



MaxPatrol VM

Система нового поколения
для управления уязвимостями

Как появился MaxPatrol VM?



Сетевые сканеры уязвимостей

Сканирование
в режиме черного ящика,
определение открытых портов



Системы анализа защищенности

Централизованное сканирование
узлов и сетевого оборудования
в режиме черного и белого
ящика, сравнение результатов

Gen 2



Системы управления уязвимостями нового поколения

Управление активами, построение
процесса приоритизации
и контроля устранения
уязвимостей

Next gen

Как должно быть



Процесс VM

Плановая обработка уязвимостей

- В IT-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с IT-отделом

Особо опасные уязвимости

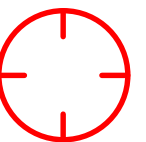
- Фокус смещается на трендовые уязвимости и на те, которые имеют эксплойт и расположены на важных активах
- О сроках устранения каждой уязвимости служба ИБ и IT-отдел договариваются отдельно

Управление уязвимостями



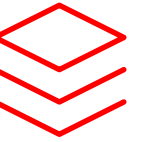
VM

**1**
Постоянная
актуализация
данных об активах

**3**
Выявление
уязвимостей

**5**
Устранение
или компенсация
уязвимостей

**2**
Классификация
и оценка активов

**4**
Сортировка
и приоритизация
уязвимостей

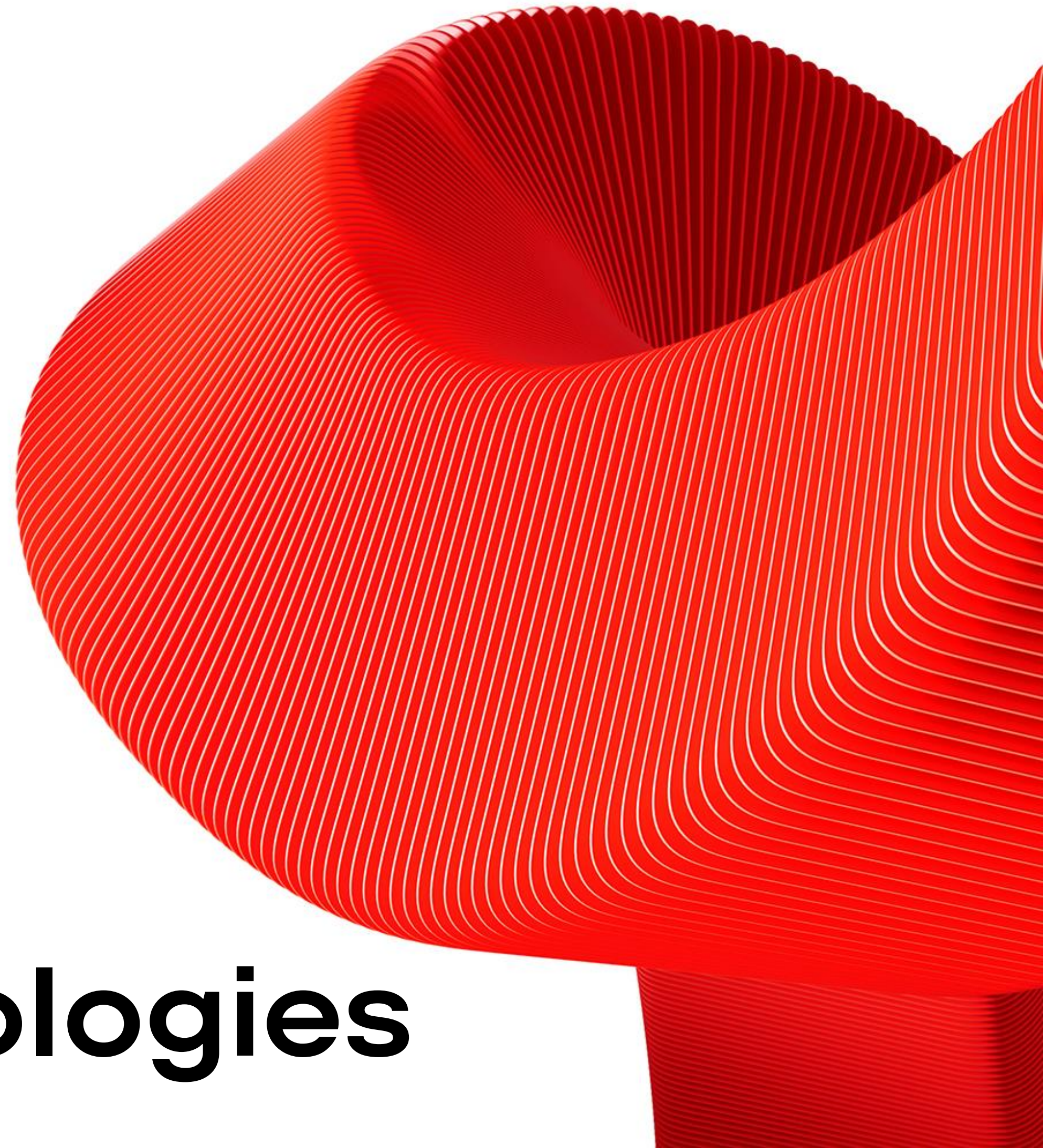
**6**
Проверка
устранения
уязвимостей



AM **Asset management**
Управление активами

VA **Vulnerability assessment**
Определение уязвимостей

VR **Vulnerability remediation**
Устранение уязвимостей



Решение
Positive Technologies



Единственное VM-решение
с гарантированным сроком доставки
информации о самых опасных **трендовых**
уязвимостях — 12 часов.

Это позволит устранить
критически опасные уязвимости быстрее,
чем злоумышленники успеют разработать
для них эксплойты.

**MaxPatrol VM
не даст хакерам
шансов использовать
уязвимости
для взлома**

MaxPatrol VM



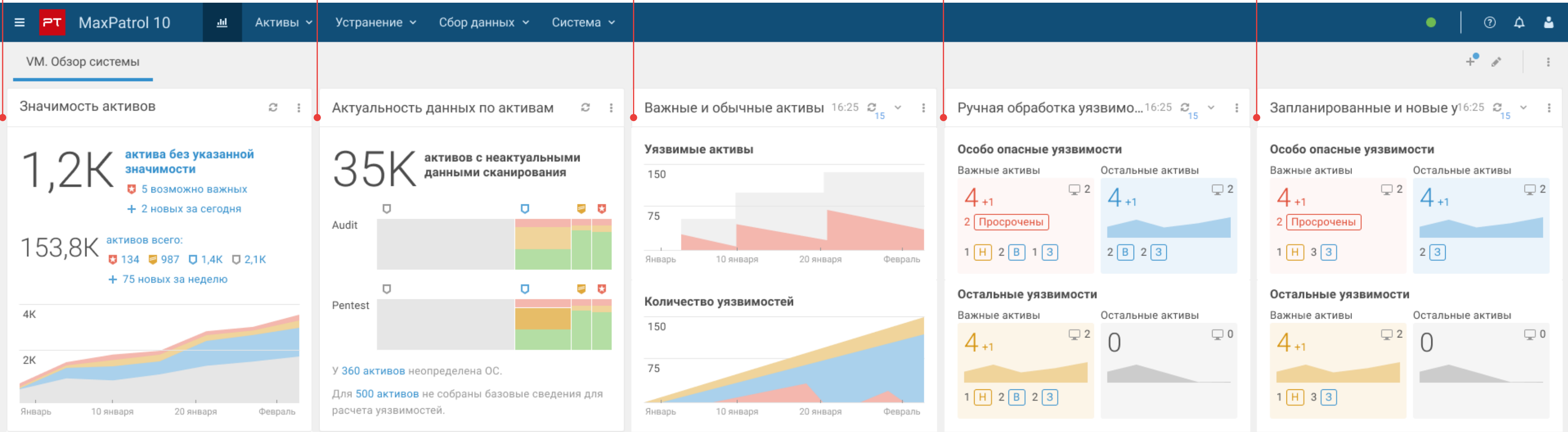
MaxPatrol VM находит все активы в сети. Приоритизируйте их, чтобы знать, что важно

Получайте свежую информацию об активах и их уязвимостях. Задайте политики сканирования

Контролируйте, что происходит на важных активах. Отслеживайте появление новых активов

Обычные уязвимости исправляет IT-отдел в рамках политик. Специалист по ИБ контролирует только особо опасные недостатки

Специалист по ИБ отслеживает нарушения политик. Контролируйте своевременное устранение недочетов



MaxPatrol VM



Получайте информацию от экспертов Positive Technologies о самых трендовых уязвимостях, которые используют хакеры и пентестеры

Следите за состоянием внедрения VM-системы

☰

PT MaxPatrol 10

Активы ▾

Устранение ▾

Сбор данных ▾

Система ▾

●

?

🔔

👤

VM. Обзор системы

Трендовые уязвимости14:36

Проверки по чек-листу14:31

■ Проблема с обработкой ссылок CVE-2020-8616

Уязвимость, связанная с отсутствием ограничения количества выборок при обработке ссылок, позволяет злоумышленникам с помощью специально сформированных ссылок снизить...

Уязвимости не обнаружены

■ Перехват контроля CVE-2020-2883

Уязвимость в Oracle WebLogic Server из Oracle Fusion Middleware (в компоненте Core) позволяет злоумышленникам, не прошедшим аутентификацию и имеющим доступ к сети по T3,...

Уязвимости не обнаружены

■ Обход аутентификации CVE-2020-11651

Уязвимость в SaltStack Salt (в версиях до 2019.2.4 и 3000 до 3000.2), связанная с некорректной проверкой вызова методов классом ClearFuncs процесса salt-master, позволяет...

Уязвимости не обнаружены

■ Удаленное выполнение кода CVE-2019-0708

Уязвимость в службах удаленных рабочих столов (ранее известных как службы терминалов), связанная с использованием протокола удаленного рабочего стола (RDP) и отправкой...

5 - -

■ Копирование произвольных файлов CVE-2019-12815

Уязвимости не обнаружены

Администрирование0 из 2

Инфраструктура3 из 5

Экспертиза0 из 4

Возможности MaxPatrol НСС



MaxPatrol НСС —
комплаенс
для результативной
безопасности

Модуль комплаенс-контроля позволяет:

- Проверять инфраструктуру **на соответствие стандартам безопасности** и отдельным **требованиям**
- **Приоритизировать** найденные риски
- Просматривать актуальные данные **о выполнении требований** на динамических дашбордах
- Устанавливать **сроки**, в которые несоответствия стандартам должны быть устранены, и контролировать их соблюдение

Как MaxPatrol VM собирает данные



- Собирает и хранит более 3000 параметров актива
- Использует безагентский режим сканирования

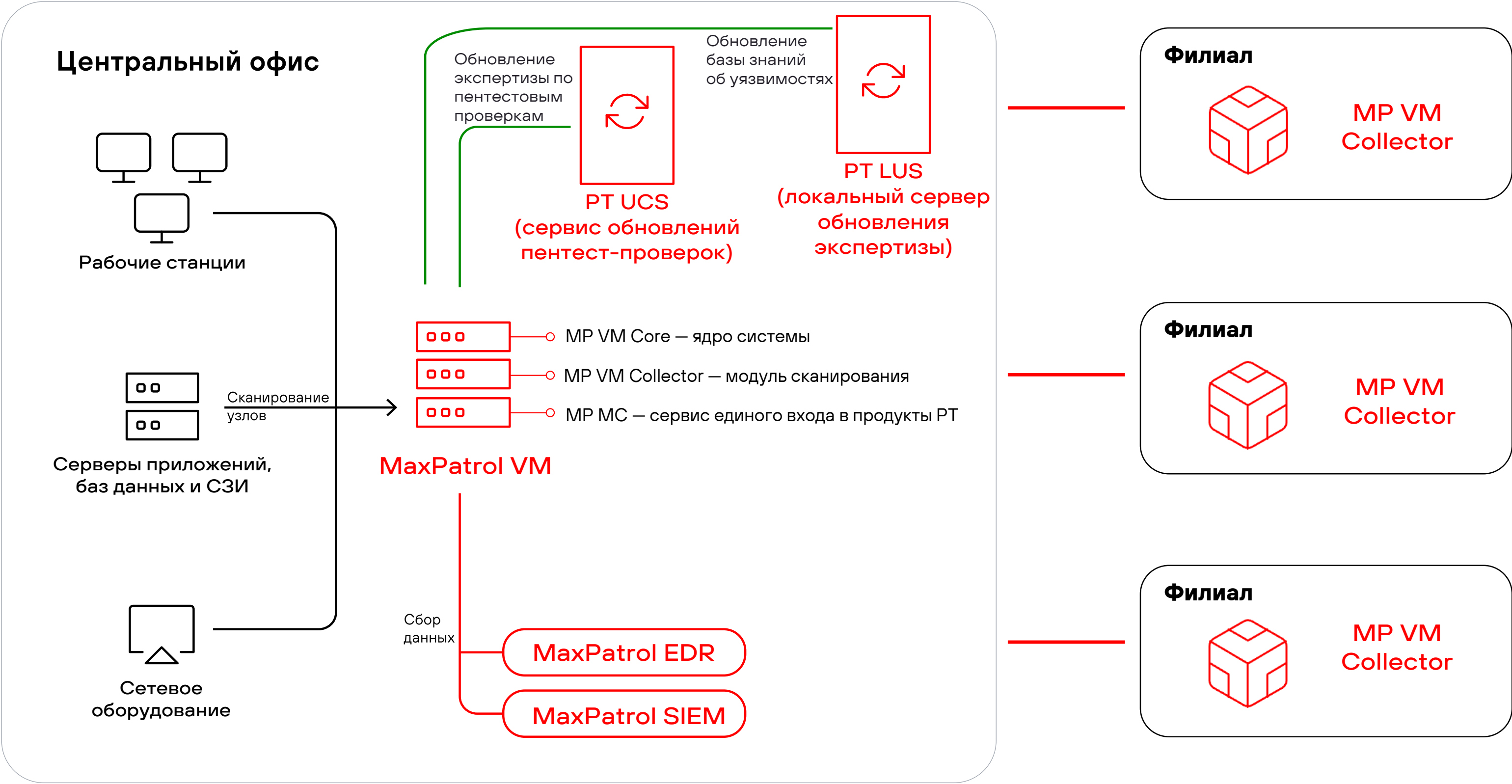


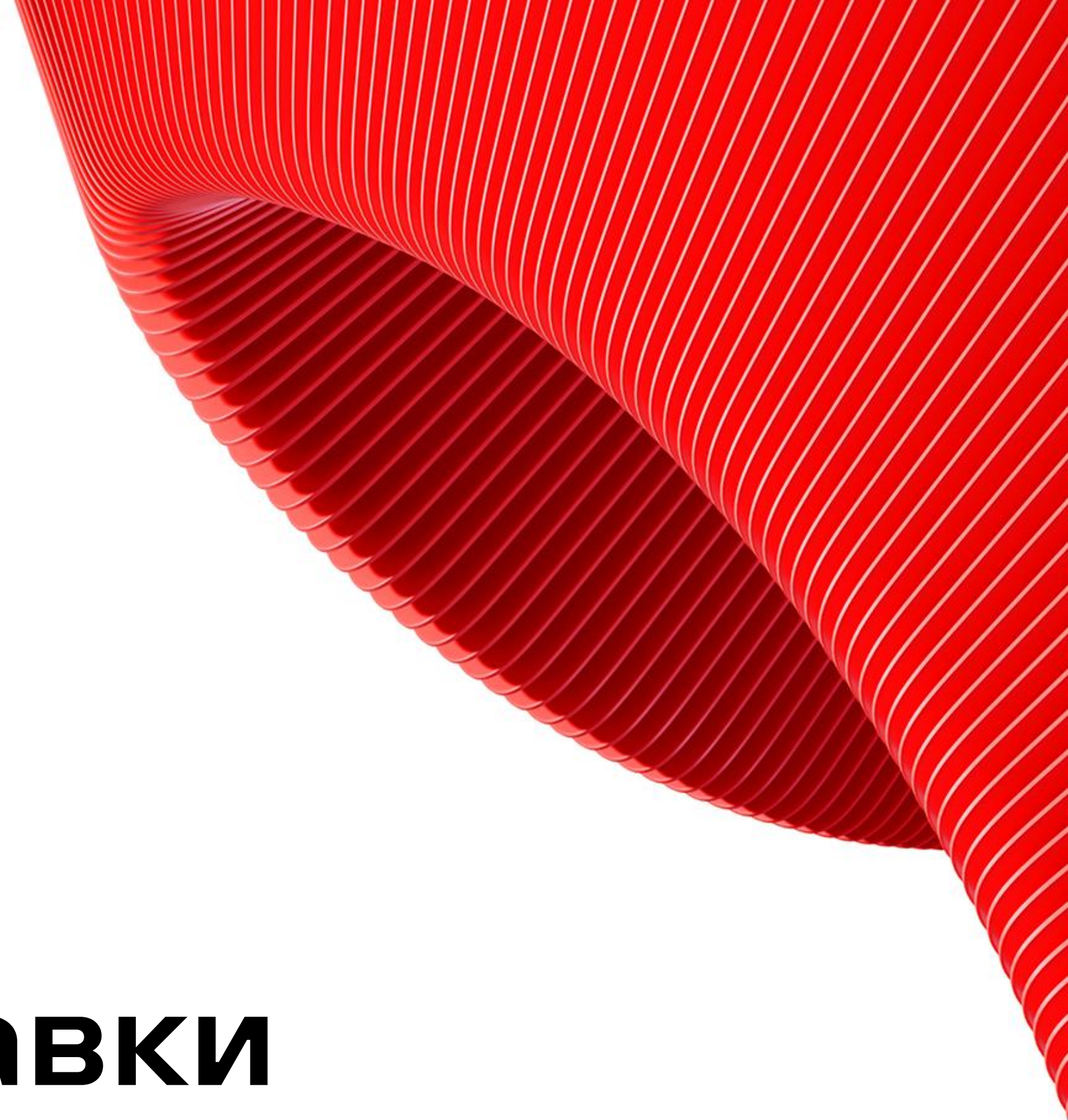
Как MaxPatrol VM собирает данные



MaxPatrol VM

позволяет сканировать узлы, расположенные в отдельных сетевых сегментах





Варианты поставки и модель лицензирования

Варианты поставки и модель лицензирования



- ПО (можно развернуть в виртуальной среде или на физическом сервере клиента)
- Программно-аппаратный комплекс



АЕС

Нет ограничений по количеству коллекторов

MaxPatrol VM

Позволит выстроить процесс
управления уязвимостями,
результаты которого видны



Новости продуктов
Positive Technologies:
t.me/ptproductupdate



Telegram-чат MaxPatrol VM,
MaxPatrol SIEM и PT XDR:
t.me/MPSIEMChat

