



Защита устройств от массовых, сложных и целевых атак

Тренды



ВПО остается основным инструментом злоумышленников



Доля применения ВПО в атаках на организации

71%

Ухищрения атакующих

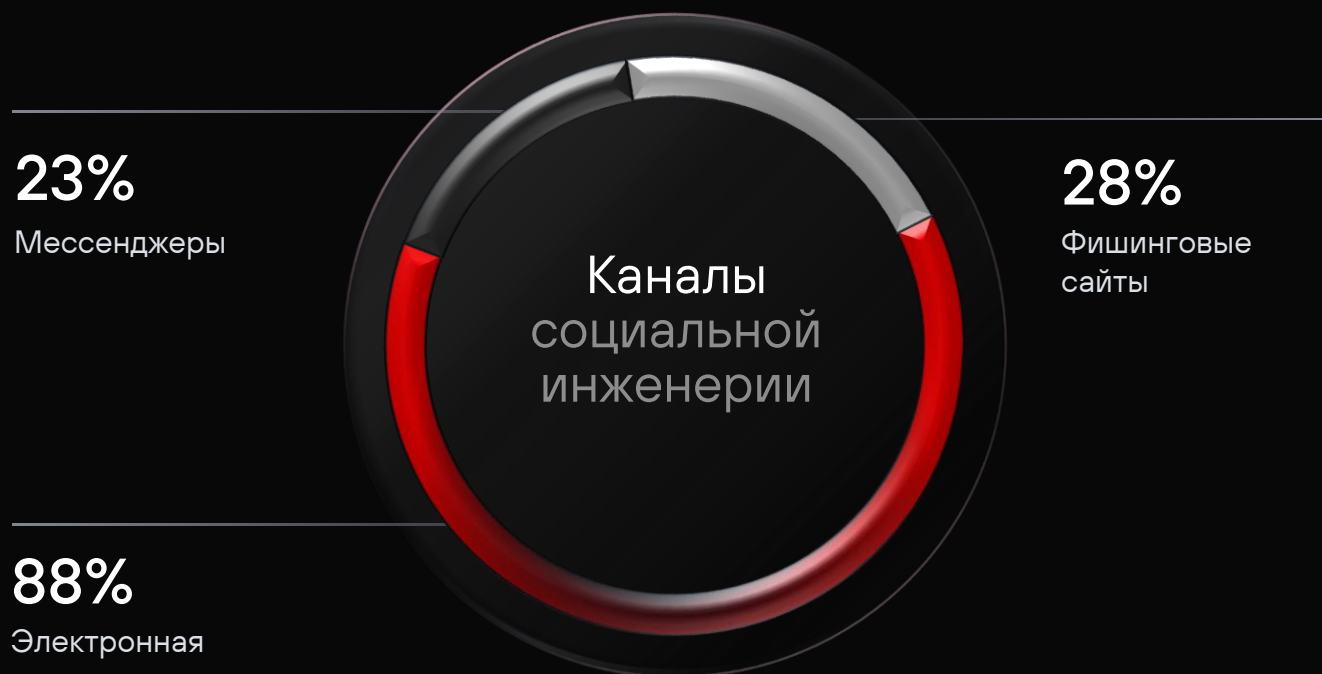
- Тренд на многоэтапные схемы доставки вредоносной нагрузки
- Расширяются возможности проникновения в разные ОС за счет портирования ВПО (языки Go, Rust, Nim и др.)

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

Тактики и техники атак



Более 75% атак начинаются
с компрометации конечных устройств



Эксплуатация уязвимостей
остаётся 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 геораспределенных инфраструктур

5

Гибкая настройка

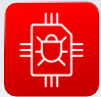
Модульная структура позволяет настроить функциональность продукта с учетом поставленных задач и внутренних регламентов

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 (АВЗ.5), приказ ФСТЭК № 117 для обеспечения защиты информации в ГИС, ГОСТ Р 57580 «Безопасность финансовых (банковских) операций»

PT Antivirus в составе MaxPatrol EPP



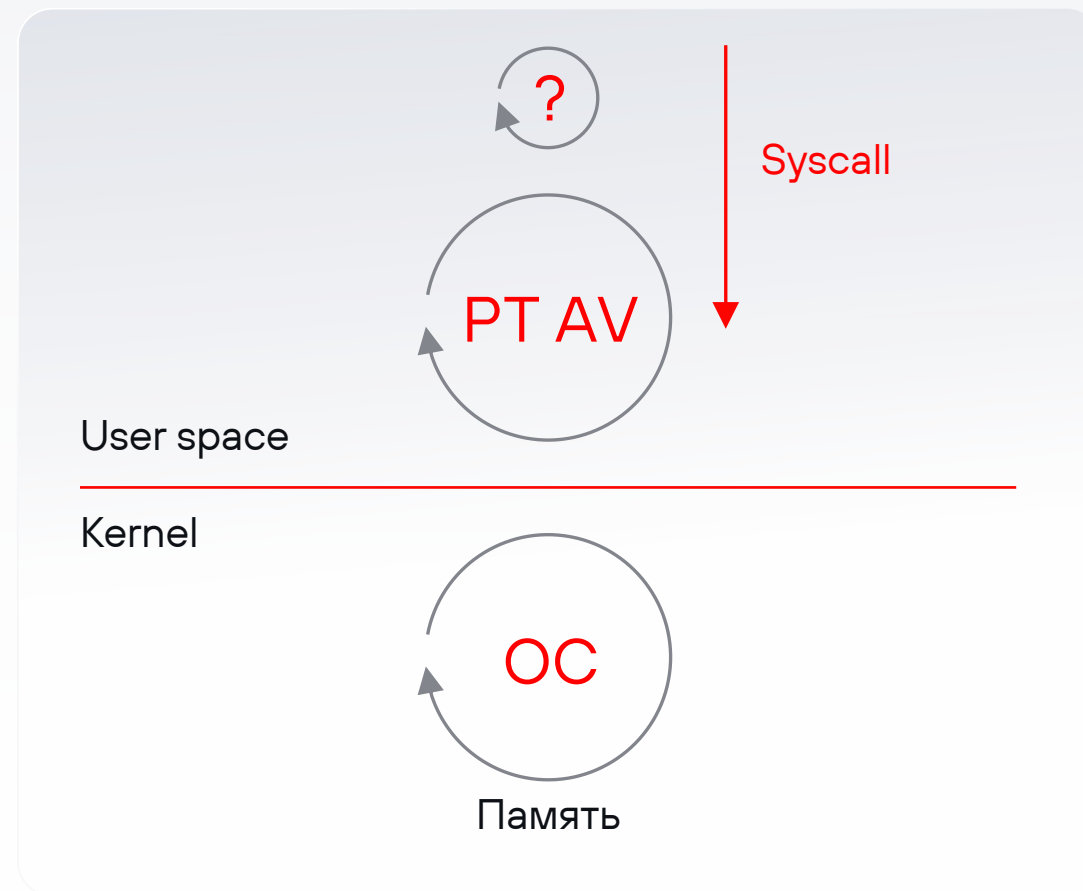
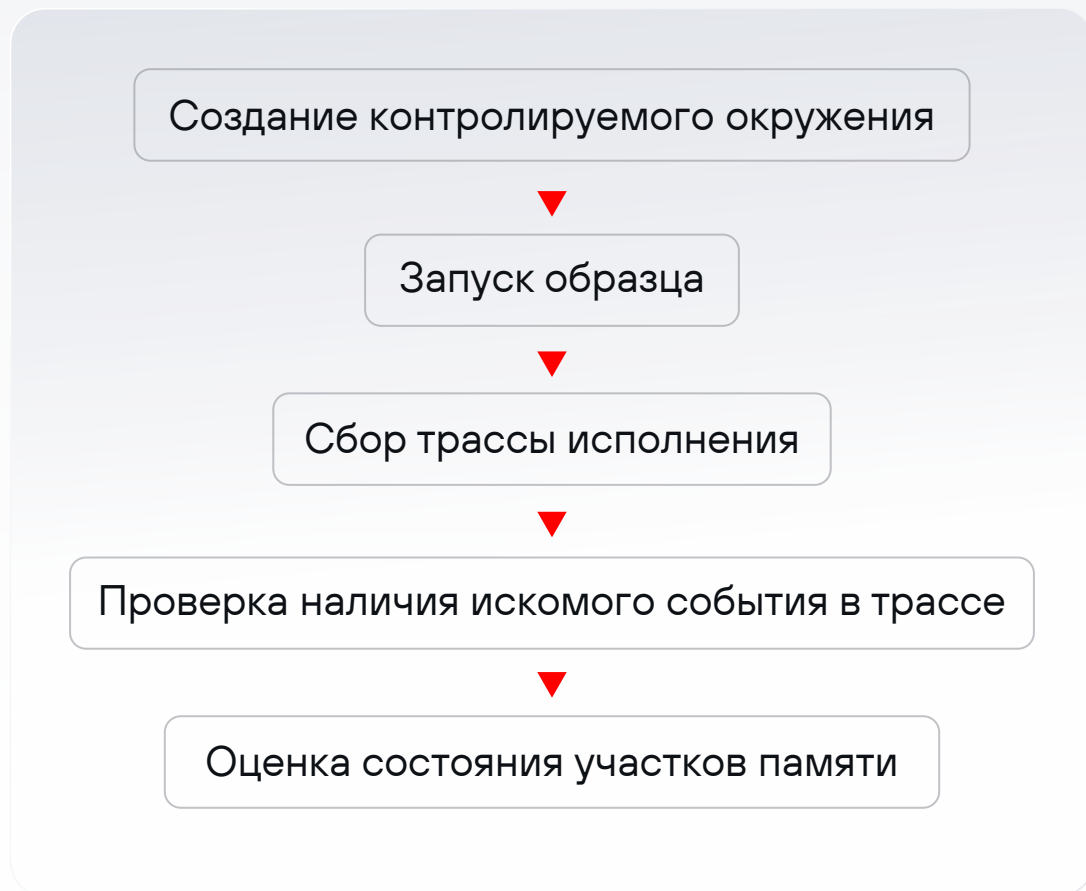
Антивирусный модуль основан на 30-летнем опыте разработки компании «ВИРУСБЛОКАДА» и экспертизе антивирусной лаборатории экспертного центра Positive Technologies (PT ESC).

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





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

Быстрое реагирование

Более 40 вариантов автоматического и ручного реагирования для оперативной защиты

Поведенческий анализ

Обнаруживает сложные угрозы на защищаемом устройстве благодаря корреляционному движку

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 зашифрованным 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



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?

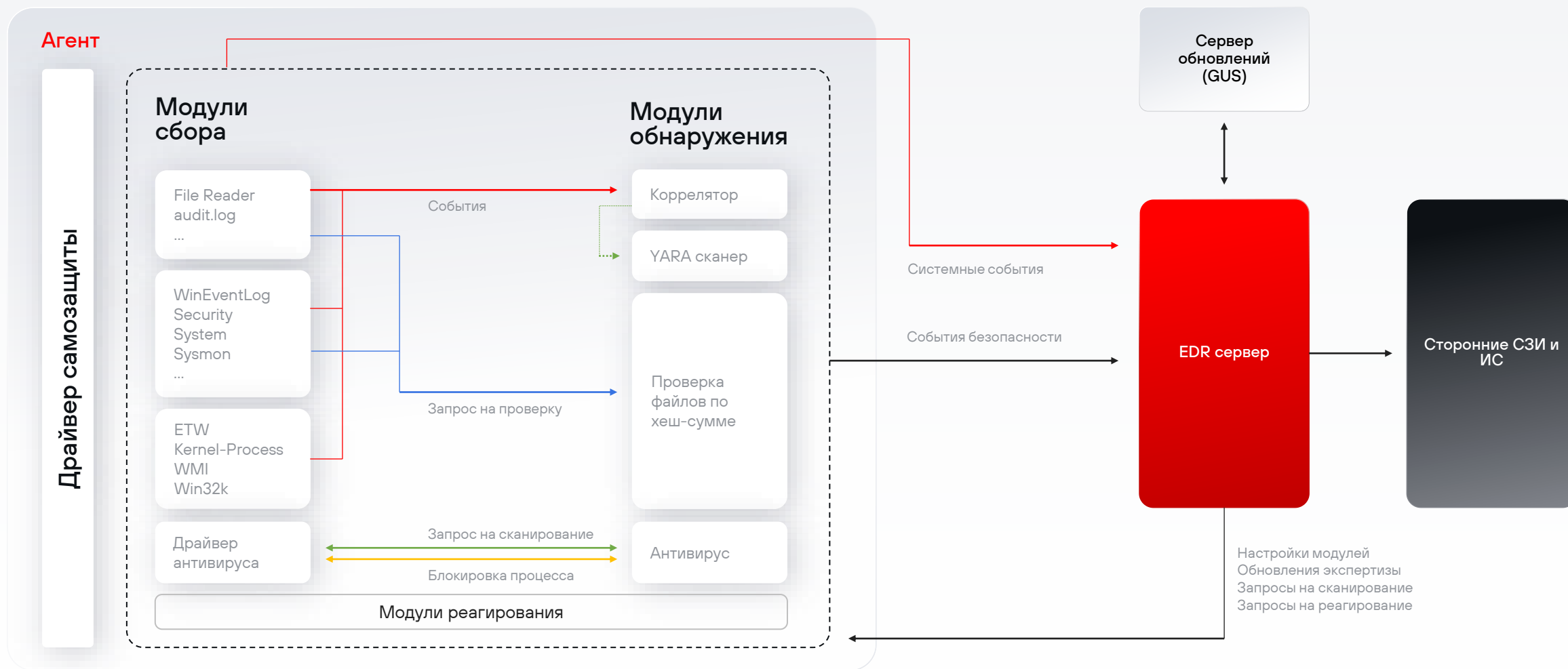
Выявление

- 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?

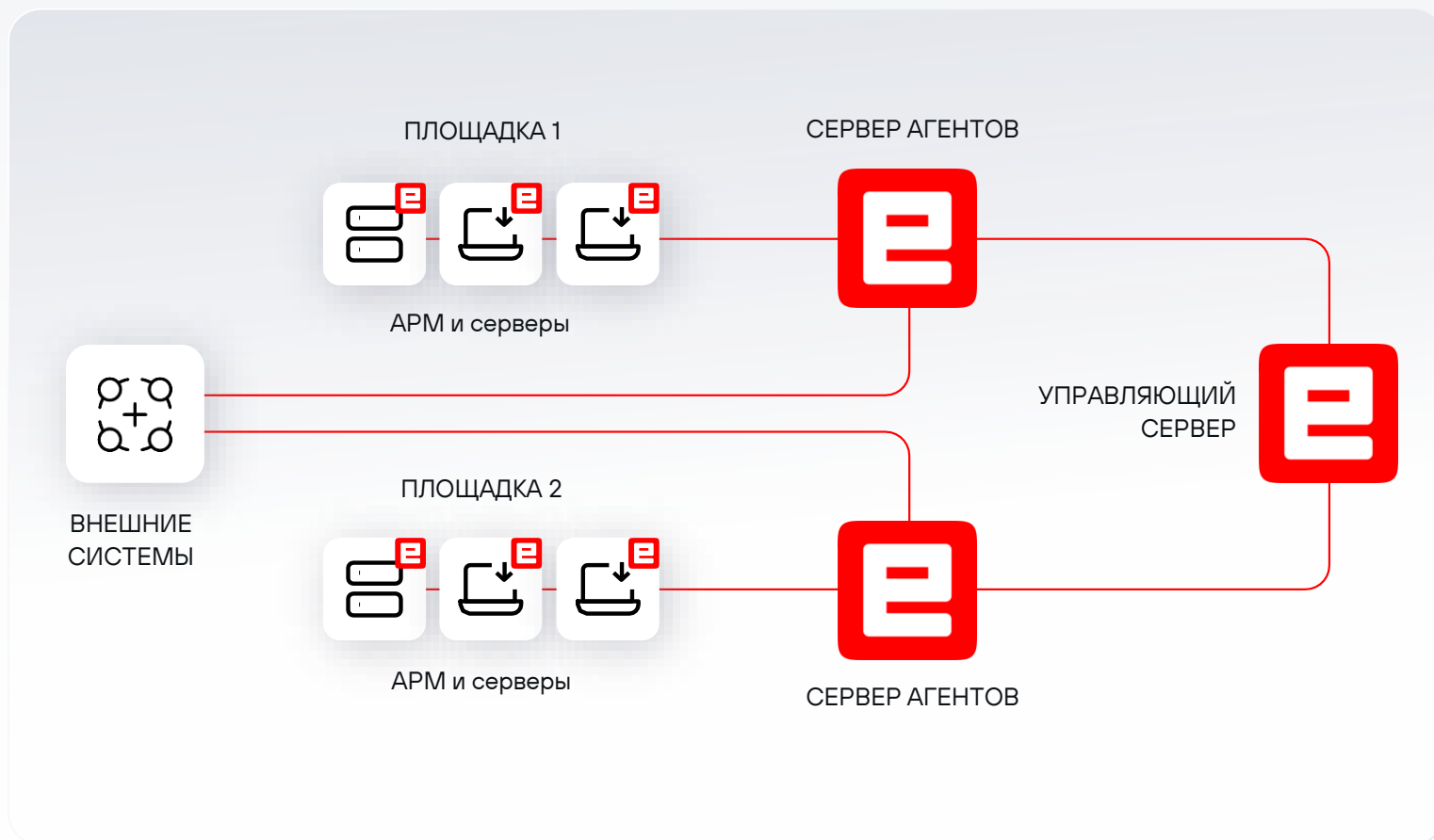
Реагирование

- 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



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	«ПЕД ОС» 7.3	«ПЕД 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

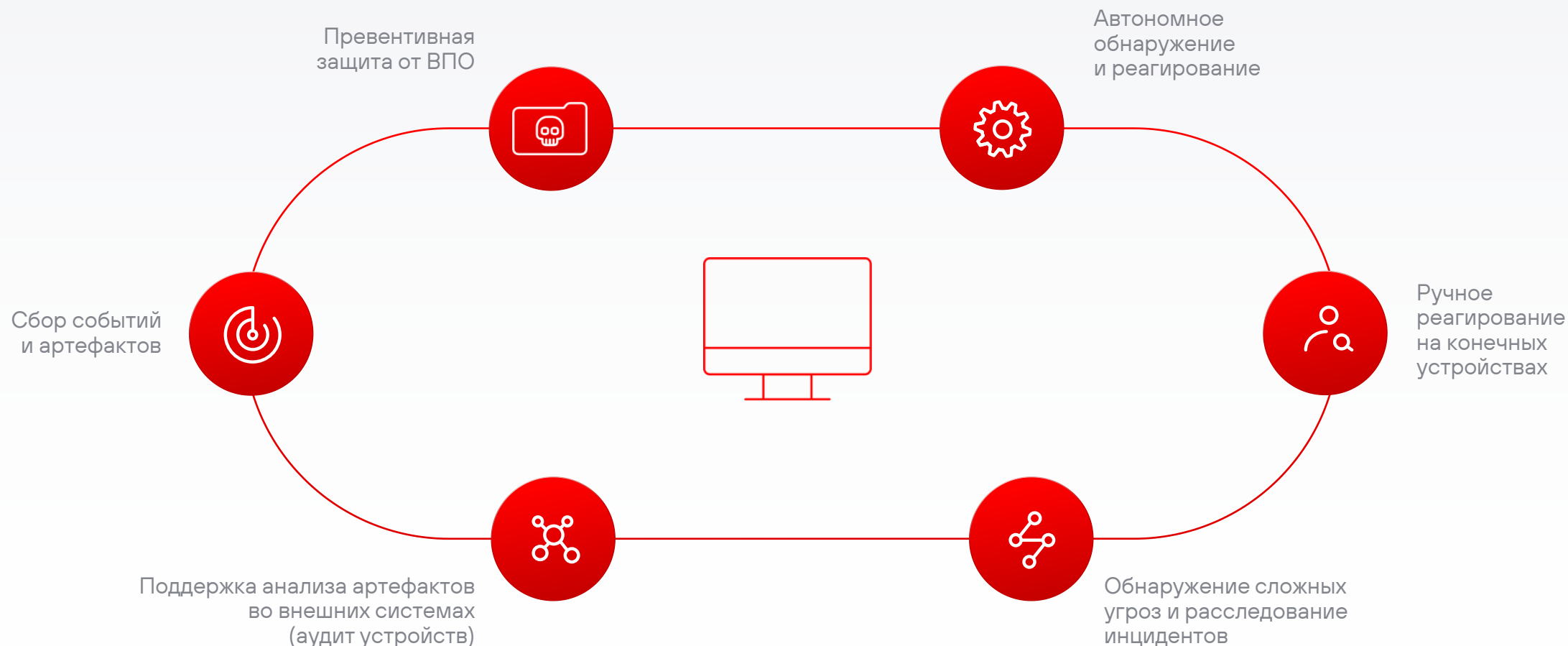


Защита инфраструктуры
на «Играх Будущего»

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



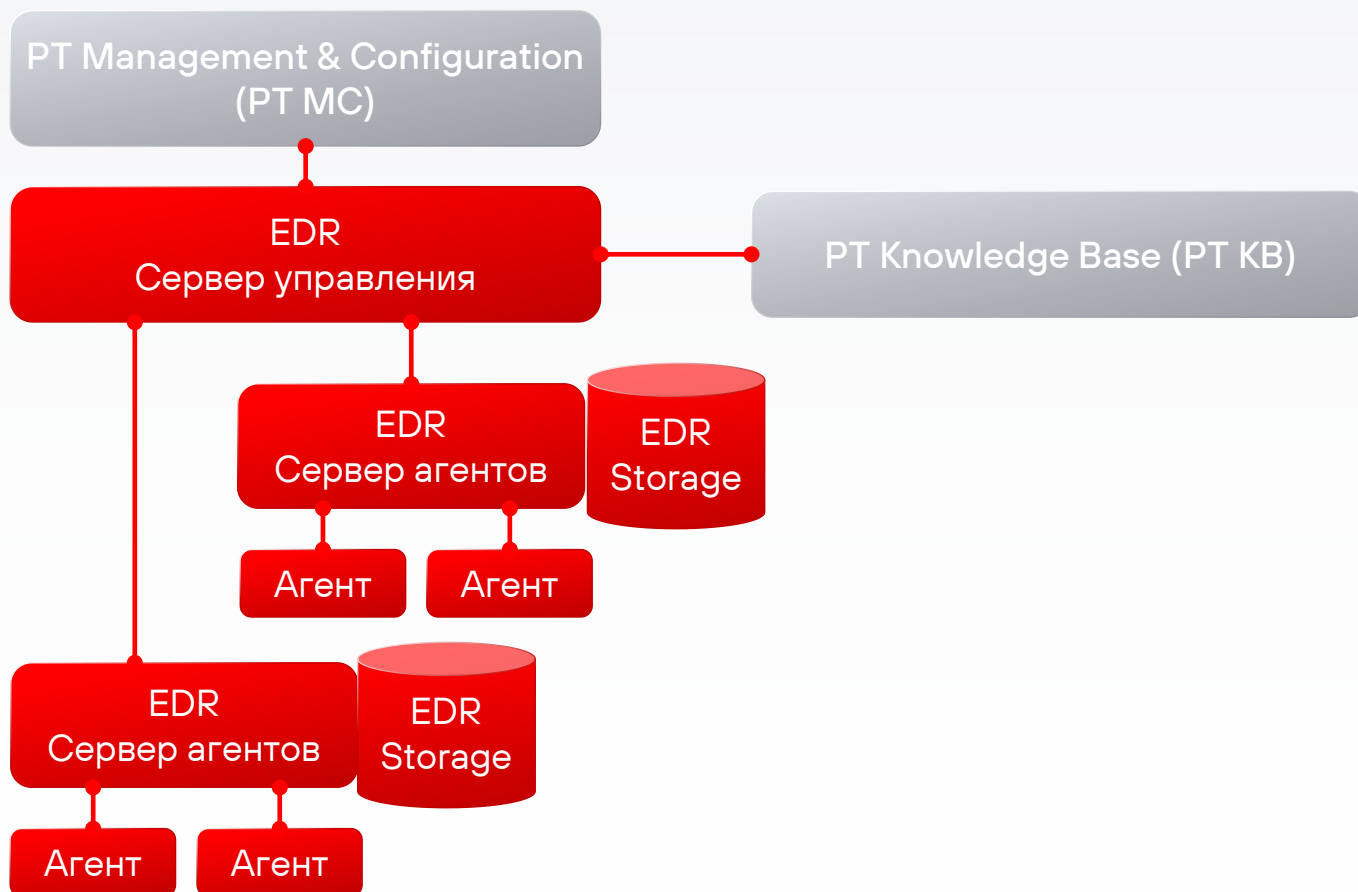
Сбор событий, обнаружение и автоматическое реагирование

- Автономное обнаружение на агентах
- Многоэтапные проверки
- Автоматизация реагирования

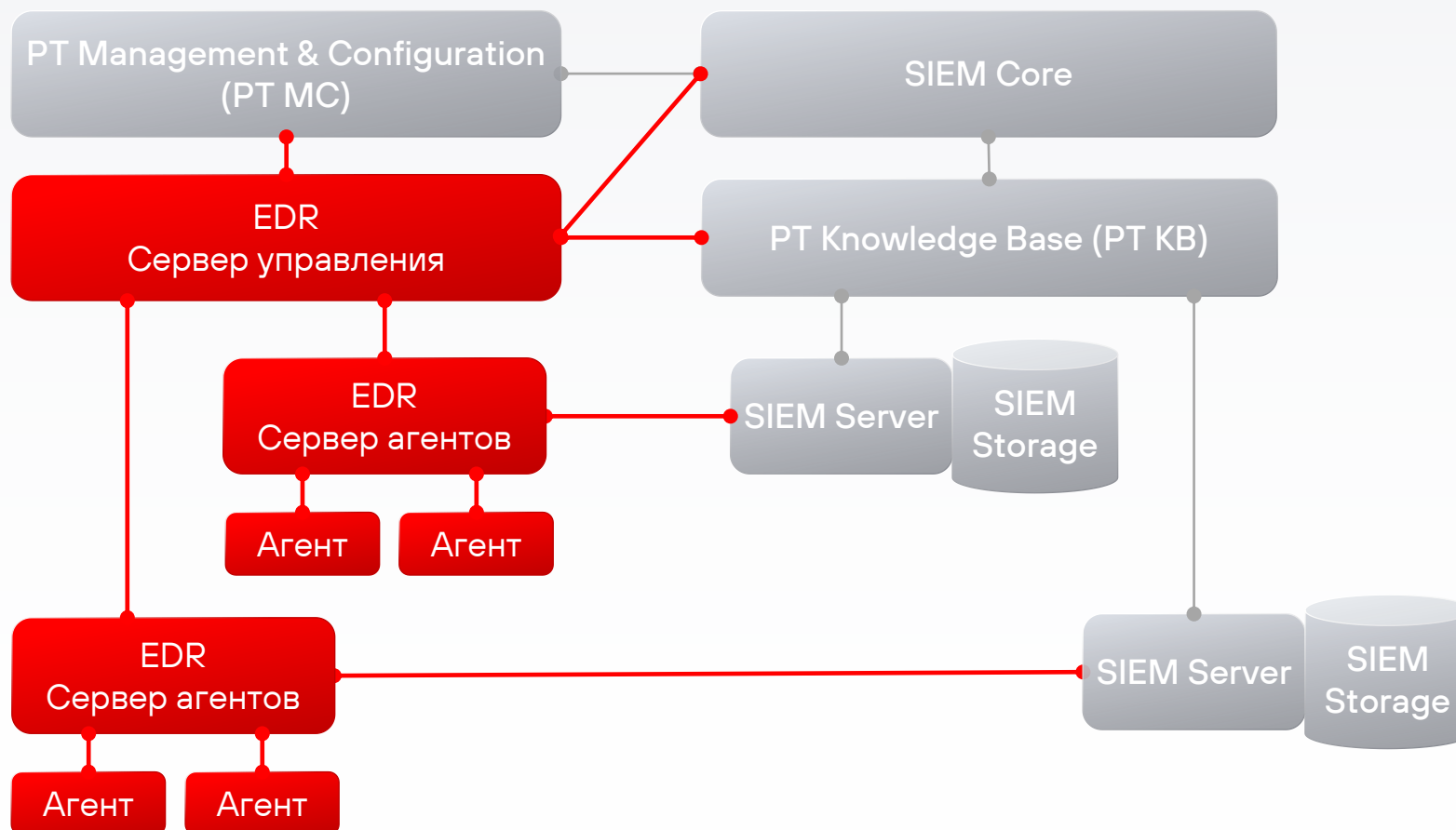


Администрирование MaxPatrol EDR

Варианты развертывания: собственное хранилище



Варианты развертывания: совместно с MaxPatrol SIEM



Развертывание за минуты

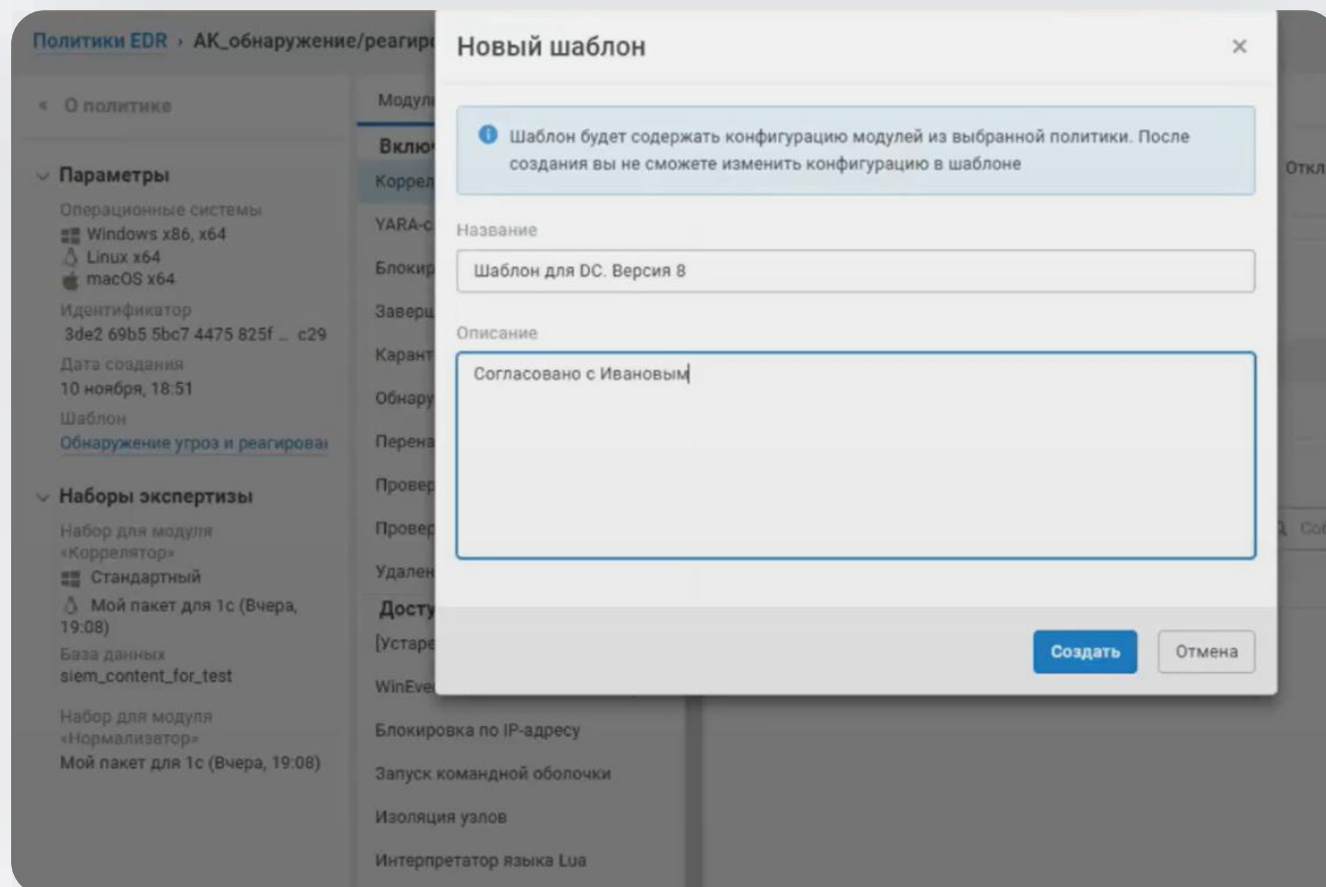


Конфигурировать
политики и исключения
на 30–60 серверов
долго и сложно

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

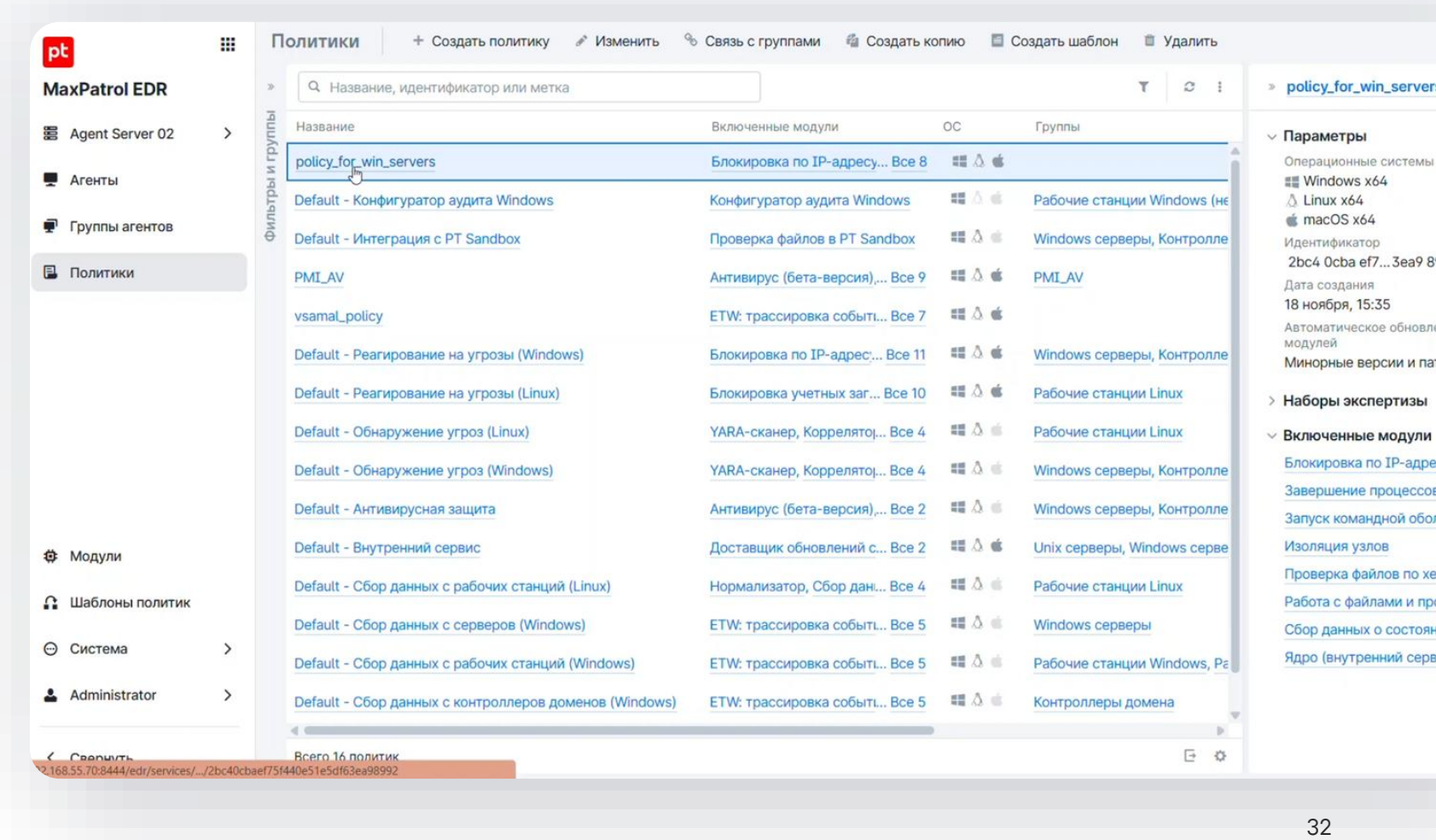


Конфигурировать политики и исключения на 30–60 серверов долго и сложно

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

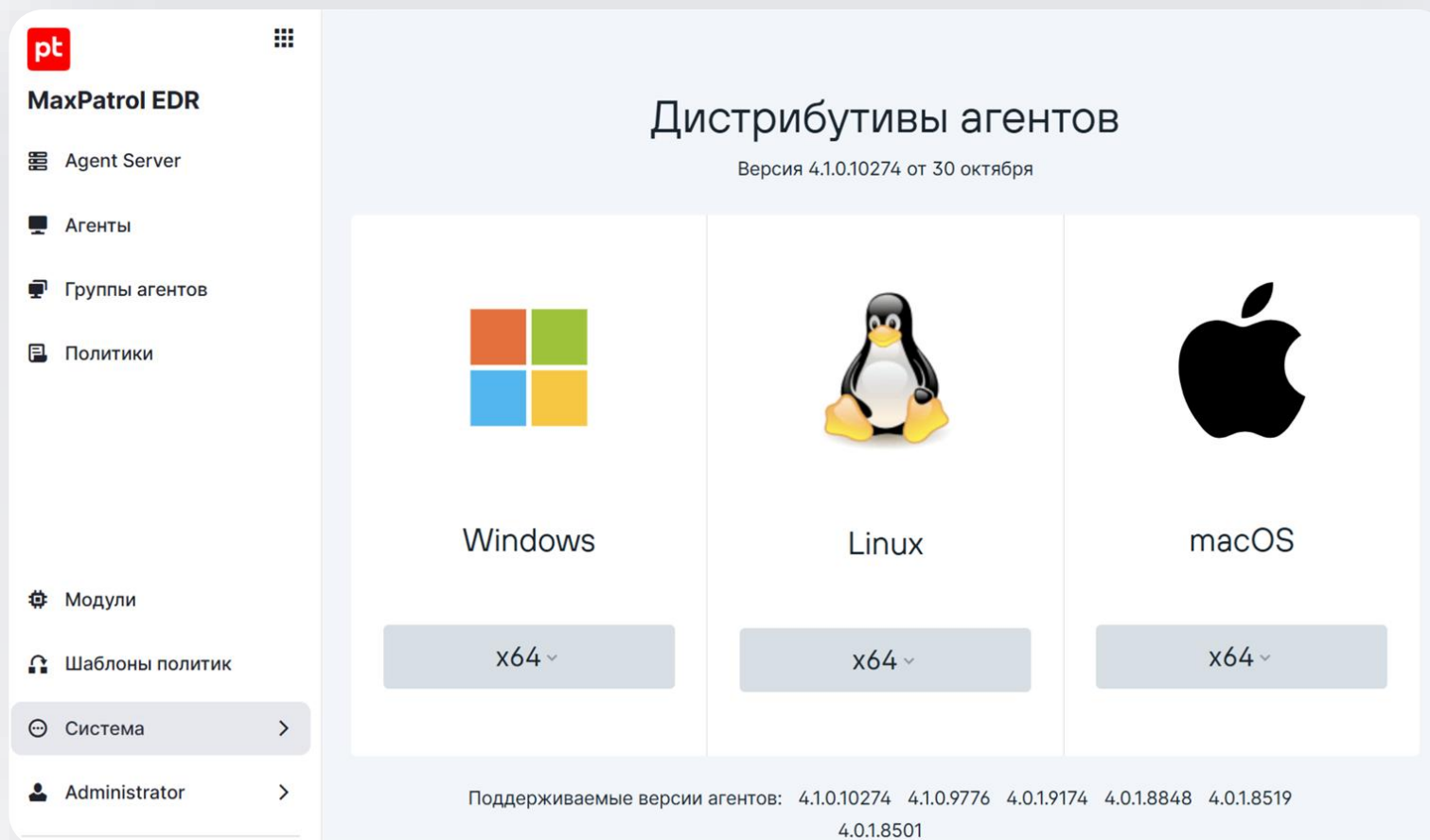


Все необходимые дистрибутивы под рукой

→ 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

The screenshot shows the 'Планировщик задач' (Task Scheduler) interface with a 'Новая задача' (New Task) modal window open. The modal contains the following fields and options:

- Название** (Name): Авторизация новых windows-серверов
- Запуск** (Run):
 - ☒ Каждые 5 минут
 - ☐ Ежедневно в 12:30
 - ☐ При добавлении нового агента
- Агенты** (Agents): Все агенты
- Дополнительное условие на языке PDQL** (Additional condition in PDQL language): Не обязательно
- Действие** (Action): Переместить в группу
- Куда** (Where): Windows серверы

At the bottom of the modal are two buttons: 'Создать' (Create) and 'Отмена' (Cancel).

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

The screenshot displays the 'Планировщик задач' (Task Scheduler) interface within the MaxPatrol EDR console. A 'Новая задача' (New task) dialog is open, allowing for the configuration of a new task. The dialog includes the following fields:

- Название** (Name): 'Агенты в критичном сегменте' (Agents in critical segment)
- Запуск** (Run): ☒ 'Каждые' (Every) 5 минут (minutes). Other options include 'Ежедневно в' (Daily at) 12:30 and 'При добавлении нового агента' (When a new agent is added).
- Агенты** (Agents): 'Все агенты' (All agents)
- Дополнительное условие на языке PDQL** (Additional condition in PDQL language): 'in_subnet (Agent.Ips, 192.168.100.0/24)'
- Действие** (Action): 'Переместить в группу' (Move to group)
- Куда** (Where): 'Критичный серверный сегмент' (Critical server segment)

Buttons at the bottom of the dialog are 'Создать' (Create) and 'Отмена' (Cancel).

Автоматизация работы с агентами



Удаление агентов

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

The screenshot shows the 'Планировщик задач' (Task Scheduler) interface. A modal dialog titled 'Новая задача' (New Task) is open. The dialog contains the following fields:

- Название** (Name): Удаление неактивных агентов (Removal of inactive agents)
- Запуск** (Run):
 - ☐ Каждые 5 минут (Every 5 minutes)
 - ☒ Ежедневно в 12:30 (Daily at 12:30)
 - ☐ При добавлении нового агента (When a new agent is added)
- Агенты** (Agents): Все агенты (All agents)
- Дополнительное условие на языке PDQL** (Additional condition in PDQL language):

```
Agent.Status = 'disconnected' AND Agent.ConnectedDate >= Now() - 1w
```
- Действие** (Action): Удалить агент (Remove agent)

At the bottom right of the dialog are two buttons: 'Создать' (Create) and 'Отмена' (Cancel).

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

Обнаружение подозрительных файлов
Версия 1.0.31872 · 📄 ⚙️ 📱

Основные параметры

* Максимальный размер файла для проверки, МБ

20

Правила обнаружения для Linux

Каталоги

/home

Каждый каталог с новой строки

Расширения

*

Каждое расширение с новой строки

Процессы

Каждый процесс с новой строки

Правила обнаружения для Windows

Папки

C:\\Program Files\\Common Files\\Microsoft Shared\\clicktorun
C:\\ProgramData\\Microsoft\\User Account Pictures
C:\\Users*\\AppData\\Roaming\\Microsoft\\Excel\\xlstart

Каждая папка с новой строки

Расширения

exe
pif
scr

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

YARA-сканер

Версия 2.1.31872 · Экспертиза 2.0.0.2430 ·

Список исключений для проверок в Linux

Файлы и каталоги, которые не требуется проверять в Linux

Список исключений для проверок в Windows

Файлы и папки, которые не требуется проверять в Windows

Список исключений для YARA-правил

Правила, которые не используются для проверок

Параметры быстрой проверки файлов в Linux

Список файлов и каталогов для быстрой проверки в Linux

Параметры быстрой проверки файлов в Windows

Список файлов и папок для быстрой проверки в Windows

Параметры быстрой проверки процессов в Linux

Список процессов для быстрой проверки в Linux

Параметры быстрой проверки процессов в Windows

Список процессов для быстрой проверки в Windows

* Максимальный размер файла для проверки, МБ

1536

Проверку файла, превышающего этот размер, можно запустить вручную

Классы вредоносного ПО

Файл признается вредоносным, если он принадлежит к одному из классов

Проверки по расписанию

* Запуск

☒ Не запускать ☐ Каждую неделю ☐ По месяцам

* Время хранения результатов сканирования процесса (в минутах)

—

60

+

* Максимальное количество используемых потоков при сканировании

—

2

+

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

✓ Проверка файлов по хеш-сумме

Версия [1.1.31872](#) · Экспертиза 1.0.0.12849 ·

Основные параметры

* Максимальный размер файла для проверки, МБ

20

События

⚡ Мастер назначения действий

🔍 Событие, действие, модуль или техника

Событие	Действия
Не удалось проверить файл по хеш-сумме	Сохранить в БД
При проверке хеш-суммы обнаружен вредоносный файл	Сохранить в БД
Файл не найден в базе вредоносных	Сохранить в БД

Действия

Идентификатор	Описание
Проверить исполняемый файл процесса-объекта по хеш-сумме	Поиск исполняемого файла процесса-объекта в базе данных вредоносных файлов
Проверить исполняемый файл процесса-субъекта по хеш-сумме	Поиск исполняемого файла процесса-субъекта в базе данных вредоносных файлов
Проверить файл-объект по хеш-сумме	Поиск файла-объекта в базе данных вредоносных файлов

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

✓ Коррелятор (Windows)

Версия [3.0.35829](#) · Экспертиза 1.0.0.1349 ·   

Основные параметры

События

⚡ Мастер назначения действий



CoercedPotato PrivEsc

T1068: Эксплуатация уязвимостей для повышения привилегий

Сохранить в БД

Command Processor Autorun Modify

T1547.001: Ключи запуска в реестре / Папка автозагрузки

Сохранить в БД

Computer Object Ldap Request

T1018: Изучение удаленных систем

Сохранить в БД

Comsvcs Minidump Usage

T1003.001: Память процесса LSASS

T1218.011: Rundll32

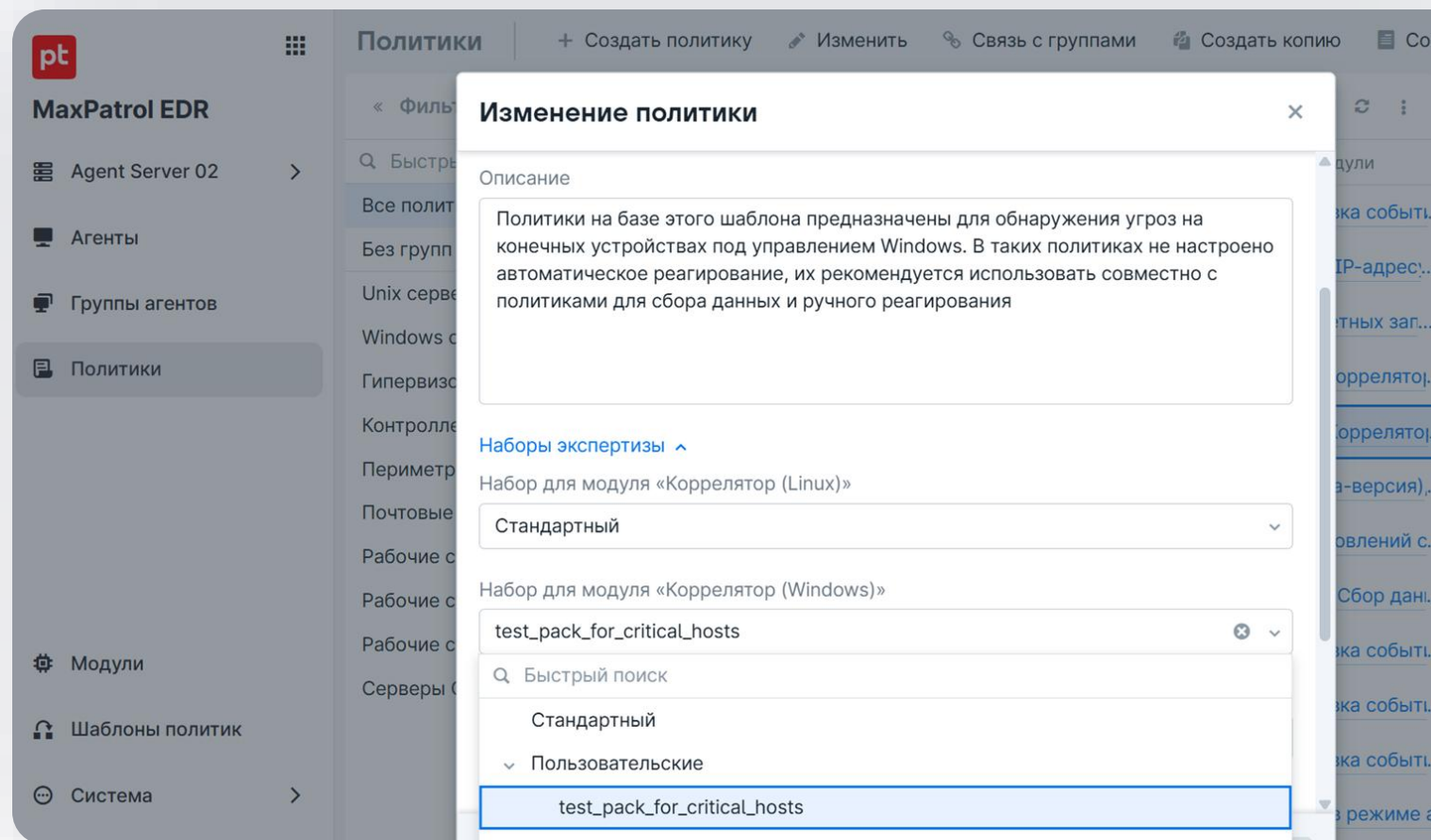
T1129: Общие модули

Сохранить в БД

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



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

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

The screenshot displays a security management interface. On the left, a list of events is shown, including a timestamp '18.11.2025, 14:15:22' and a description 'Обнаружена попытка получения доступа к данным процесса LSASS.exe через приложение mspeng.exe'. A red arrow points from the 'Реагировать' (React) button at the bottom of the event list to the 'Реагирование' (Reaction) panel on the right.

The 'Реагирование' panel contains a search bar and a list of actions:

- Завершить дерево процессов, используя путь к исполняемому файлу и идентификатор родительского процесса-субъекта c:\programdata\microsoft\windows defender\platform\4.18.25090.3009-0\msmpeng.exe 5228
- Завершить деревья процессов, используя имя процесса-объекта lsass.exe
- Завершить деревья процессов, используя имя процесса-субъекта msmpeng.exe
- Завершить деревья процессов, используя путь к исполняемому файлу-объекту \device\harddiskvolume2\windows\system32\lsass.exe
- Завершить деревья процессов, используя путь к исполняемому файлу-субъекту c:\programdata\microsoft\windows defender\platform\4.18.25090.3009-0\msmpeng.exe
- Завершить деревья процессов, используя путь к файлу-объекту \device\harddiskvolume2\windows\system32\lsass.exe
- Завершить процесс, используя имя и идентификатор процесса-объекта 808 lsass.exe
- Завершить процесс, используя имя и идентификатор процесса-субъекта 5228 msmpeng.exe
- Завершить процесс, используя путь к исполняемому файлу и идентификатор процесса-объекта \device\harddiskvolume2\windows\system32\lsass.exe 808
- Завершить процесс, используя путь к исполняемому файлу и идентификатор процесса-субъекта c:\programdata\microsoft\windows defender\platform\4.18.25090.3009-0\msmpeng.exe 5228

Below the list, there are sections for 'Изоляция узлов' (Node Isolation) and 'Удаление файлов' (File Removal):

- Изоляция узлов:**
 - Полностью изолировать узел
 - Снять частичную изоляцию узла
 - Частично изолировать узел
- Удаление файлов:**
 - Удалить исполняемый файл процесса-объекта \device\harddiskvolume2\windows\system32\lsass.exe
 - Удалить исполняемый файл процесса-субъекта c:\programdata\microsoft\windows defender\platform\4.18.25090.3009-0\msmpeng.exe
 - Удалить файл-объект, используя путь \device\harddiskvolume2\windows\system32\lsass.exe

Реагирование из карточки агента в три клика



⚡ Реагировать

Агент

Статус

Подключен

• Авторизован

Зарегистрирован12 ноя, 19:35

Группа

Рабочие станции Windows

Версия4.1.0.10274

IP-адрес192.168.55.152

Идентификатор0f22700484415c6036bed1004422c3cc

Самозащита

✓ Включена

Ссылки

События ↗ Актив ↗

Узел

ИмяWORKSTATION01

ОС

Microsoft Windows 10 10.0.19045.6456 x64

FQDNWORKSTATION01.edr2.local

Политики

Включенные модули

Сетевые интерфейсы

Статус	Имя и MAC-адрес	IP-адреса
✓	Ethernet0 2 00:50:56:83:55:e2	192.168.55.152/24
✓	Loopback Pseudo-Interface 1	::1/128 127.0.0.1/8

Пользователи

Реагирование на агента windows_WORKSTATION01_of2270

Изолировать

Завершить работу

Работа с файлами

Проверить, удалить

Работа с процессами

Проверить, завершить, создать дамп

Карантин

Изолировать файлы в зашифрованном хранилище на время их проверки

🔒 Заблокировать соединения по IP-адресу

✖ Перенаправить DNS-запросы (sinkholing)

Перенаправление трафика с подозрительных и вредоносных доменов на заданный IP-адрес с помощью файла hosts

🔒 Заблокировать учетную запись

Или завершить сеанс

[] YARA-сканер

Выполнить сигнатурный анализ файлов или процессов

📄 Сканировать узел в режиме аудита

И отправить результаты в MaxPatrol VM

</> Запустить командную оболочку

📄 Собрать данные о системе

Запущенные процессы, сетевые соединения, учетные записи,

Реагирование на множестве агентов

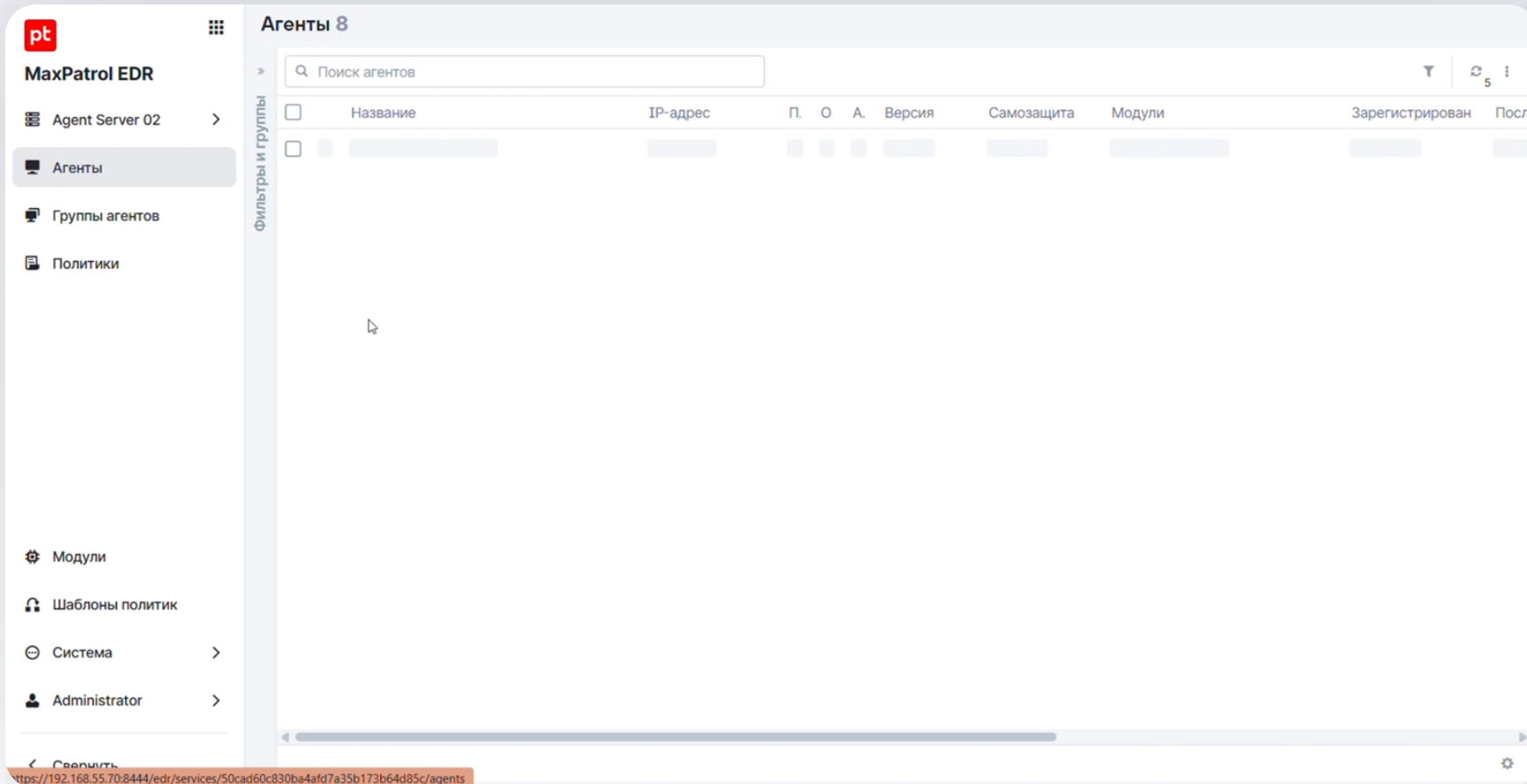


Просто начать и удобно продолжить

- 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

The screenshot displays the MaxPatrol EDR interface. On the left, a sidebar contains navigation options: Agent Server 02, Агенты (selected), Группы агентов, and Политики. Below these are sections for Модули, Шаблоны политик, Система, and Administrator. The main panel, titled 'Агенты 6', shows a table of agents with columns for Name, IP address, Platform (П), OS (О), Version (A), Group, and Tags. Three agents are selected: windows_SERVER01_744064, windows_WORKSTATION02_62fca7, and windows_WORKSTATION01_0f2270. A context menu is open over the selected agents, listing various actions such as 'Заблокировать учетную запись (объект) по логину', 'Завершить все сеансы', 'Популярное', 'Частично изолировать узел', 'Снять частичную изоляцию узла', 'Процесс', 'Завершить все процессы, используя путь к файлу-объекту', 'Завершить все процессы, используя имя процесса-объекта', 'Запустить задачу проверки важных системных процессов YARA-правилами', 'Сеть', 'Заблокировать IP-адрес', 'Разблокировать IP-адрес', 'Частично изолировать узел', 'Снять частичную изоляцию узла', 'Перенаправить трафик с доменов', 'Отменить перенаправление трафика с доменов', 'Файл', and 'Удалить файл-объект, используя путь'. At the bottom, a 'Журнал реагирования' (Incident Response Log) window is open, showing a table of actions with columns for Agent, Platform, Last seen in network, Executed time, and Result. Two actions are listed: one for 'windows_WORKSTATION...' completed at 16:37:54, and another for 'windows_WORKSTATION...' failed at 16:37:47 with the message 'Не удалось выполнить действие'.

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

The screenshot displays the MaxPatrol EDR interface. On the left is a sidebar with navigation options: Agent Server 02, Агенты, Группы агентов, Политики, Модули, Шаблоны политик, Система, and Administrator. The main area shows a file explorer view for the path C:\Tools\mimikatz-master (2)\mimikatz-master. A list of files and folders is shown, including inc, lib, mimidrv, mimikatz, mimilib, mimilove, mimispool, modules, README.md, appveyor.yml, kiwi_passwords.yar, mimicom.idl, mimikatz.sln (highlighted), notrunk.lst, and trunk.lst. On the right, a detailed view of the selected file 'mimikatz.sln' is shown, including options to 'Проверить' (Check), 'В карантин' (Quarantine), and 'Скачать' (Download). A dropdown menu for 'Проверить' shows options: 'С помощью YARA-правил' (With YARA rules), 'По хеш-сумме' (By hash sum), 'Антивирусом' (By antivirus), and 'В PT Sandbox' (In PT Sandbox). The 'По хеш-сумме' option is selected, showing a hash of 32:28 and a timestamp of 5:38:21. At the bottom right, there is a link to 'События с этим файлом' (Events with this file).

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

The screenshot displays the MaxPatrol EDR interface. On the left is a sidebar with navigation options: Agent Server 02, Агенты (selected), Группы агентов, and Политики. Below this are settings for Модули, Шаблоны политик, Система, and Administrator. The main panel shows a list of processes for the host windows_WORKSTATION01_0f2270. The processes listed include OneDrive.Sync.Service.exe, Explorer.EXE, vm3dservice.exe (highlighted), SecurityHealthSystray.exe, csrss.exe, winlogon.exe, wininit.exe, and another csrss.exe. A detailed view of vm3dservice.exe is shown on the right, displaying its PID (5400), start time (31 Oct, 15:18:29), and memory usage (0.09% (7 MB)). The view also shows the process's parent (csrss.exe), its command line, and its full path (C:\Windows\System32\vm3dservice.exe).

Имя процесса	PID	Запущен ↓	ОЗУ ↓
OneDrive.Sync.Service.exe	9080	13 ноя, 16:34:35	0,1%
Explorer.EXE	7940	31 окт, 15:17:29	2,5%
vm3dservice.exe	5400	31 окт, 15:18:29	0,09%
SecurityHealthSystray.exe	9284	31 окт, 15:18:28	0,2%
csrss.exe	3904	31 окт, 15:17:18	0%
winlogon.exe	5840	31 окт, 15:17:18	0,1%
wininit.exe	556	29 окт, 17:03:19	0%
csrss.exe	564	29 окт, 17:03:19	0%
winlogon.exe	656	29 окт, 17:03:19	0,1%
csrss.exe	452	29 окт, 17:03:18	0%
<Данные недоступны>	0		0%

vm3dservice.exe

Завершить ↓ Проверить + Дамп

Процесс: 5400

Исключения: 31 окт, 15:18:29

ОЗУ: 0,09% (7 МБ)

ЦП: 0%

Учетная запись: EDR2\Administrator

Исполняемый файл: [vm3dservice.exe](#)

Путь к файлу: C:\Windows\System32\vm3dservice.exe

Команда запуска: "C:\Windows\System32\vm3dservice.exe" -u

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.

Мастер назначения действий · Шаг 2 из 2

События-триггеры для действия «Завершить дерево процессов, используя путь к испо...

События	Выбранные	
Q Быстрый поиск	Q Быстрый поиск	ProcDump Usage
PPLmedic Process Dump	IIS Module Filter Installation	ProcDump_Usage
PrinterPort Backdoor	KeePass Keys Extraction	
PrintSpooler PrivEsc	Lsass Dump via SilentProcessExit	
PrintSpooler PrivEsc CVE 2022 30206	LSASS Memory Dump	
PrivEsc via Comctl32	LSASS Shtinkering Dump	
PrivEsc via UAC Elevated Data	Malware Trojan Powershell PowerSploit i	
Process from Mounted Disk	Malware Trojan Win32 Wiper a	
PuntoSwitcher Diary Open	Masquerading Microsoft Signed Library	
Reading Registry Objects	MSBuild AWL Bypass	
Remote Potato Capture Hash	ProcDump Usage	
Remote Potato Relay Hash		
Remote SSP Dump		
Remoting WinExec		

Выбрать другое действие

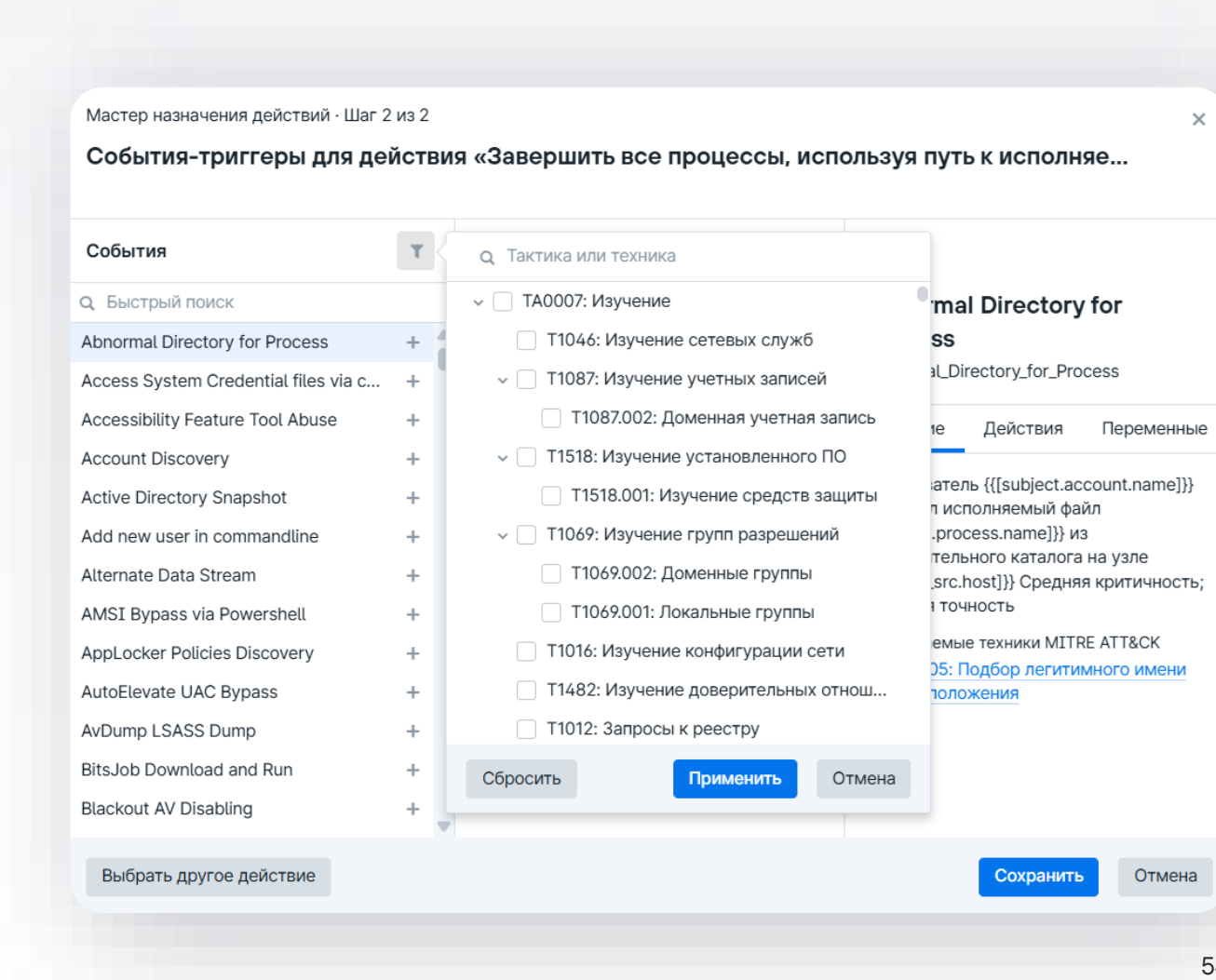
СохранитьОтмена

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



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, Уста... Все 4	🖥️ 🍏	11 сентября, 13:28
🛡️	Сбор данных с серверов (Linux)	Нормализатор, Сбор данных из файлов журналов, Уста... 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, 3... 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 P1... 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, Уста... 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

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

MaxPatrol EDR

Agent Server 02 >

Агенты

Группы агентов

Политики

Модули

Шаблоны политик

Система >

Administrator >

Агенты 9

Поиск агентов

Название	IP-адрес	П.	О.	А.	Версия	Самозащита	Модули	Зар...
windows_DESKTOP-6DTVQ47_7dedf6	192.168.10.66	🔌	🖥️	👤	4.1.0.10274	🛡️	WinEventLog: сбор данны... Все 5	18 н
windows_WORKSTATION06_d8c127	192.168.55.134	🔌	🖥️	👤	4.1.0.10274	🛡️	Антивирус (бета-версия)... Все 8	18 н
windows_WORKSTATION05_96bb85	192.168.55.135	🔌	🖥️	👤	4.1.0.10274	🛡️	ETW: трассировка собы... Все 24	18 н

Фильтры и группы

windows_WORKSTATION05_96bb85

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Program Files\Positive Technologies\EDR Agent> get-service

Status Name DisplayName
-----
Stopped AarSvc_20418e Agent Activation Runtime_20418e
Stopped AJRouter AllJoyn Router Service
Stopped ALG Application Layer Gateway Service
Stopped AppIDSvc Application Identity
Running AppInfo Application Information
Stopped AppMgmt Application Management
Stopped AppReadiness App Readiness
Stopped AppVClient Microsoft App-V Client
```

Как выглядит на практике: изоляция узлов на Windows и Linux



The screenshot displays the MaxPatrol EDR console interface. On the left, a sidebar contains navigation links: "Agent Server 02", "Агенты", "Группы агентов", "Политики", "Модули", "Шаблоны политик", "Система", and "Administrator". The main panel, titled "Агенты 9", lists various agents with columns for "Название", "IP-адрес", and status icons. The agent "windows_SERVER01_744064" is selected. A right-hand panel, titled "Реагирование на агенте windows_SERVER01_744064", shows a dropdown menu for "Изолировать" and a "Завершить работу" button. Below these, a list of isolation actions is shown:

- Полностью**
Отключив все сетевые адаптеры
- Частично**
У агента останется связь с сервером агентов и адресами из списка исключений
- Исключения** (with a help icon)
- События с изоляцией** (with an external link icon)
- Карантин**
Изолировать файлы в зашифрованном хранилище на время их проверки
- Заблокировать соединения по IP-адресу**
- Перенаправить DNS-запросы (sinkholing)**
Перенаправление трафика с подозрительных и вредоносных доменов на заданный IP-адрес с помощью файла hosts
- Заблокировать учетную запись**
Или завершить сеанс
- YARA-сканер**
Выполнить сигнатурный анализ файлов или процессов
- Запустить командную оболочку**



Уже используете решения Positive Technologies?

Усиьте 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



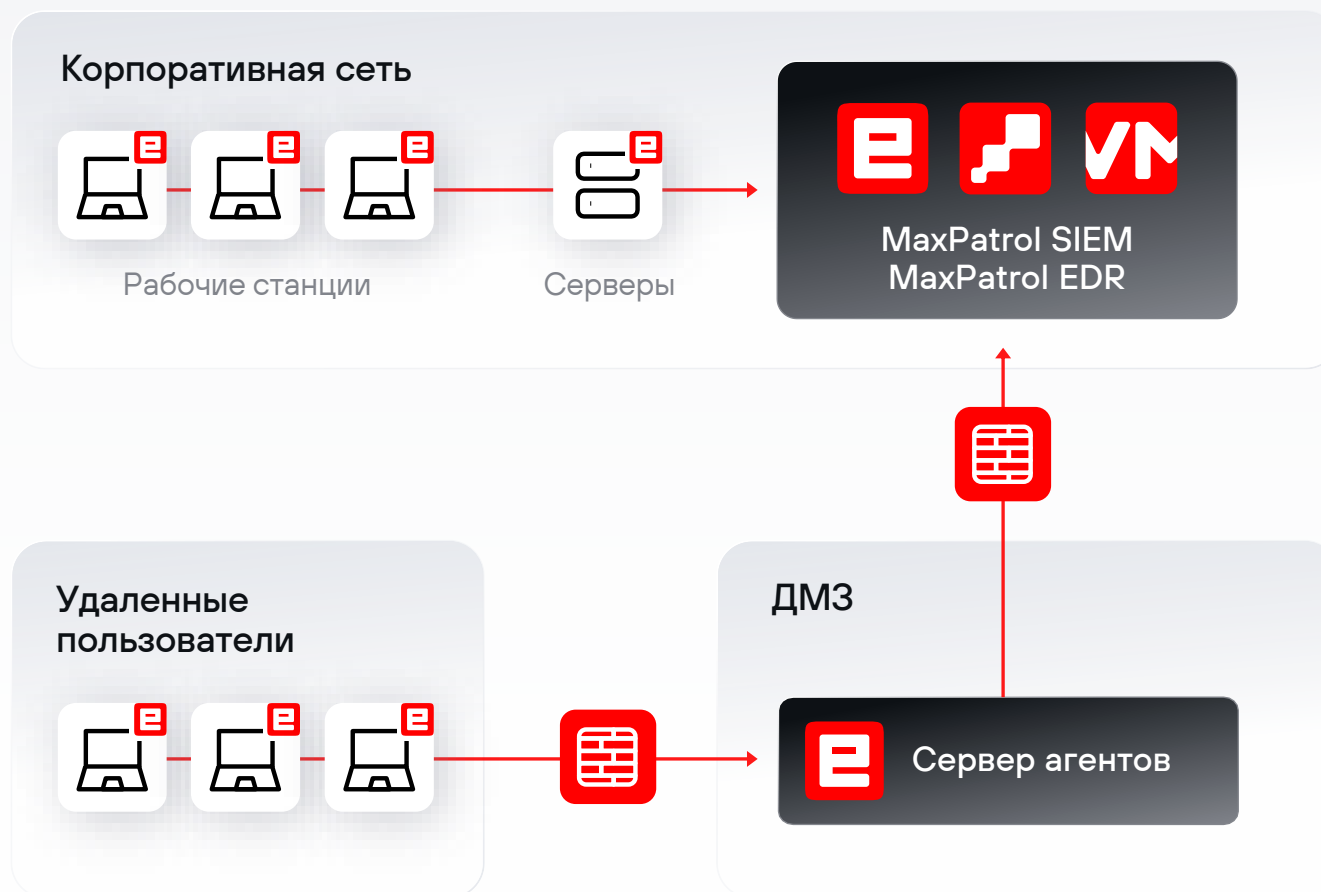
PT Sandbox

- Защита от ВПО, распространяемого через зашифрованные 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



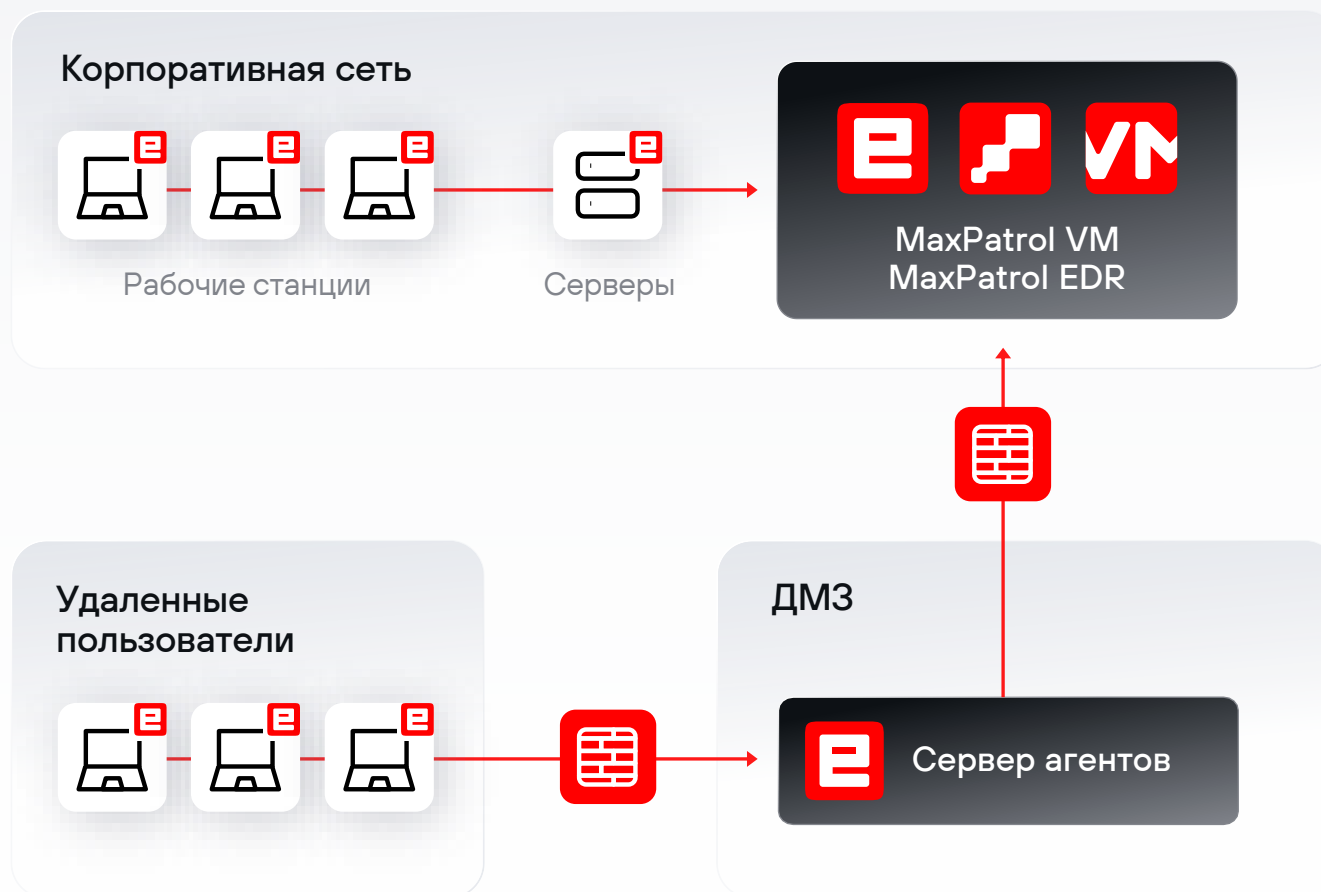
- > Контролируемый сбор событий (включая устройства вне домена или периметра)
- > Расширенные возможности сбора данных (агент EDR собирает то, что не умеет SIEM-система)
- > Оптимизация архитектуры и нагрузки на MaxPatrol SIEM
- > Реагирование и работа с исключениями из карточки события
- > Единая консоль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

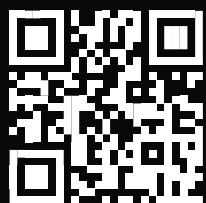
(для обеспечения антивирусной защиты конечных устройств),
обновления в течение года.

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

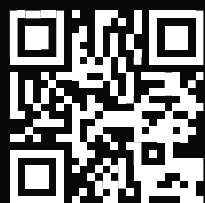
(базовый набор модулей и модули обеспечения антивирусной защиты конечных устройств), обновления в течение года.



Узнайте больше о Позитиве



Обзор
MaxPatrol EDR



Telegram-чат
пользователей



Заказать бесплатный
«пилот»



Telegram-канал
Positive Technologies



Покрытие матрицы
MITRE ATT&CK