



MaxPatrol Endpoint Security: от мониторинга до реагирования, универсальный агент на страже инфраструктуры

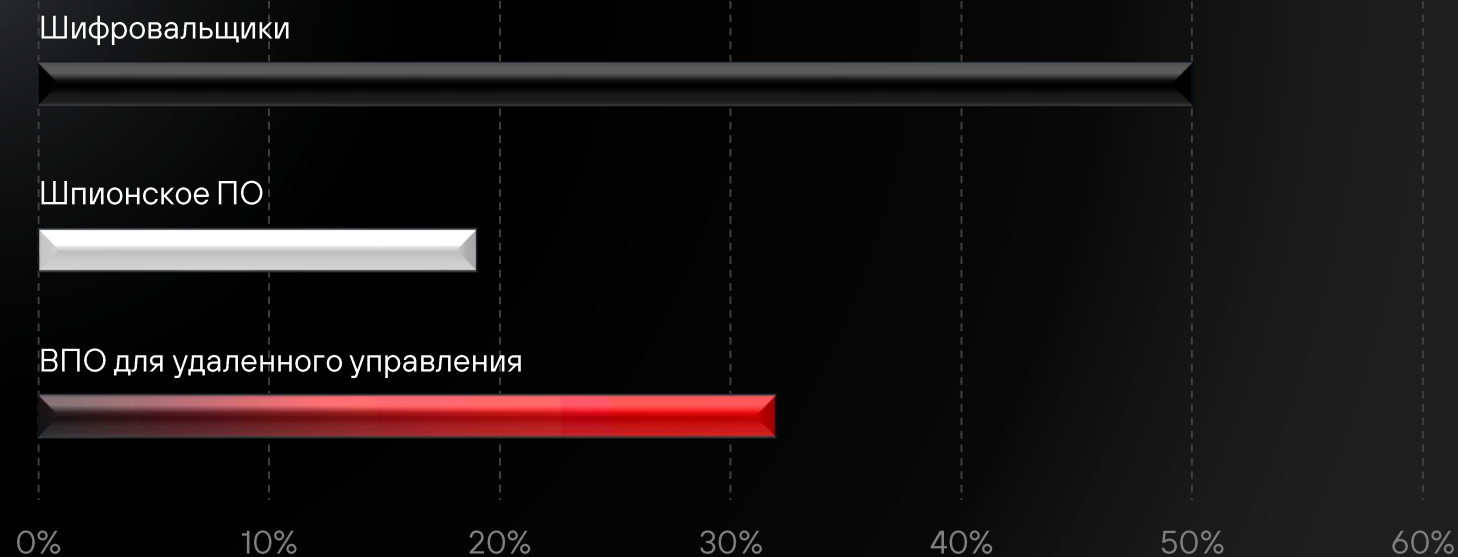
Владимир Яцюк

Руководитель отдела региональной поддержки продаж

Тренды



ВПО остается основным инструментом злоумышленников



Типы ВПО, чаще всего применяемые в успешных атаках на организации



Malware-free-активность, не требующая классического ВПО

82%

Ухищрения атакующих

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

Тактики и техники атак



88%

> хакерской активности происходит вне рабочего времени



Самая быстрая зафиксированная атака

27 секунд

Время атакующих

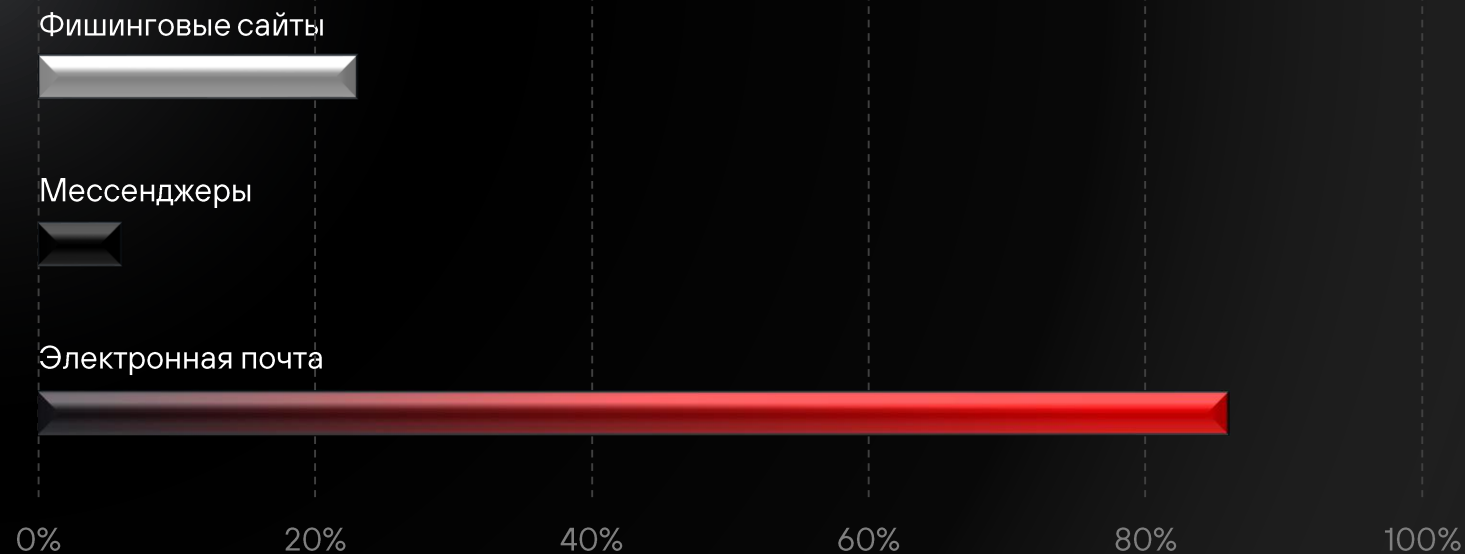
- В среднем злоумышленнику требуется **29 минут**, чтобы начать перемещаться в другие системы внутри инфраструктуры после проникновения
- Чтобы найти путь к AD, нужно **3–4 часа**

Время защитников

- Злоумышленник находится внутри инфраструктуры **14 дней** до момента обнаружения
- Скрытые вторжения могут сохраняться неделями и месяцами

- Эксплуатация уязвимостей вышла на первое место как способ первоначального проникновения
- Ночная и выходная активность делает мониторинг 24/7 критически важным
- Переход от первоначального доступа к движению по инфраструктуре может происходить быстрее, чем реагирование в ручную

Тактики и техники атак



Каналы социальной инженерии, которые чаще всего используются в успешных атаках на организации

Эксплуатация уязвимостей остается одним из самых эффективных методов атак на организации: она использовалась в 35% инцидентов

Учетные данные пользователей были скомпрометированы в 18% успешных атак



EDR

Атакующему интересен не сам
компьютер

Защита конечных устройств: чек-лист



Сбор данных

- События собираются со всех устройств?
- Достаточно ли этих событий для выявления атак?
- Возможно ли оперативно корректировать профиль мониторинга?
- У вас есть информация об узлах?
- Вы контролируете устройства удаленных сотрудников?

Выявление

- Есть ли у вас инструменты для оперативного выявления угроз?
- Вы уверены в качестве обнаружения?
- Можете ли вы обработать весь поток инцидентов и уведомлений?
- Достаточно ли быстро можете проанализировать ситуацию и подтвердить инцидент?

Реагирование

- Есть ли у вас 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?

Что считать конечной точкой в инфраструктуре



Пользовательские рабочие места >

- Рабочие станции
- Ноутбуки
- Виртуальные рабочие столы (VDI)
- Рабочие места удаленных пользователей

Привилегированные рабочие места >

- Защищенные рабочие станции администраторов (PAW)
- Промежуточные серверы доступа, bastion host, jump host
- APM администраторов
- CI/CD runners

Смежные узлы без EDR-агентов

- Гипервизоры, системы хранения, межсетевые экраны, VPN, сетевые устройства, часть контейнерной и Kubernetes-инфраструктуры
- Часто оказываются в слепой зоне, но при этом остаются приоритетными целями атакующего

Серверные системы >

- Серверы Windows и Linux
- Файловые серверы
- Серверы баз данных
- Серверы приложений
- Веб-серверы
- Терминальные серверы
- Виртуальные машины в облаке

Инфраструктурные системы >

- Контроллеры домена (DC)
- Системы управления резервным копированием
- Системы управления средствами информационной безопасности
- Системы управления виртуализацией

Почему конечная точка остается ключевым элементом атаки



1	Важен не тип устройства	а возможность использовать его как доверенную точку для выполнения команд, управления ВПО и продвижения по инфраструктуре
2	Конечные точки связаны сразу с несколькими тактиками MITRE ATT&CK	такими как Execution, Persistence, Credential Access, Discovery, Lateral Movement, Collection, Command and Control и Impact
3	Конечная точка может играть разную роль для хакера	Например, быть точкой входа, точкой наблюдения, инструментом для дальнейшего движения и иногда — конечной целью атаки
4	Рабочая станция может дать злоумышленнику	одну учетную запись и удобную позицию в сети
5	Серверы содержат	данные многих пользователей, сервисные учетные записи, ключи, доступ к базе данных и доверенные связи
6	Станция администратора или сервер управления	может сразу дать возможность выполнять команды на множестве систем и является критически значимым узлом

Новый подход

- Защищать нужно не только устройство, а доверие, которое организация ему выдала
- Важно обезопасить пользовательскую идентичность, сессии, токены, сетевое положение и административные возможности

Современные атаки: блокировать вредоносное ПО уже недостаточно



Современная модель NEW

- 1 Основной объект анализа — поведение пользователя и системы в контексте их роли и уровня доверия
- 2 Анализируется цепочка процессов, команд, скриптов, сетевой активности и событий аутентификации
- 3 Компрометация одного устройства рассматривается как возможная точка развития атаки на AD, облако, механизм резервного копирования и инфраструктуру виртуализации
- 4 Реагирование начинается уже на ранних признаках выполнения вредоносных действий, компрометации учетных данных и перемещения по инфраструктуре

Старая модель

- 1 Основной объект анализа — вредоносный файл
- 2 Обнаружение выполняется по сигнатурам и репутации
- 3 Заражение рабочего места рассматривается как локальный инцидент
- 4 Реагирование начинается после обнаружения вредоносной активности

- Классическая картина «письмо → вредоносный EXE-файл → антивирус» уже не описывает значительную часть корпоративных атак
- Атакующие все чаще используют штатные средства ОС, украденные учетные данные, браузерные сессии, RMM и облачные сервисы
- EDR-решение должно отвечать не только на вопрос «Известен ли этот файл как вредоносный?», но и на более важный: «Нормальна ли такая последовательность действий для этого пользователя, устройства и его роли?»

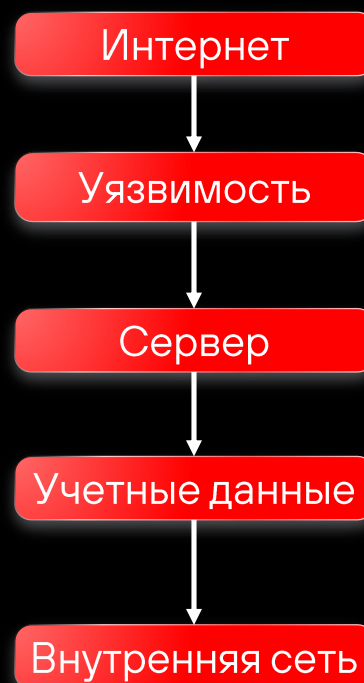
Как сегодня получают первоначальный доступ



Основные точки входа:

- Уязвимости доступных из интернета систем
- Фишинг и социальная инженерия
- Украденные учетные данные и сессии
- Подрядчики и доверенные связи
- Легитимные средства удаленного доступа

Защита конечной точки начинается с управления внешней поверхностью атаки, уязвимостями и привилегиями пользователя



Первой скомпрометированной точкой может быть:

- веб-сервер
- сервер приложений
- VPN
- почтовый сервер
- система удаленного управления
- инфраструктура виртуализации

Приоритет защиты должен зависеть не от типа ОС, а от доступности извне и потенциального ущерба

Пользователю уже не обязательно запускать вирус



Получить доступ к инфраструктуре организации можно даже без заражения корпоративного компьютера

Рекомендации «не открывайте вложения» уже недостаточно. Пользователям нужно объяснять, какие риски несут вставка команд по чужой инструкции, выполнение просьб «починить учетную запись», сканирование неизвестных QR-кодов и использование мессенджеров, а также прохождение поддельных CAPTCHA

Сообщение, сайт

Fake CAPTCHA

Пользователь сам запускает команду

PowerShell

Загрузка

Развитие атаки

- Вложение может вообще отсутствовать
- Пользователь сам запускает штатный инструмент
- Легитимные программы становятся частью атаки
- Обучения «не открывайте подозрительные EXE-файлы» уже недостаточно

Пароль — уже не единственный объект кражи

- Пароли
- Cookies
- Session tokens
- OAuth, refresh tokens
- VPN credentials
- SSH, API, PAT keys
- Данные password manager

Легитимные инструменты становятся инструментами атаки



Утилиты ОС

- PowerShell
- cmd
- Bash
- rundll32
- mshta
- WinRM, WMI
- RDP || SSH
- Curl || nc

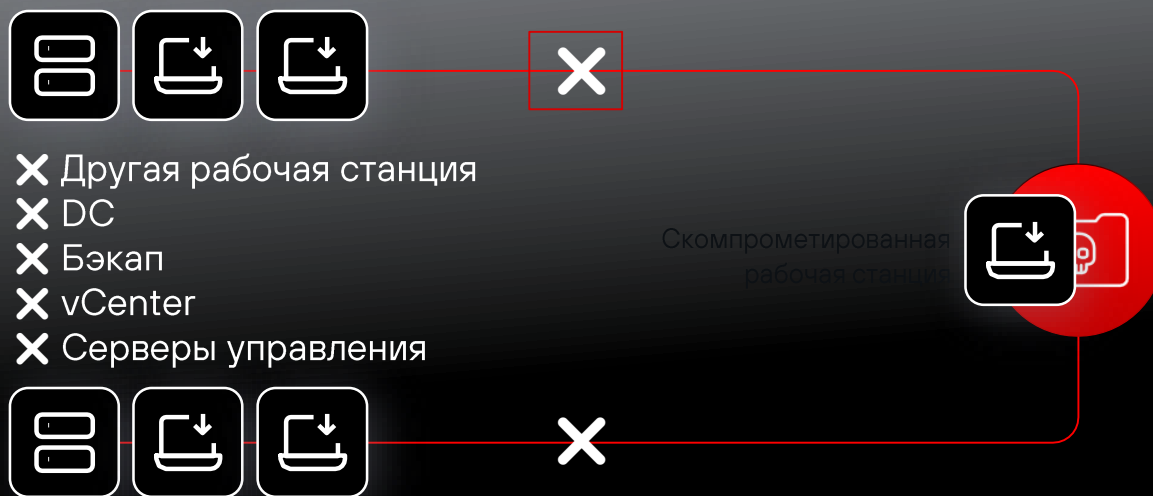
Средства удаленного управления

- AnyDesk
 - TeamViewer
 - ScreenConnect
 - Atera и т. п.
-

Проблема не в том, что инструмент запущен

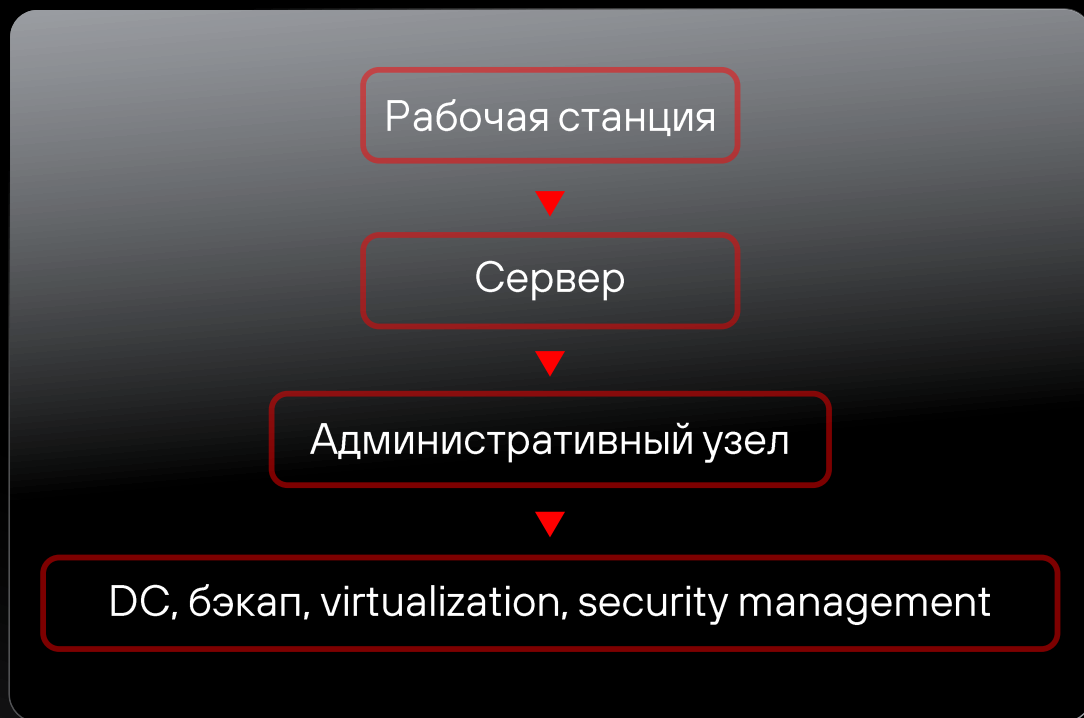
Важно то, кто, где, когда, зачем и что делает после его запуска

Скомпрометированный эндпойнт должен стать тупиком



- Задача защиты — разорвать цепочку раньше, чем атакующий доберется до систем с широкими полномочиями
- Компрометация одного устройства не должна автоматически открывать путь ко всей инфраструктуре
- Внутри должны быть барьеры: сегментация, host firewall, PAM, jump host, ограничение административных протоколов, системы EDR, NDR, NTA

Самые важные эндпойнты — те, которые управляют другими



- Domain controllers
- PAW
- Jump host
- Backup management
- Virtualization management
- Security management

-
- 21% — компрометация DC в организациях
 - 11% — компрометация серверов централизованного управления средствами защиты

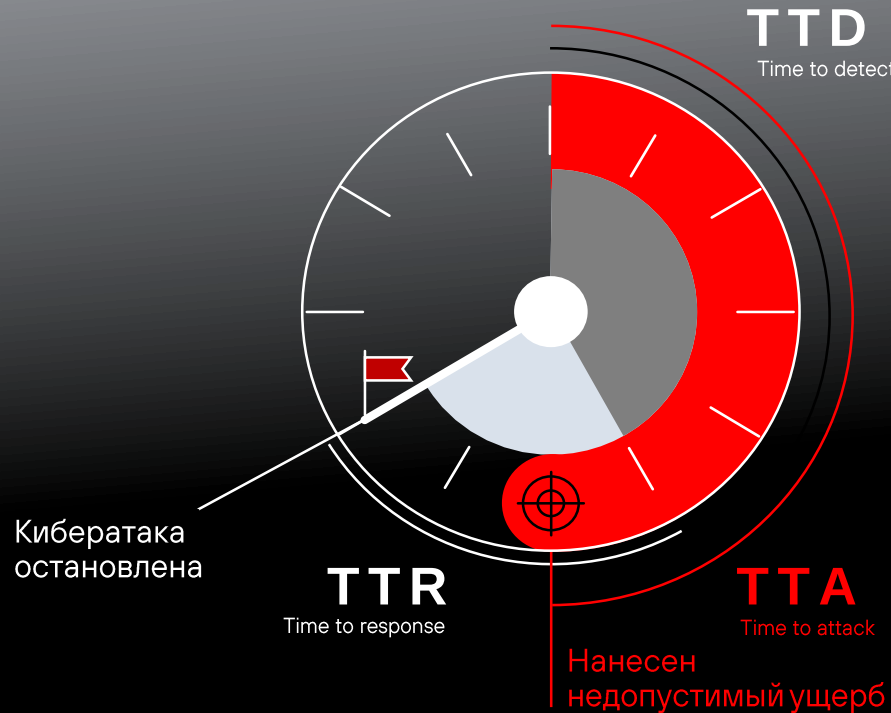
Чем больше систем способен контролировать узел
легитимно, тем опаснее его компрометация

Скорость атаки и скорость обнаружения — разные вещи



14 дней

в среднем требуется службе ИБ, чтобы выявить и локализовать утечку данных



От 3 часов

Атакующий может начать движение за минуты, а обнаружен быть только через дни

Нет выхода времени, чтобы остановить хакера

Что должен делать современная EDR-система



Наблюдать:



- процессы
- команды
- сеть
- пользователей
- скрипты
- изменения системы

Обнаруживать:



- аномальное поведение
- цепочки событий
- известные индикаторы

Расследовать:



- анализировать дерево процессов
- строить таймлайн
- Определять масштаб компрометации

Реагировать:



- останавливать процессы
- изолировать узлы
- блокировать IoC
- собирать артефакты

Threat hunting

EDR-система — это не «антивирус получше», а инструмент для наблюдения за развитием атаки и реагирования на нее

Где EDR-система нужна в первую очередь



1 Пользовательские рабочие места	Станции Ноутбуки VDI
2 Серверные системы	Windows, Linux Файловые БД Приложения Терминальные серверы Облачные VM
3 Привилегированные рабочие места	PAW Jump host, bastion host APM администраторов CI/CD
4 Инфраструктурные системы	DC Бэкапы Управление ИБ Виртуализация

Приоритет определяется не количеством устройств, а потенциальными последствиями их компрометации

Особый приоритет имеют административные станции, контроллеры домена, системы для резервного копирования, управления виртуализацией и средствами безопасности. Их компрометация может привести к негативным последствиям сразу для большого числа систем

EDR-система — ТОЛЬКО ОДИН СЛОЙ

ЗАЩИТЫ



Защита строится вокруг цепочки атаки, а не вокруг одного продукта



Endpoint

Hardening → EPP → application control → EDR



Attack surface

Инвентаризация → VM → patch management



Identity

MFA → ITDR → PAM, PIM или JIT



Detection and response

SIEM или XDR → SOC или MDR → SOAR



Network

Сегментация → NTA → NDR



Recovery

Immutable backup → DR



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 PT ESC*
- Покрытие 60% техник атакующих из матрицы MITRE ATT&CK
- 6000 YARA-правил
- Более 65 000 актуальных хеш-сумм в базе данных PT ESC*

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 шифрованным каналам)
- MaxPatrol VM (анализ уязвимостей)
- MaxPatrol SIEM (анализ событий и отчетность)
- PT NAD (реагирование на сетевые угрозы)

Конструктор MaxPatrol EDR



Охват инфраструктуры

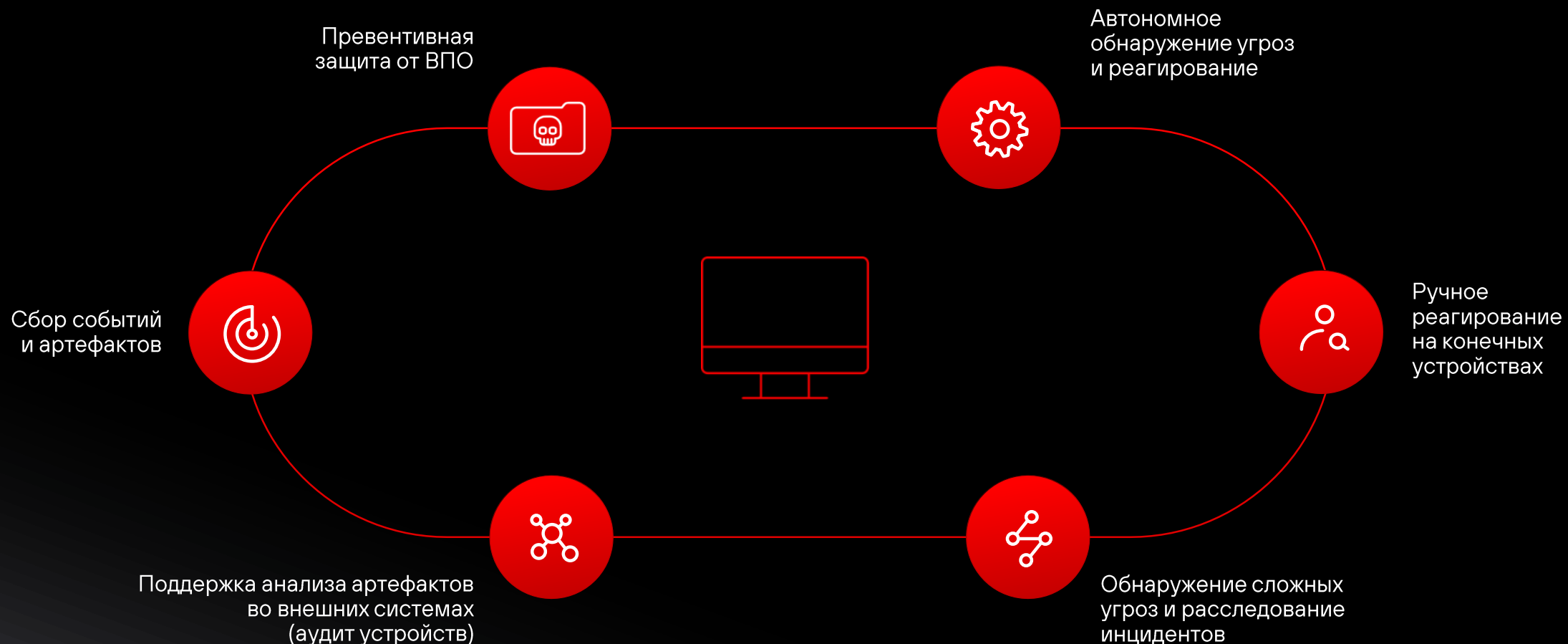


Можно установить на большинство
операционных систем

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

Полная защита устройств с помощью одного агента





Цель современной endpoint security —
не просто не допустить заражения устройства

Необходимо, чтобы компрометация одного
устройства не превратилась в компрометацию
всей инфраструктуры

Дополнительные
материалы



[Заказать
бесплатный пилот](#)



[Telegram-канал
Positive Technologies](#)



[Покрытие матрицы
MITRE ATT&CK](#)

Задай
вопрос
спикеру

