

PT SANDBOX

Песочница для защиты от сложного
и неизвестного вредоносного ПО



PT Sandbox





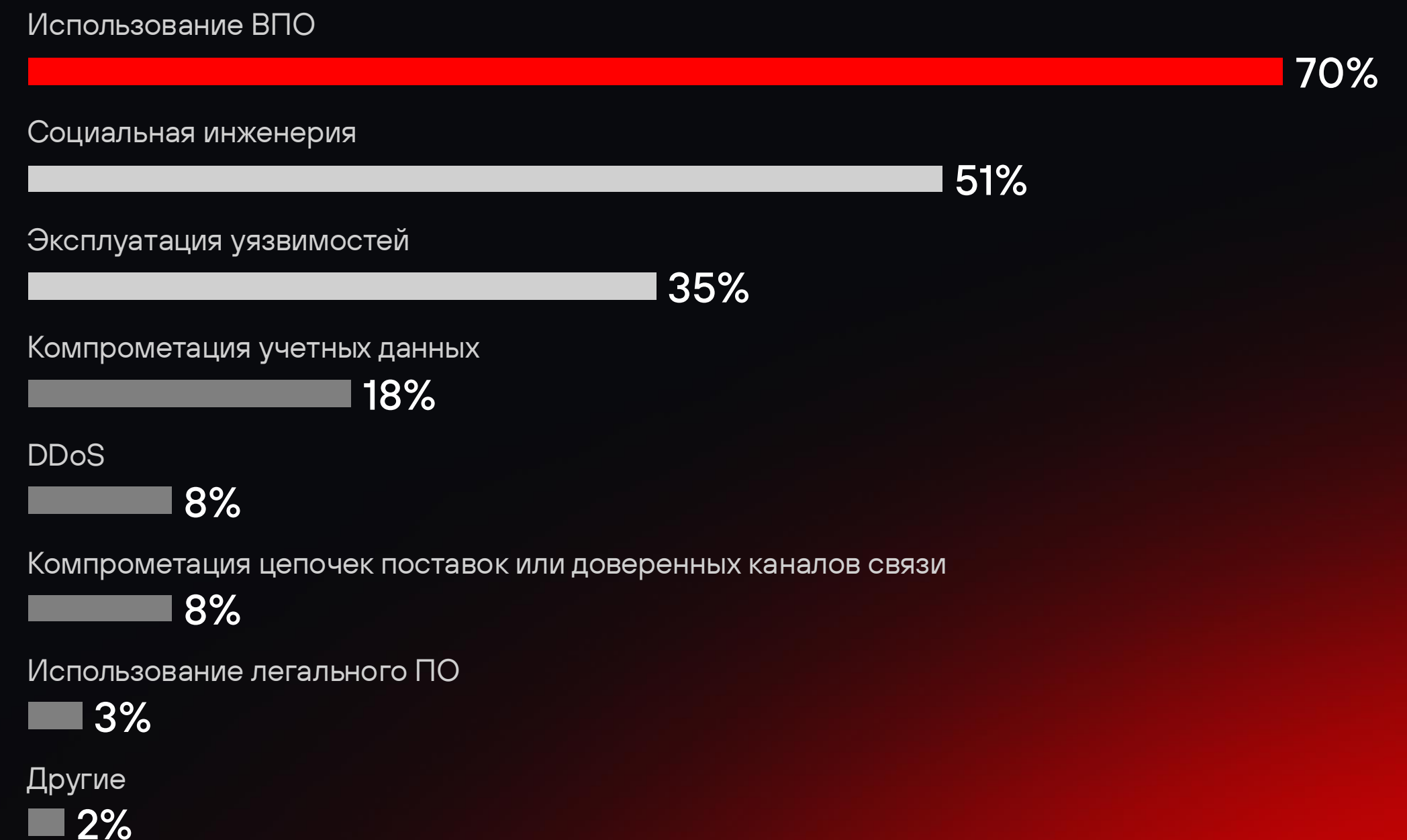
PT Sandbox

АТАКИ С ПРИМЕНЕНИЕМ ВРЕДНОСНОГО ПО



Методы атак в 2025 году

Использование ВПО
не первый год становится
самым популярным
способом реализации атак

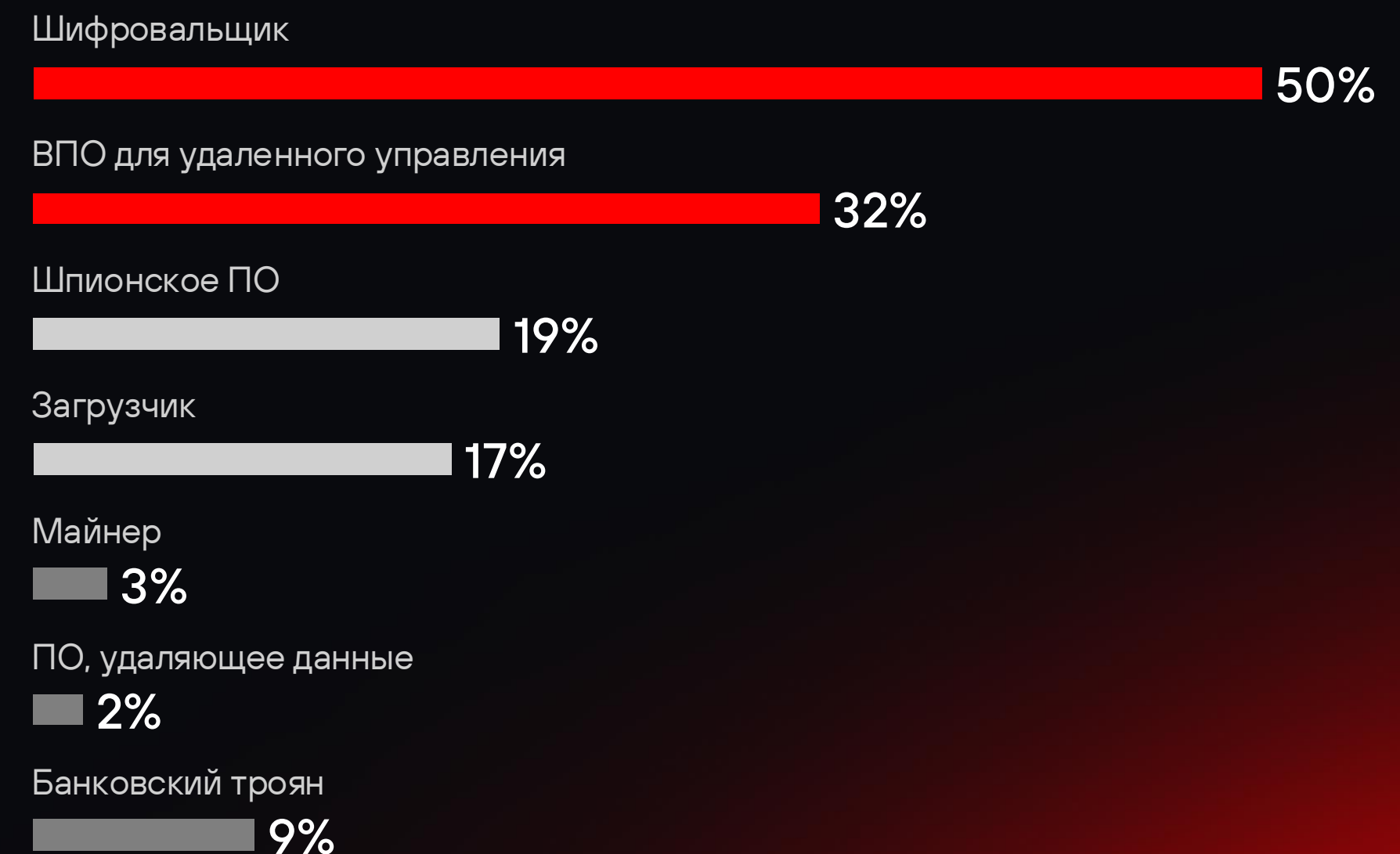


Типы ВПО в успешных атаках в 2025 году

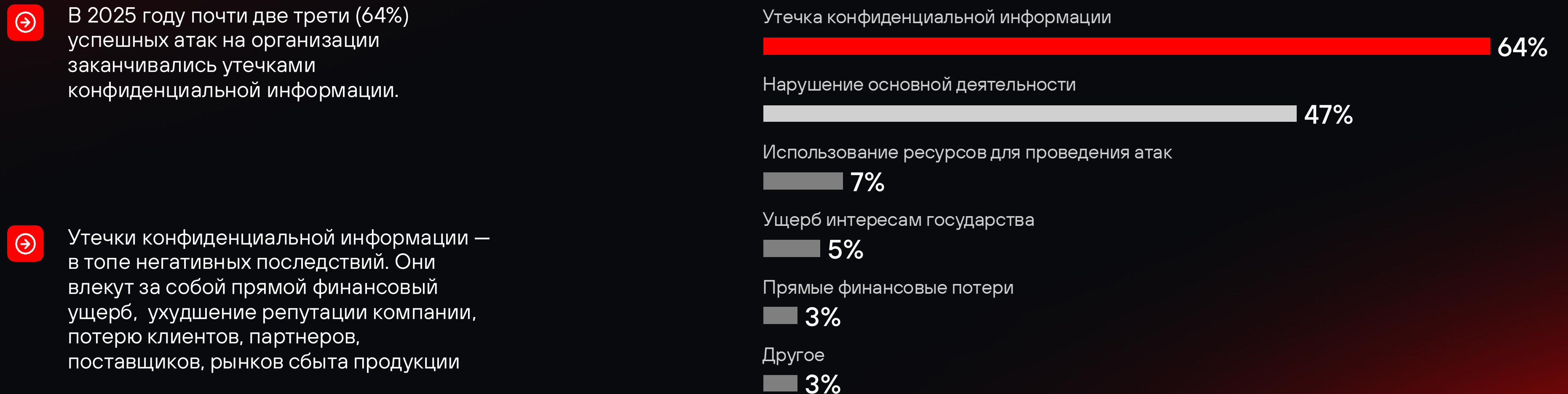
В половине случаев заражений вредоносным ПО на организации использовались шифровальщики



В трети атак на организации с использованием ВПО мы наблюдали применение троянов удаленного доступа (RAT)



Последствия атак в 2025 году



Негативные последствия хакерских атак с применением ВПО

21 января 2025 14:56

Злоумышленники получили доступ к базам данных клиентов телеком-оператора

[Подробнее](#) →

07 июня 2023, 10:34

Данные клиентов «Ашана», Gloria Jeans и «Твоего дома» оказались в сети

[Подробнее](#) →

22 мая 2023, 13:31

Российский разработчик VPN-технологий «Инфотекс» сообщил об утечке 60 тысяч записей базы данных

[Подробнее](#) →

11 апреля 2023, 13:48

Хакеры обрушили электронную систему ФТС

Таможенные органы вынуждены частично перейти на бумажный документооборот

[Подробнее](#) →

05 июля, 2023, 07:15

Хакеры взломали лагерь. ПДн детей и их родителей оказались в открытом доступе

[Подробнее](#) →

03 июня 2024, 11:17

«Верный» атаковали хакеры

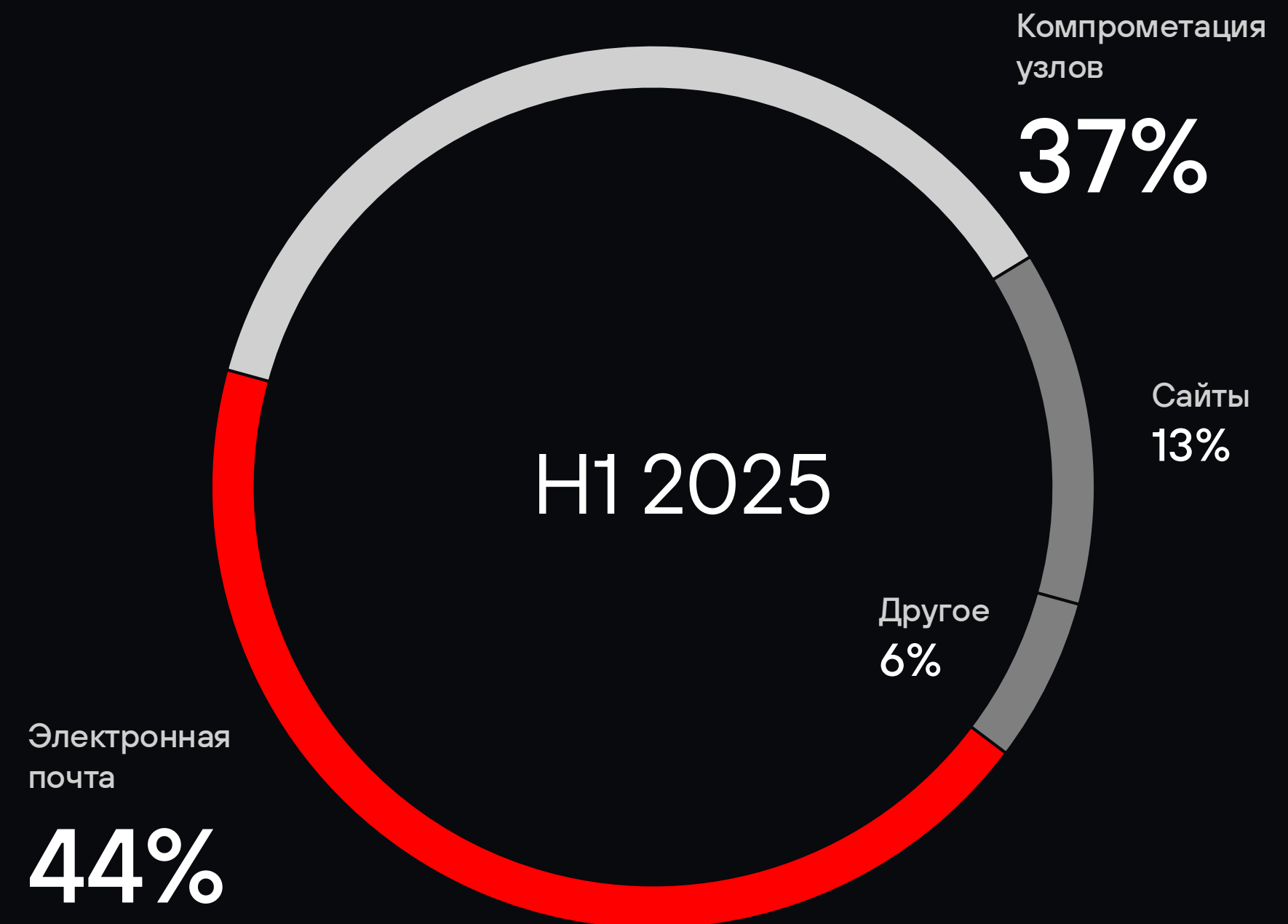
Ритейлер перестал принимать онлайн-заказы и карты к оплате

[Подробнее](#) →

Каналы распространения ВПО

Три основных канала распространения ВПО:

-  Электронная почта
-  Узлы
-  Веб-ресурсы





PT Sandbox

КАК ОБНАРУЖИТЬ ВРЕДОНОСНОЕ ПО



Решение — сетевые песочницы

Песочницы позволяют обезопасить внутреннюю сеть организации от еще неизвестных вредоносных программ, а также выявить целевые атаки на инфраструктуру

1

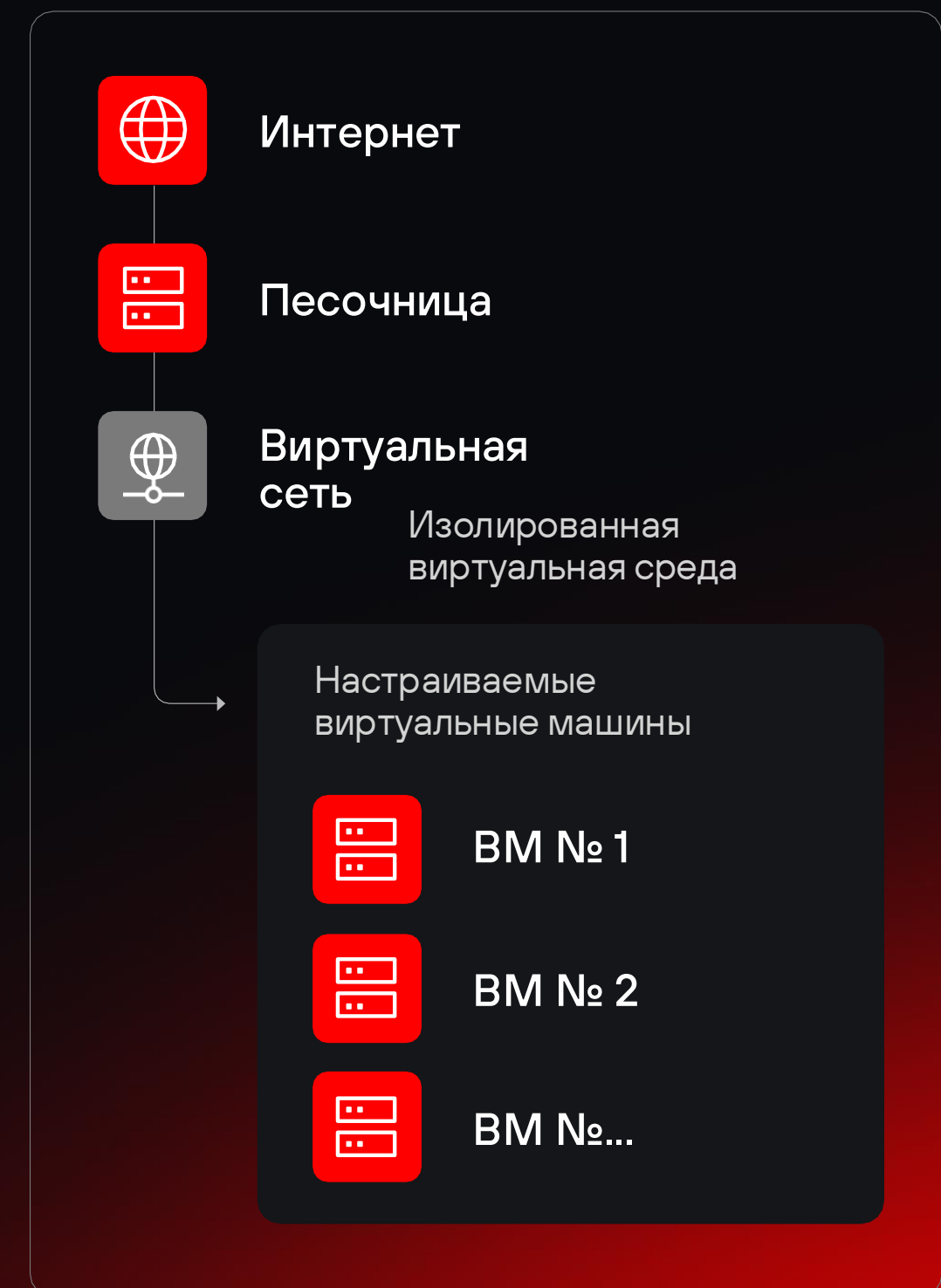
Выполняют запуск файлов в изолированной среде, не связанной напрямую с инфраструктурой

2

Можно запустить файл в этой среде, посмотреть, **как он себя ведет**, какие процессы запускает, что откуда скачивает

3

После проверки **принимается решение**, безопасен ли файл и можно ли пропустить его в инфраструктуру



Песочница PT Sandbox



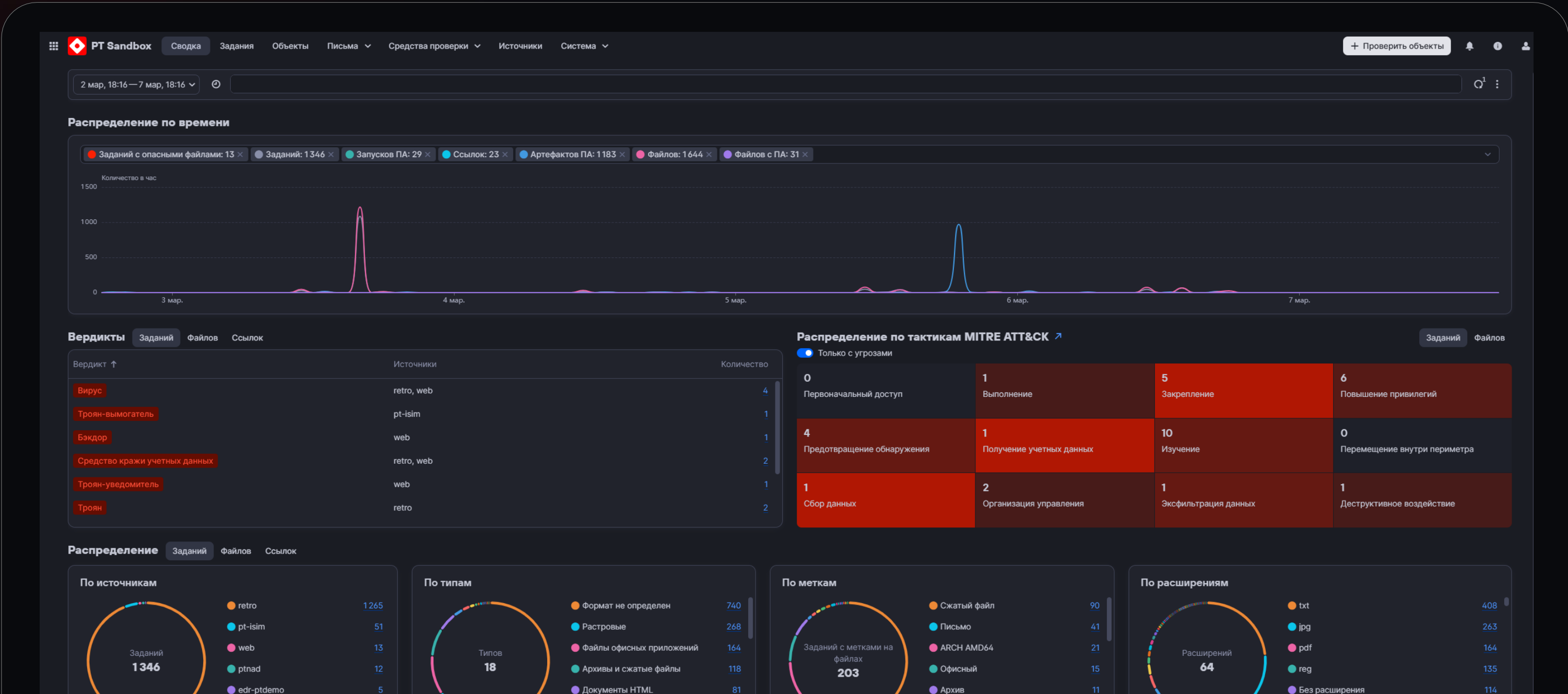
Обнаруживает вредоносное ПО на уровне гипервизора, операционной системы и виртуальной машины



Легко встраивается в инфраструктуру и контролирует основные каналы передачи файлов и ссылок



Адаптируется к особенностям бизнеса, обеспечивая защиту от целенаправленных атак



Как работает PT Sandbox

Песочница получает объекты из различных типов источников, обрабатывает файлы и ссылки и определяет в них вредоносное содержимое



Что защищает PT Sandbox

Песочница контролирует основные каналы передачи файлов и ссылок в компании за счет легкой интеграции с любыми ИТ- и ИБ-системами — источниками объектов для анализа



Электронная почта

Интеграция с почтовыми серверами организации. PT Sandbox проверяет тело письма и ссылки в нем, почтовые вложения, в том числе архивированные, разделенные на части и защищенные паролями



API-коннектор

Благодаря асинхронному API- коннектору поддерживается интеграция с любыми ИТ- и ИБ-системами как источниками по HTTP и HTTPS



Объекты из сетевого трафика

Интеграция по ICAP с IDS- и IPS-, NDR- и NTA-системами, прокси-серверами, межсетевыми экранами (NGFW) и системами защиты веб- приложений (WAF)



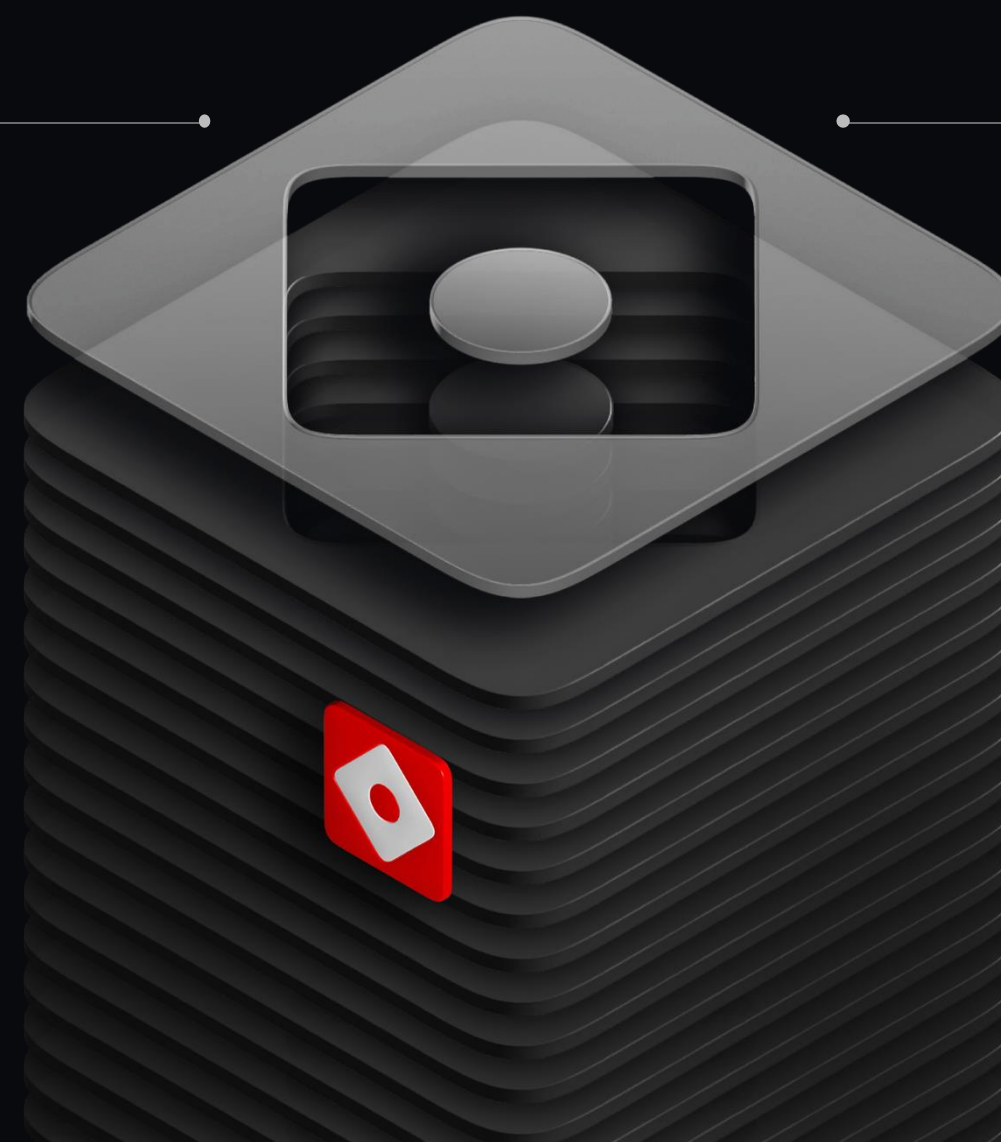
Файловые хранилища

PT Sandbox проверяет на наличие угроз файлы в корпоративных системах обмена данными, в том числе самописных



Ручная загрузка файлов

Любой файл, вызывающий сомнения, можно вручную отправить на проверку в PT Sandbox и получить вердикт о его безопасности



Статический анализ файлов и ссылок

Для защиты от известных угроз и проверки легитимности ссылок PT Sandbox использует комбинацию методов анализа

Собственные YARA-правила



Правила от экспертного центра PT ESC, создаваемые в ходе расследования инцидентов и анализа деятельности хакерских группировок

Категоризация веб-ресурсов



Классификация интернет-ресурсов по их назначению и типу контента для предотвращения инцидентов ИБ

Репутационный анализ



Репутационный анализ файлов и ссылок по базе индикаторов компрометации (PT IoC) для точечного выявления угроз

Антивирусный анализ



Собственный антивирусная лаборатория PT AV и дополнительные средства

Анализ содержимого ссылок



Поиск и скачивание контента по ссылкам с проверкой его легитимности

Политики предварительной фильтрации в PT Sandbox

Для снижения нагрузки на систему поведенческого анализа можно управлять правилами проверки объектов



Пользовательские правила определения объектов с угрозами

Персональные настройки, по которым PT Sandbox будет относить файлы и ссылки к опасным или потенциально опасным объектам



Правила для проверки офисных документов

Настройка параметров проверки файлов OpenDocument и Microsoft Office методом поведенческого анализа



Правила для проверки PDF-файлов

Настройка параметров проверки файлов PDF методом поведенческого анализа



Фильтрация извлеченных ссылок

PT Sandbox скачивает и проверяет контент только по тем ссылкам, которые удовлетворяют указанным пользователем параметрам

Поведенческий анализ в PT Sandbox

Для защиты от неизвестных угроз, нового вредоносного ПО и целевых атак песочница использует многоуровневую проверку в сочетании с инструментами от PT ESC

МНОГОУРОВНЕВАЯ ПРОВЕРКА ФАЙЛОВ



Анализ сетевого трафика
и подключений



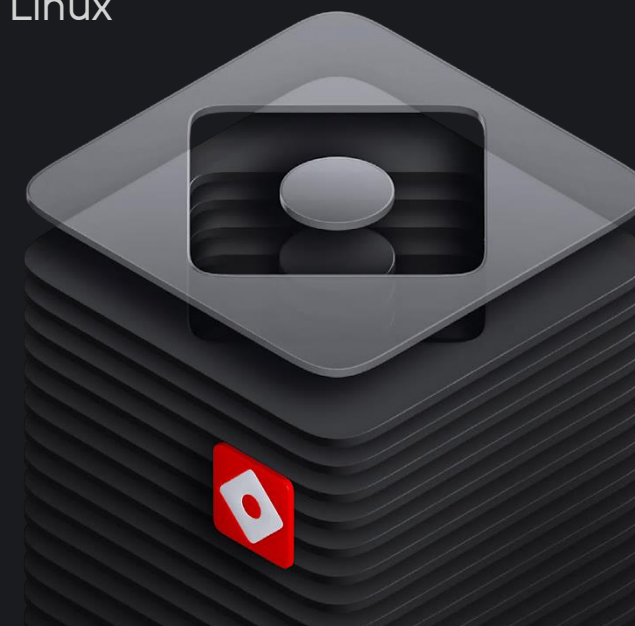
Анализ дампов
памяти и процессов



ML-технологии
для выявления
аномального поведения

Изолированная среда PT Sandbox

Поддерживает виртуальные
среды с ОС Windows, Linux



ЭКСПЕРТНЫЕ ИНСТРУМЕНТЫ



Кастомизация виртуальных машин
в соответствии с реальными
рабочими станциями



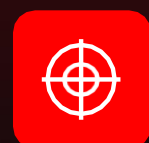
Уникальные приманки,
имитирующие настоящие
файлы, процессы или данные,
характерные для разных отраслей



Анти-evasion защита от популярных
техник обхода виртуальных сред

Режимы работы PT Sandbox

РЕШАЕМЫЕ ЗАДАЧИ



Обнаружение ВПО

Подключение песочницы к различным источникам, сбор файлов и ссылок на анализ с последующим уведомлением об угрозах.

Не влияет на бизнес-процессы

- Определение активности ВПО
- Выявление хакерских инструментов
- Обнаружение эксплуатации уязвимостей

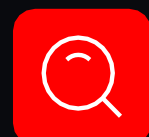


Блокировка ВПО

Защитное взаимодействие с почтовыми системами, системами контроля сетевого трафика и коннекторами API с целью недопуска вредоносного содержимого.

Минимальное влияние на бизнес-процессы

- Блокировка неизвестного ВПО
- Защита от хакерских инструментов
- Доставка пользователям сообщений и файлов без вредоносных вложений



Исследование угроз

Автоматизация труда специалистов SOC: анализирует объекты, включая загруженные вручную, предоставляет результаты с возможностью выгрузки нужных артефактов.

Снижает время, затрачиваемое на исследование угроз

- Получение безопасных обновлений программного обеспечения
- Автоматизация анализа объектов
- Ретроспективный анализ инцидентов

Уникальность PT Sandbox

Гибкость при интеграциях



Может получать объекты на анализ из множества источников

Приманки



Оснащена «ловушками», которые провоцируют вредоносное ПО на активные действия

Экспертиза



Доставка знаний о новых угрозах за 2,5 часа, собственная антивирусная лаборатория

Защита от обнаружения



Обнаруживает все популярные техники обхода песочниц



Работает на результат

Однозначно выявляет вредоносное ПО и оперативно блокирует актуальные угрозы

Применение PT Sandbox



Защита
электронной почты



Защита
от массовых атак



Защита файловых
хранилищ



Выявление ВПО
(при API-интеграции
с корпоративными системами)



Защита веб-приложений
(при интеграции
с web application firewall)



Автоматизация проактивного
поиска угроз и хакерского
инструментария



Контроль объектов
в сетевом трафике



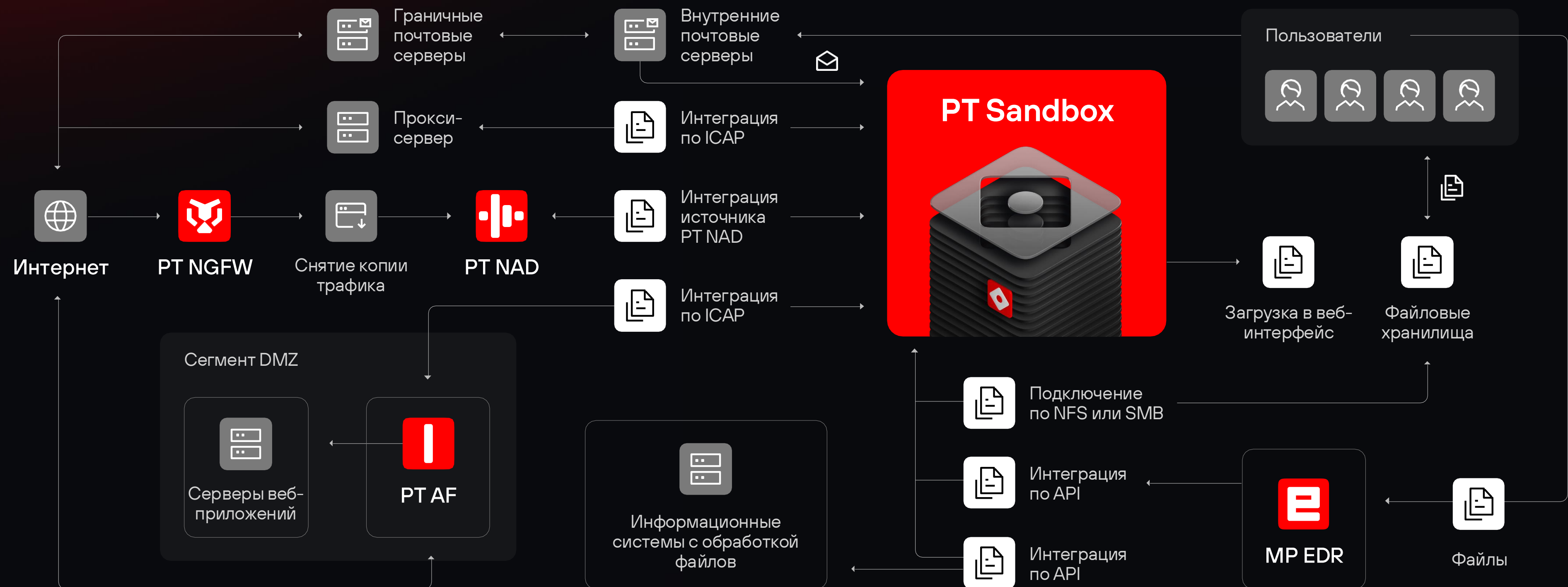
Защита конечных устройств
(вместе с MaxPatrol EDR)



Защита от сложных целевых
атак (в составе PT Anti-APT)

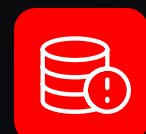
PT Sandbox в инфраструктуре

PT Sandbox устанавливается в инфраструктуре и подключается ко множеству источников, обеспечивая своевременное обнаружение неизвестного ВПО и угроз нулевого дня



Интеграция PT Sandbox со сторонними системами

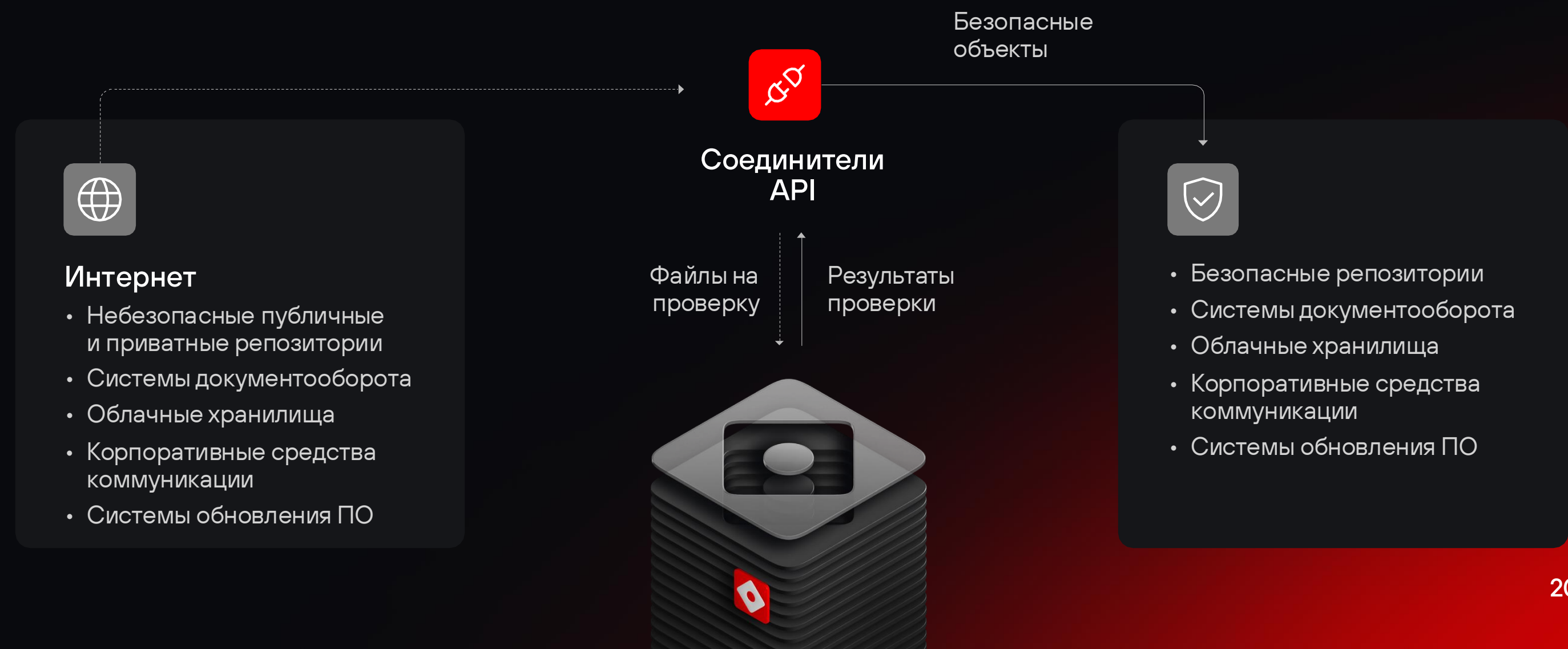
PT Sandbox может интегрироваться по API со сторонними системами. Продукт отдает результаты проверки в соединителях API*, который может выполнять блокировку на основе полученных данных

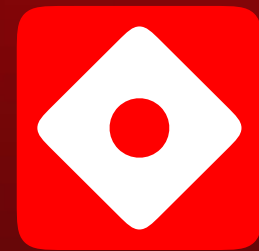


PT Sandbox обеспечивает безопасность данных в репозиториях, хранилищах и корпоративных системах коммуникации



* Написать соединитель можно с помощью руководства разработчика





PT Sandbox

ПОЧЕМУ PT SANDBOX



Преимущества PT Sandbox

Широкий список источников, поддерживаемых «из коробки»

Контроль основных каналов передачи файлов и ссылок в инфраструктуре

Встроенные средства ML для обнаружения ВПО

Анализ сетевого трафика и 8500 признаков поведения объекта с помощью машинного обучения. PT Sandbox обучается и адаптируется с учетом специфики компании

Глубокая кастомизация образов и приманок

Настройка среды эмуляции, как Windows так и Linux и приманок с учетом отраслевой специфики организации

Гипервизор с уникальными плагинами

Анализ снимков памяти, выявление ВПО, работающего на уровне загрузчика операционной системы

Обновление экспертизы за 2,5 часа

Оперативная доставка обновленных наборов правил для обнаружения ВПО от PT Expert Security Center и собственной антивирусной лаборатории PT AV

Поддержка отечественных ОС

Готовность к установке на Astra Linux и Основа, поддержка виртуальных образов поведенческого анализа с Astra Linux, «РЕД ОС», Alt Linux

Неограниченные возможности интеграции

Проверка объектов в информационных системах любой конфигурации с использованием API-соединителей

Возможности интерактивного поведенческого анализа

Для углубленного изучения объектов не нужно отдельное решение – проверка объектов с необходимыми действиями доступна как в потоковом режиме, так и через интерфейс продукта



PT Sandbox

ЛИЦЕНЗИРОВАНИЕ И ВАРИАНТЫ ВНЕДРЕНИЯ



Варианты поставки и модель лицензирования PT Sandbox

ПОСТАВКА



На аппаратной платформе

Все узлы PT Sandbox разворачиваются на аппаратной платформе



Совмещенное размещение

Основной узел разворачивается на виртуальной машине, а узлы поведенческого анализа — на аппаратной платформе

ГОДОВОЕ ЛИЦЕНЗИРОВАНИЕ

Инфраструктурные лицензии

1

Лицензия основного серверного узла

2

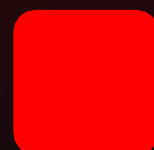
Лицензии узлов для отказоустойчивого кластера и горизонтального масштабирования узлов без поведенческого анализа

Лицензии на источники анализа

- Электронных писем (по числу почтовых ящиков)
- Файлов из сетевого трафика (по нагрузке на канал)
- Файлов, поступающих через API
- Файлов из файловых хранилищ
- Файлов из промышленного сетевого трафика (по нагрузке на канал обработки)

Варианты поставки PT Sandbox с объединенными лицензиями

ПОСТАВКА



На аппаратной платформе

Все узлы PT Sandbox разворачиваются на аппаратной платформе



Совмещенное размещение

Основной узел разворачивается на виртуальной машине, а узлы поведенческого анализа — на аппаратной платформе

ГОДОВОЕ ЛИЦЕНЗИРОВАНИЕ ALL-IN-ONE

Объединенная лицензия

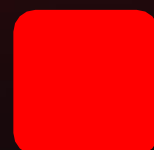
Включает функции основного серверного узла без функций отказоустойчивого кластера и масштабирования основного узла

Источники

- До 100 почтовых ящиков, до 100 Мбит/с, 1 хранилище, до 10 DFPN (файлов в час для поведенческого анализа) по API
- До 500 почтовых ящиков, до 500 Мбит/с, 1 хранилище, до 50 DFPN (файлов в час для поведенческого анализа) по API
- До 1000 почтовых ящиков, до 1000 Мбит/с, 1 хранилище, до 100 DFPN (файлов в час для поведенческого анализа) по API
- До 2000 почтовых ящиков, до 2000 Мбит/с, 1 хранилище, до 200 DFPN (файлов в час для поведенческого анализа) по API

Варианты поставки PT Sandbox для небольших инфраструктур (SME)

ПОСТАВКА



На аппаратной платформе

Все узлы PT Sandbox разворачиваются на аппаратной платформе



Совмещенное размещение

Основной узел разворачивается на виртуальной машине, а узлы поведенческого анализа — на аппаратной платформе

ГОДОВОЕ ЛИЦЕНЗИРОВАНИЕ ALL-IN-ONE

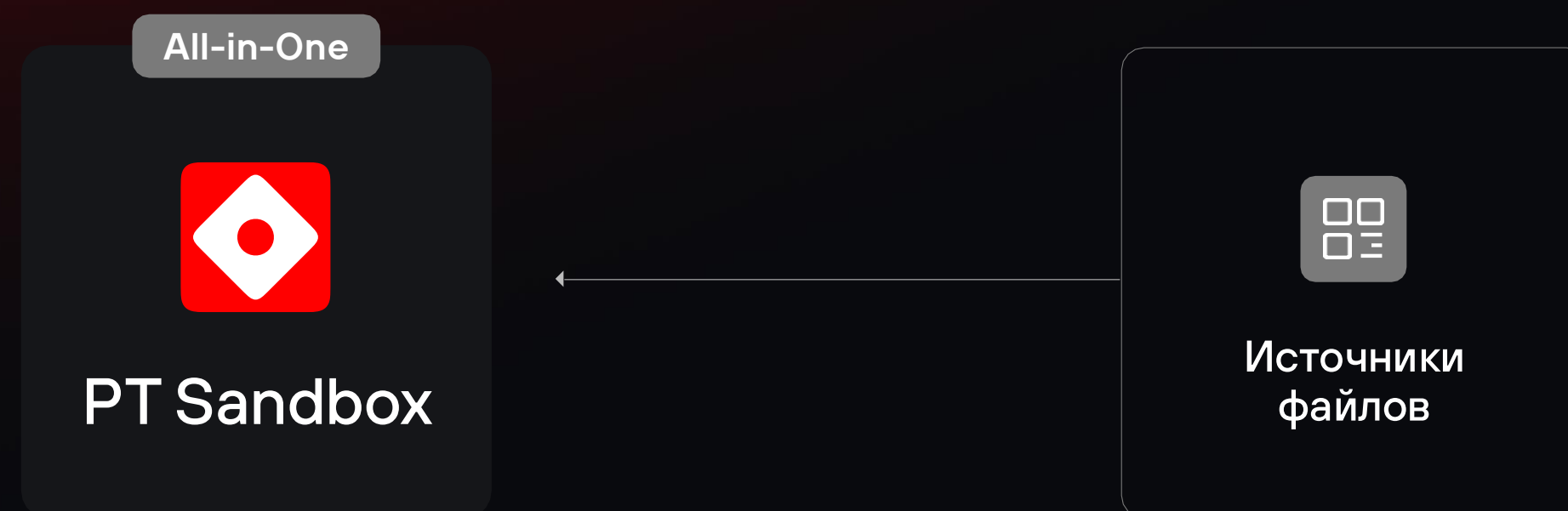
Объединенная лицензия

Включает функции основного серверного узла без функций отказоустойчивого кластера и масштабирования основного узла

Источники

- Электронных писем (по числу почтовых ящиков)
- Файлов из сетевого трафика (по нагрузке на канал обработки)
- Файлов из файловых хранилищах
- Расширения для перечисленных источников

Минимальный вариант поставки PT Sandbox



Производительность:
до 20 000 файлов
в сутки на одном узле
поведенческого анализа

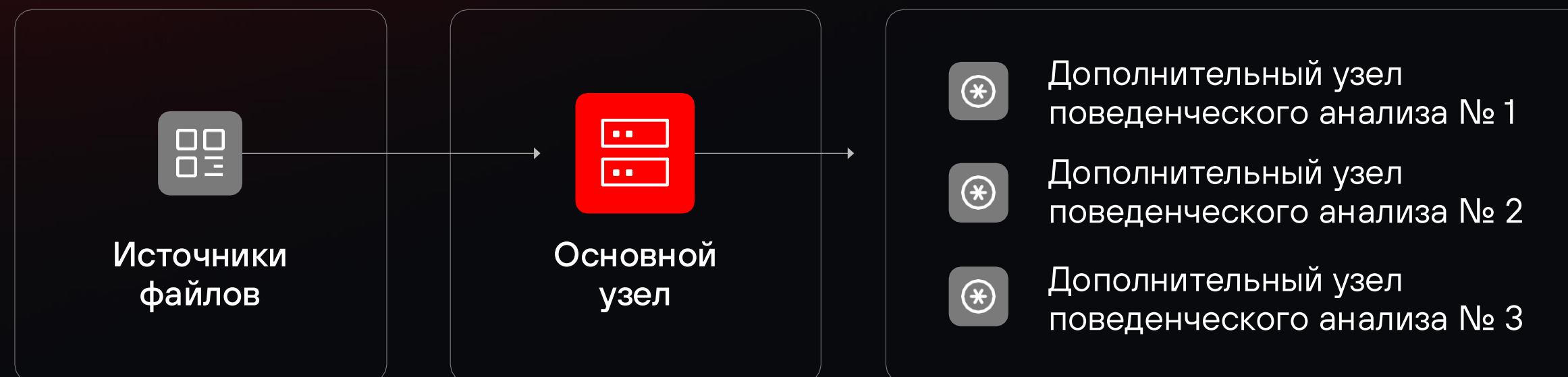
1

Размещение основного узла и узла поведенческого анализа на одной аппаратной платформе

2

Лицензирование не ограничивает возможность переноса узлов поведенческого анализа на отдельные серверы для повышения производительности

Рекомендуемый вариант поставки PT Sandbox



Каждый дополнительный узел обеспечивает прирост производительности до 20 000 файлов в сутки

1

Добавление дополнительных узлов поведенческого анализа для повышения суммарной производительности

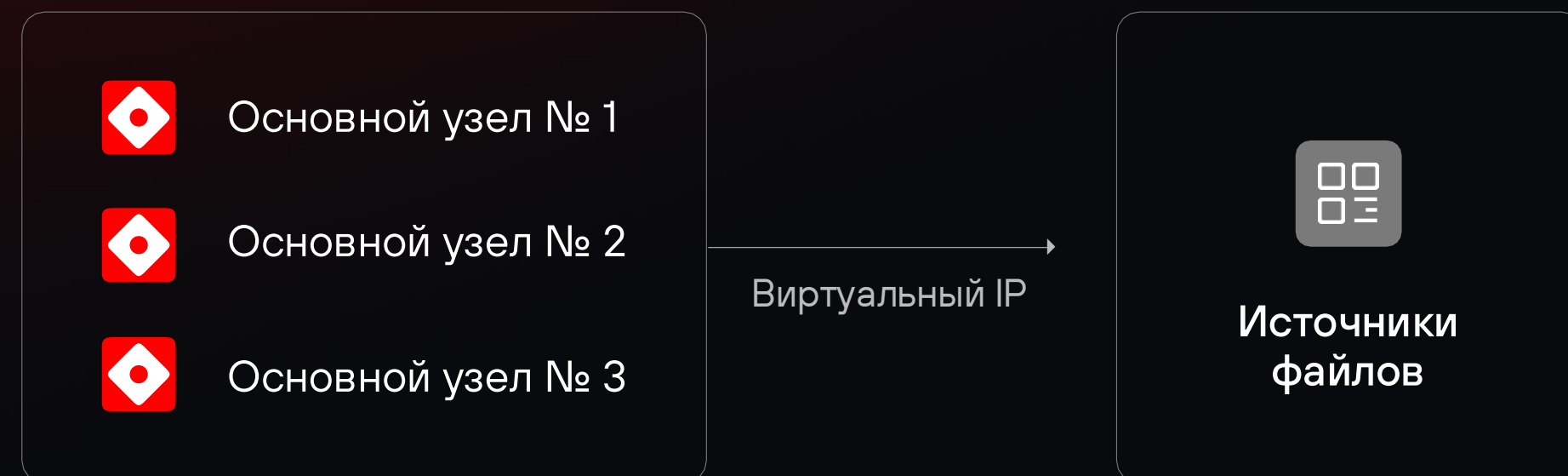
2

Дополнительные узлы поведенческого анализа учитываются в составе инфраструктурных лицензий и лицензий источников

3

Возможность добавления основных узлов для отказоустойчивости или горизонтального масштабирования

Отказоустойчивый вариант поставки PT Sandbox



1

Добавление основных узлов для обеспечения отказоустойчивости за счет создания кластера с нечетным количеством узлов

2

Рекомендовано при использовании PT Sandbox в блокирующем режиме работы источников



PT Sandbox

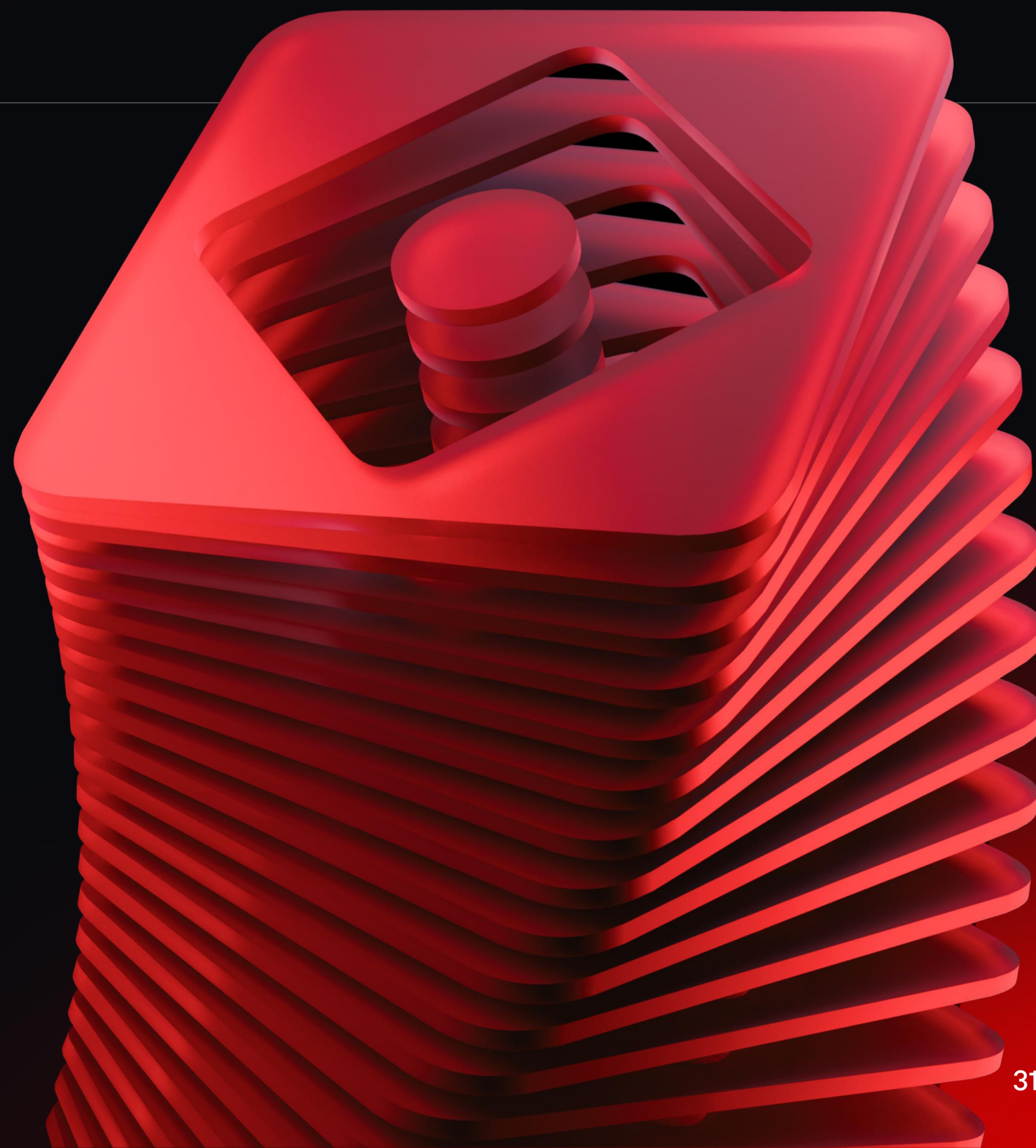
КАК НАЧАТЬ РАБОТУ С PT SANDBOX



Провести пилотный проект PT Sandbox



Оставить заявку
на демонстрацию



Сертификаты

PT Sandbox внесен в реестр российского ПО (запись № 8642 от 31.12.2020г) и сертифицирован ФСТЭК (сертификат № 4604 от 25.10.2022г) с 4-м уровнем доверия.

Соответствует профилям защиты средств антивирусной защиты (САВЗ) типа А и Б четвертого класса (ИТ.САВЗ.А4.ПЗ и ИТ.САВЗ.Б4.ПЗ), а также требованиям к САВЗ и техническим условиям на изделие

**СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ**

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

**СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4604**

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
25 октября 2022 г.

Выдан: 25 октября 2022 г. Переоформлен: 24 декабря 2025 г.
Действителен до: 25 октября 2027 г.

Настоящий сертификат удостоверяет, что программное изделие «Система статического и динамического анализа для выявления вредоносных объектов Positive Technologies Sandbox», разработанное и производимое АО «Позитив Текнолоджиз», является программным средством статического и динамического (поведенческого) анализа объектов информационных технологий в информационных системах, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А четвертого класса защиты. ИТ.САВЗ.А4.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б четвертого класса защиты. ИТ.САВЗ.Б4.ПЗ» (ФСТЭК России, 2012) (для исполнений «Система статического и динамического анализа для выявления вредоносных объектов Positive Technologies Sandbox» и «Система многопоточной проверки файловых ресурсов Positive Technologies MultiScanner») и технических условиях 83128364.SB_SB ТУ (для исполнения «Система статического и динамического анализа для выявления вредоносных объектов Positive Technologies Sandbox»), при выполнении указаний по эксплуатации, приведенных в формуляре 83128364.SB_SB 30 01 (для исполнения «Система статического и динамического анализа для выявления вредоносных объектов Positive Technologies Sandbox»), технических условиях 83128364.SB_MS ТУ (для исполнения «Система многопоточной проверки файловых ресурсов Positive Technologies MultiScanner»), при выполнении указаний по эксплуатации, приведенных в формуляре 83128364.SB_MS 30 01 (для исполнения «Система многопоточной проверки файловых ресурсов Positive Technologies MultiScanner»).

Сертификат выдан на основании технического заключения от 06.07.2022, оформленного по результатам сертификационных испытаний испытательной лабораторией АО Центр «Атомзащитаинформ» (аттестат аккредитации от 24.09.2018 № СЗИ RU.0001.01БИ00.Б028), экспертного заключения от 22.08.2022, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), и технических заключений от 18.05.2023, 29.06.2023, 04.08.2025 и 06.11.2025, оформленных АО «Позитив Текнолоджиз».

Заявитель: АО «Позитив Текнолоджиз»
Адрес: 107061, г. Москва, вн.тер.г. муниципальный округ Преображенское, Преображенская пл., д. 8, помещ. 60
Телефон: (495) 744-0144

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

Полезные ссылки

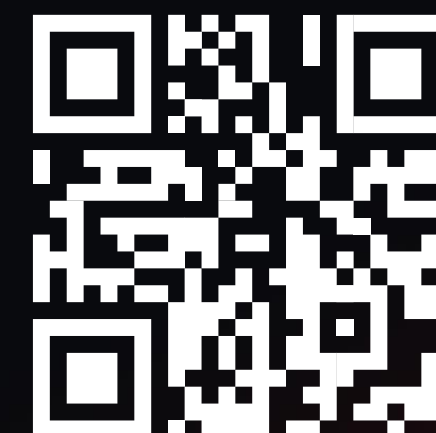
Telegram-чат
о PT Sandbox



Дополнительные
материалы о PT Sandbox

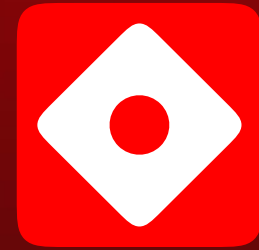


Каталог расширений
Positive Technologies



pt@ptsecurity.com

ptsecurity.com



PT Sandbox

Спасибо!