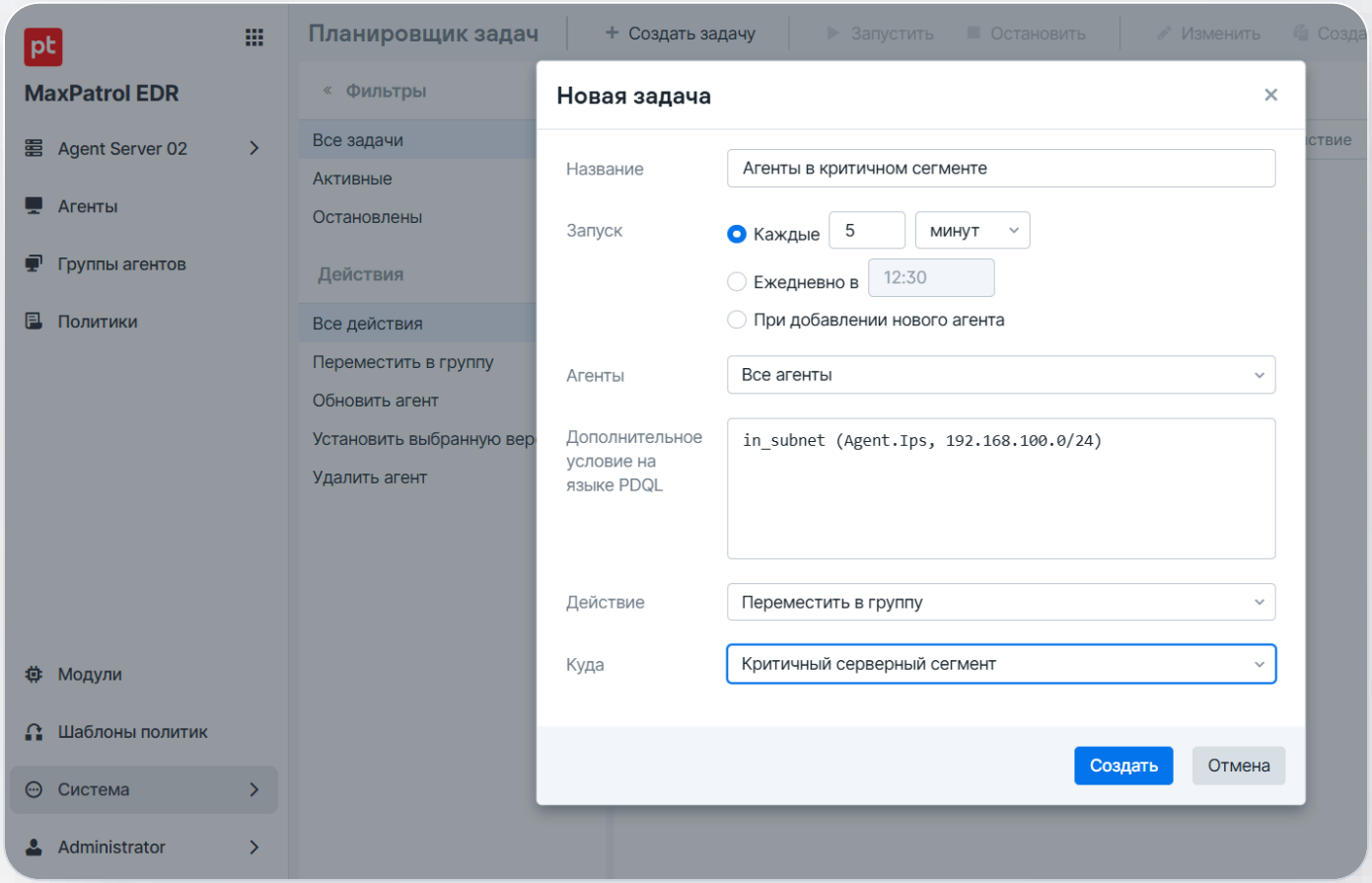
- Авторизация агентов
- Удаление агентов
- Обновление агентов
- Установка выбранной версии агента



Автоматизация работы с агентами

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

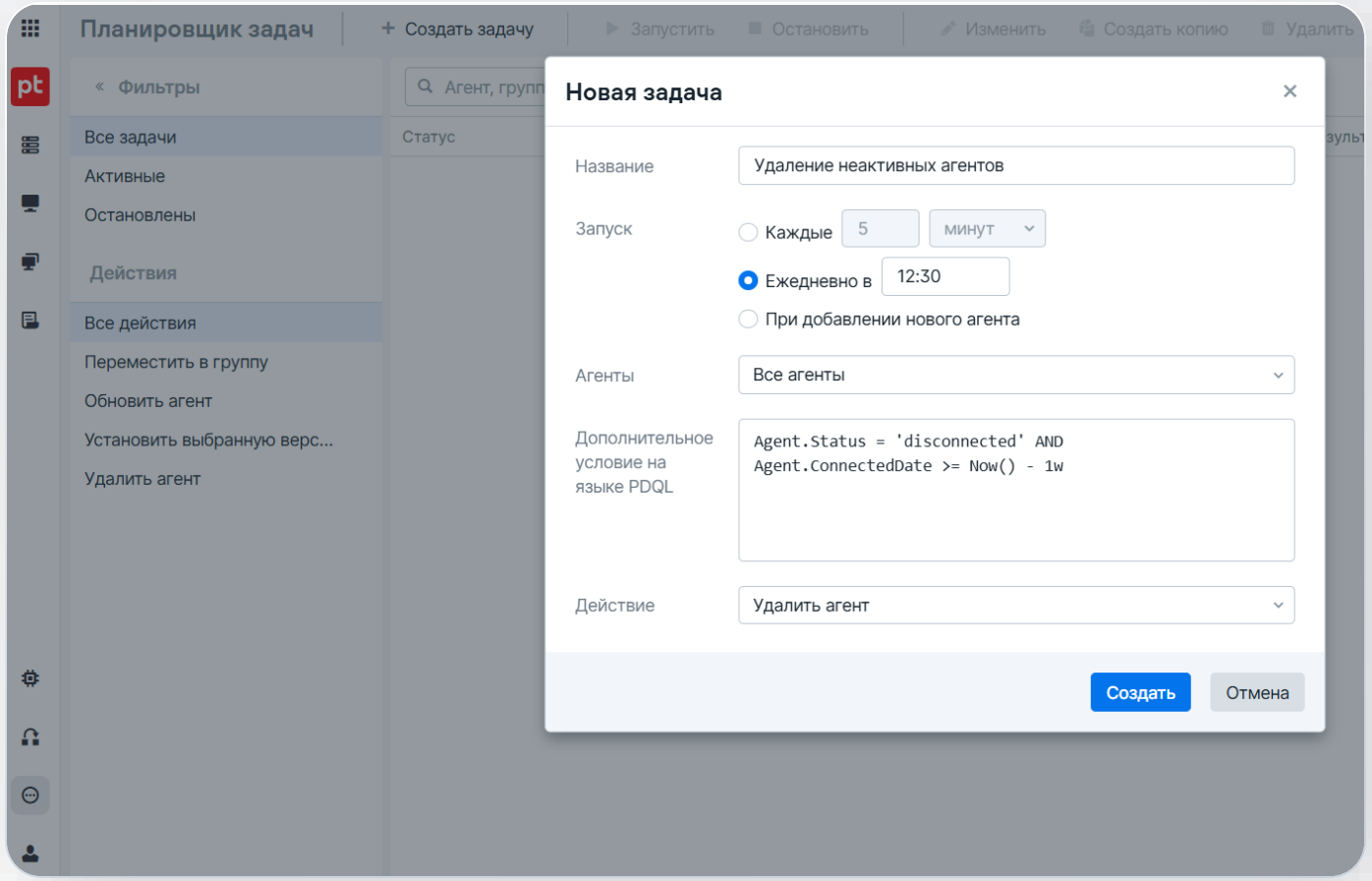
- Отслеживание перемещения агентов по подсетям
- Настройка нужного уровня защиты в зависимости от сетевого сегмента агента



Автоматизация работы с агентами

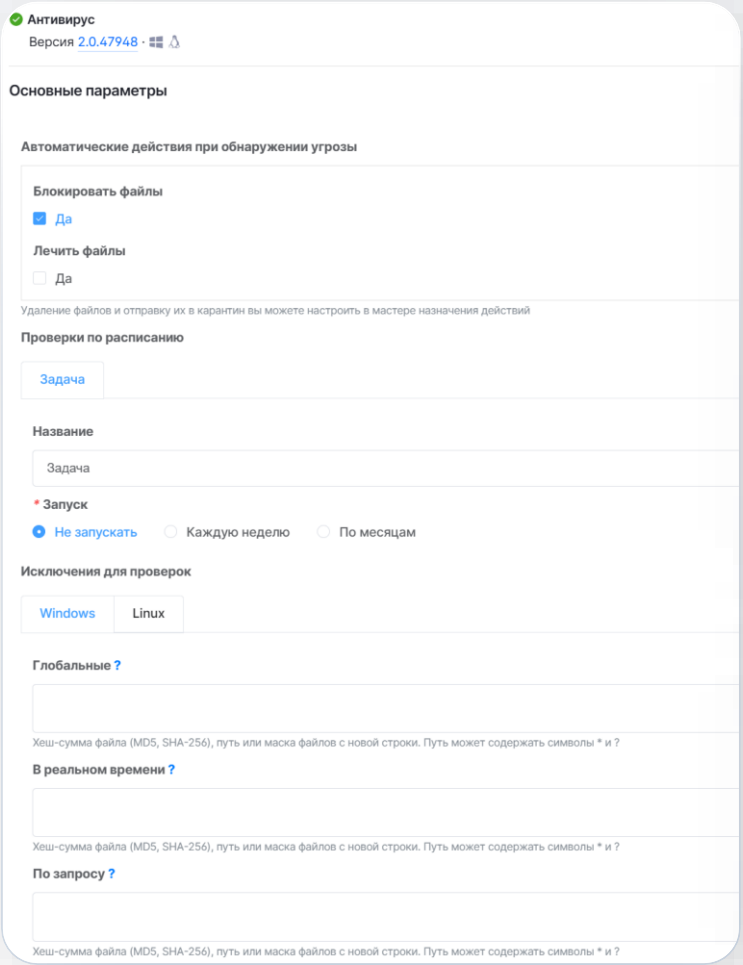
Удаление агентов

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



Эксплуатация MaxPatrol EPP

Антивирусная защита



События

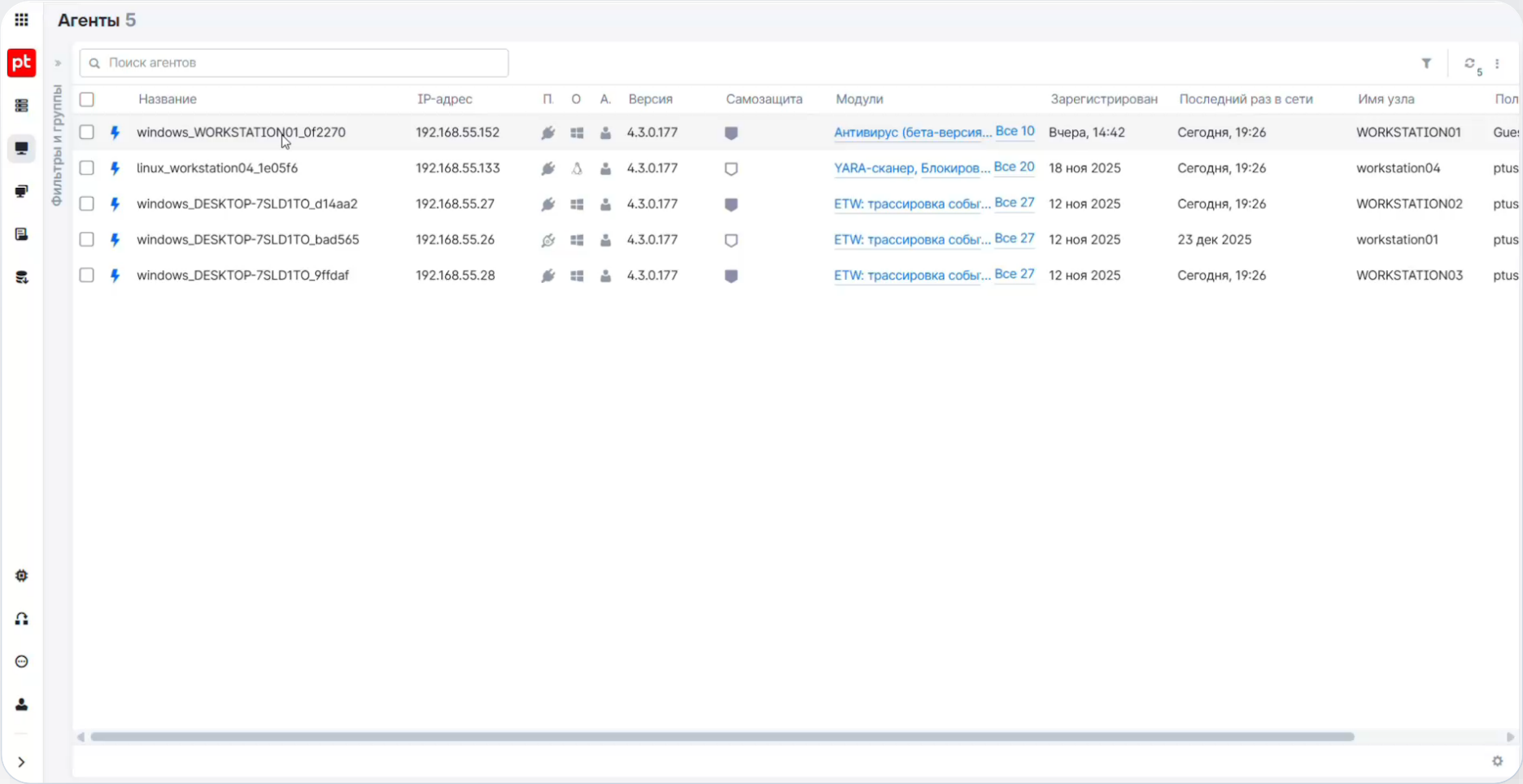
Мастер назначения действий

Событие	Действия
Вредосный файл заблокирован антивирусом	Сохранить в БД Поместить копию файла-объекта в карантин Изолирует в зашифрованном хранилище копию файла-объекта
Файл проверен антивирусом. Вердикт: вредоносный	Сохранить в БД Поместить копию файла-объекта в карантин Изолирует в зашифрованном хранилище копию файла-объекта
Объект проверен антивирусом. Вердикт: вредоносный	Сохранить в БД
Процесс проверен антивирусом. Вердикт: вредоносный	Сохранить в БД Завершить процесс, используя путь к исполняемому файлу и идентификатор процесса-объекта Завершение процесса с указанным путем и идентификатором процесса-объекта
Не удалось выполнить проверку антивирусом	Сохранить в БД
Завершена проверка антивирусом	Сохранить в БД
Запущена проверка антивирусом	Сохранить в БД
Антивирусные базы обновлены	Сохранить в БД
Не удалось включить антивирус	Сохранить в БД

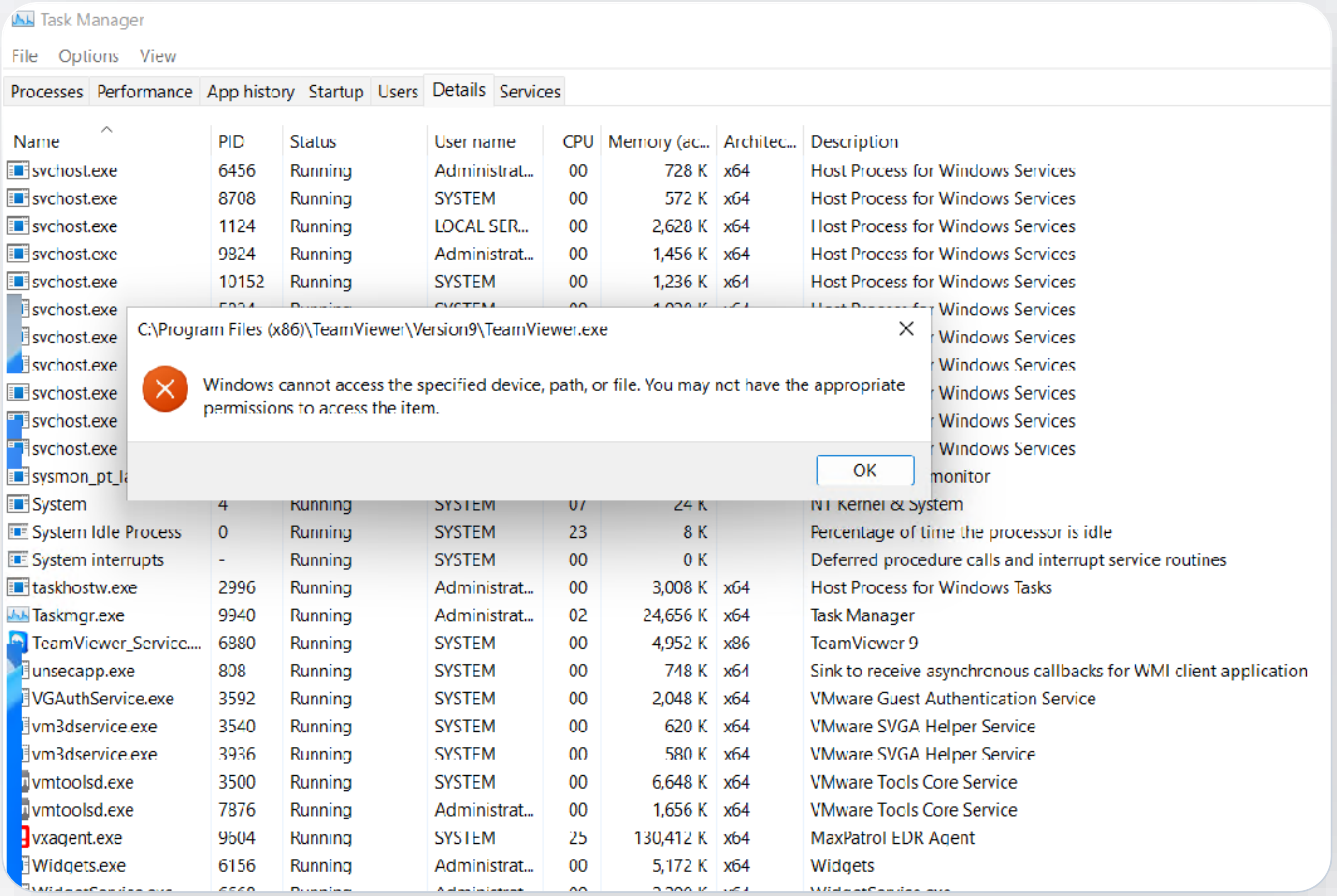
Действия

Идентификатор	Описание
Запустить быструю проверку антивирусом	Проверка важных системных файлов антивирусом
Запустить полную проверку антивирусом	Полная проверка узла антивирусом
Проверить оперативную память и автоматически запускаемые файлы антивирусом	Проверка оперативной памяти и автоматически запускаемых файлов
Проверить папку антивирусом	Проверка папки антивирусом
Проверить файл антивирусом	Проверка файла антивирусом

Антивирусная защита



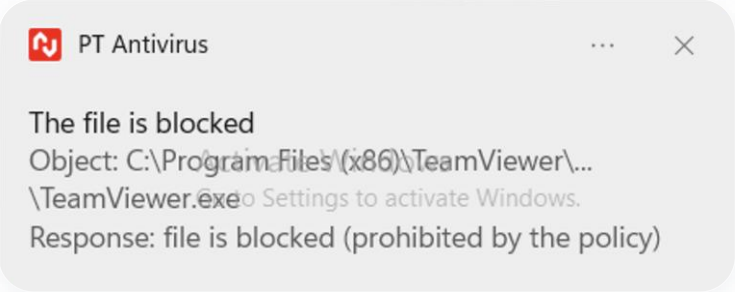
Контроль приложений



Блокировка запуска приложений

- По контрольной сумме (MD5, SHA-256) исполняемого файла
- По пути или маске файлов

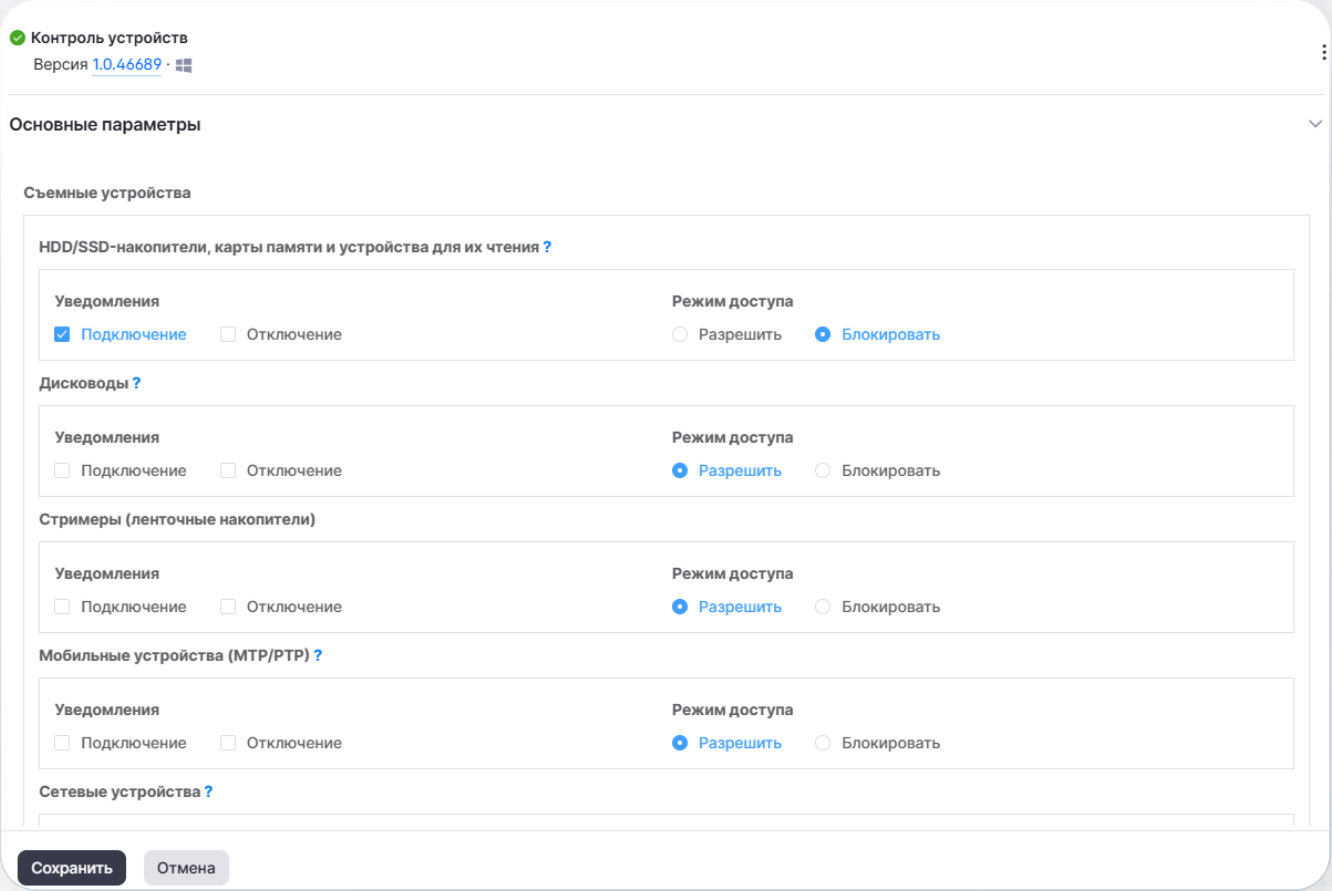
Можно оставить комментарий к каждому файлу, который будет добавлен в событие безопасности



Контроль подключаемых устройств

Блокируем подключение внешних устройств к защищаемым компьютерам с помощью драйвера

- Жесткие диски и карты памяти
- Съемные диски (дисководы)
- Стримеры (ленточные накопители)
- Мобильные устройства (MTP, PTP)
- Сетевые устройства
- Принтеры
- Сканеры и фотокамеры
- Видеокамеры
- Smart card readers
- Generic USB и другие



АнтиШифровальщик

- В основу технологии легли результаты исследования актуальных семейств шифровальщиков (54 шт.) и вайперов (19 шт.)
- Реальные атаки: учитывался опыт TI и IR
- Технология проверена на оригинальных образцах ВПО и уже обкатана внутри Positive Technologies

1 Резервные копии

Драйверная часть обеспечивает актуальность теневых копий защищаемых файлов

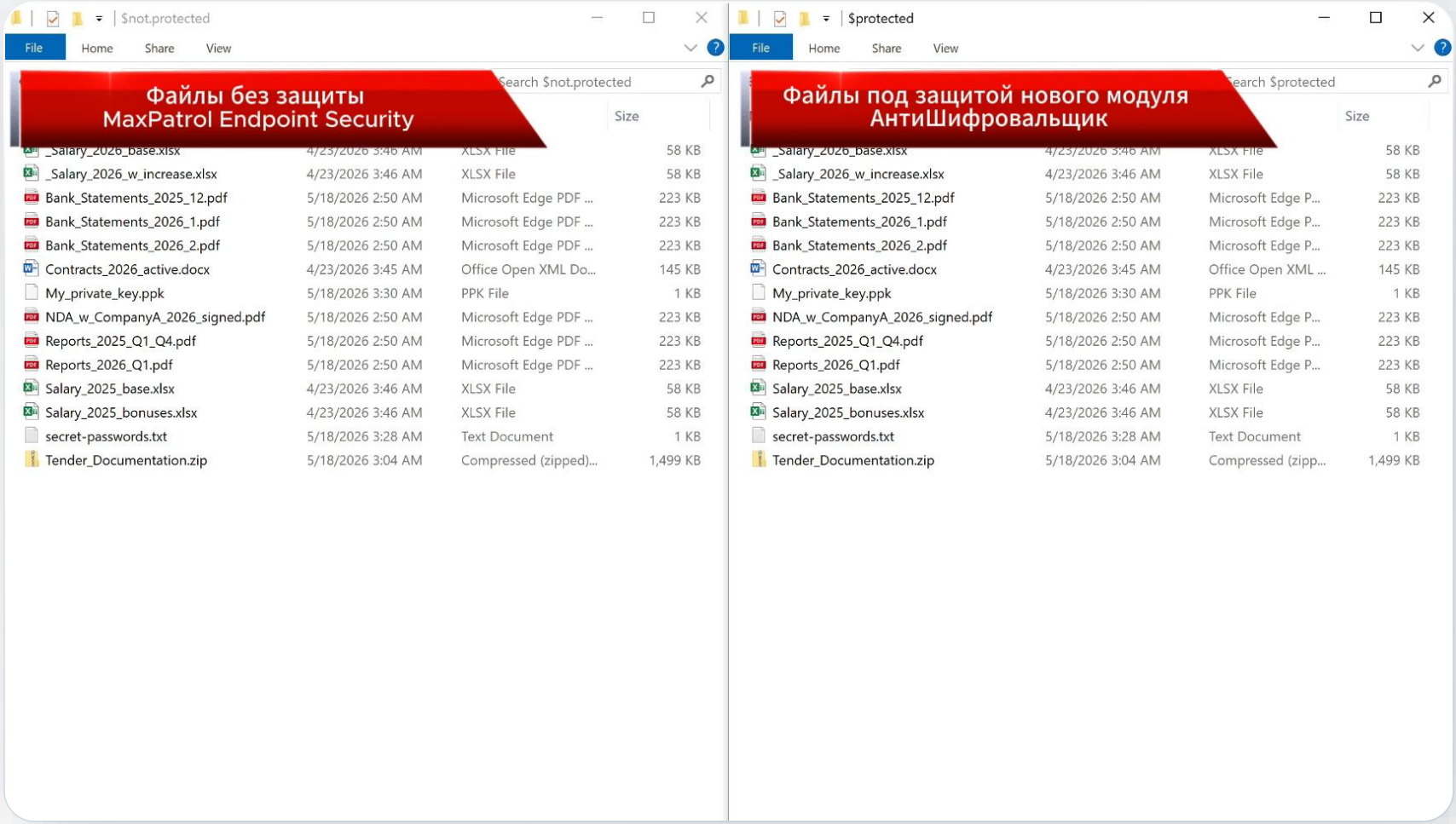
2 Поведенческие эвристики

Поведение каждого стартующего процесса оценивается по шагам

3 Восстановление файлов

Мгновенное возобновление работы бизнеса и устранение последствий атаки

АнтиШифровальщик



Эксплуатация MaxPatrol EDR

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
- eBPF

Управление 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-специалистов 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, eBPF
- 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

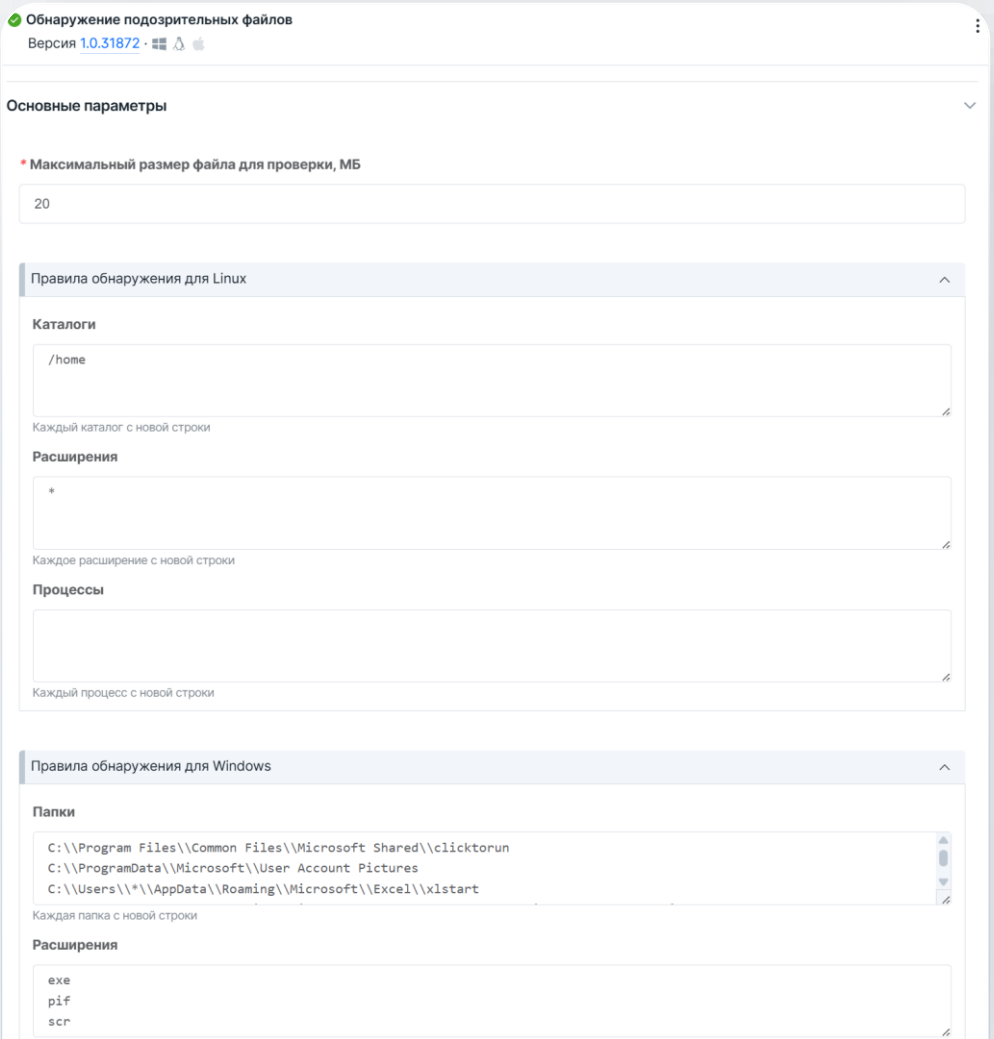
- Выявляет опасные файлы и процессы
- Проверка файлов и процессов YARA-правилами — 6000 «из коробки»
- Проверка по хеш-суммам файлов — более 65 000 (на основе перечня самых актуальных угроз от PT ESC)

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

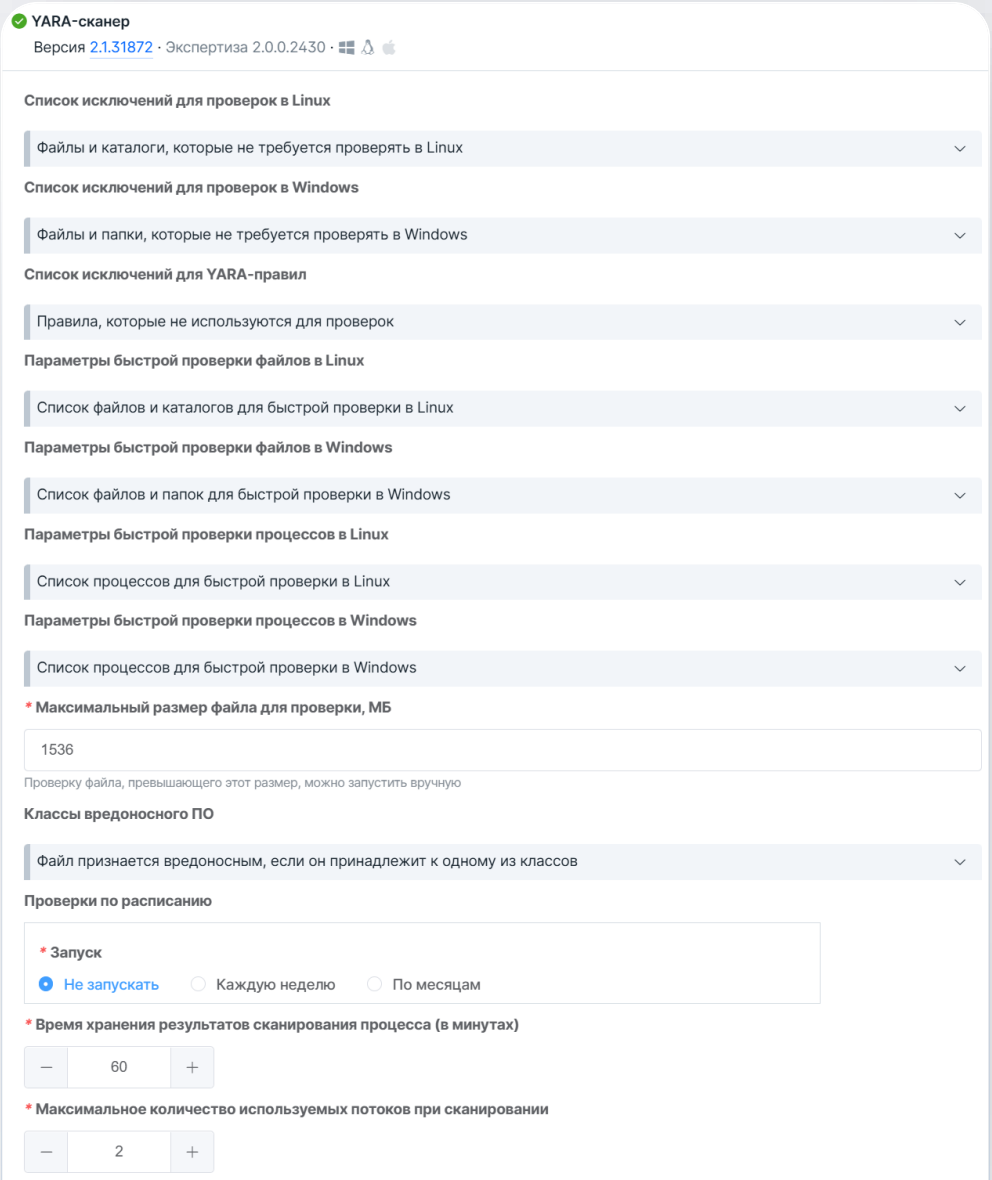
Обнаружение подозрительных файлов

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



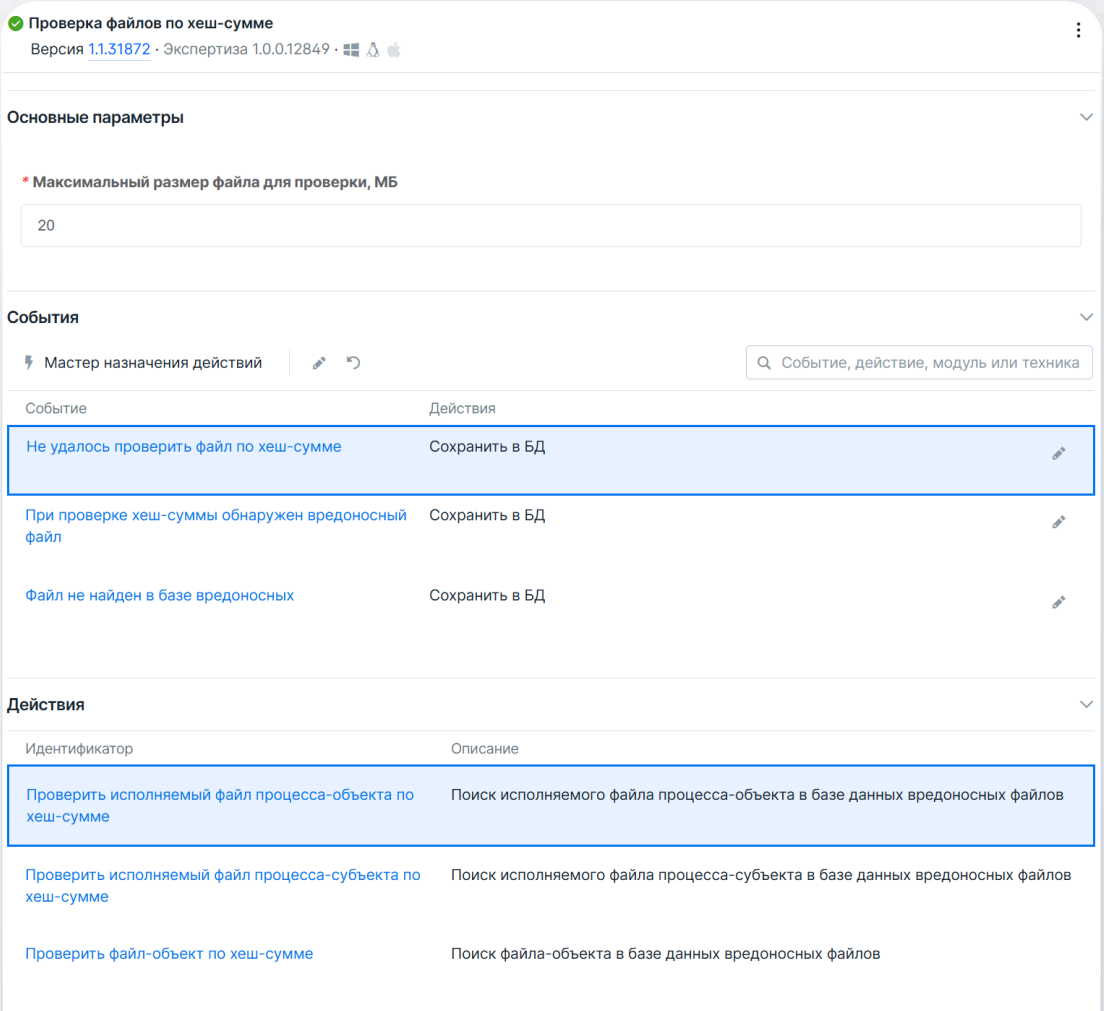
YARA-сканер

- 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



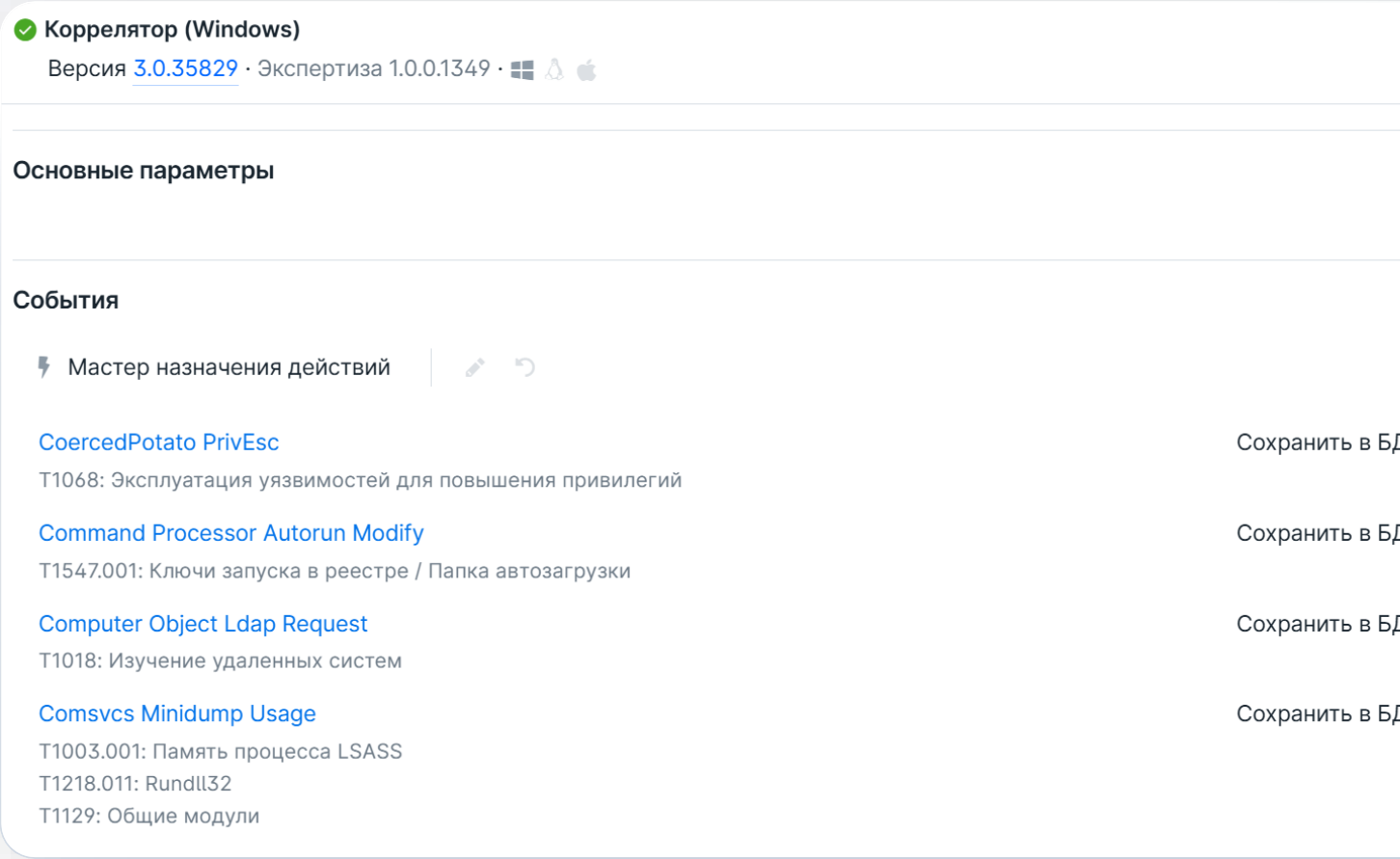
Проверка файлов по хеш-сумме

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



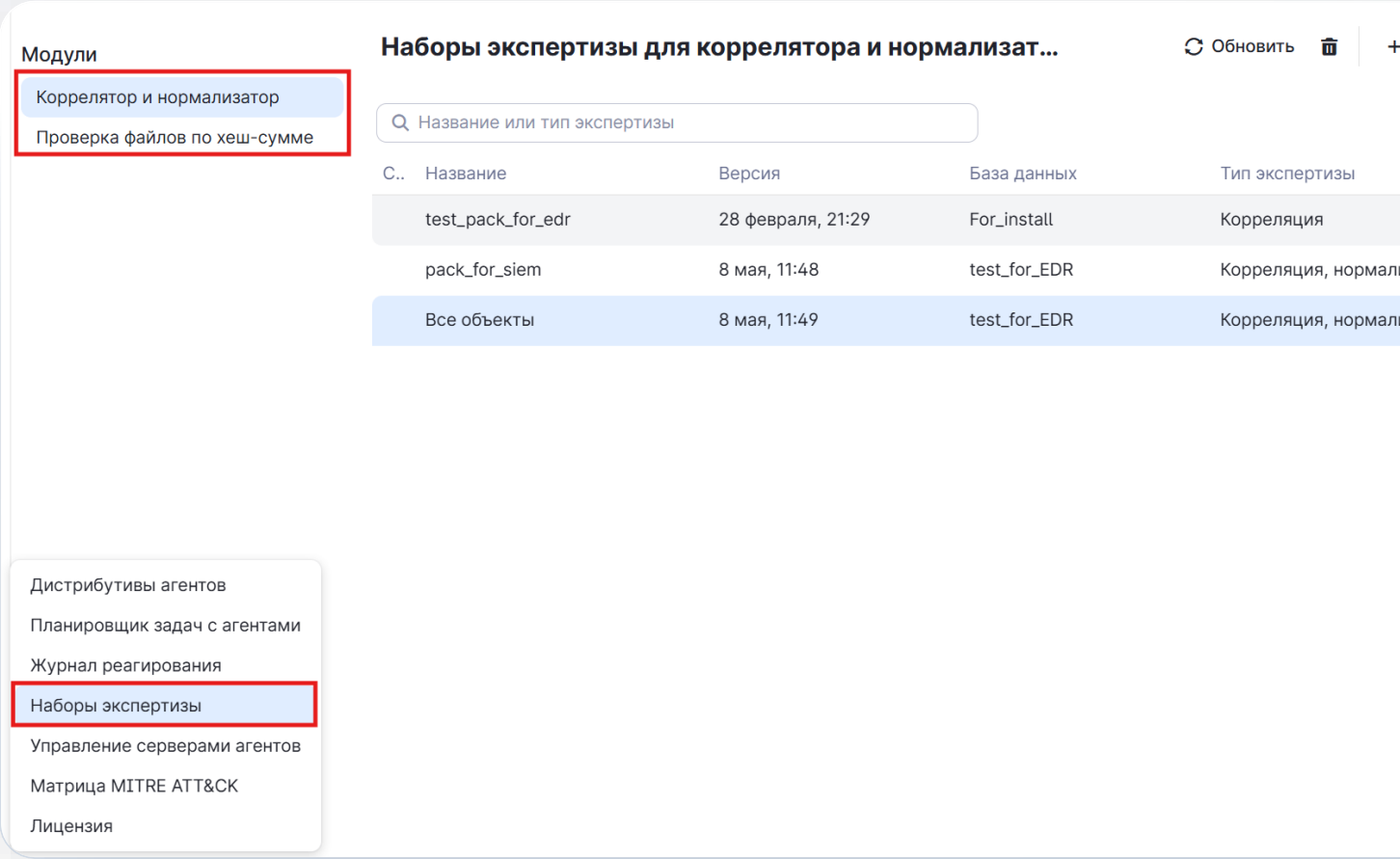
Поведенческий анализ

- 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 и хеш-суммы



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 модулей, доступных на операционных системах

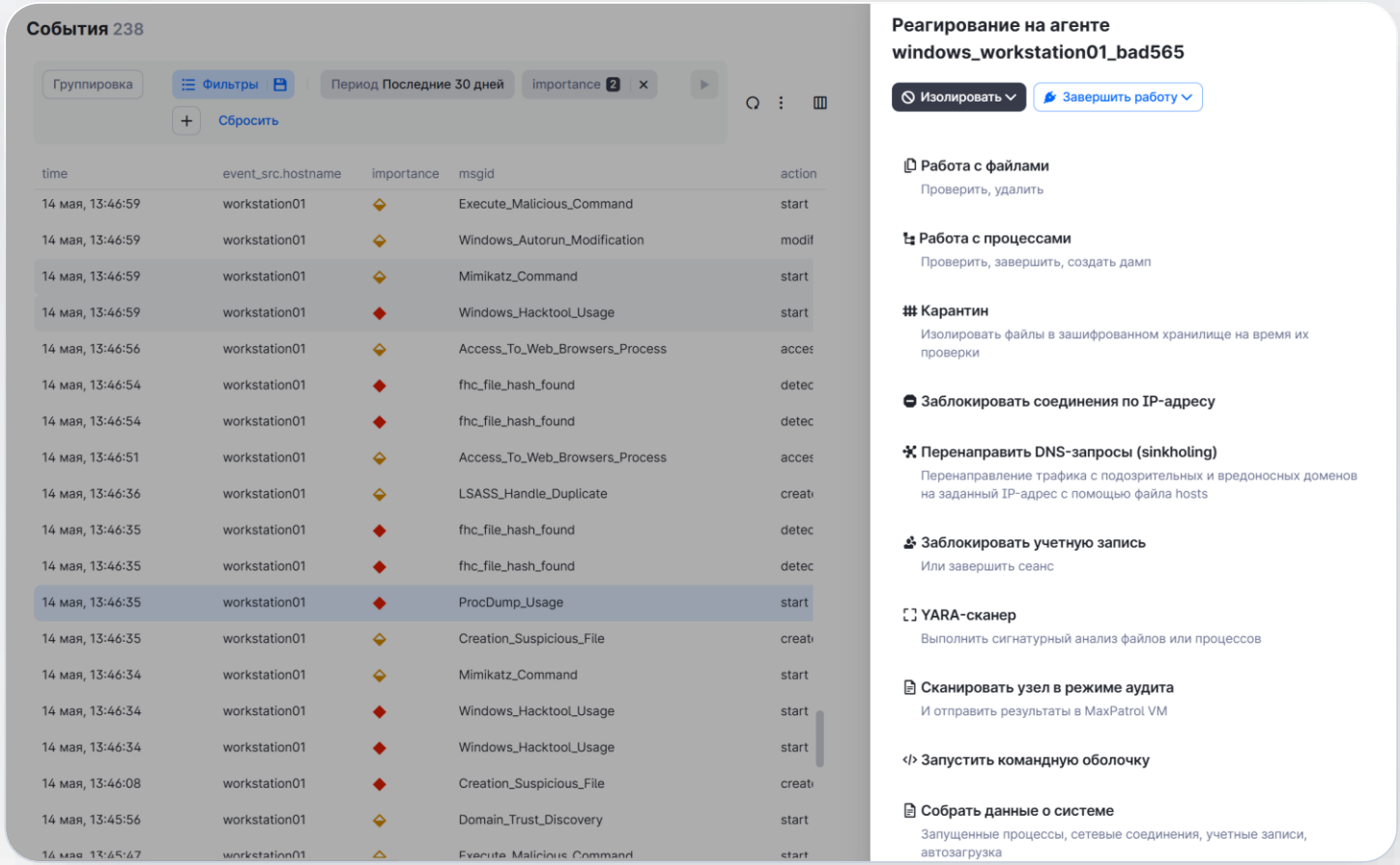
Реагирование

Реагирование
на угрозы в ручном
и автоматическом
режимах

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

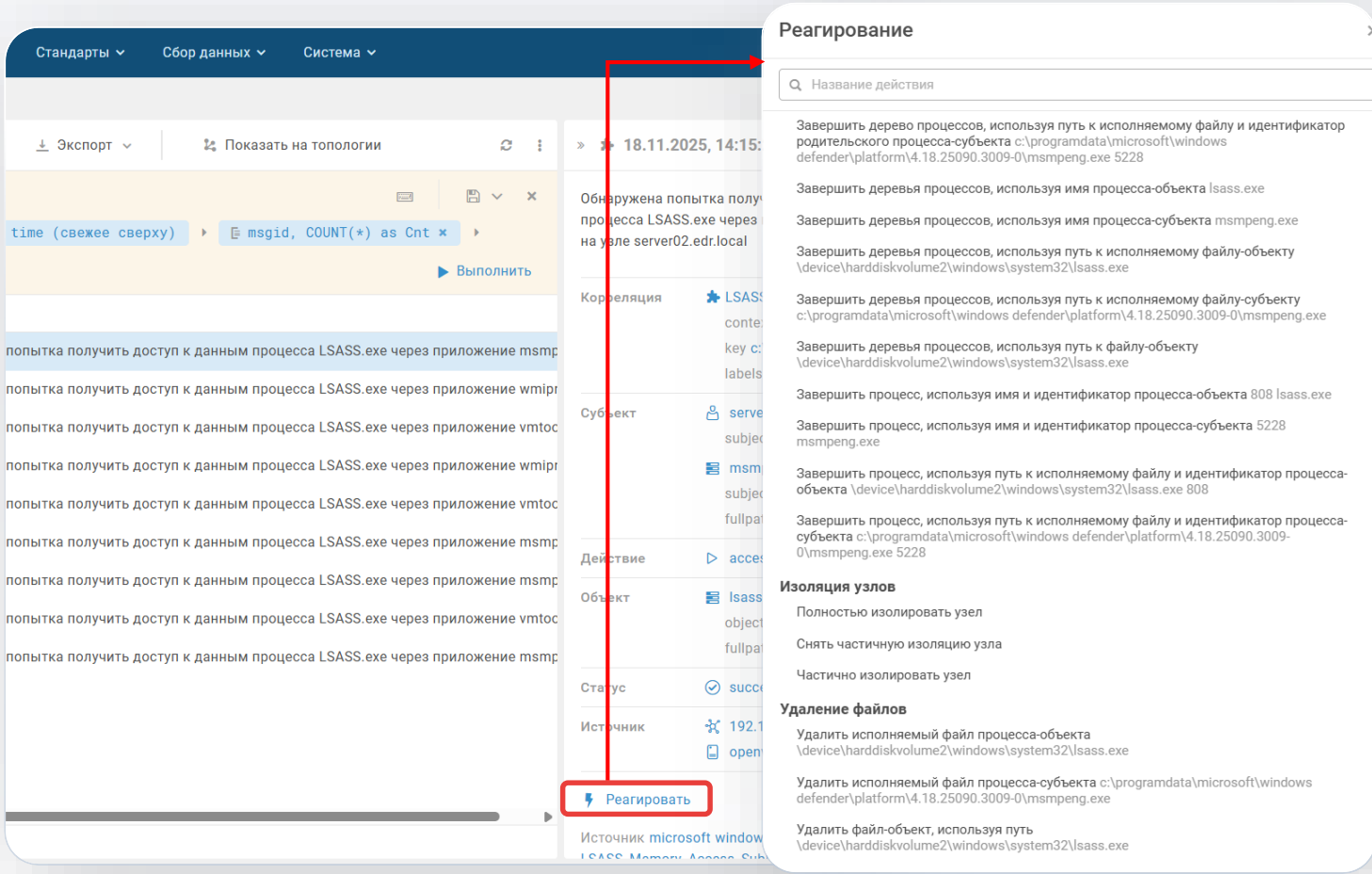
Реагирование из карточки события в два клика

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

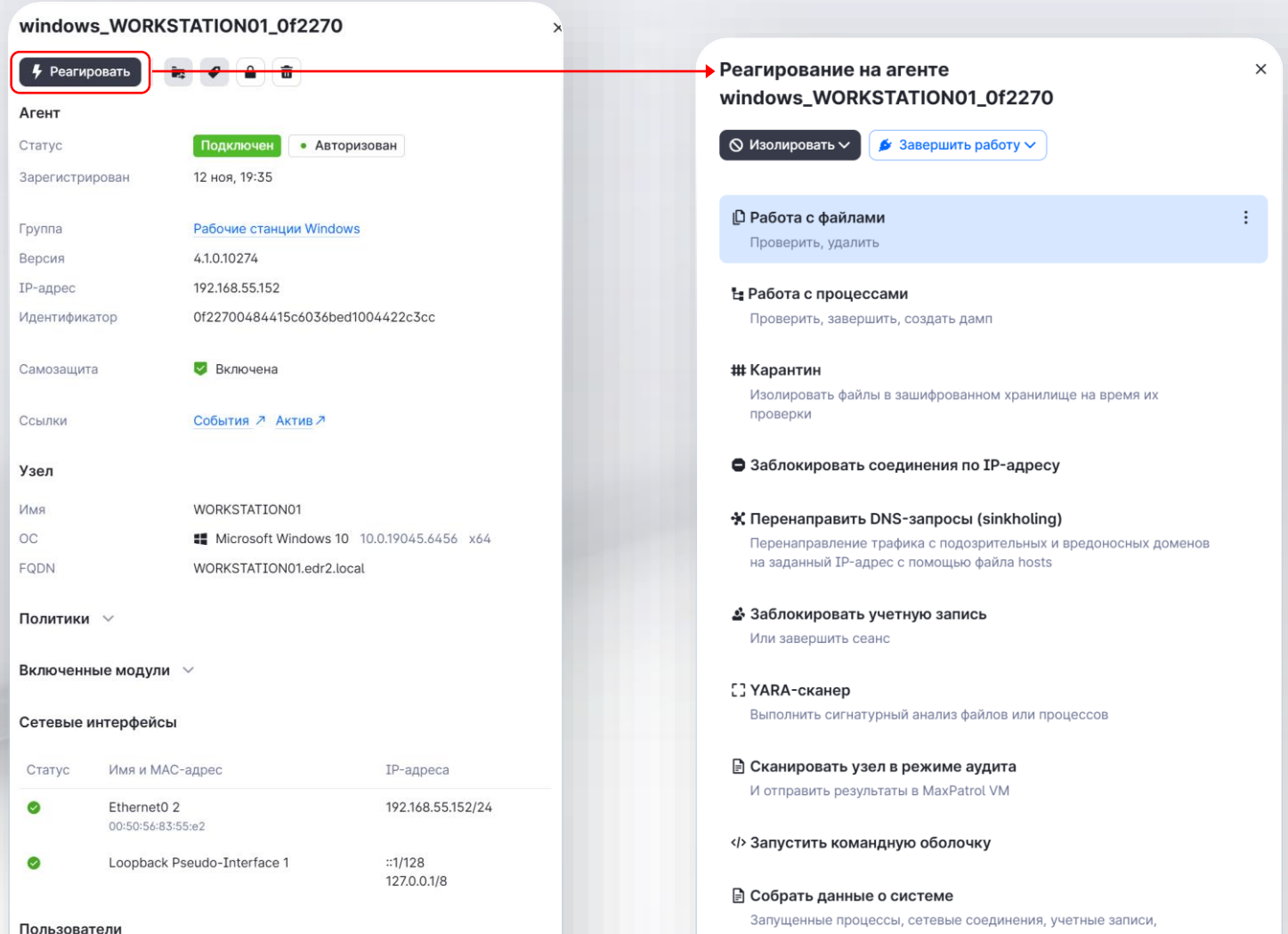


Реагирование из карточки события в MaxPatrol SIEM

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



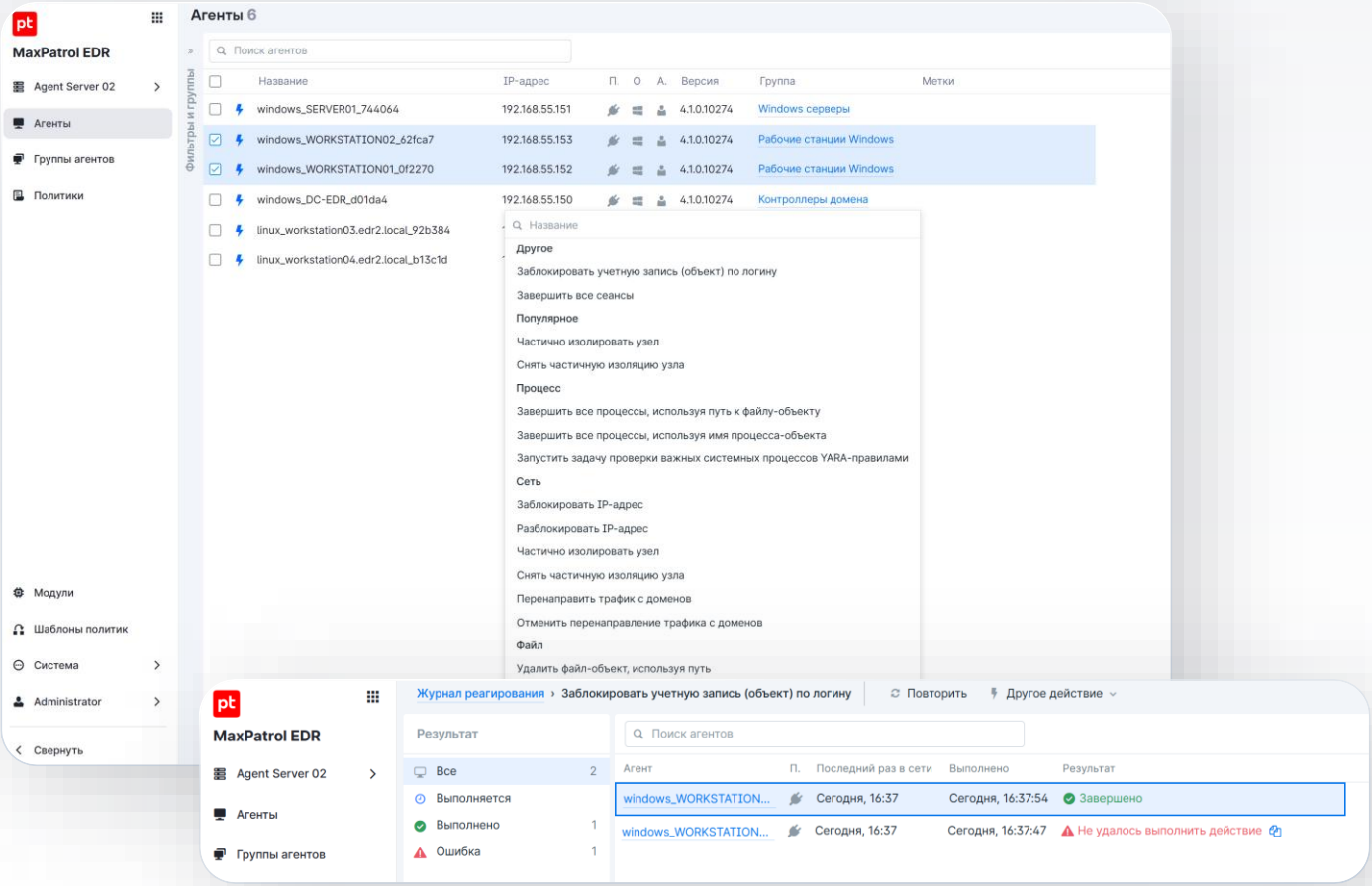
Реагирование из карточки агента в три клика



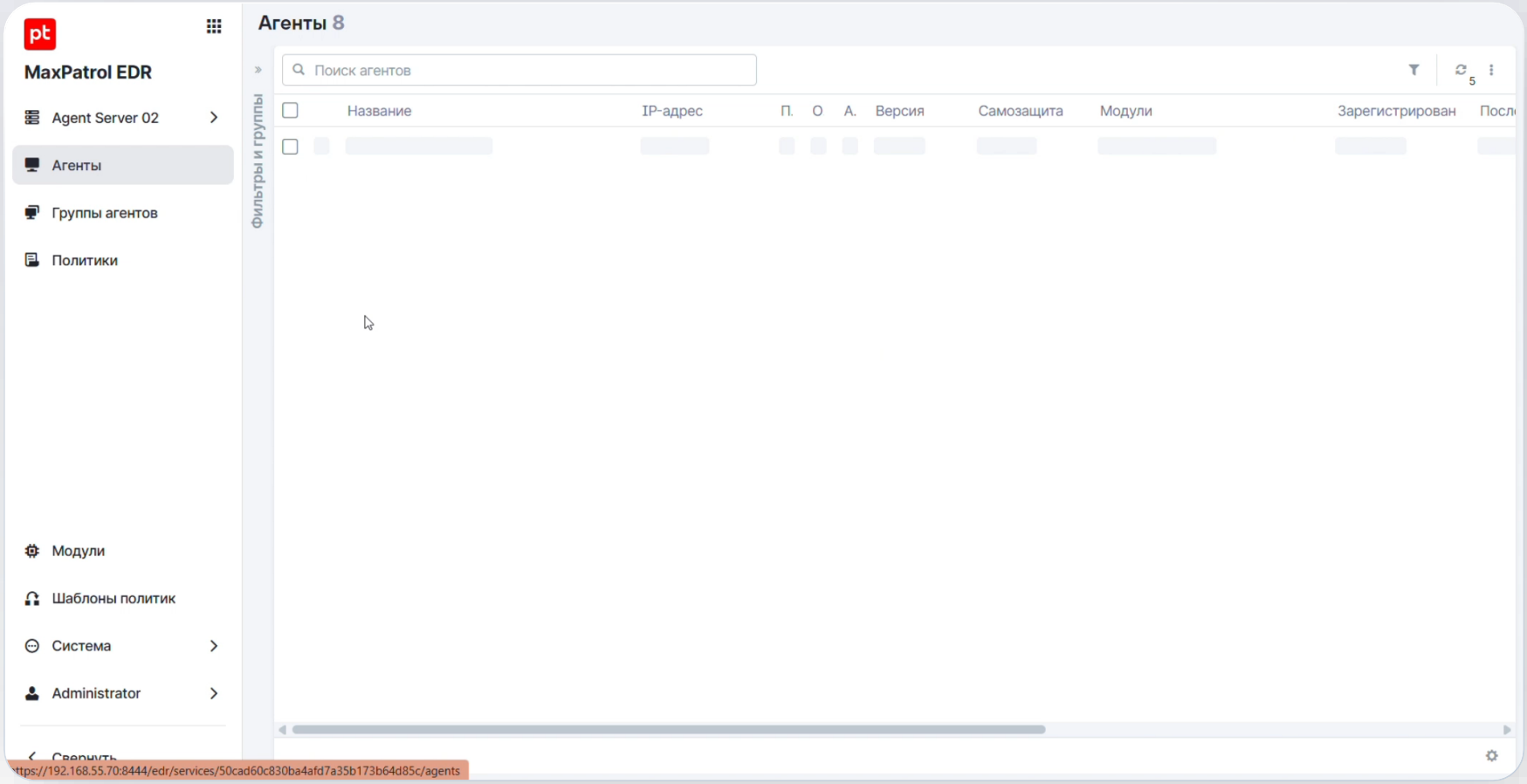
Реагирование на множестве агентов

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

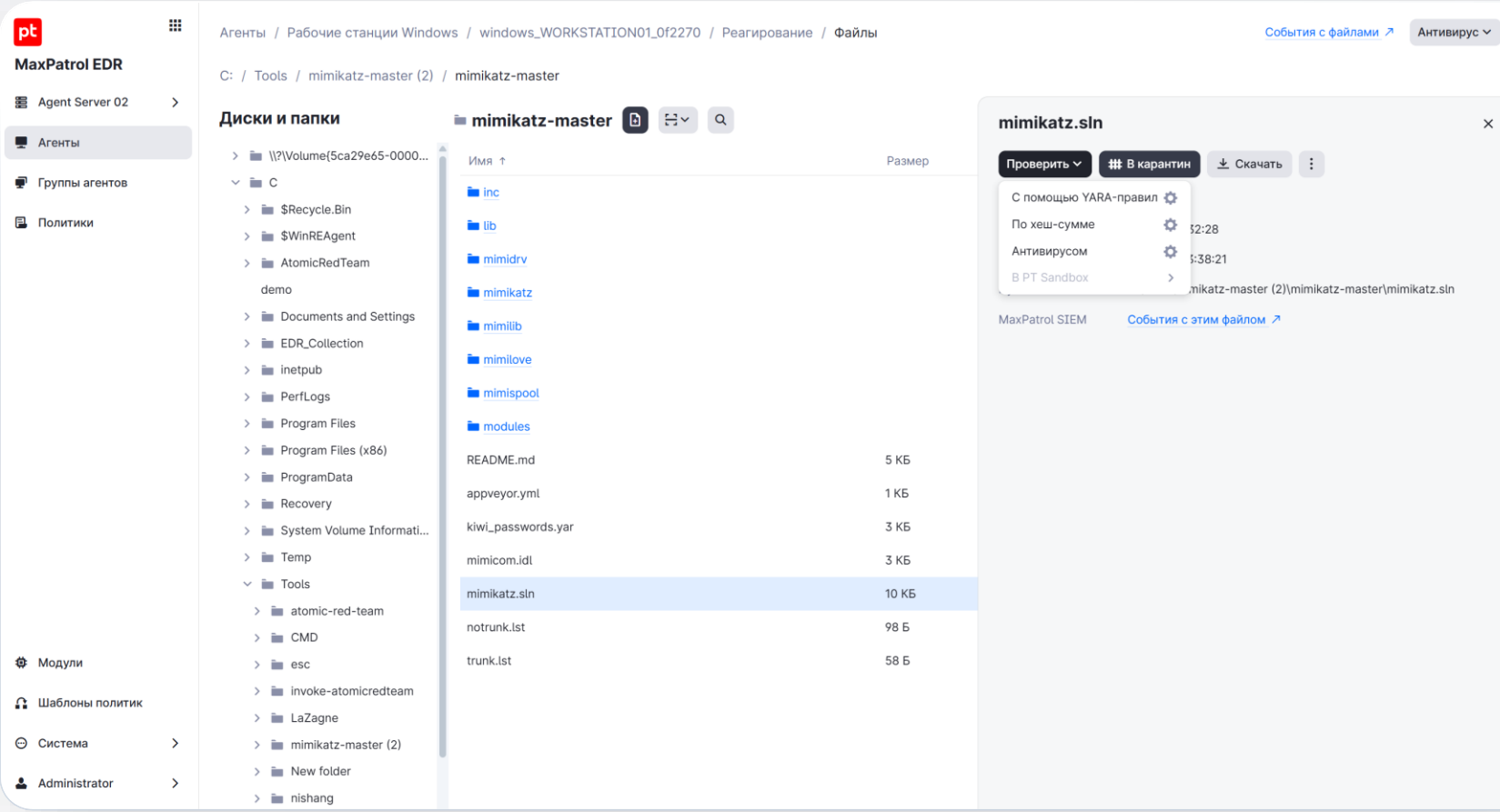


Пример реагирования на множестве агентов



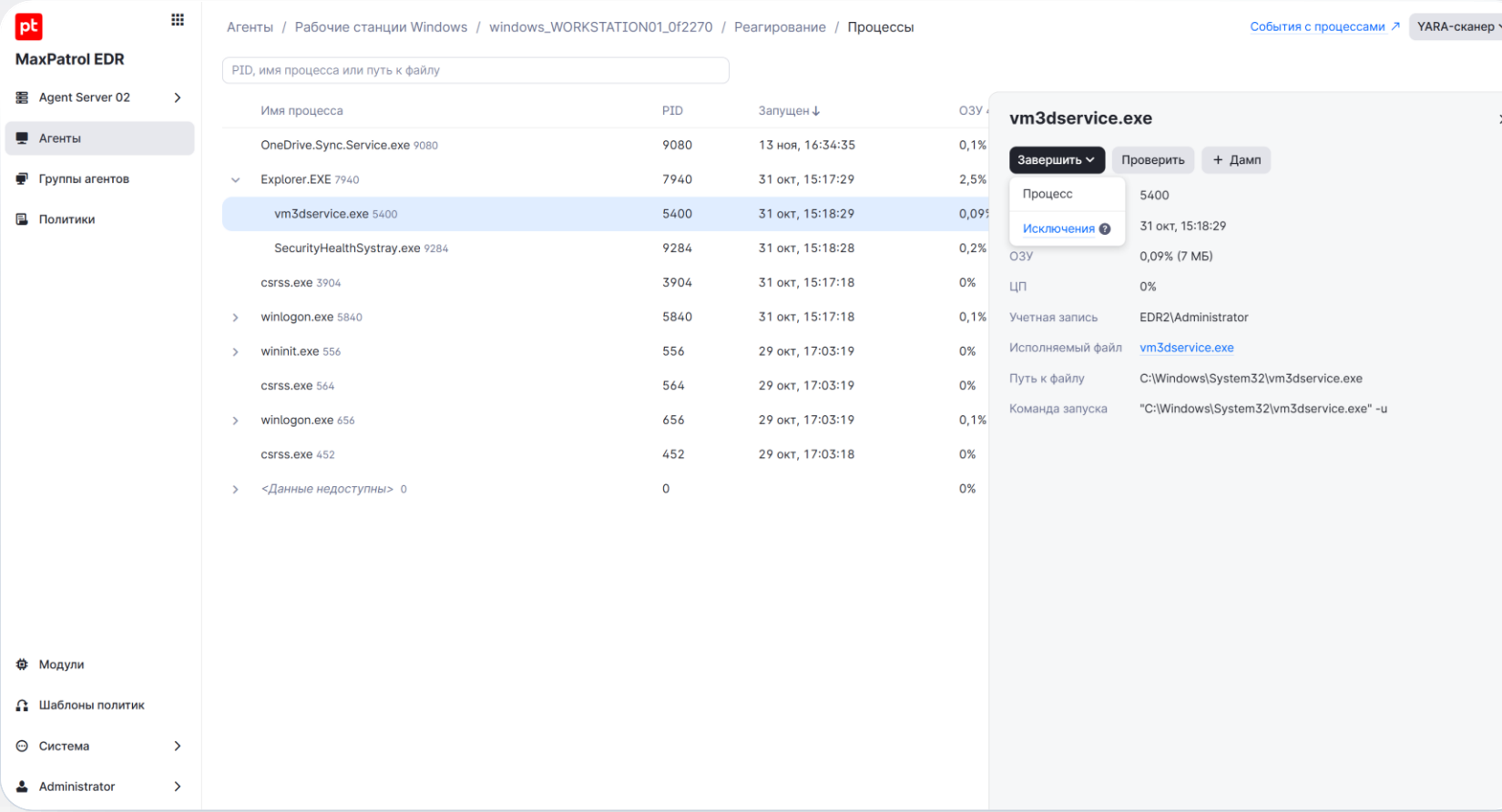
Работа с файлами

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



Работа с процессами

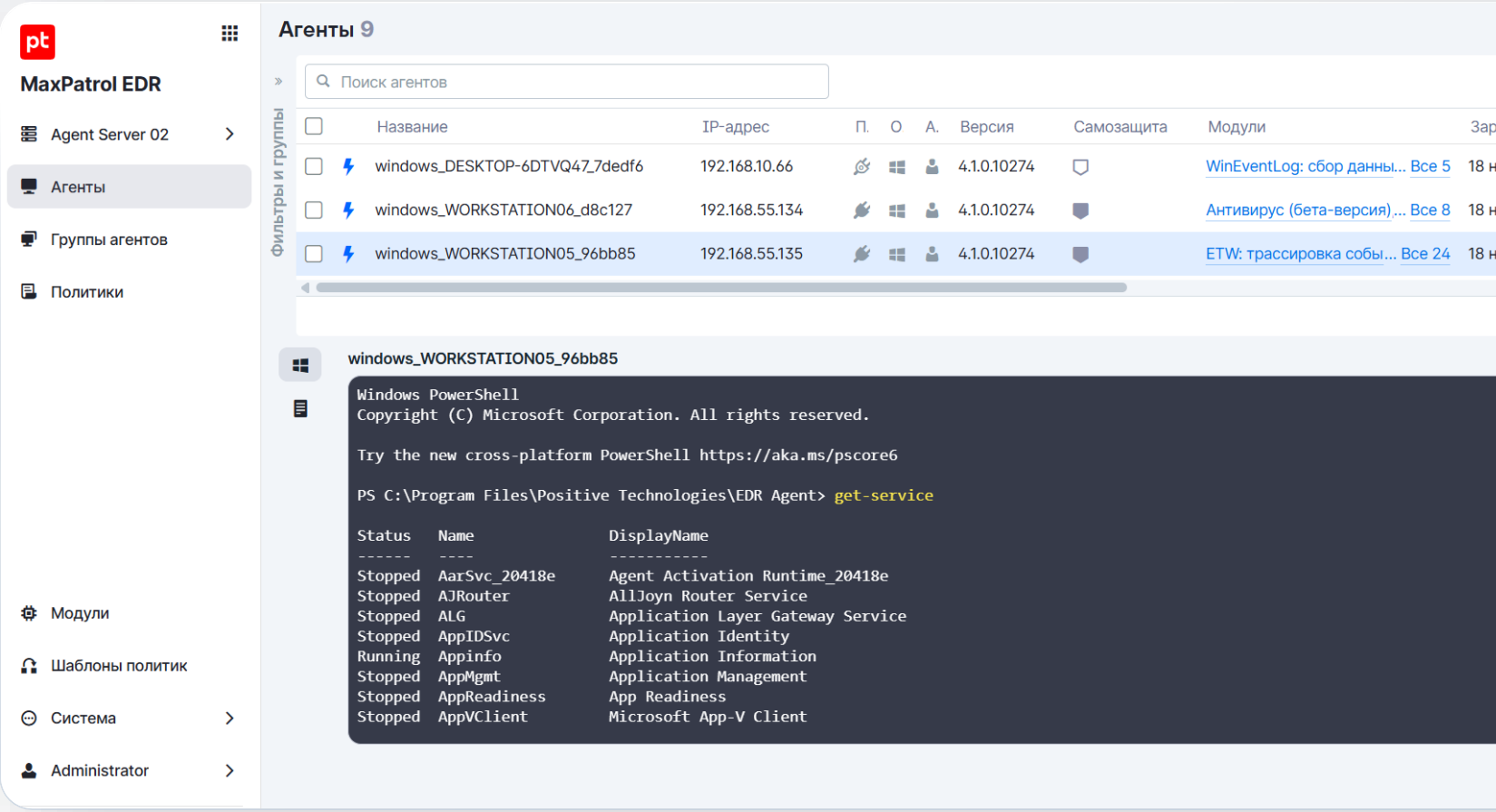
- Детальная информация обо всех запущенных процессах
- Поиск процессов по атрибутам
- Все операции с процессами в одном окне
- Быстрый переход к исполняемым файлам и операциям над ними
- Переход к событиям с процессами в один клик



Расширенные возможности реагирования

Remote shell

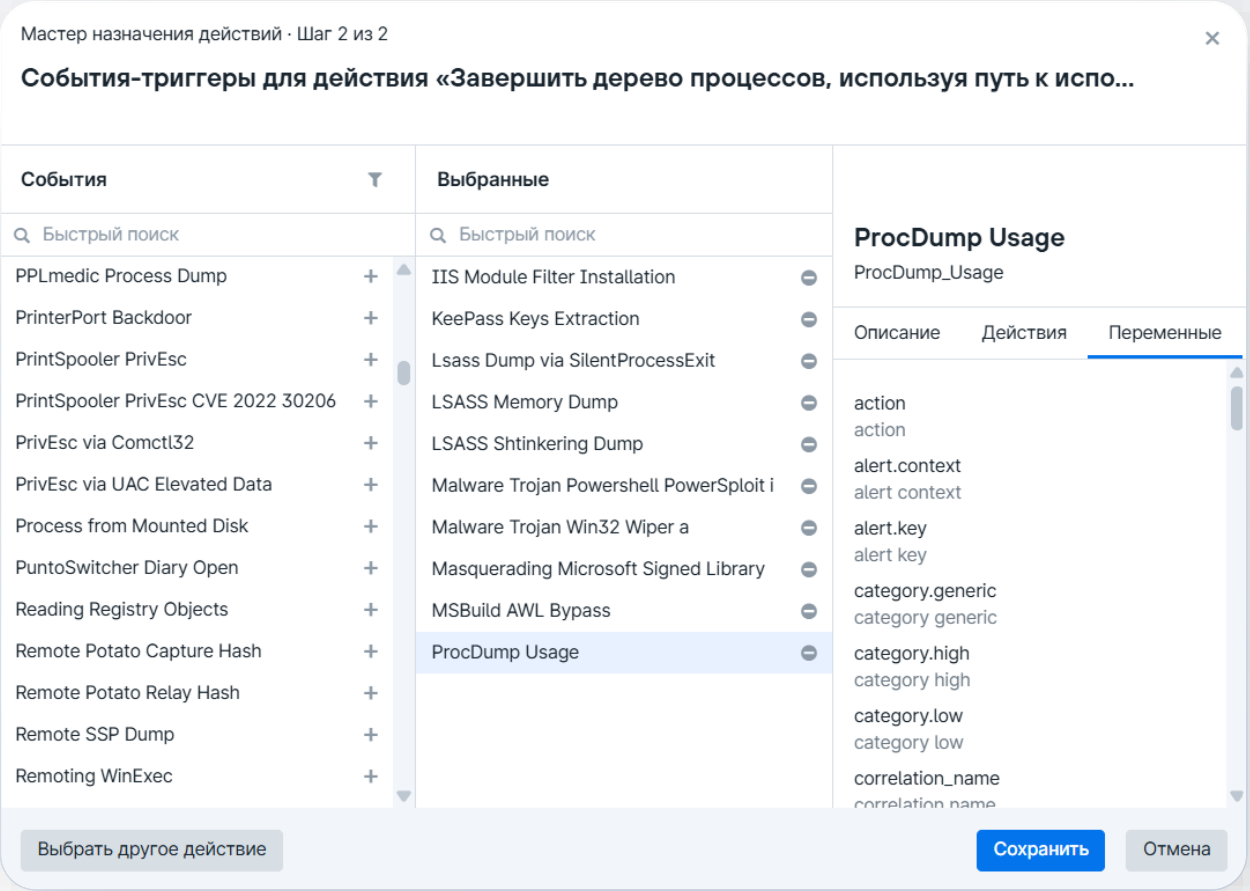
- Работает на узлах под управлением Windows и Linux
- Команды выполняются в PowerShell или Bash
- Выполняет расследование инцидентов, сбор необходимых данных
- Устраняет нарушения независимо от того, где находится конечное устройство
- Все выполненные команды сохраняются в журнале
- Доступ к журналу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



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

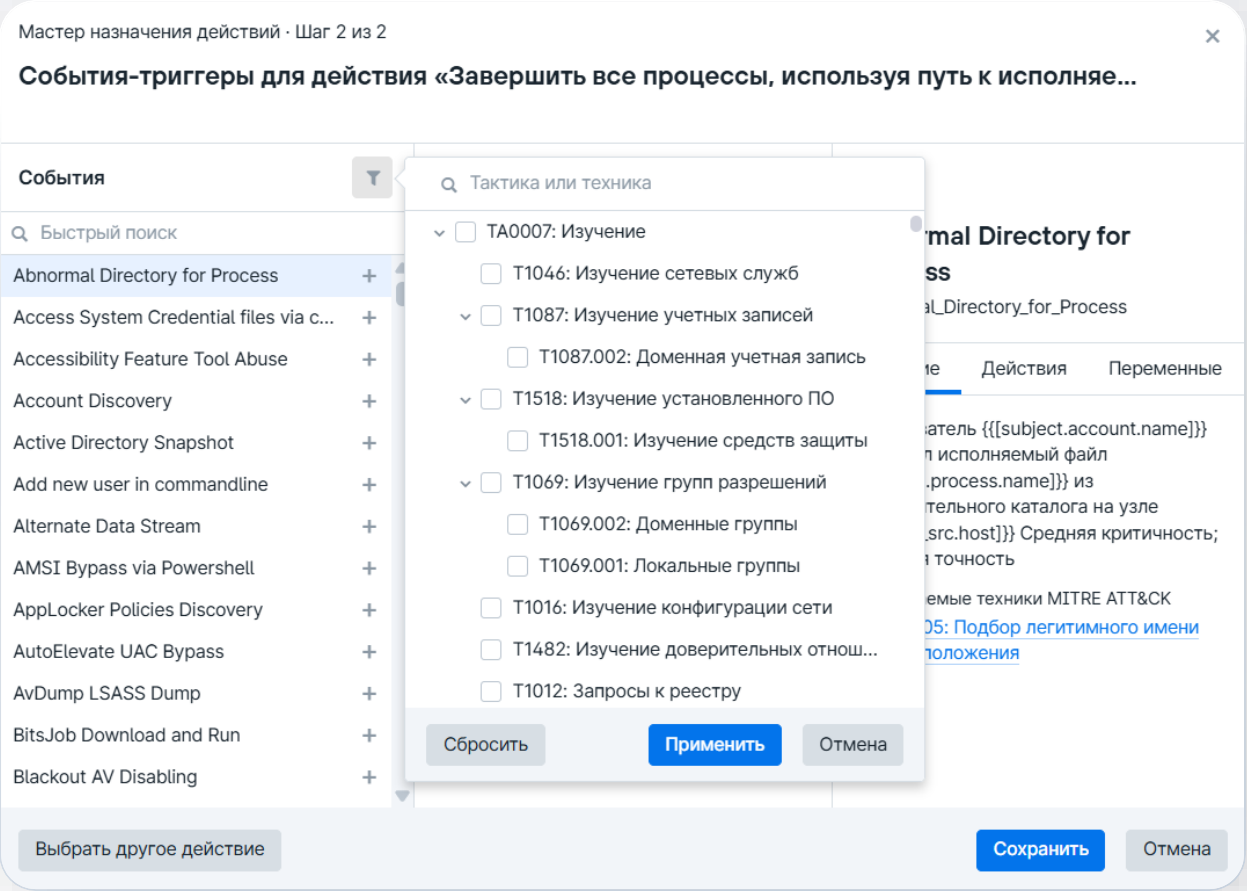


* Если не подразумевают взаимодействия с внешними системами

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

MaxPatrol EDR API 1.0.0 OAS 3.0

Серверы агентов

POST `/api/edr/external/v1/agent_servers/list` Список серверов агентов

Группы агентов

POST `/api/edr/external/v1/groups/list` Список групп агентов

Агенты

POST `/api/edr/external/v1/agents/list` Список агентов

POST `/api/edr/external/v1/agents/change_group` Перемещение агентов в другую группу

Реагирование

POST `/api/edr/external/v1/agent_actions/list` Список доступных действия для реагирования на агенте

POST `/api/edr/external/v1/agent_actions/execute` Запуск реагирования

Сценарий применения

Возможности массового реагирования

Расследование инцидента

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

Устранение

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

Постанализ

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

Остановка распространения

Изолирую от сети выборку устройств

Снятие ограничений

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

Уже используете решения Positive Technologies?

Усильте их за счет
MaxPatrol Endpoint Security

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 NAD

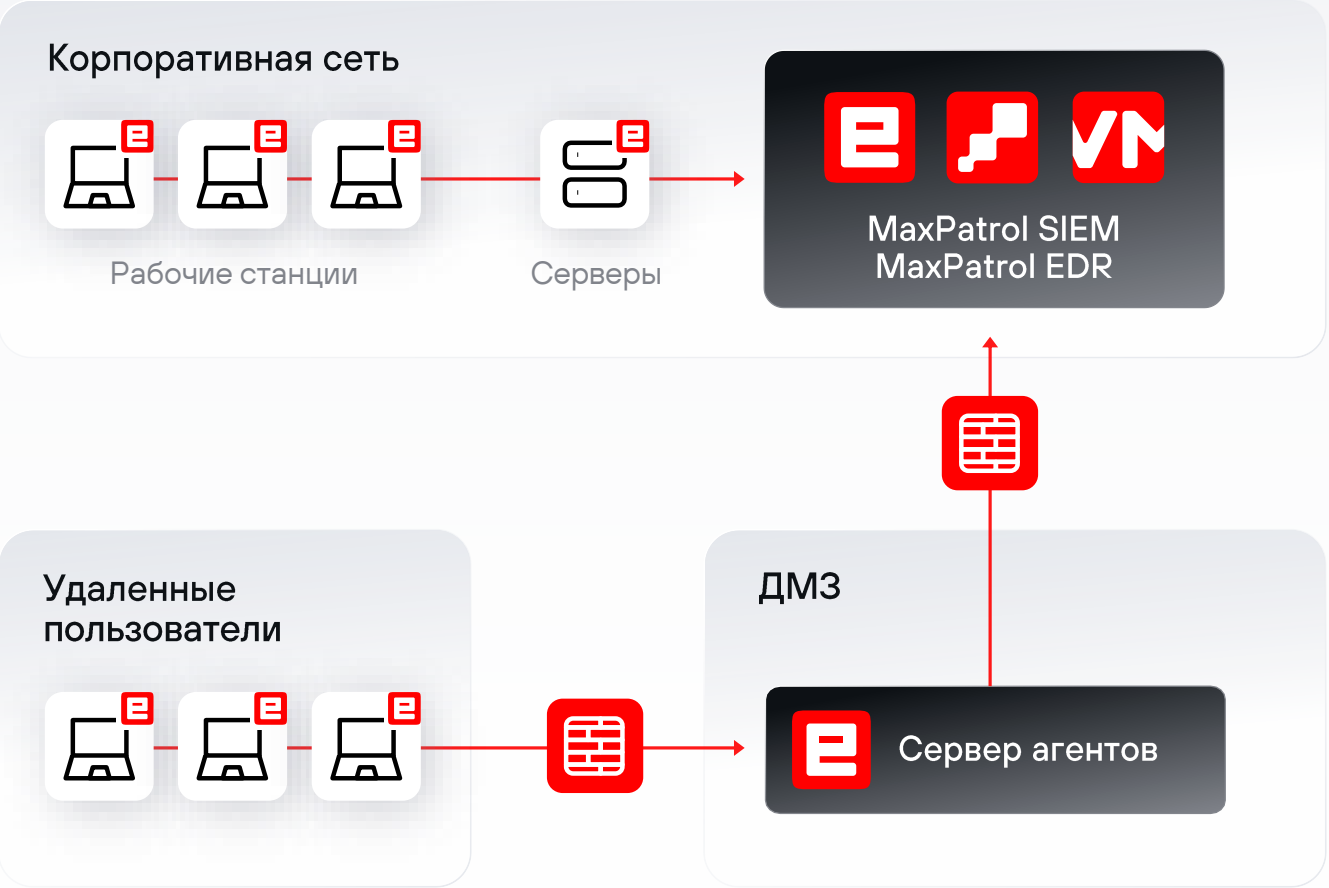
Интеграция с MaxPatrol Endpoint Security усиливает PT NAD в части сдерживания, открывая возможность блокировки угроз, выявленных в сетевом трафике.

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

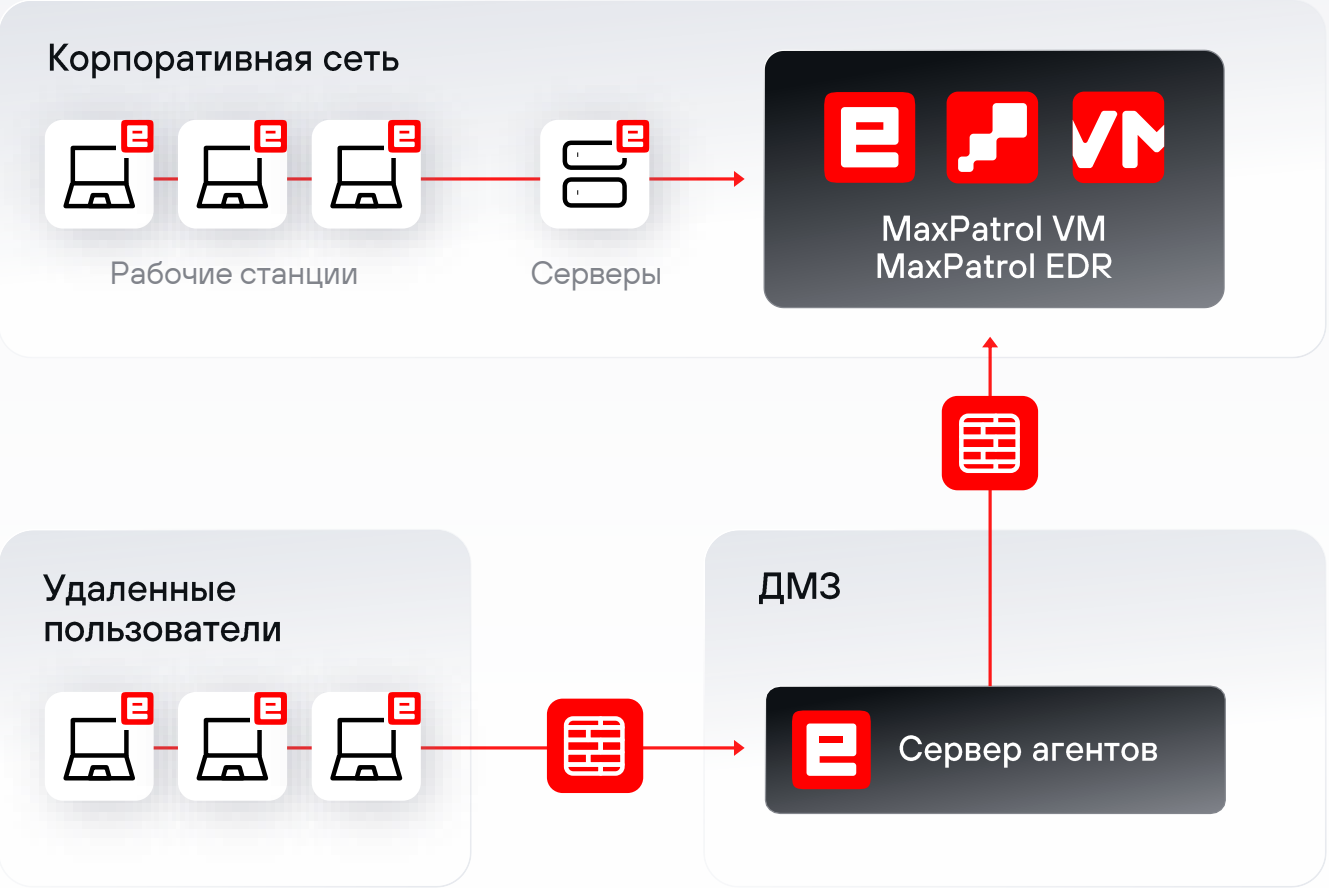
MaxPatrol EDR + MaxPatrol SIEM

- 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



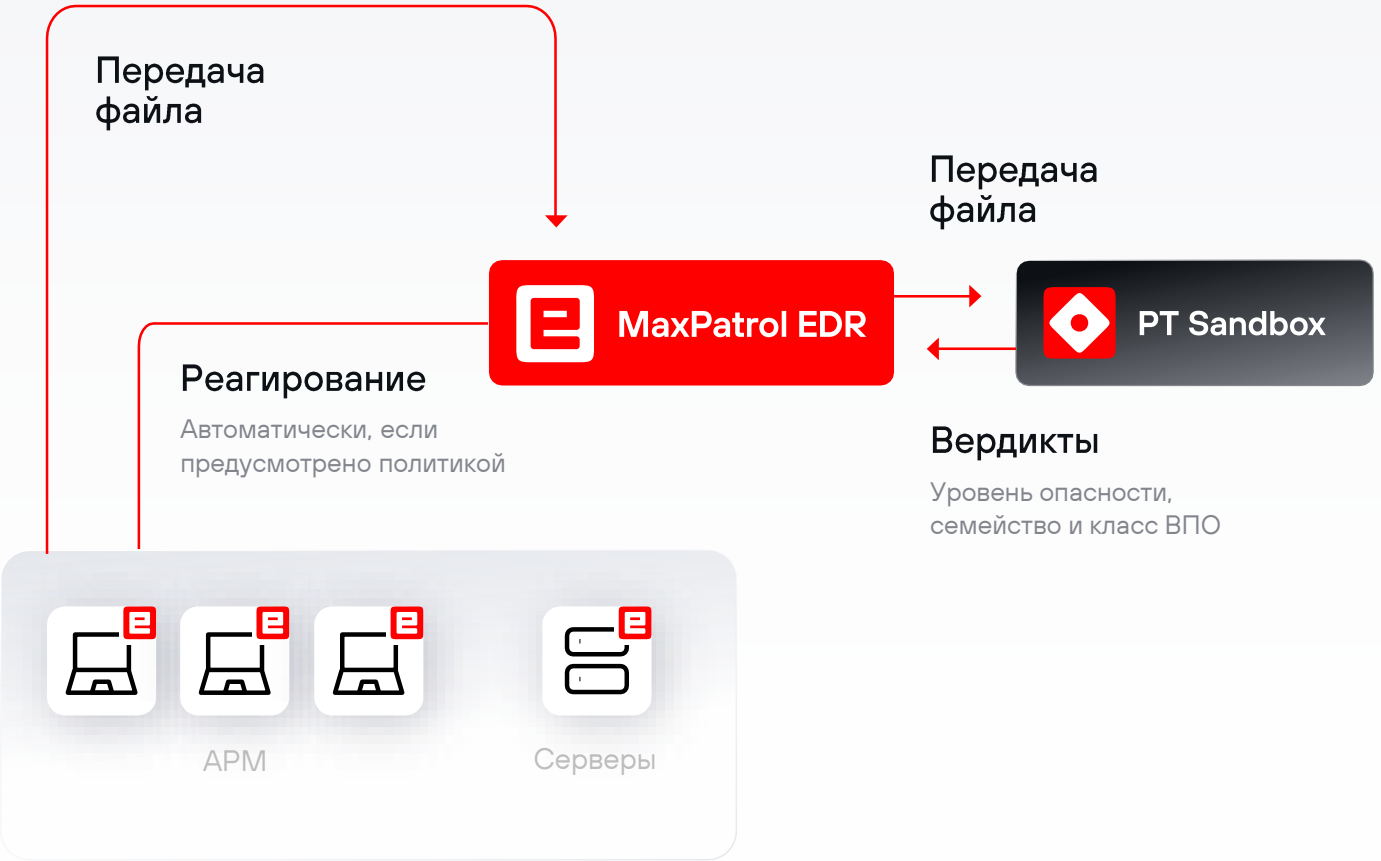
MaxPatrol EDR + MaxPatrol VM

- 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

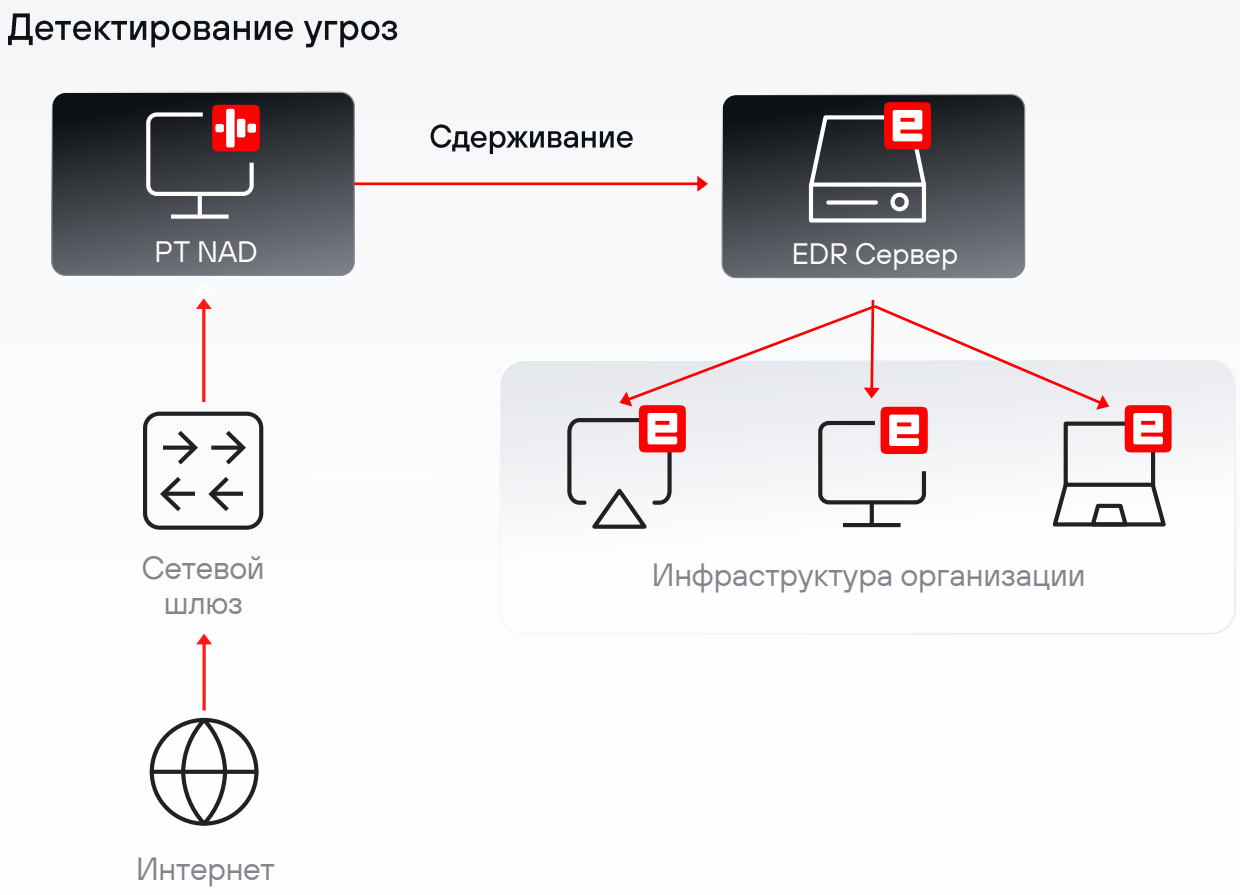
- Агенты EDR обнаруживают скачиваемые файлы (в браузерах, Telegram, с помощью P2P и пр.) и передают на анализ в PT Sandbox
- PT Sandbox проводит подробный статический и поведенческий анализ и отправляет вердикт
- Можно настроить автоматическое реагирование исходя из вердикта песочницы
- Вердикт песочницы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



MaxPatrol EDR + PT NAD

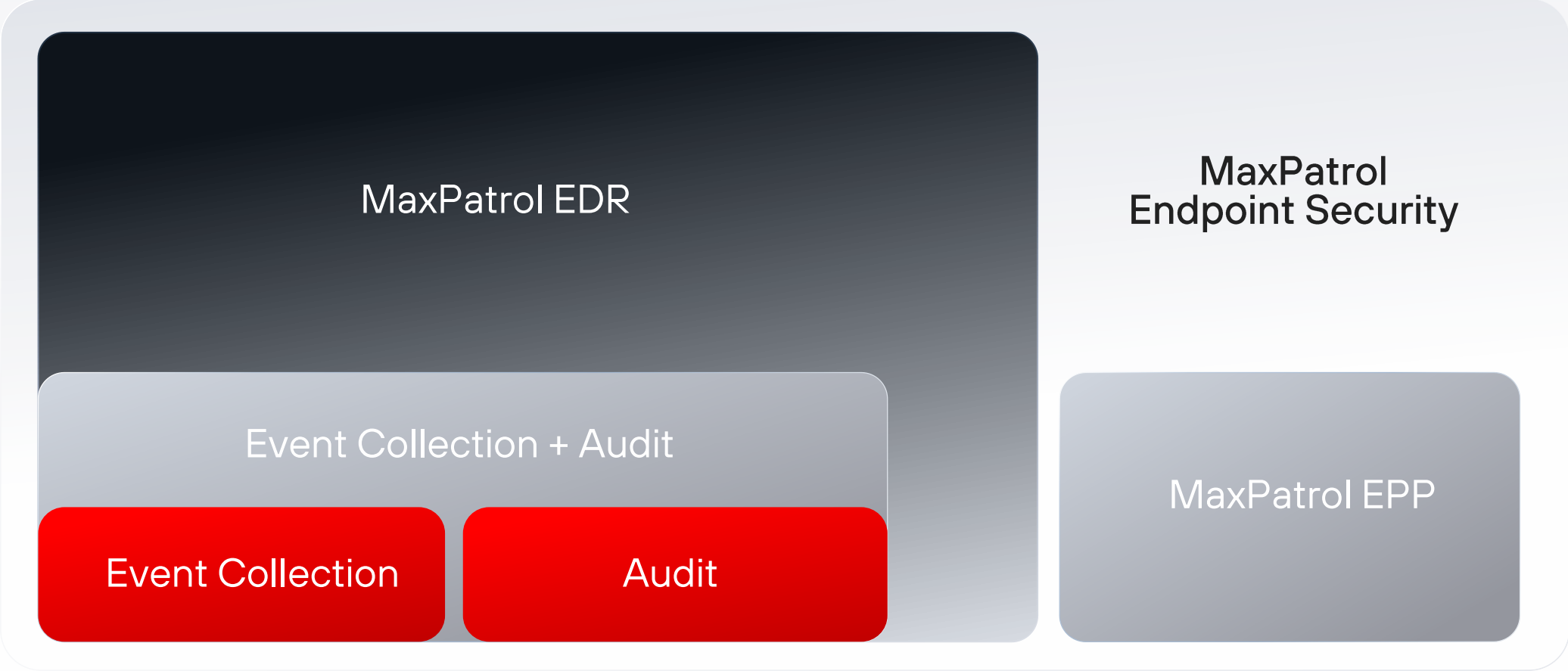
Сдерживание угроз:

- Изоляция узла на сетевом уровне
- Изоляция узла на уровне адаптера
- Блокировка УЗ



Лицензирование

Варианты поставки MaxPatrol Endpoint Security



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-EVC-AAAA-BBBB, конфигурация Event Collection:

доступны модули для сбора и передачи журналов событий операционной системы

PT-MXEDR-A-AAAA-BBBB, конфигурация Audit:

доступны модули для локального сбора данных в режиме аудита

PT-MXEDR-EVCA-AAAA-BBBB, конфигурация Event Collection + Audit:

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

PT-MXEDR-STD-AAAA-BBBB, конфигурация EDR Standard:

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-MXEPP-EP-AAAA-BBBB, конфигурация MaxPatrol Endpoint Protection Platform

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

PT-MXEDR-ESE-AAAA-BBBB, конфигурация MaxPatrol Endpoint Security

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

Испытайте MaxPatrol Endpoint Security в деле

Демо

Подробная демонстрация функций продукта и сценариев его использования

Тест-драйв

Предоставляется доступ к стенду для тестирования в облаке Positive Technologies: продукт, агенты, виртуальная машина для выполнения действий от лица атакующих

Пилот

Предоставляются дистрибутивы и тестовая лицензия. Наиболее подробное знакомство с продуктом в инфраструктуре клиента

Спасибо!

Дополнительные материалы

Заказать бесплатный пилот

Telegram-канал Positive Technologies

Покрытие матрицы MITRE ATT&CK