positive technologies

MaxPatrol Endpoint Detection & Response

MaxPatrol EDR — защитит конечные устройства от сложных и целевых атак

66% атак на организации

совершены с помощью вредоносного ПО

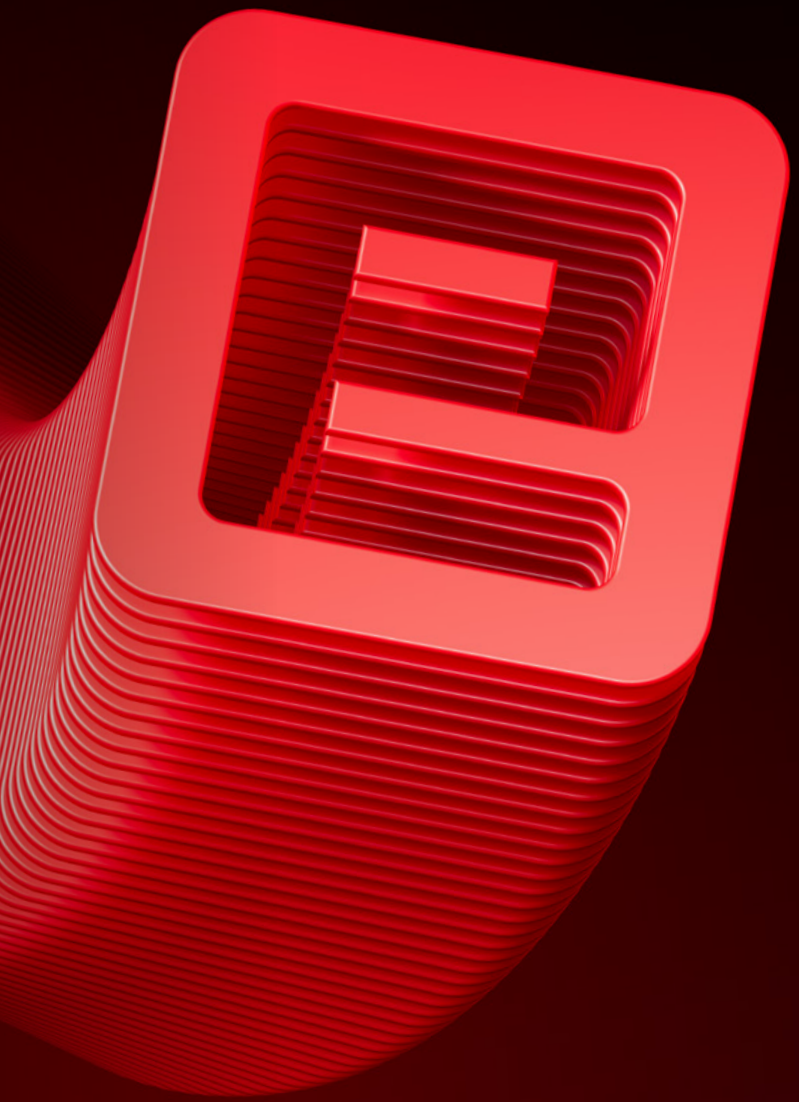
Топ-3 ВПО

- Шифровальщики
- ВПО для удаленного доступа
- Шпионское ПО

Ухищрения хакеров

- Многоэтапные схемы
- Портирование ВПО под разные ОС
- Маскировка для обхода средств защиты

Преимущества MaxPatrol EDR



Возможность автономной работы
Агент не требует доступа в интернет и поддерживает работу в закрытых сегментах сети

Поведенческий и статический анализ
Поставляется с набором экспертных правил PT ESC, благодаря чему способен выявлять популярные техники злоумышленников из матрицы MITRE ATT&CK (67 техник для Windows и 26 для Linux)

Поддержка российских ОС и Windows
Удобное решение для задач импортозамещения — как на стороне сервера системы, так и на стороне агентов для конечных устройств

Автоматическое реагирование
Предоставляет богатый выбор действий для своевременного реагирования: остановка процессов, удаление файлов, изоляция устройства, отправка файлов на анализ, синкхолинг, выполнение произвольных команд, блокирование учетных записей и другие действия. Автоматически или вручную.

Единый агент экосистемы Positive Technologies
Выступает в роли единого агента для обнаружения, реагирования, управляемого сбора телеметрии и информации об уязвимостях на узлах. Отправляет подозрительные файлы на глубокий анализ в песочнице

Что нужно защитить

- Рабочие станции
- Ноутбуки удаленных сотрудников
- Виртуальные машины
- Серверы организации

Какие риски снизить

- Компрометация устройств через скрытые в фишинге инструменты
- Проникновение атакующих на серверы в ДМЗ
- Повышение привилегий, использование прав администратора для перемещения по сети
- Шифрование или удаление данных на ключевых устройствах организации

Как это сделать с MaxPatrol EDR

- Анализировать происходящее на устройствах, выявлять подозрительную активность и атаки на ранних этапах их развития
- Собирать события, дампы памяти и другие артефакты, необходимые для расследования
- Применять методы реагирования в автоматическом или ручном режиме

MaxPatrol EDR в цифрах и фактах

Десятки серверов для поддержки крупных георасределенных инсталляций

1 час требуется для доставки в продукт данных о новых опасных угрозах (IoC)

Выявляет топ техник из матрицы MITRE ATT&CK для Windows и Linux

700+ правил корреляции на агенте

6000+ YARA-правил и индикаторы компрометации «из коробки»

Все возможности обнаружения и реагирования на угрозы — в автономном режиме

30+ поддерживаемых ОС

Доли секунды для обнаружения атак — за счет мощного коррелятора на агенте

40+ действий для реагирования, в том числе в автоматическом режиме

Как MaxPatrol EDR взаимодействует с другими продуктами Positive Technologies

MaxPatrol SIEM

- Контроль сбора событий с серверов и рабочих станций
- Расширенный контекст для принятия решений
- Возможность оперативного реагирования на угрозы

MaxPatrol VM

- Упрощение взаимодействия подразделений ИБ и ИТ
- Сбор данных с устройств, с которых не получалось собрать их средствами сетевого сканера
- Не нужны сервисные учетные записи
- Более частое обновление данных об активах
- Снижение нагрузки на каналы связи и упрощение маршрутизации

PT Sandbox

- Защита от ВПО, распространяемого через шифрованные каналы (Telegram, браузеры, P2P)
- Повышение точности обнаружения угроз
- Результат анализа PT Sandbox доступен на всех агентах, что позволяет быстрее блокировать атаки

Телеграм-чат пользователей

ТЕСТ-ДРАЙВ

Телеграм-канал Positive Technologies