Антон Киселев
Бизнес-лидер MaxPatrol VM

Юрий Бережной
Руководитель направления по развитию защиты конечных устройств Positive Technologies

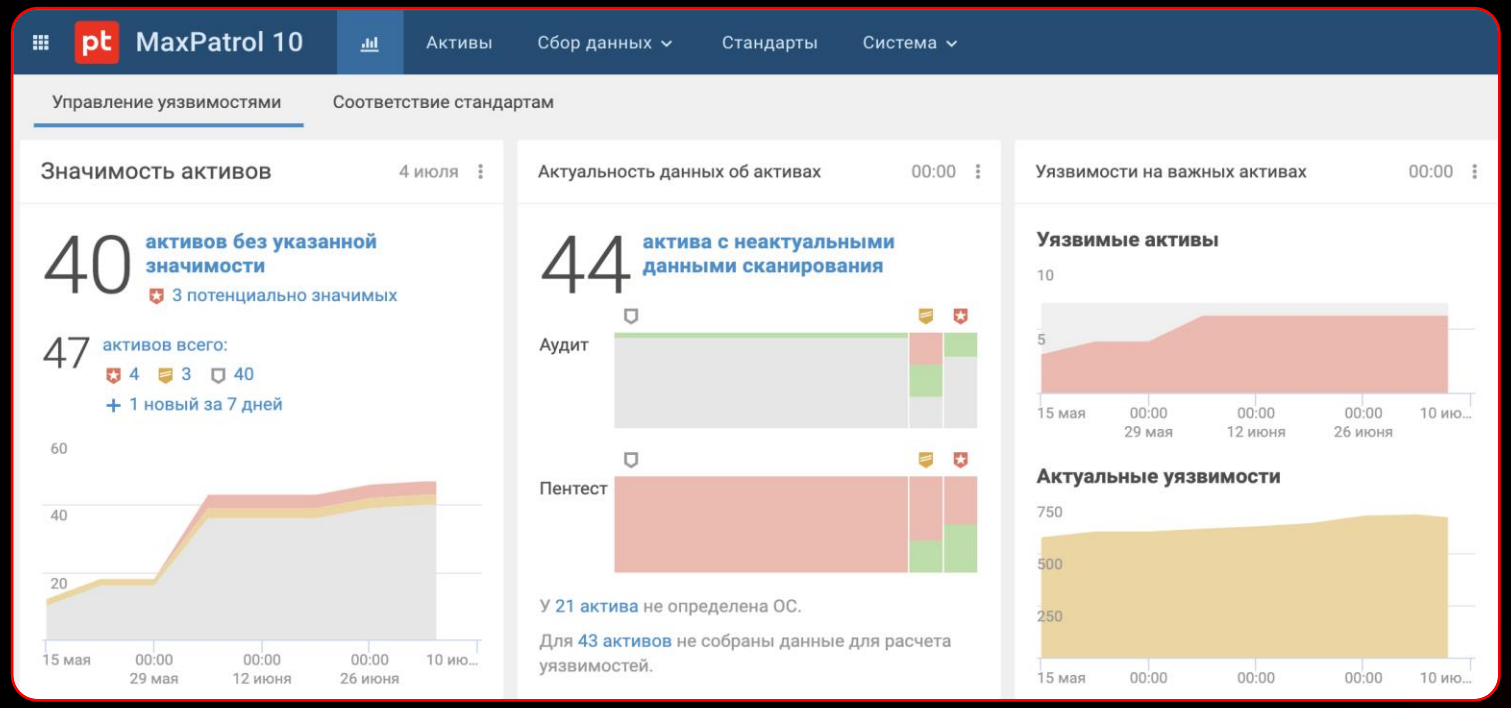
MaxPatrol VM и MaxPatrol EDR:

управление уязвимостями и защита устройств инфраструктуры

01

Max Patrol VM коротко

MaxPatrol VM



Решение,
для **построения полноценного**
процесса управления
уязвимостями
и контроля
соответствия
стандартам

02

Max Patrol VM,
ЧТО НОВОГО В НОВОМ

Ближайший релиз 2.5

Уязвимости в WEB

Проверка подключения

Кастомный сбор информации об активе

Уязвимости ПО, запущенного в docker-контейнерах

Технологические окна для сканирования

Мобильный сканер экспорт импорт результатов сканирования

Библиотека требований, новые стандарты PT Essentials

Ближайший релиз 2.5

- Обновление pentest проверок из облака
- Глобальные исключения
- Популярные отчеты из MaxPatrol 8 в MaxPatrol VM
- Приоритет выполнения задач сканирования
- Ролевая модель доступа к группам
- Написание собственных требований и соответственно стандартов в HCC 1.5
- Топология в отдельном окне

Камера, мотор

Max Patrol VM

хостовой коллектор

Сканирование выключенных машин в период сетевого сканирования

Сканирование удаленных пользователей

Сканирование в архитектурно независимых сегментах

Немного о наших планах

- VM Light
- Reporting portal
- Иерархия ядер
- Упрощение установки и обновления продуктов
- Контроль лицензионных метрик

03

Max Patrol EDR

больше чем сенсор

Современные угрозы

78%

атак в 2022 году были целенаправленными*

Топ-3

ВПО, которое злоумышленники используют прямо сейчас: шифровальщики, инфостилеры, ВПО для удаленного доступа*

ВПО для разных систем

Злоумышленники осуществляют активный поиск уязвимостей в российских ОС на базе Linux

Расширяют возможности проникновения в разные ОС за счет портирования ВПО (языки Go, Rust, Nim и др.)

* Актуальные киберугрозы

Экспертиза на каждом узле

1 **Поставляется с набором экспертизы для обнаружения актуальных угроз:**

600+
правил корреляции

5000+
YARA-правил

2 **Позволяет создавать и использовать собственные yara-правила**

3 **Обрабатывает поступающие события и обогащает их полезной информацией:**

- определяет уровень привилегий учетных записей,
- от имени которых запускаются процессы
- фиксирует контрольные суммы процессов и исполняемых файлов
- отслеживает цепочки подозрительных действий

Больше чем сенсор

1 Автономная работа

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

2 Поддержка отечественных ОС

Доступен для всех популярных ОС, включая отечественные (Astra Linux, «РЕД ОС», «Альт» и др.).

3 Ручное или автоматическое реагирование

Богатый выбор действий, которые можно полностью автоматизировать: остановка процесса, удаление файлов, изоляция устройства, отправка на анализ, синкхолинг.

4 Своевременное и непрерывное обнаружение

Поставляется с набором экспертных правил PT ESC, благодаря чему способен обнаружить актуальные угрозы, включая тактики и техники из матрицы MITRE ATT&CK (топ-50 для Windows и топ-20 для Linux), даже в полностью автономном режиме. Новые пакеты экспертизы поставляются непрерывно.

Обнаружение

Доставка и установка инструментов для расширенного мониторинга на конечные устройства

Комбинирование автономных механизмов обнаружения:
- Статический анализ
- Поведенческий анализ

Многоэтапные проверки — последовательный автоматический запуск механизмов обнаружения

Гарантированное хранение артефактов для расследования

Обнаруживает самые популярные техники из матрицы mitre att&ck

Топ-50
для Windows

Топ-20
для Linux

Реагирование

- Полная или частичная сетевая изоляция узлов
- Выполнение команд в удаленной консоли
- Завершение процессов
- Проверка по хешам файлов
- Отправка в карантин и/или удаление файлов
- Перенаправление сетевых соединений (синкхолинг)

Автоматизация процессов SOC

- Политики реагирования
- Автономные агенты

Контроль устройств, находящихся вне КСПД

- Реагирование на устройствах вне корпоративного периметра

04

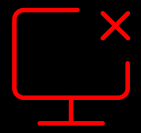
Max Patrol EDR

синергия решений

MaxPatrol EDR + MaxPatrol VM:

Задачи

Сканировать инфраструктуру полностью. Следить за маршрутами от сканера до каждой цели

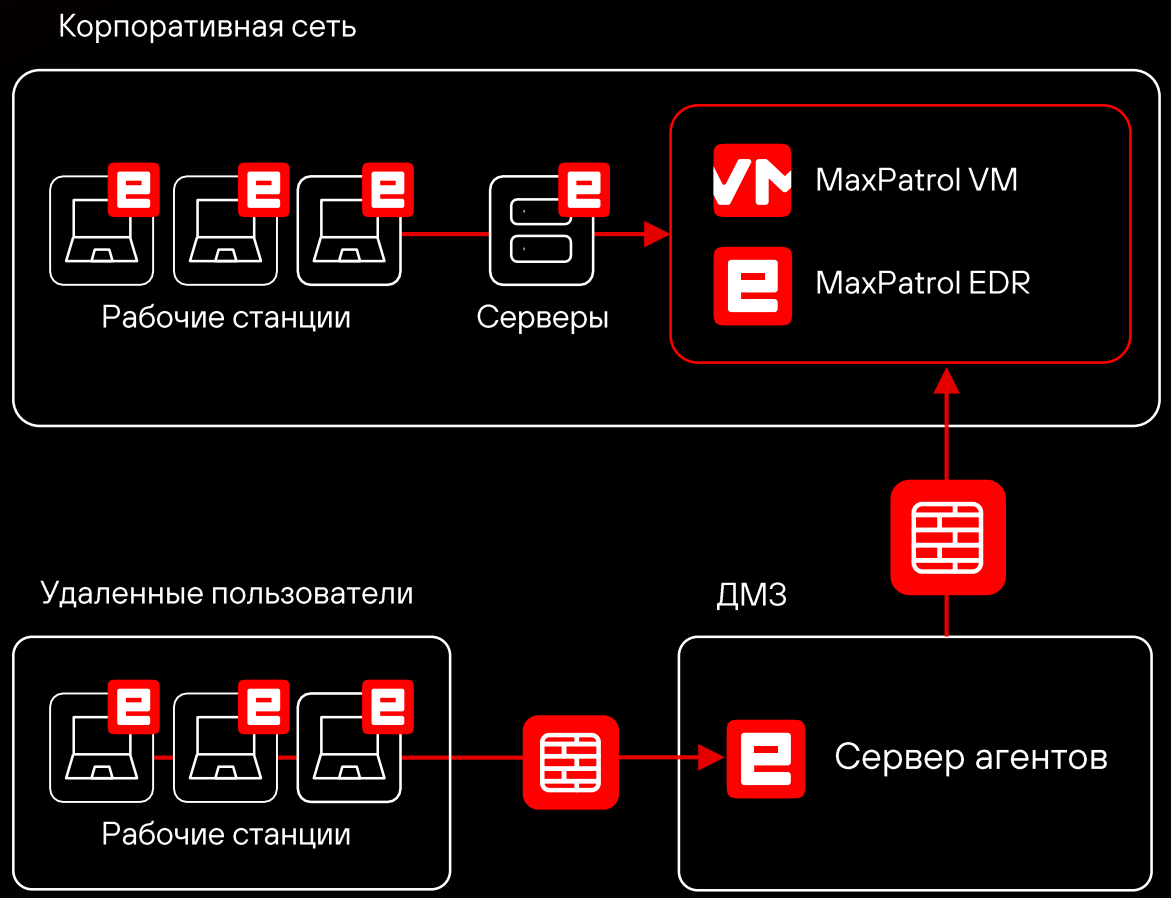


Устройства могут быть выключены или недоступны во время сканирования

Информация об активах обновляется недостаточно часто, данные не соответствуют действительности

Согласовать с ИТ доступы и учетные записи для сканирования чувствительных сегментов

MaxPatrol EDR + MaxPatrol VM



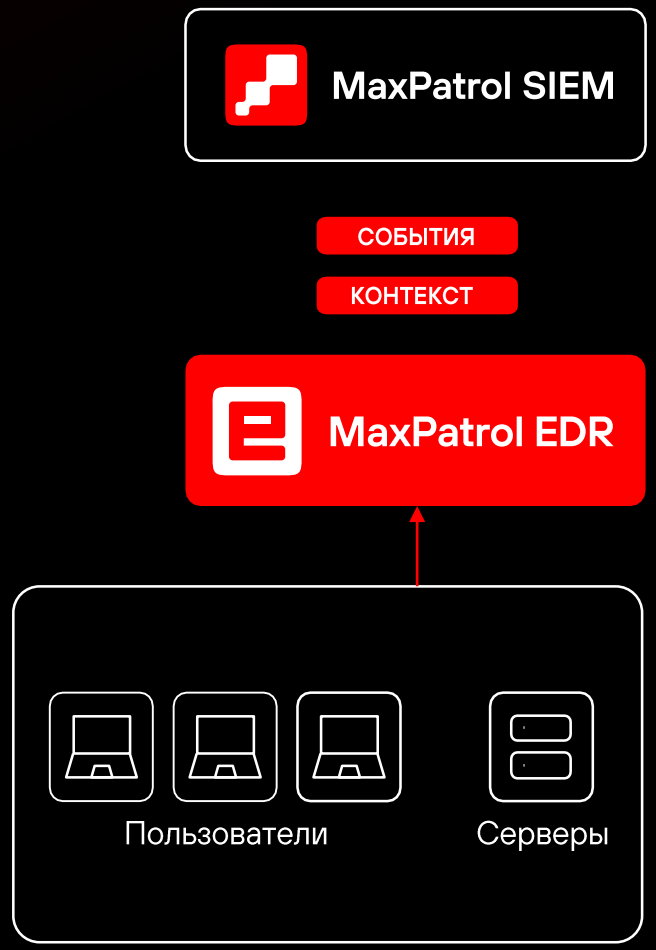
> Задачи

- Сбор данных с устройств, с которых их не получалось собрать средствами MaxPatrol VM
- Частое обновление данных об активах
- Снижение нагрузки на сканирующий сервер и каналы связи
- Упрощение диалога между ИБ и ИТ

> Каким образом

- Модули сканирования не требуют сервисных УЗ, собирают данные с узлов вне домена и с устройств удаленных сотрудников
- Узловое сканирование происходит параллельно на всех активах в группе
- Отсутствует «паразитный» трафик, создаваемый сетевым сканером, сканирование производится с помощью мощностей самого узла с агентом
- Не нужны УЗ с повышенными привилегиями, не нужно тратить время на маршрутизацию

MaxPatrol EDR + MaxPatrol SIEM



> Задачи

- Контроль сбора событий с серверов и рабочих станций
- Раннее обнаружение следов атак и подозрительной активности на устройствах
- Возможность оперативного реагирования на устройствах
- Сокращение операционных расходов
- Упрощение диалога между ИТ и ИБ

> Каким образом

- Настройка профиля мониторинга прямо из консоли EDR. Централизованно для всех групп устройств, в т. ч. вне домена
- Поведенческий и статический анализ прямо на устройствах. Корреляционный и YARA-движки на агентах
- Широкий набор действий для своевременного реагирования
- События, контекст и возможность реагирования прямо из карточки события, в единой консоли
- Договоренности => политики EDR. Автоматизация реагирования в согласованных случаях

MaxPatrol EDR + PT Sandbox

> Задачи

- Защита от ВПО, распространяемого через шифрованные каналы
- Повышение точности обнаружения угроз
- Молниеносное реагирование на угрозы

> Каким образом

- Обнаруживаются файлы, скачиваемые, например, через Telegram, браузеры, P2P и пр.
- Проводится подробный статический и поведенческий анализ
- Результат анализа становится доступен на всех агентах группы

MaxPatrol EDR

планы

- Отправка сырых событий
- API для реагирования
- Обновление UX и UI
- Работа в кластере и HA
- Улучшение интеграций
- Расширение возможностей реагирования

MaxPatrol EDR:

Обзор
MaxPatrol EDR

MaxPatrol EDR

Обзор
MaxPatrol VM

MaxPatrol VM

Спасибо!