

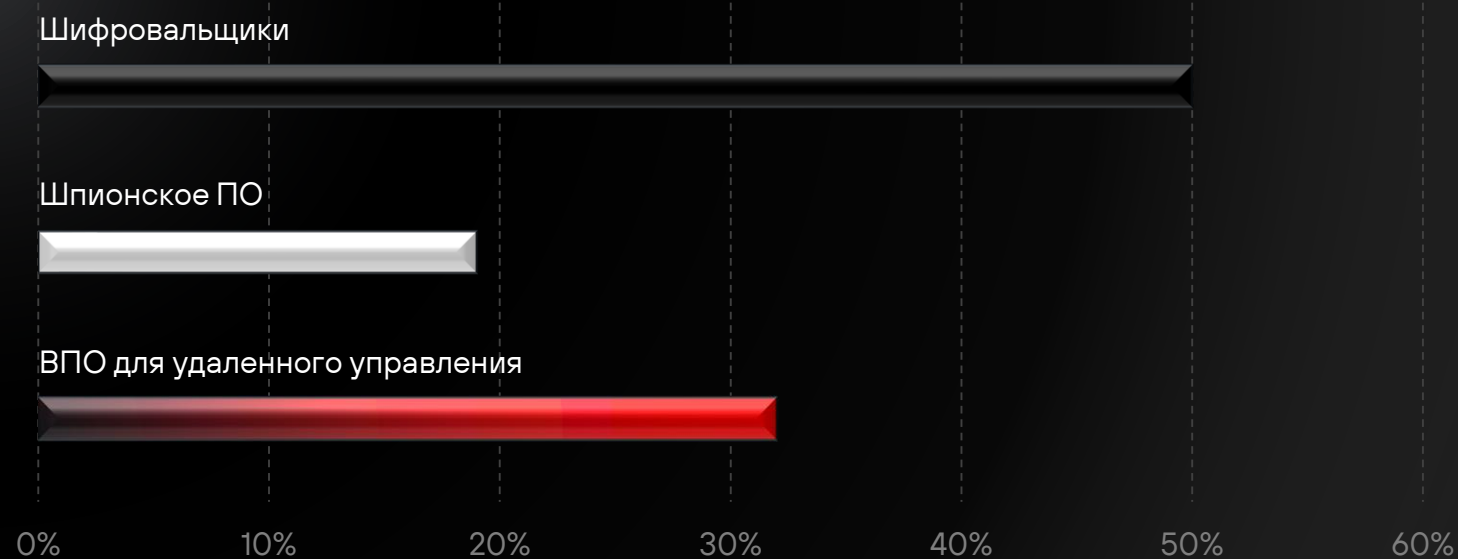


**Непрерывная работа
бизнеса начинается
с непробиваемой защиты
конечных устройств**

Тренды



ВПО остается основным инструментом злоумышленников



Типы ВПО, чаще всего применяемые в успешных атаках на организации



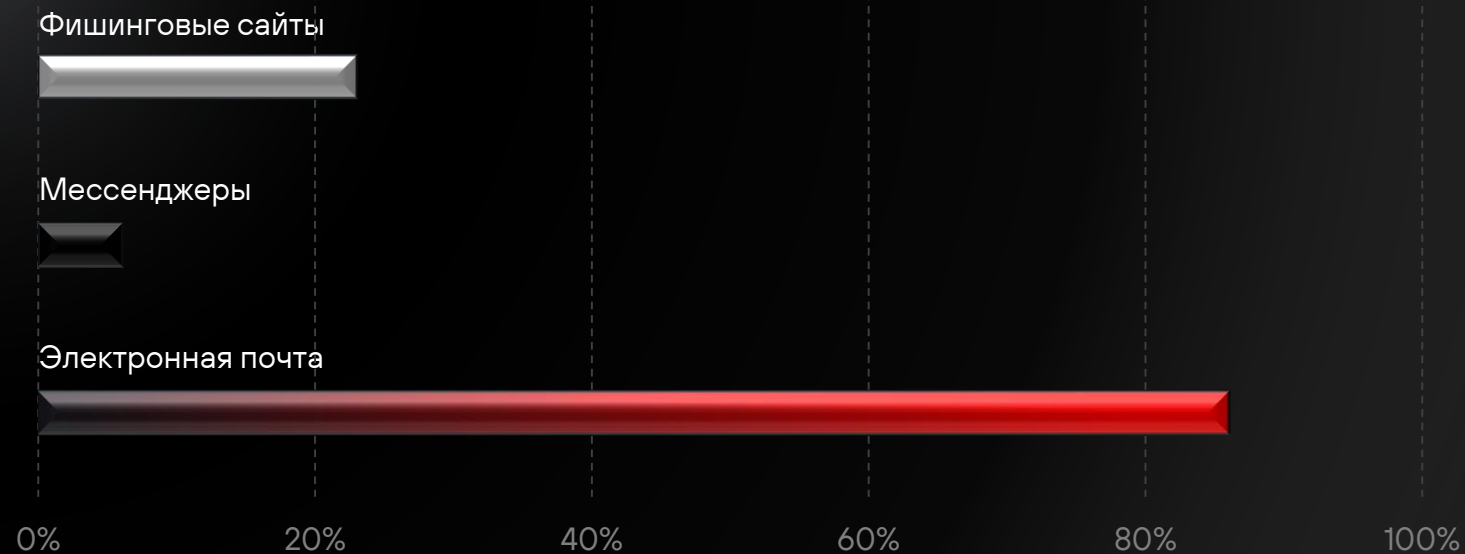
Доля применения ВПО в атаках на организации

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 считанные 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 (АВЗ.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 геораспределенных инфраструктур

5

Гибкая настройка

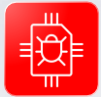
Модульная структура позволяет настроить функциональность продукта с учетом поставленных задач и внутренних регламентов

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



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

PT Antivirus в составе MaxPatrol EPP

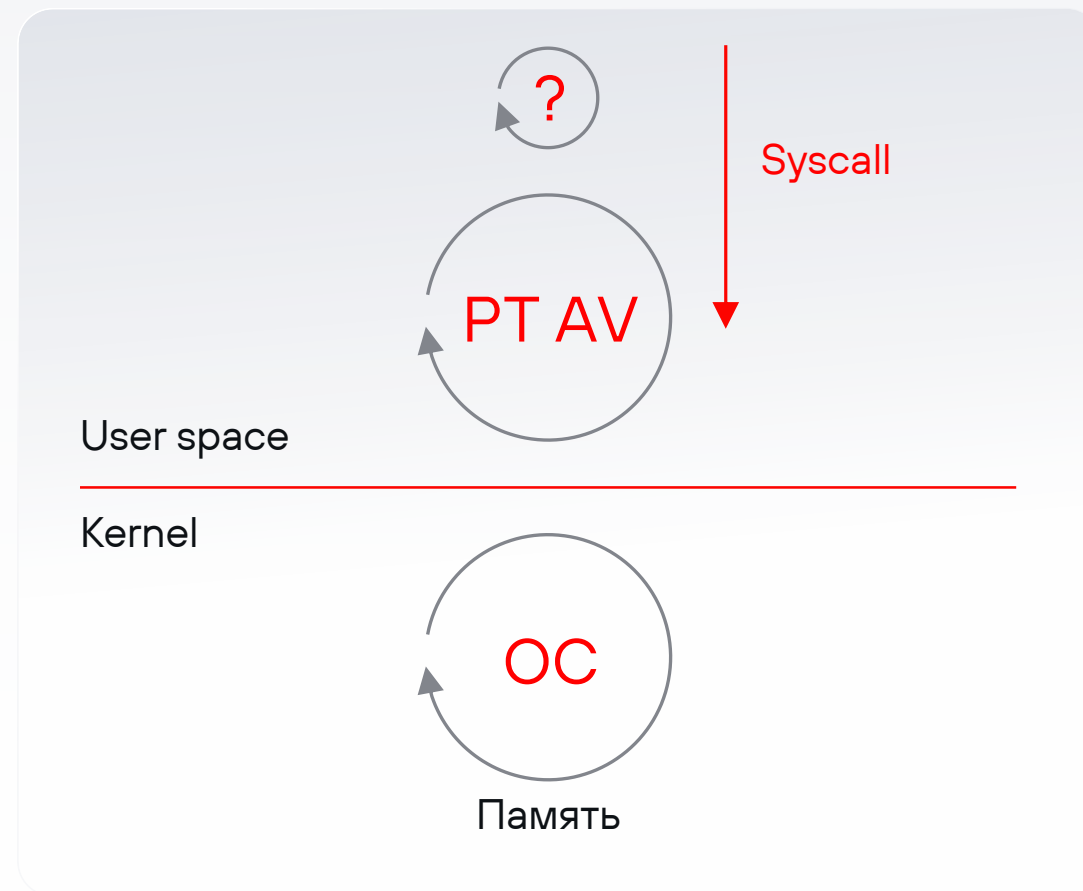
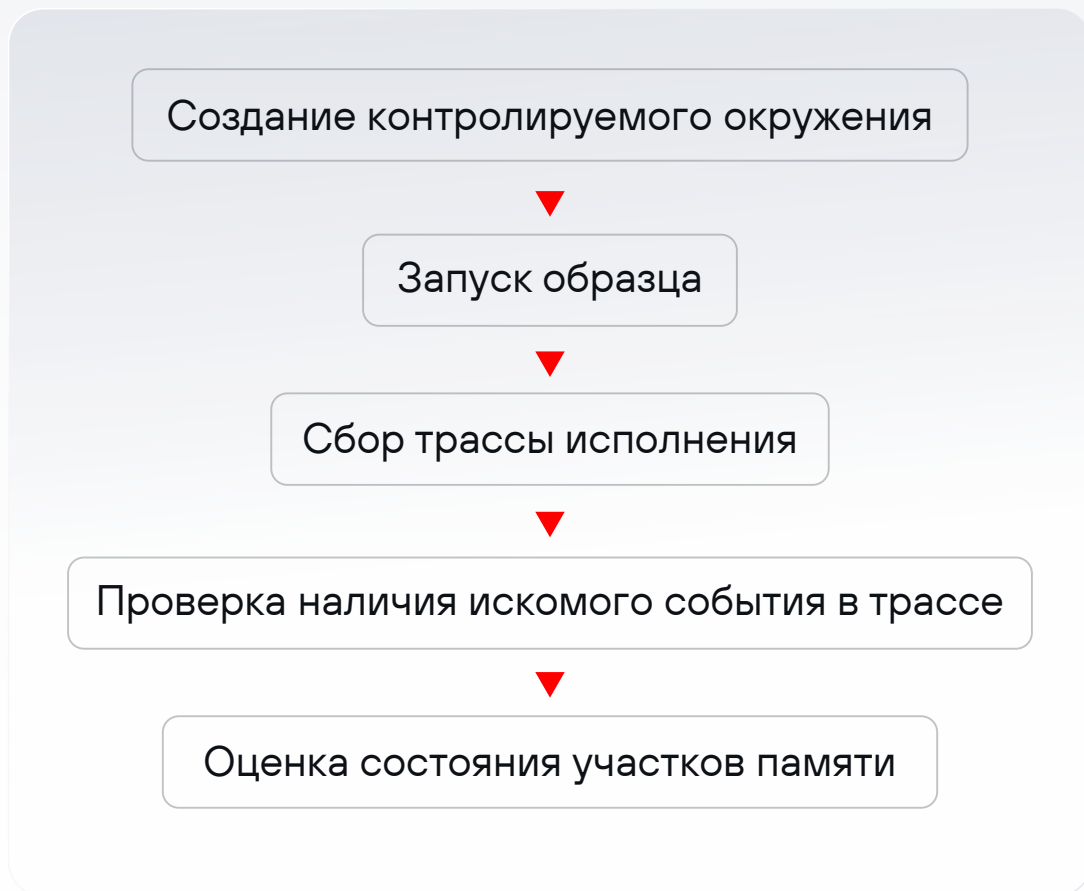


1	Статический анализ	Поиск уникальных характеристик файлов по базе сигнатур для выявления известных угроз
2	Карантин для расследования	Помещает файлы в изолированное хранилище для последующего анализа
3	Эмуляционный движок	Позволяет проводить динамический анализ для выявления продвинутого и неизвестного 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





**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 зашифрованным 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



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?

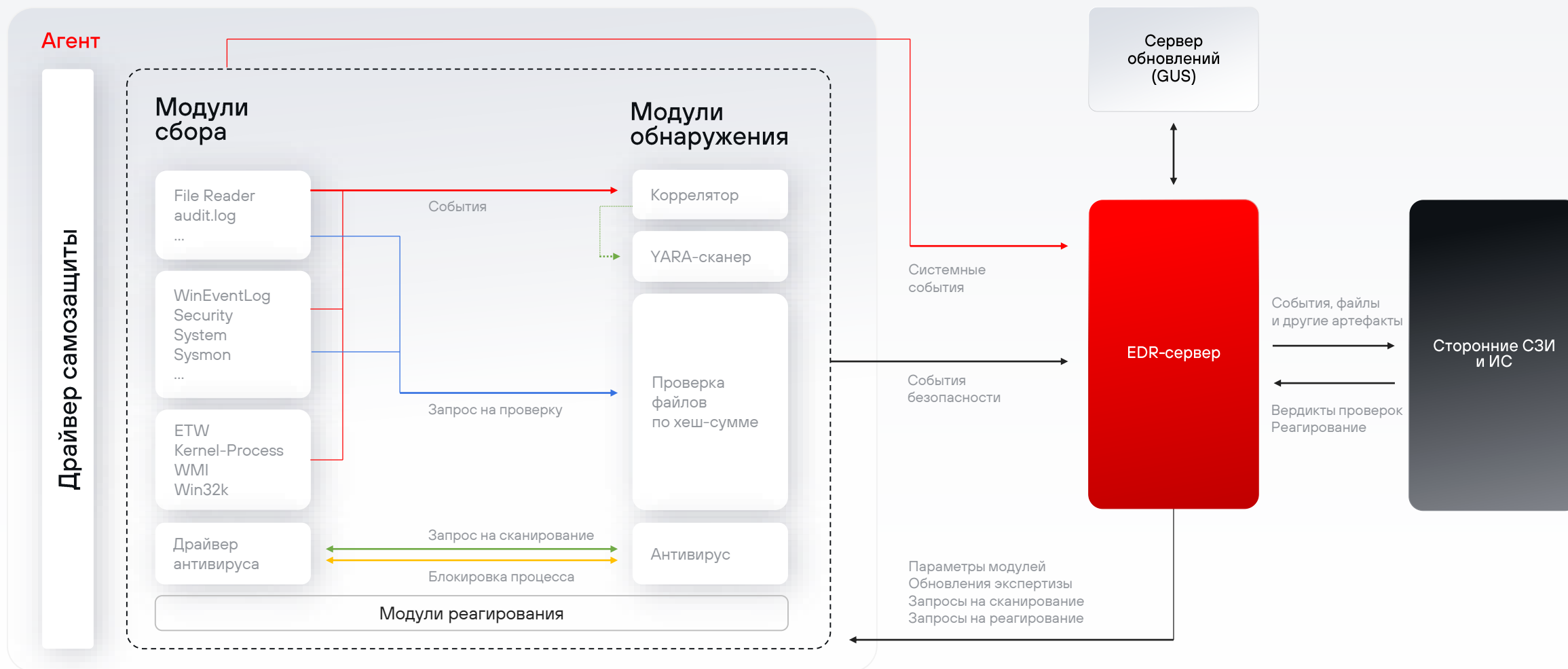
Выявление

- 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?

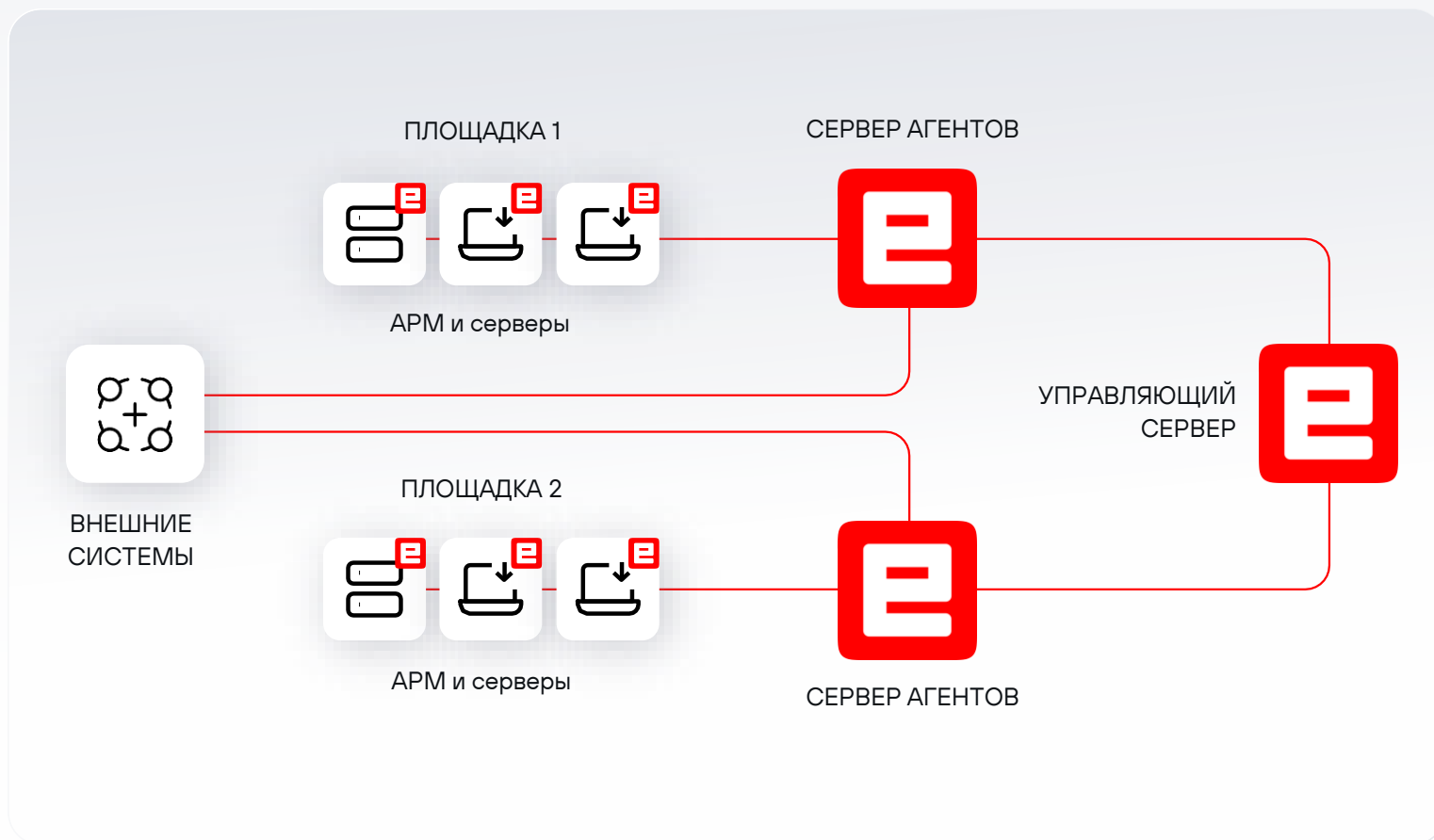
Реагирование

- 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

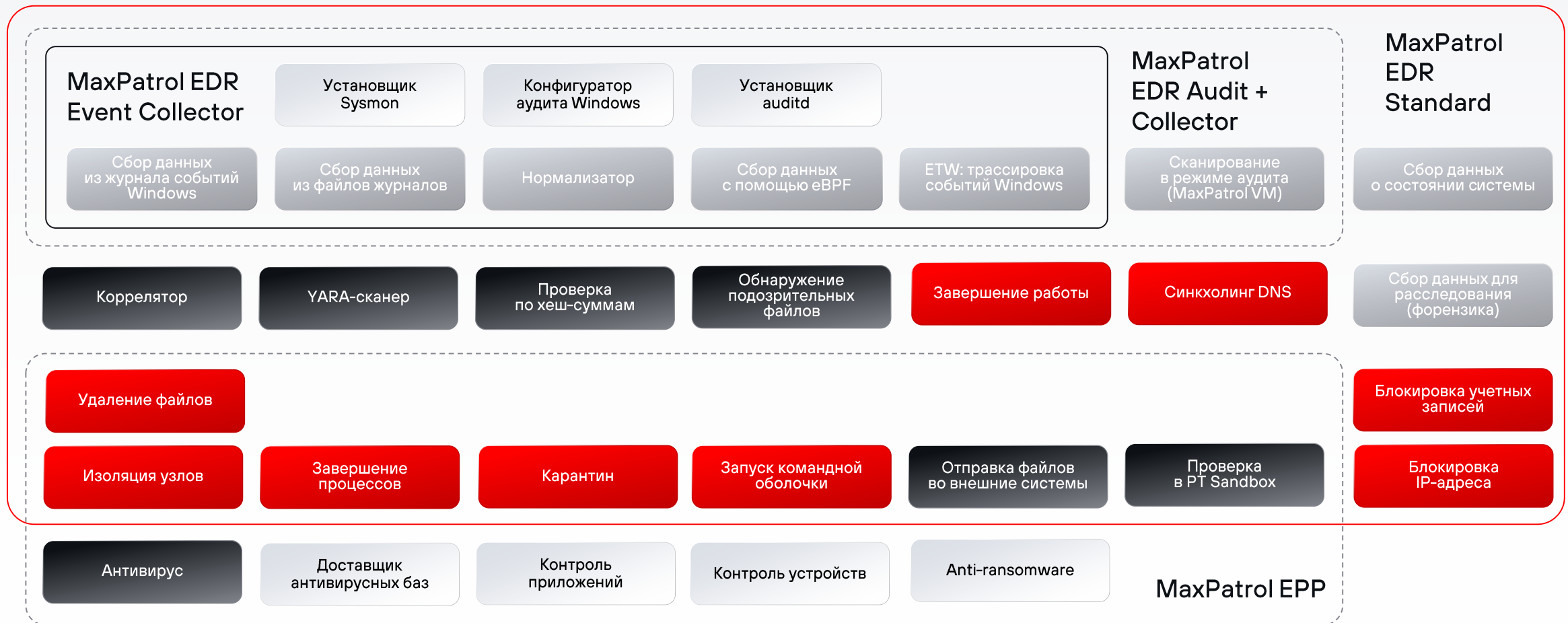


- **MaxPatrol EDR** состоит из серверной части и агентов, устанавливаемых на конечные устройства
- **Серверная часть** состоит из управляющего сервера и сервера агентов
- **Управляющий сервер** — основной компонент системы, который позволяет конфигурировать ее через веб-интерфейс. Поддерживается кластерная 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	«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 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

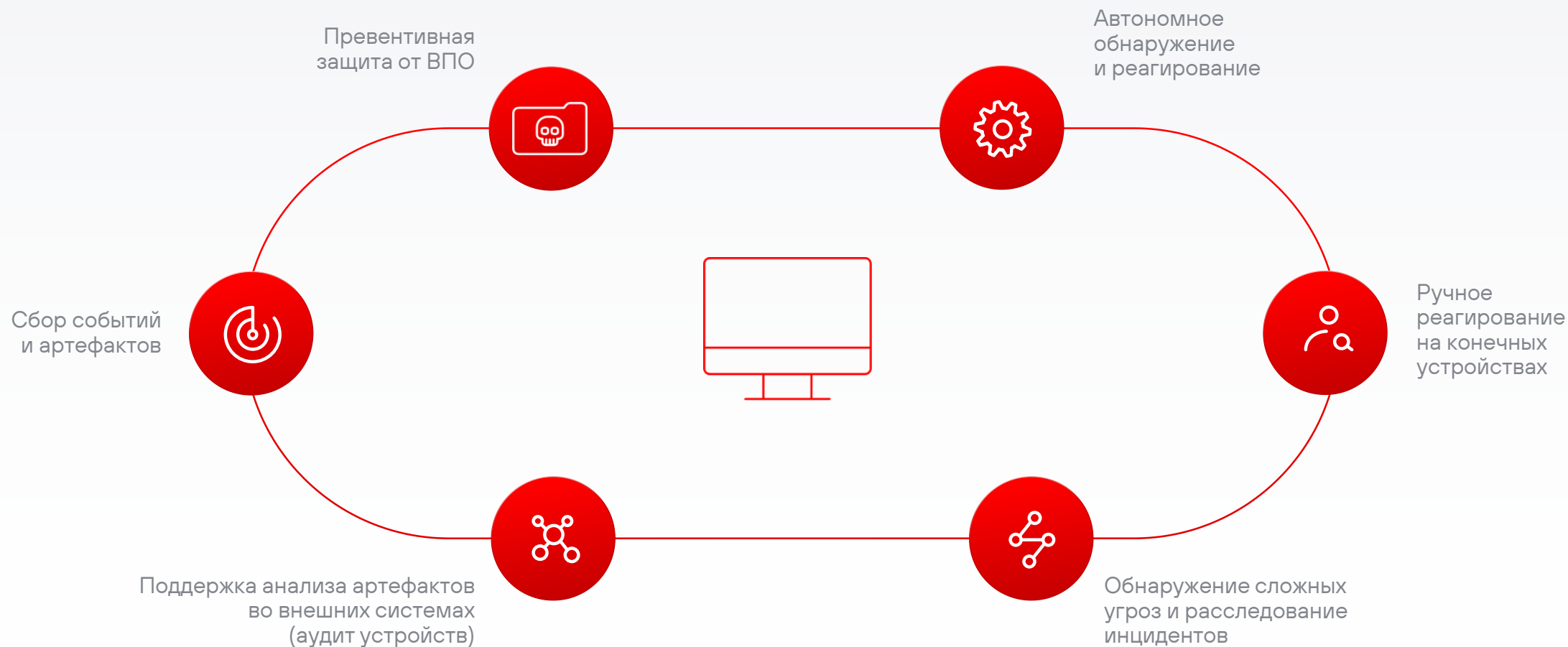
Инструмент команды
защитников в рамках
кибербитв Standoff

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



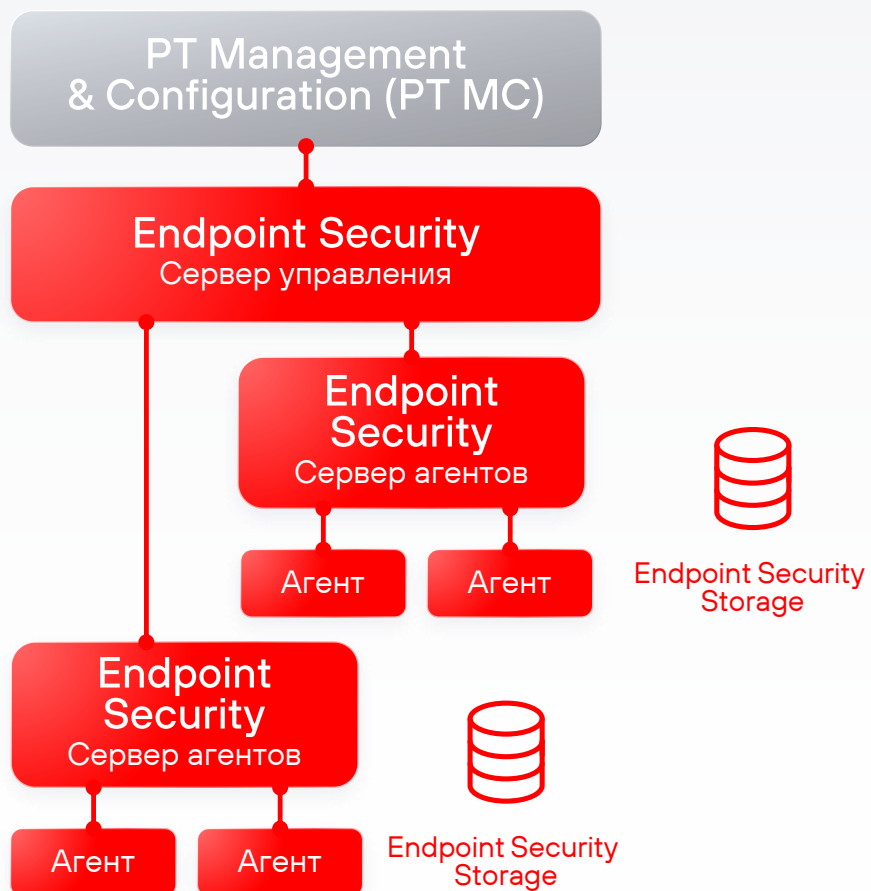
Сбор событий, обнаружение и автоматическое реагирование

- Автономное обнаружение на агентах
- Многоэтапные проверки
- Автоматизация реагирования

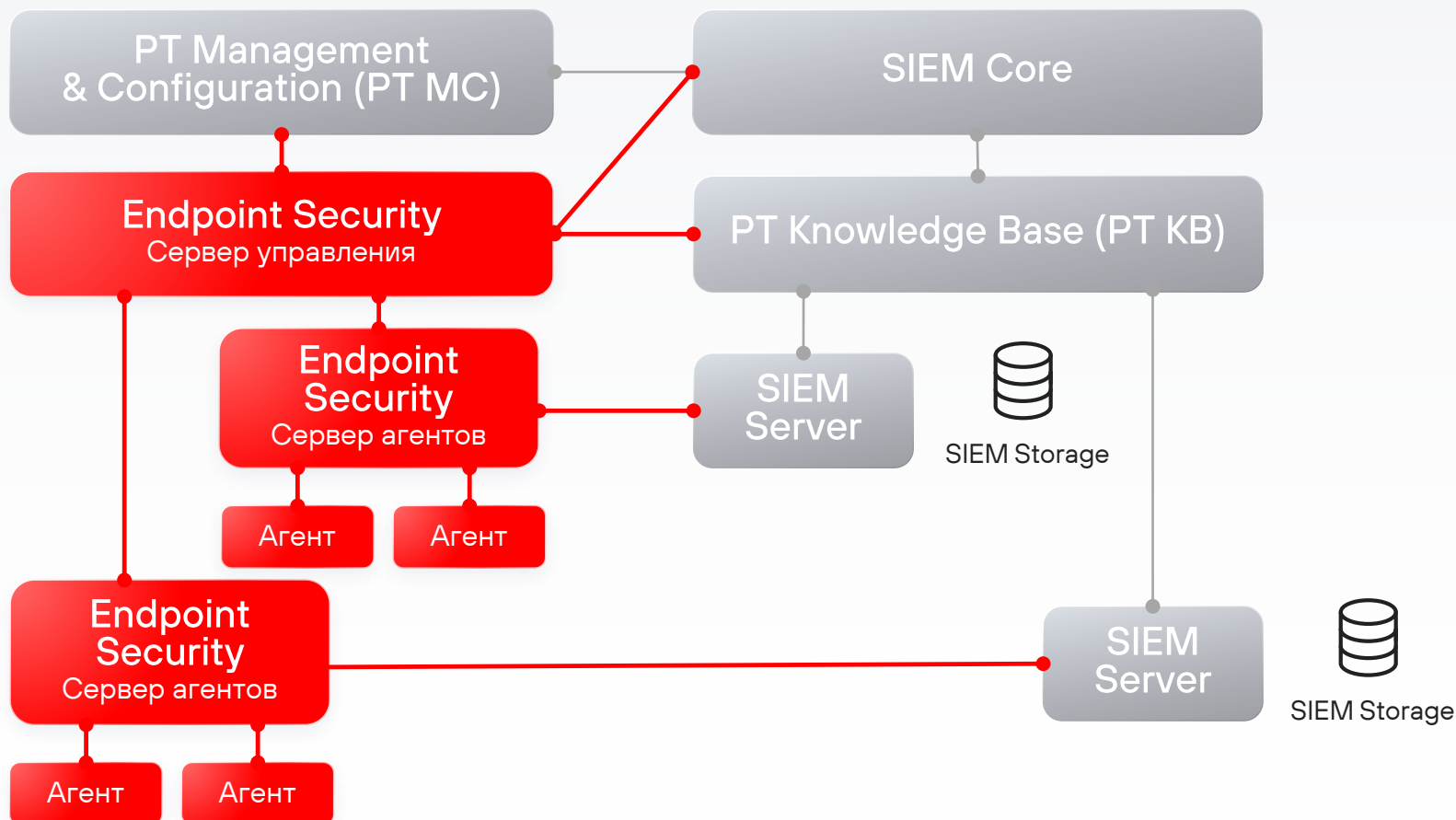


Установка и настройка MaxPatrol Endpoint Security

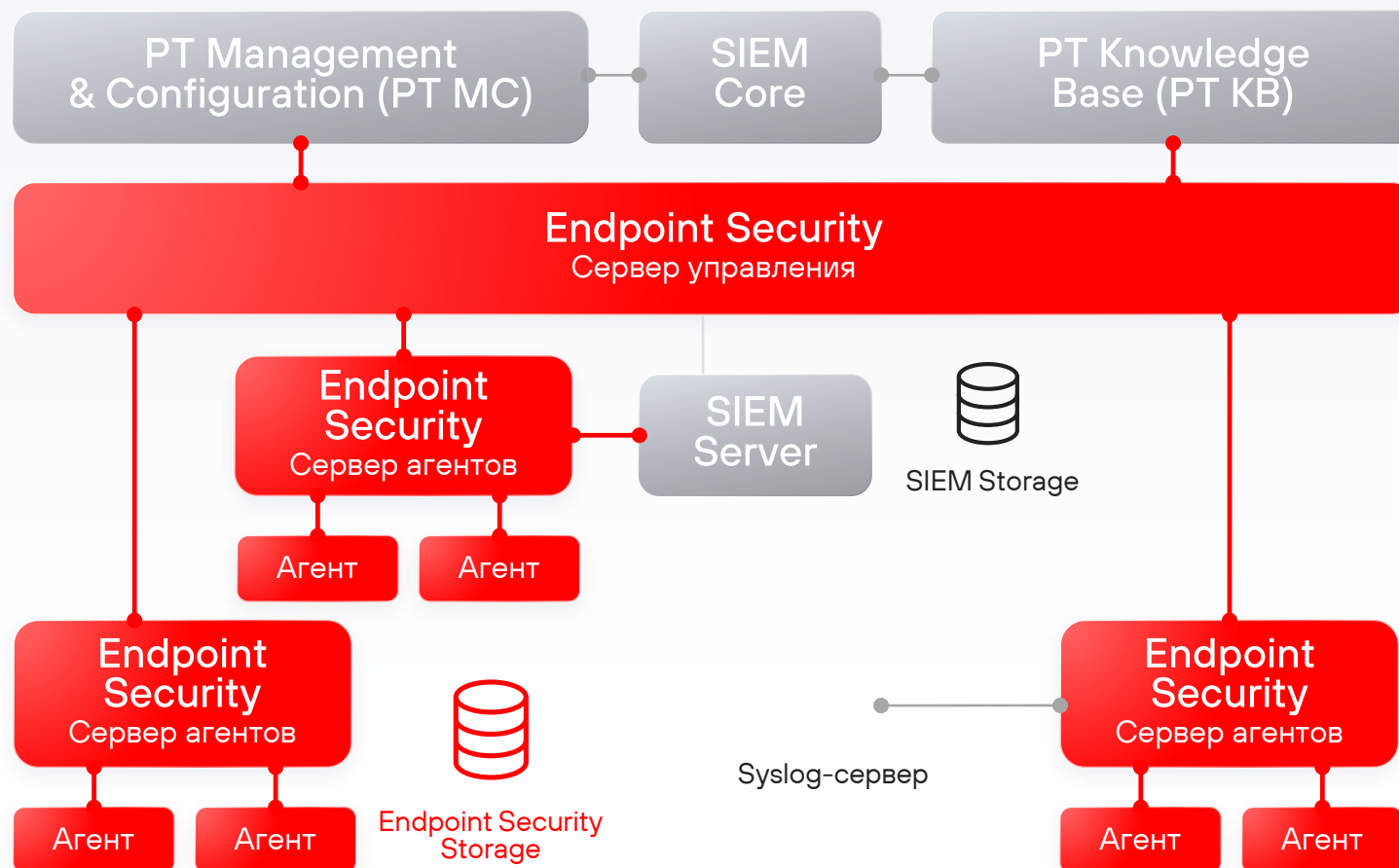
Варианты развертывания: собственное хранилище



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		

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

pt

Активы 268

Фильтры +

🔍

👁️ 👁️ Все активы 🔍 ⌵

☐	IP-адрес	MAC-адрес	FQDN	OC	Версия агента	Агент	Первоист...	Добавлен	Изменен	Мет
☐	10.50.34.17	fa:16:3e:a0:46:8c	v8304509-a...	🏠	4.3.0+416-ab070...	🟢 Установлен	👤	12 мая, 13:54	Сегодня, 12:43	
☐	10.50.34.214	fa:16:3e:36:99:38	v8304509-a...	🏠	4.3.0+416-ab070...	🟢 Установлен	👤	12 мая, 13:54	Сегодня, 12:43	
☐	10.20.155.163	00:50:56:af:e2:17	edr-qa-deb3...	🏠	4.3.0+416-ab070...	🔄 Устанавливается	👤	Вчера, 06:16	Сегодня, 12:16	
☐	127.0.0.2		vasya	🌐		🔄 Устанавливается	📄	Сегодня, 10...	Сегодня, 10:39	
☐	127.0.0.1			🌐		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:39	
☐	96.11.248.74	58:ed:06:38:43:09	d-edl113.b56...	🏠		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:36	
☐	126.239.233.179	c6:26:22:37:97:83		🌐		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:36	
☐	231.241.13.70	84:0d:6b:b4:a0:37	c0cra2.ssa4...	🌐		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:36	
☒	242.112.220.149			🏠		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:36	
☒	23.186.150.174	b9:83:2c:c2:3c:41	jtb4vofd.3tb...	🌐		❌ Не установлен	📄	Сегодня, 10...	Сегодня, 10:36	
☒	172.29.0.7	02:42:ac:1d:00:07	deployment-...	🏠	4.3.0+416-ab070...	🟢 Установлен	👤	Вчера, 12:13	Вчера, 16:00	Те
☐	172.29.0.7	02:42:ac:1d:00:07				🟢 Установлен	👤	Вчера, 15:59	Вчера, 15:59	
☐	172.29.0.6	02:42:ac:1d:00:06				🔄 Устанавливается	👤	Вчера, 11:23	Вчера, 11:23	
☐	172.29.0.4	02:42:ac:1d:00:04				🔄 Устанавливается	👤	Вчера, 11:22	Вчера, 11:22	
☐	172.29.0.5	02:42:ac:1d:00:05				🔄 Устанавливается	👤	Вчера, 11:22	Вчера, 11:22	
☐	172.29.0.2	02:42:ac:1d:00:02				🚨 Ошибка установки	👤	Вчера, 11:22	Вчера, 11:22	
☐	10.20.155.3	00:1c:7f:a3:6a:a0				🚨 Ошибка установки	👤	Вчера, 06:52	Вчера, 06:52	
☐	9.237.184.195	0e:05:91:2d:b4:f5		🏠		🚨 Ошибка установки	📄	undefined	13 мая, 09:54	
☐	49.17.231.69						📄	undefined	13 мая, 09:54	
☐	22.188.35.156	76:15:12:b5:cb:3e					📄	undefined	13 мая, 09:54	

Выбрано: 3 | Установить агент 📄 🔄 👁️ ⌵

96.11.248.74

58:ed:06:38:43:09

▶ Установить агент

Агент ☒ Не установлен

OC ☒ Windows

FQDN d-edl113.b56.75kuxw.ptsecurity

Добавлен Сегодня, 10:36

Изменен Сегодня, 10:36

Первоисточник данных 📄 CSV-файл

Метки [Добавить](#)

Централизация политик и групп



> Централизованное управление группами и политиками в продукте

> Автоматическое применение изменений политик сразу на всех серверах агентов

MaxPatrol EDR

- Agent Server 03 (E... >
- Агенты
- Группы агентов
- Политики** >
- Активы
- События

Политики

- Default - Антивирусная защита 9
- Default - Интеграция с MaxPatrol VM 9
- Default - Интеграция с PT Sandbox 9
- Default - Конфигуратор аудита Wind... 1
- Default - Обнаружение и реагирова... 3
- Default - Обнаружение и реагиров... 10
- Default - Сбор данных для расслед...**
- Default - Сбор данных с контролле... 5
- Default - Сбор данных с рабочих ст... 4
- Default - Сбор данных с рабочих ст... 6
- Default - Сбор данных с серверов ... 3
- adenisova - new_policy 1
- egpimashin 0
- lartemova - T3_10.0 0

Default - Сбор данных для расследования

Модули 1 Группы 5 Параметры Экспертиза

Поиск

Группа Сервер агентов

- ☐ PRESALE - Серверы Windows 2
- ☐ PRESALE - Рабочие станции Windows (не доменные) 2
- ☐ PRESALE - Рабочие станции Windows 2
- ☐ PRESALE - Рабочие станции Linux 2
- ☐ PRESALE - Контроллеры домена 2

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

Агенты

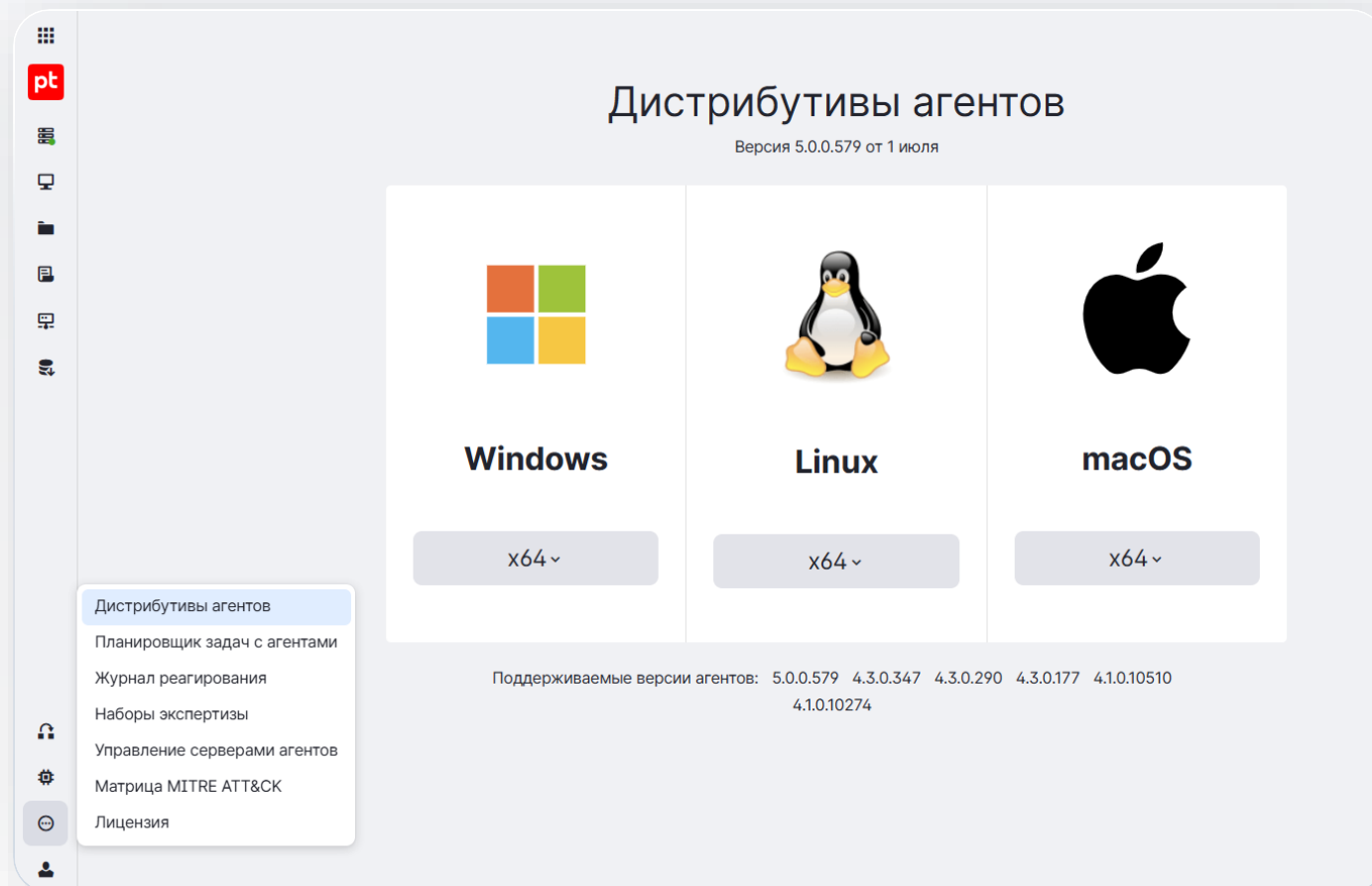


Все необходимые дистрибутивы под рукой

- 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

The screenshot displays a web-based 'Task Scheduler' interface. The main window has a sidebar with a 'pt' logo and a list of filters: 'Все задачи', 'Активные', 'Остановлены', 'Действия', and 'Все действия'. The 'Действия' section is expanded, showing options like 'Переместить в группу', 'Обновить агент', 'Установить выбранную версию...', and 'Удалить агент'. The main area shows a table with columns for 'Агент, группа' and 'Статус'. A 'Новая задача' (New Task) dialog box is open in the foreground. It contains the following fields: 'Название' (Name) with the value 'Авторизация новых windows-серверов'; 'Запуск' (Run) with radio buttons for 'Каждые' (Every) 5 minutes, 'Ежедневно в' (Daily at) 12:30, and 'При добавлении нового агента' (When a new agent is added); 'Агенты' (Agents) with a dropdown set to 'Все агенты' (All agents); 'Дополнительное условие на языке PDQL' (Additional condition in PDQL) with a text area containing 'Необязательно' (Optional); 'Действие' (Action) with a dropdown set to 'Переместить в группу' (Move to group); and 'Куда' (Where) with a dropdown set to 'Windows серверы' (Windows servers). At the bottom of the dialog are 'Создать' (Create) and 'Отмена' (Cancel) buttons.

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 MaxPatrol EDR interface with a 'Новая задача' (New Task) dialog box open. The dialog box contains the following fields and options:

- Название** (Name): Агенты в критичном сегменте
- Запуск** (Run):
 - ☒ Каждые 5 минут (Every 5 minutes)
 - ☐ Ежедневно в 12:30 (Daily at 12:30)
 - ☐ При добавлении нового агента (When adding a new agent)
- Агенты** (Agents): Все агенты (All agents)
- Дополнительное условие на языке PDQL** (Additional condition in PDQL): 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)

At the bottom of the dialog box, there are two buttons: '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).



Эксплуатация MaxPatrol EPP

Антивирусная защита



Антивирус

Версия 2.0.47948

Основные параметры

Автоматические действия при обнаружении угрозы

Блокировать файлы

☒ Да

Лечить файлы

☐ Да

Удаление файлов и отправку их в карантин вы можете настроить в мастере назначения действий

Проверки по расписанию

Задача

Название

Задача

*Запуск

☒ Не запускать ☐ Каждую неделю ☐ По месяцам

Исключения для проверок

Windows

Linux

Глобальные ?

Хеш-сумма файла (MD5, SHA-256), путь или маска файлов с новой строки. Путь может содержать символы * и ?

В реальном времени ?

Хеш-сумма файла (MD5, SHA-256), путь или маска файлов с новой строки. Путь может содержать символы * и ?

По запросу ?

Хеш-сумма файла (MD5, SHA-256), путь или маска файлов с новой строки. Путь может содержать символы * и ?

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

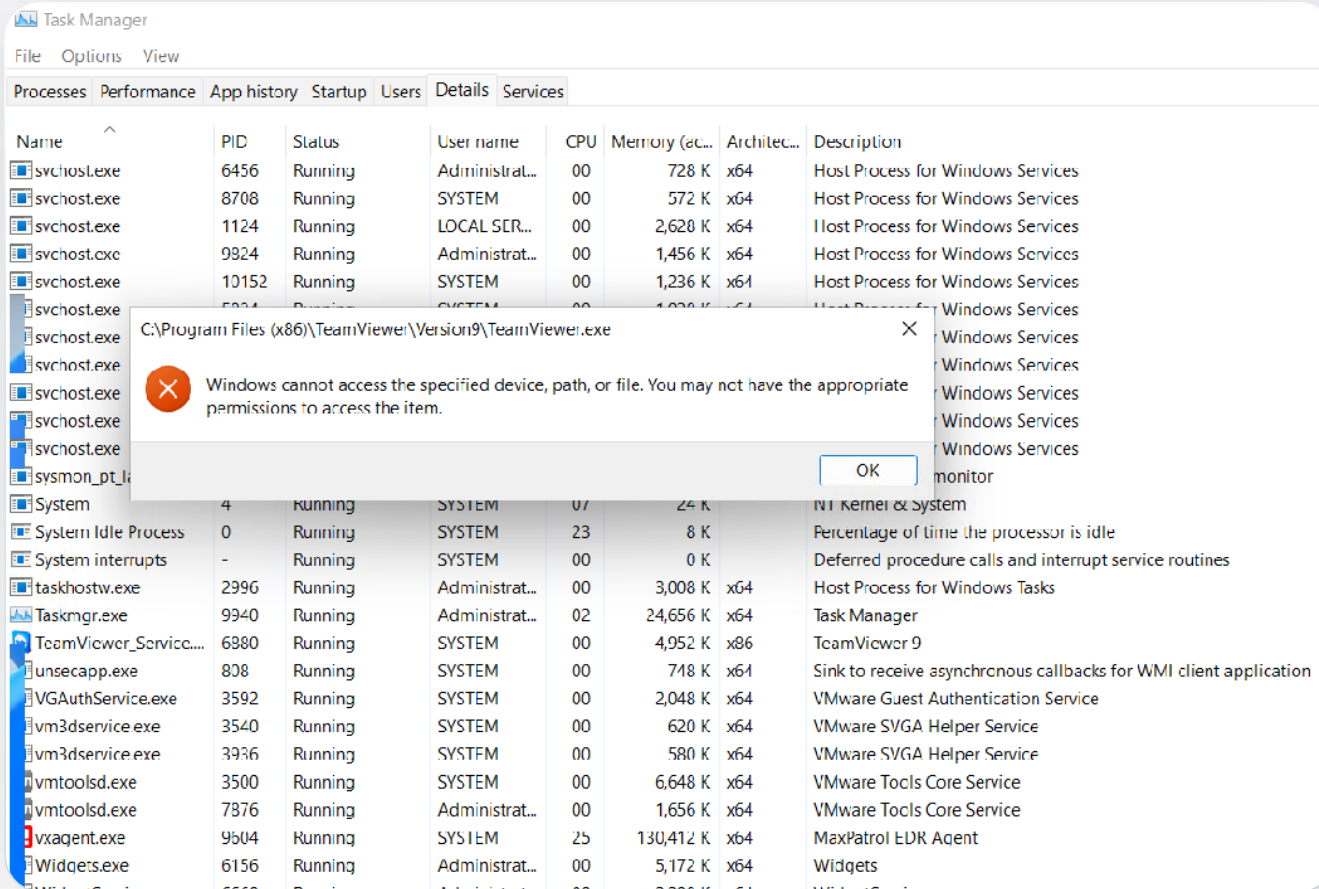


Агенты 5

Поиск агентов

	Название	IP-адрес	П.	О.	А.	Версия	Самозащита	Модули	Зарегистрирован	Последний раз в сети	Имя узла	Пол
☐	windows_WORKSTATION01_of22270	192.168.55.152				4.3.0.177		Антивирус (бета-версия... Все 10	Вчера, 14:42	Сегодня, 19:26	WORKSTATION01	Gue:
☐	linux_workstation04_1e05f6	192.168.55.133				4.3.0.177		YARA-сканер, Блокиров... Все 20	18 ноя 2025	Сегодня, 19:26	workstation04	ptus
☐	windows_DESKTOP-7SLD1TO_d14aa2	192.168.55.27				4.3.0.177		ETW: трассировка собы... Все 27	12 ноя 2025	Сегодня, 19:26	WORKSTATION02	ptus
☐	windows_DESKTOP-7SLD1TO_bad565	192.168.55.26				4.3.0.177		ETW: трассировка собы... Все 27	12 ноя 2025	23 дек 2025	workstation01	ptus
☐	windows_DESKTOP-7SLD1TO_9ffdaf	192.168.55.28				4.3.0.177		ETW: трассировка собы... Все 27	12 ноя 2025	Сегодня, 19:26	WORKSTATION03	ptus

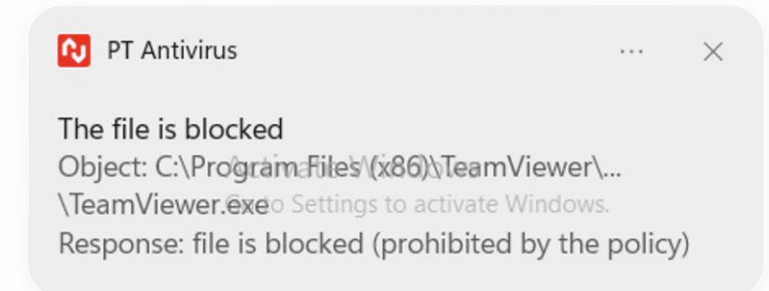
Контроль приложений



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

✓ Контроль устройств
Версия 1.0.46689 · 🖥️

Основные параметры ▾

Съёмные устройства

HDD/SSD-накопители, карты памяти и устройства для их чтения ?

Уведомления	Режим доступа
☒ Подключение ☐ Отключение	☐ Разрешить ☒ Блокировать

Дисководы ?

Уведомления	Режим доступа
☐ Подключение ☐ Отключение	☒ Разрешить ☐ Блокировать

Стримеры (ленточные накопители)

Уведомления	Режим доступа
☐ Подключение ☐ Отключение	☒ Разрешить ☐ Блокировать

Мобильные устройства (MTP/PTP) ?

Уведомления	Режим доступа
☐ Подключение ☐ Отключение	☒ Разрешить ☐ Блокировать

Сетевые устройства ?

Сохранить Отмена

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

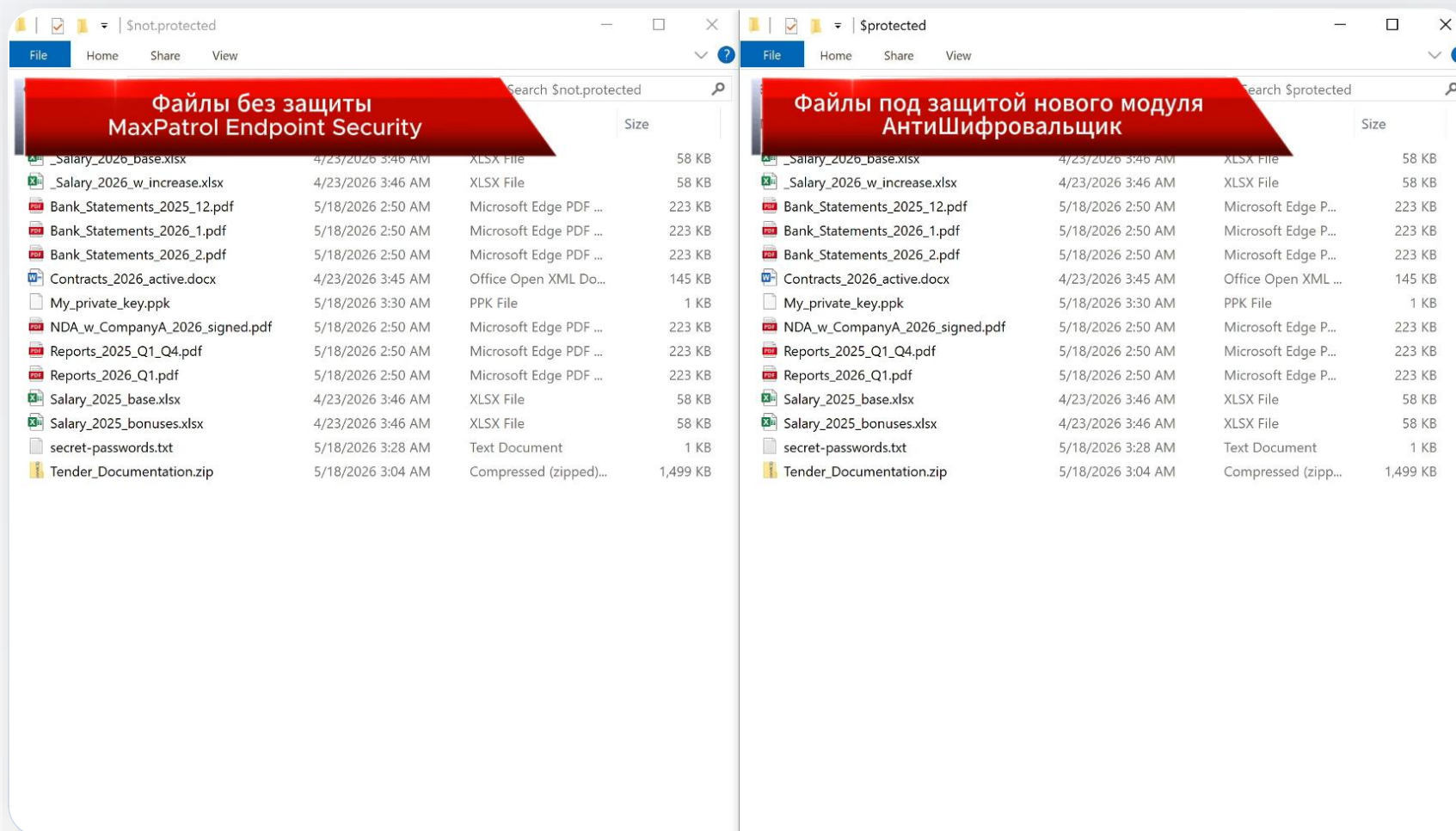
2 Поведенческие эвристики

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

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 хеш-сумм от PT ESC

> Начиная с релиза 8.3 можно добавлять пользовательские хеш-суммы

> 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 и хеш-суммы

Модули

Коррелятор и нормализатор
Проверка файлов по хеш-сумме

Дистрибутивы агентов
Планировщик задач с агентами
Журнал реагирования
Наборы экспертизы
Управление серверами агентов
Матрица MITRE ATT&CK
Лицензия

Наборы экспертизы для коррелятора и нормализат...

Обновить

Название или тип экспертизы

С..	Название	Версия	База данных	Тип экспертизы
	test_pack_for_edr	28 февраля, 21:29	For_install	Корреляция
	pack_for_siem	8 мая, 11:48	test_for_EDR	Корреляция, нормал
	Все объекты	8 мая, 11:49	test_for_EDR	Корреляция, нормал

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

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

События 238

Группировка

Фильтры

Период Последние 30 дней

importance 2 x

Сбросить

time	event_src_hostname	importance	msgid	action
14 мая, 13:46:59	workstation01	🟡	Execute_Malicious_Command	start
14 мая, 13:46:59	workstation01	🟡	Windows_Autorun_Modification	modif
14 мая, 13:46:59	workstation01	🟡	Mimikatz_Command	start
14 мая, 13:46:59	workstation01	🔴	Windows_Hacktool_Usage	start
14 мая, 13:46:56	workstation01	🟡	Access_To_Web_Browsers_Process	acce
14 мая, 13:46:54	workstation01	🔴	fhc_file_hash_found	detec
14 мая, 13:46:54	workstation01	🔴	fhc_file_hash_found	detec
14 мая, 13:46:51	workstation01	🟡	Access_To_Web_Browsers_Process	acce
14 мая, 13:46:36	workstation01	🟡	LSASS_Handle_Duplicate	crea
14 мая, 13:46:35	workstation01	🔴	fhc_file_hash_found	detec
14 мая, 13:46:35	workstation01	🔴	fhc_file_hash_found	detec
14 мая, 13:46:35	workstation01	🔴	ProcDump_Usage	start
14 мая, 13:46:35	workstation01	🟡	Creation_Suspicious_File	crea
14 мая, 13:46:34	workstation01	🟡	Mimikatz_Command	start
14 мая, 13:46:34	workstation01	🔴	Windows_Hacktool_Usage	start
14 мая, 13:46:34	workstation01	🔴	Windows_Hacktool_Usage	start
14 мая, 13:46:08	workstation01	🔴	Creation_Suspicious_File	crea
14 мая, 13:45:56	workstation01	🟡	Domain_Trust_Discovery	start
14 мая, 13:45:47	workstation01	🟡	Execute_Malicious_Command	start

Реагирование на агента
windows_workstation01_bad565

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, автозагрузка

Реагирование из карточки события в MaxPatrol SIEM



> Принятие защитных мер
в едином интерфейсе

> Журналирование
выполняемых действий

> Сокращение затрат
на работу с инцидентами

The screenshot displays the MaxPatrol SIEM interface. On the left, a list of incidents is shown, with one incident selected. The incident details are displayed in the center, including a timeline of events and a list of related processes. On the right, the 'Реагирование' (Response) panel is open, showing a list of available response actions. A red arrow points from the 'Реагировать' (React) button in the incident card to the 'Реагирование' panel.

Реагирование

Название действия

- 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

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



The image shows a workflow in the MaxPatrol interface. On the left, a card for agent `windows_WORKSTATION01_of2270` is displayed. A red box highlights the **Реагировать** (React) button. A red arrow points from this button to a secondary window on the right titled **Реагирование на агенте windows_WORKSTATION01_of2270**. This window lists various actions that can be performed on the agent.

Агент

Статус: Подключен Авторизован

Зарегистрирован: 12 ноя, 19:35

Группа: [Рабочие станции Windows](#)

Версия: 4.1.0.10274

IP-адрес: 192.168.55.152

Идентификатор: 0f22700484415c6036bed1004422c3cc

Самозащита: Включена

Ссылки: [События](#) [Актив](#)

Узел

Имя: WORKSTATION01

ОС: Microsoft Windows 10 10.0.19045.6456 x64

FQDN: WORKSTATION01.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 агенте 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

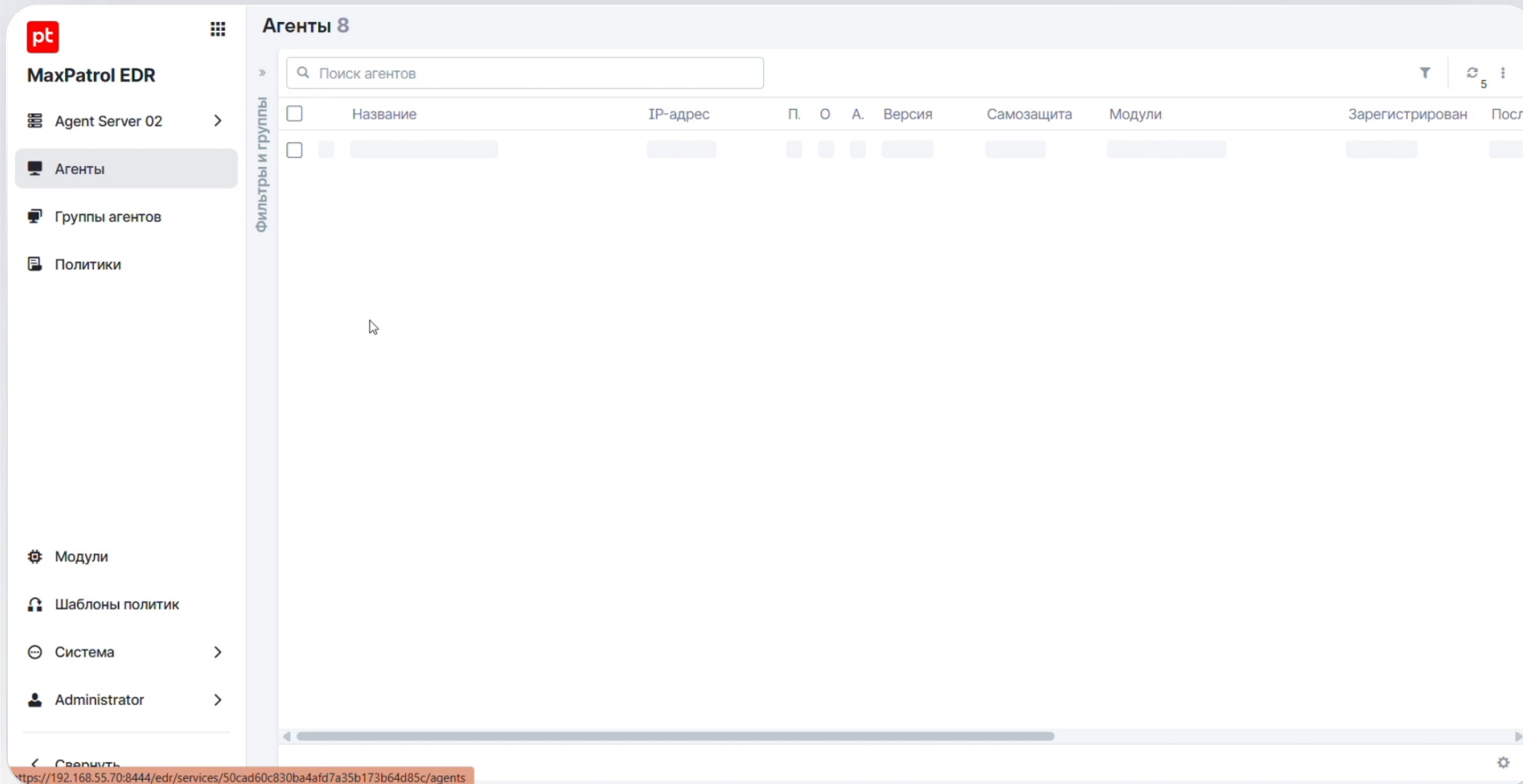
- Меньше затрат на ручные операции
- Запуск любых действий реагирования на любой выборке агентов
- Отслеживание статусов задач — понятная обратная связь от всех устройств
- Возможность повтора действий
- Возможность быстро применить другое действие для выбранной группы или некоторых агентов

The screenshot displays the MaxPatrol EDR web interface. The left 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 area is titled 'Агенты 6' and 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 dropdown menu is open, showing various actions like 'Заблокировать учетную запись (объект) по логину' and 'Завершить все сеансы'. Below the main table, a 'Журнал реагирования' (Response Log) window is open, showing a table of executed actions with columns for Agent, Platform, Last network time, Execution time, and Result. The log shows two successful actions for the selected agents.

Название	IP-адрес	П	О	А	Версия	Группа	Метки
windows_SERVER01_744064	192.168.55.151				4.1.0.10274	Windows серверы	
windows_WORKSTATION02_62fca7	192.168.55.153				4.1.0.10274	Рабочие станции Windows	
windows_WORKSTATION01_0f2270	192.168.55.152				4.1.0.10274	Рабочие станции Windows	
windows_DC-EDR_d01da4	192.168.55.150				4.1.0.10274	Контроллеры домена	
linux_workstation03.edr2.local_92b384							
linux_workstation04.edr2.local_b13c1d							

Результат	Агент	П.	Последний раз в сети	Выполнено	Результат
Выполняется	windows_WORKSTATION...		Сегодня, 16:37	Сегодня, 16:37:54	Завершено
Выполнено	windows_WORKSTATION...		Сегодня, 16:37	Сегодня, 16:37:47	Не удалось выполнить действие
Ошибка					

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

The screenshot displays the MaxPatrol EDR interface. On the left, a sidebar contains navigation options: 'Агенты' (Agents), 'Группы агентов' (Agent Groups), 'Политики' (Policies), 'Модули' (Modules), 'Шаблоны политик' (Policy Templates), 'Система' (System), 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 displayed, 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 a 'Проверить' (Check) button, a 'В карантин' (Quarantine) button, and a 'Скачать' (Download) button. Below these buttons, a table shows analysis results: 'С помощью YARA-правил' (Using YARA rules), 'По хеш-сумме' (By hash sum), 'Антивирусом' (By antivirus), and 'В PT Sandbox' (In PT Sandbox). The interface also includes a top navigation bar with 'Агенты / Рабочие станции Windows / windows_WORKSTATION01_0f2270 / Реагирование / Файлы' and a bottom status bar with 'MaxPatrol SIEM' and 'События с этим файлом'.

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 sections for Модули, Шаблоны политик, Система, and Administrator. The main panel shows a breadcrumb trail: Агенты / Рабочие станции Windows / windows_WORKSTATION01_of2270 / Реагирование / Процессы. A search bar is present above a table of running processes. The table has columns for process name, PID, start time, and memory usage. The process 'vm3dservice.exe' with PID 5400 is highlighted. To the right, a detailed view for 'vm3dservice.exe' is shown, including buttons for 'Завершить', 'Проверить', and '+ Дамп'. It lists attributes such as Process ID (5400), Start time (31 Oct, 15:18:29), Memory usage (0.09% (7 MB)), CPU usage (0%), User (EDR2\Administrator), Executable file (vm3dservice.exe), Path (C:\Windows\System32\vm3dservice.exe), and Command (C:\Windows\System32\vm3dservice.exe -u).

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

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

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
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

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
```

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	Описание Действия Переменные
PrintSpooler PrivEsc CVE 2022 30206	LSASS Memory Dump	action
PrivEsc via Comctl32	LSASS Shtinkering Dump	action
PrivEsc via UAC Elevated Data	Malware Trojan Powershell PowerSploit i	alert.context
Process from Mounted Disk	Malware Trojan Win32 Wiper a	alert context
PuntoSwitcher Diary Open	Masquerading Microsoft Signed Library	alert.key
Reading Registry Objects	MSBuild AWL Bypass	alert key
Remote Potato Capture Hash	ProcDump Usage	category.generic
Remote Potato Relay Hash		category generic
Remote SSP Dump		category.high
Remoting WinExec		category high
		category.low
		category low
		correlation_name
		correlation name

Выбрать другое действие

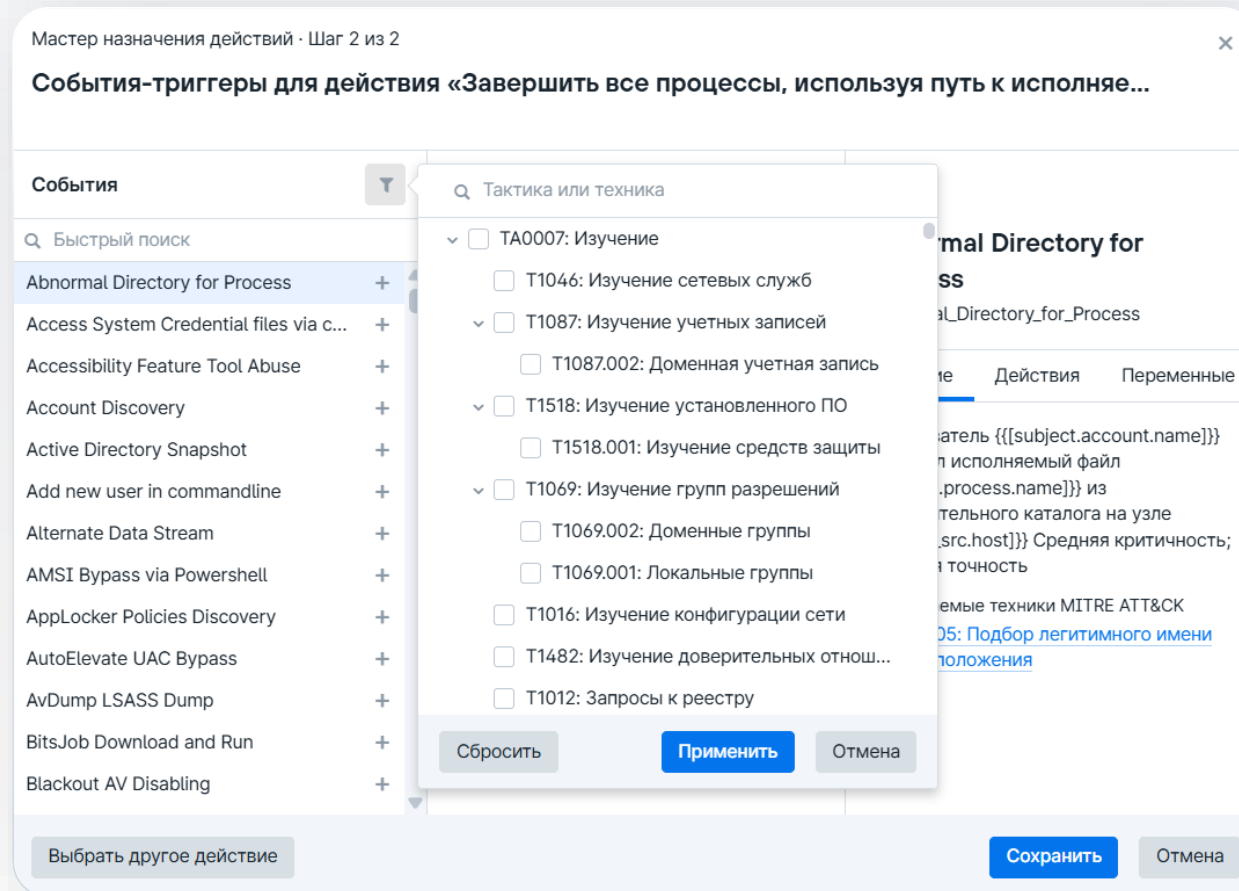
Сохранить Отмена

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





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.



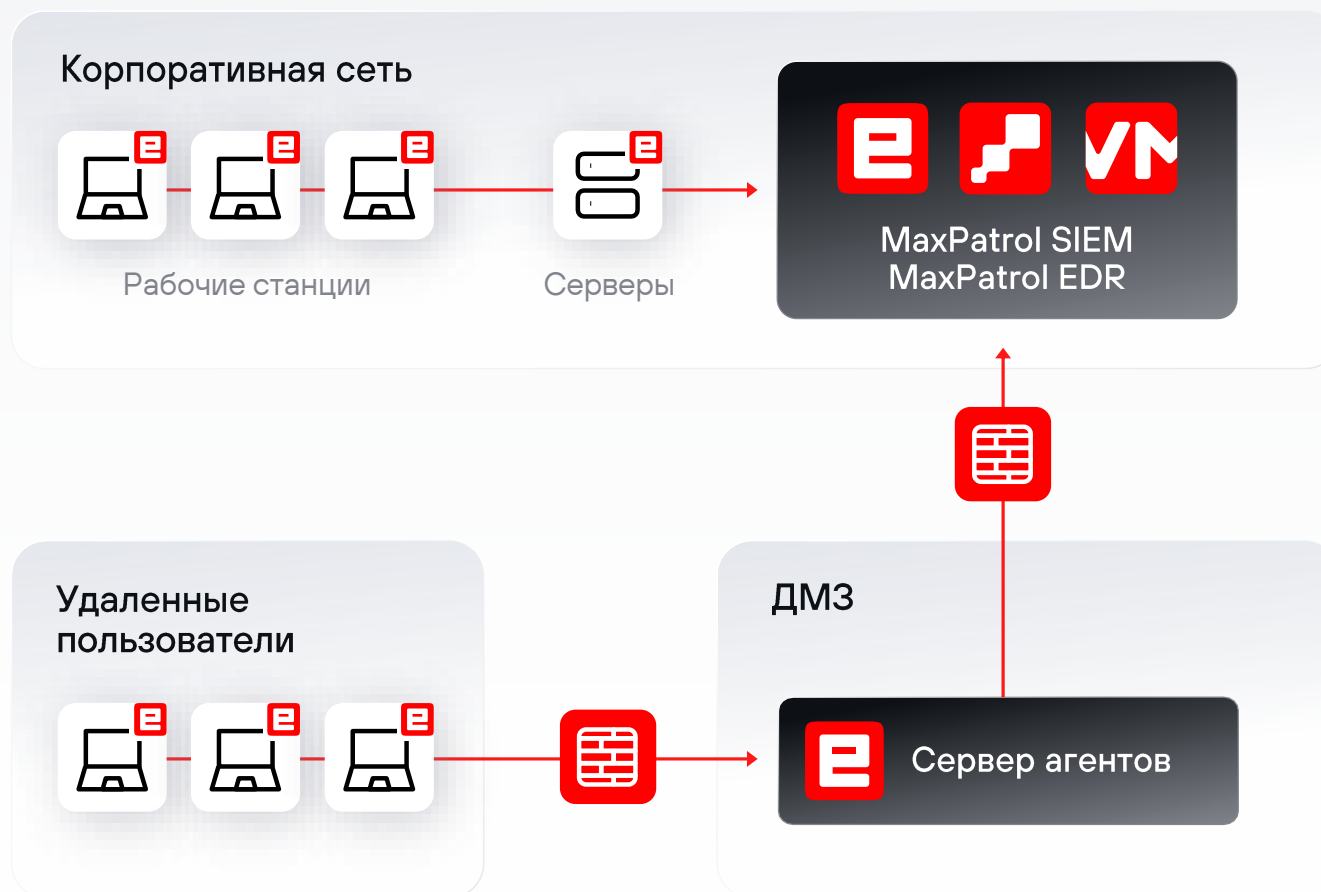
PT Sandbox

- Защита от ВПО, распространяемого через 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



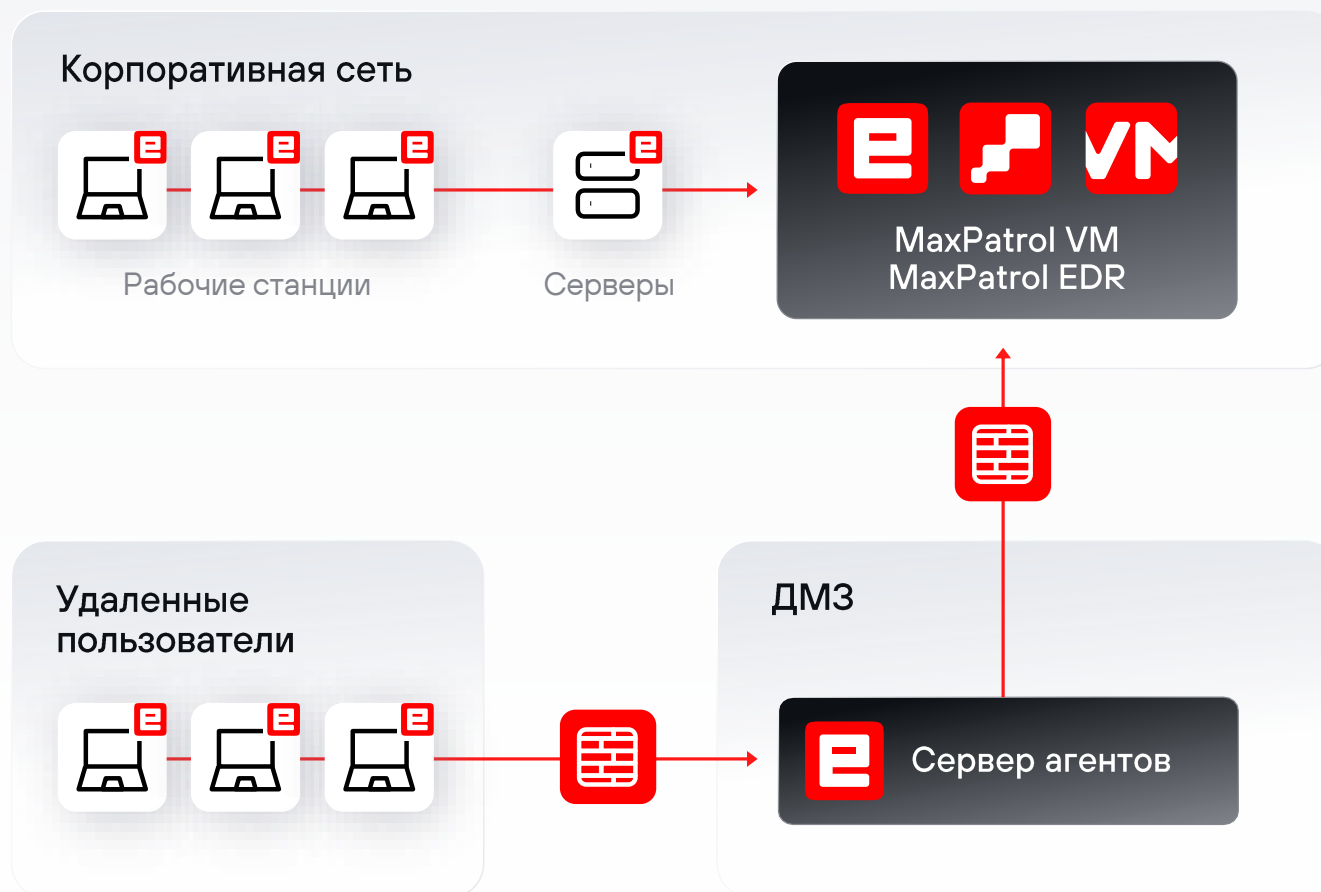
- > Контролируемый сбор событий
(включая устройства вне домена или периметра)
- > Расширенные возможности сбора данных
(агент EDR собирает то, что не умеет SIEM-система)
- > Оптимизация архитектуры
и нагрузки на MaxPatrol SIEM
- > Реагирование и работа
с исключениями из карточки события
- > Единая консоль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



MaxPatrol EDR + MaxPatrol VM



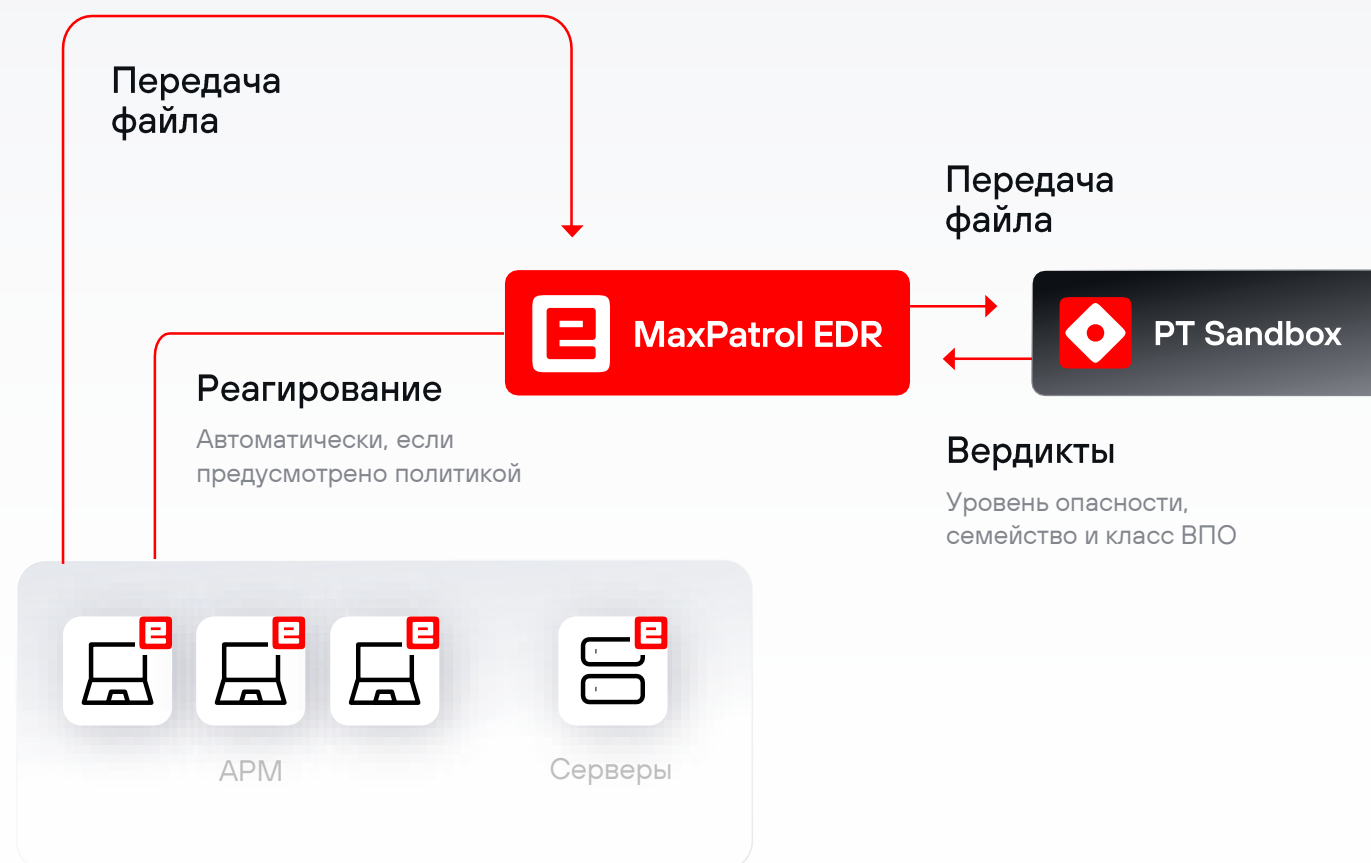
- > Нет необходимости использовать сервисные учетные записи
- > Сбор данных с узлов вне домена и устройств удаленных сотрудников
- > Настраиваемое расписание сканирования
- > Частое обновление данных об активах
- > Снижение нагрузки на сканирующий сервер и каналы связи
- > Единая консоль управления



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



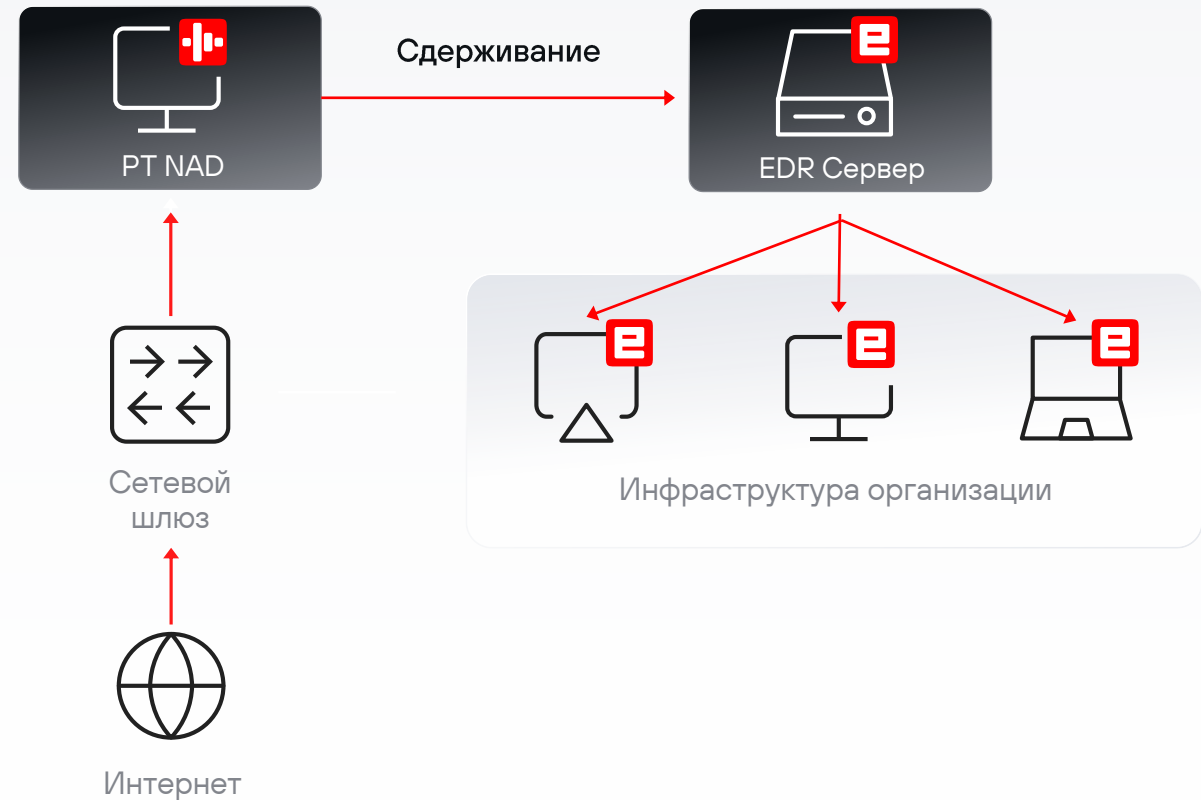
MaxPatrol EDR + PT NAD



Сдерживание угроз:

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

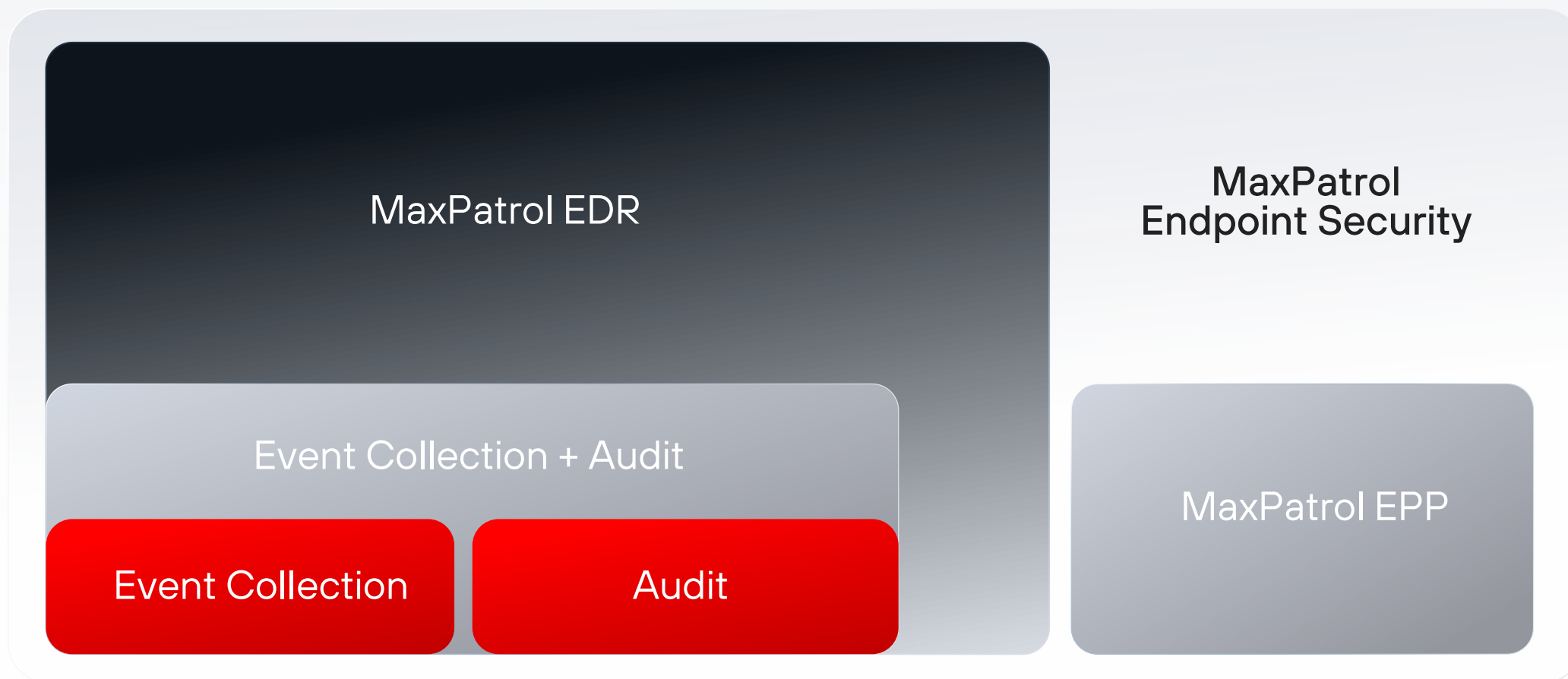
Детектирование угроз





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