



PT EMAIL SECURITY

Система многоуровневой защиты
корпоративной почты



АТАКИ ЧЕРЕЗ ЭЛЕКТРОННУЮ ПОЧТУ



Главные тенденции почтовых угроз



Электронная почта остается главным вектором кибератак на организации. При этом атаки эволюционируют: массовый фишинг уступает место сложным целевым кампаниям, которые трудно выявить с помощью традиционных решений. Основные тенденции, осложняющие их обнаружение:

1

Усложнение фишинга — переход от примитивных писем к многоступенчатым атакам с применением социальной инженерии

2

Рост количества BEC-атак (Business Email Compromise, компрометации эл. почты), не использующих вредоносные ссылки

3

Кражи учетных данных через поддельные формы авторизации

4

Отказ от простых вложений в пользу QR-кодов и легитимных файлообменных сервисов

5

Атаки на цепочки поставок через взлом электронной почты контрагентов

6

Проникновение в инфраструктуру через уязвимости почтовых серверов

Электронная почта остается главной точкой входа в инфраструктуру

№1

Тренды современного фишинга



Несмотря на регулярную борьбу с фишингом, атак становится больше, а их механика — сложнее. Ключевые тренды:

1

Обход средств защиты

Фишинговые сообщения преодолевают фильтрацию за счет обхода CAPTCHA, применения QR-кодов и маскировки под офисные документы

2

Использование ИИ

Злоумышленники применяют искусственный интеллект для подготовки персонализированных сообщений и автоматизации атак

3

Атаки на различные пути коммуникаций

Для создания иллюзии подлинности отправителя и поиска пути коммуникаций, которому доверяет получатель, атаки ведутся одновременно через несколько средств коммуникации

4

Использование файлообменных ресурсов

Легитимные файлообменники используются для обхода фильтрации и снижения подозрений у пользователей

5

Phishing-as-a-Service (PhaaS)

Порог входа снижается — фишинговые сервисы становятся доступными даже для неквалифицированных злоумышленников

86%

успешных атак с применением социальной инженерии осуществляется через электронную почту

Актуальные киберугрозы:
I–II кварталы 2025 года ↗

КАК ОБНАРУЖИТЬ УГРОЗЫ В СООБЩЕНИЯХ ЭЛЕКТРОННОЙ ПОЧТЫ



PT Email Security — система многоуровневой защиты корпоративной почты



PT Email Security объединяет базовые и продвинутые механизмы выявления почтовых угроз в одном продукте:

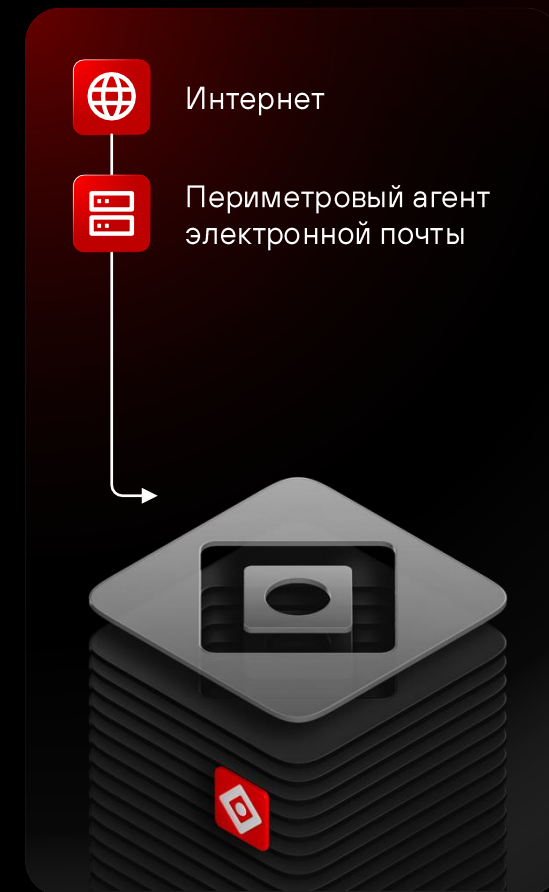
- Безопасный шлюз электронной почты — защита электронной почты от угроз (спам, фишинг, вредоносное ПО)
- Проверка объектов в песочнице выявляет сложные и целевые угрозы

1

Защита от массового спама и выявление фишинга за счет использования движка APAS

2

Защита от адресного фишинга с помощью механизмов распознавания QR-кодов, PT Crawler и обработки зашифрованных архивов



Ключевые преимущества PT Email Security



Единое решение
для защиты почты (подход
«все в одном решении»)



Технологическая основа
от PT Sandbox — удобство
установки и работы, гибкость
продукта, быстрая доставка
обновлений



Базы знаний, антивирусная
лаборатория, источники данных
об угрозах из экспертного центра
PT Expert Security Center (PT ESC)

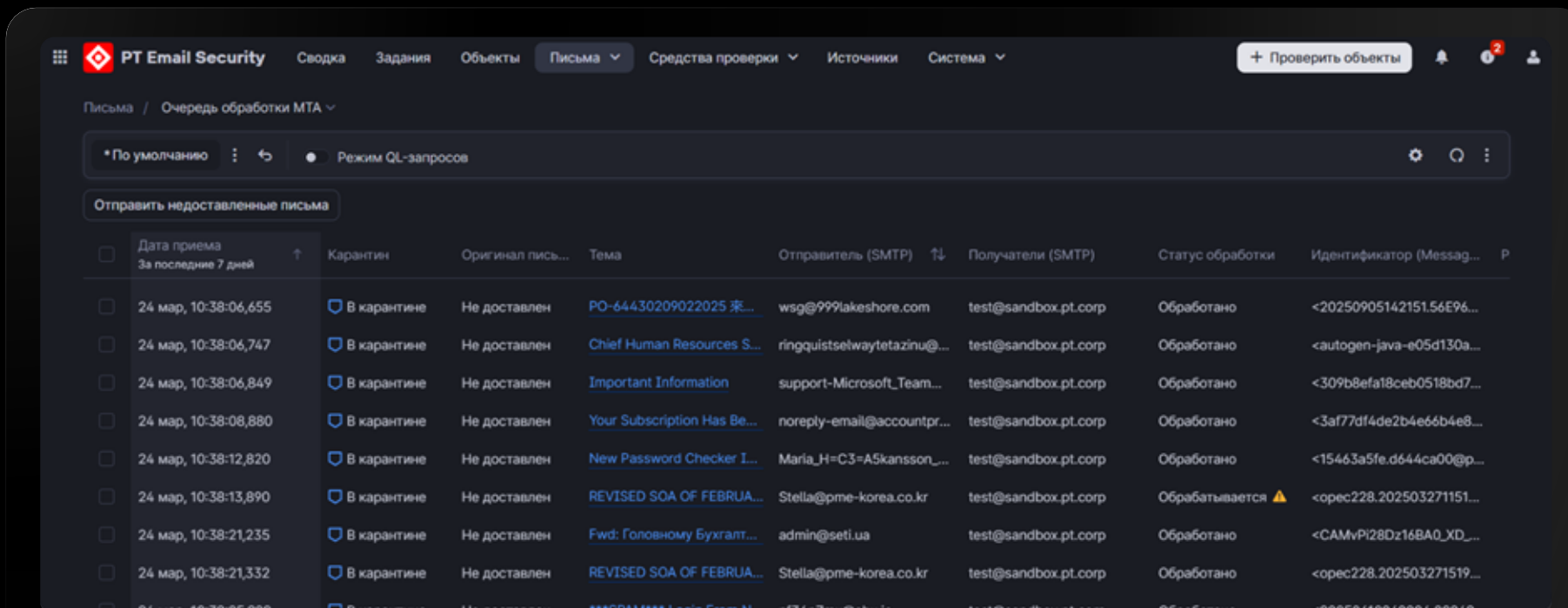
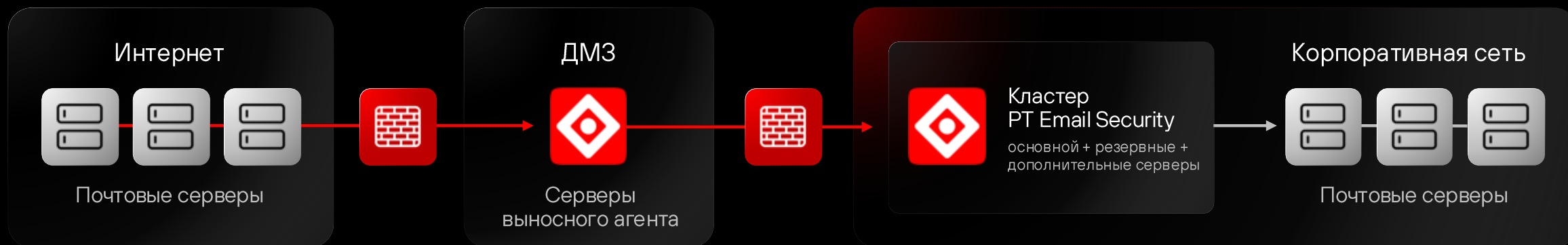


Схема подключения PT Email Security к ПОЧТОВЫМ СИСТЕМАМ



PT Email Security устанавливается
в инфраструктуре и подключается к почтовым
серверам в режиме блокировки ВПО

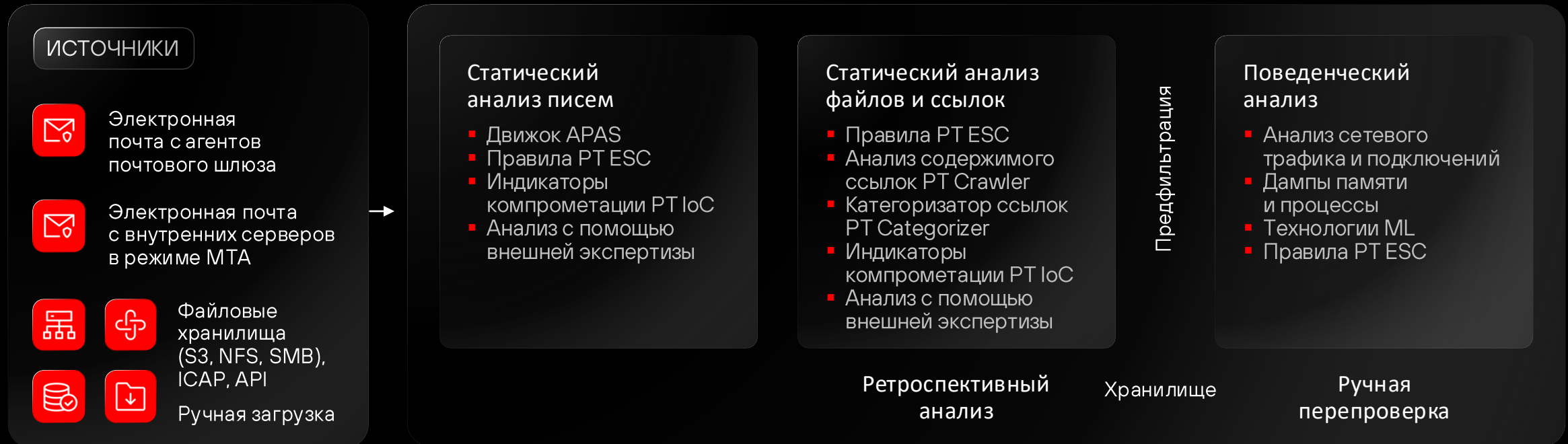
Анализ почтовых сообщений
с вложениями и ссылками обычно
занимает не более 5 минут. Время
анализа гибко настраивается



Как работает PT Email Security



Система получает письма от внешних почтовых серверов через почтовый шлюз или через транспорт с почтовых серверов организации, затем передает их на средства проверки



Средства для работы с электронной почтой



Почтовый шлюз



Для обеспечения безопасности приема электронных писем с фильтрацией подключений

Встроенный почтовый транспортный агент



Для управления транспортом электронных писем в инфраструктуре

Обезвреживание писем с угрозами



Настраиваемая правилами доставка письма с удаленным активным содержимым

Обработка писем в зависимости от отправителя и получателей



Конфигурируемые правила обработки писем

Антифишинг и антиспам (APAS) проверка писем



Средства анализа фишинга и спама разработки PT ESC

Проверка адресов в письмах по спискам DNS-блокировок



Подключение внешних репутационных списков для проверки IP-адресов и доменных имен, найденных в заголовках и ссылках

Статический анализ файлов и ссылок



Для защиты от известных угроз и проверки легитимности ссылок PT Email Security 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



Собственная антивирусная лаборатория PT AV и дополнительные средства

Анализ содержимого ссылок



Поиск и скачивание контента по ссылкам с проверкой его легитимности

Политики предварительной фильтрации при анализе файлов



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



Пользовательские правила определения объектов с угрозами

Персональные параметры, по которым PT Email Security 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 Email Security скачивает и проверяет контент только по тем ссылкам, которые удовлетворяют указанным пользователем параметрам

Поведенческий анализ



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

МНОГОУРОВНЕВАЯ ПРОВЕРКА ФАЙЛОВ



Анализ сетевого трафика и подключений



Анализ дампов памяти и процессов



ML-технологии для выявления аномального поведения в системных событиях и сетевом трафике

Изолированная среда PT Email Security

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

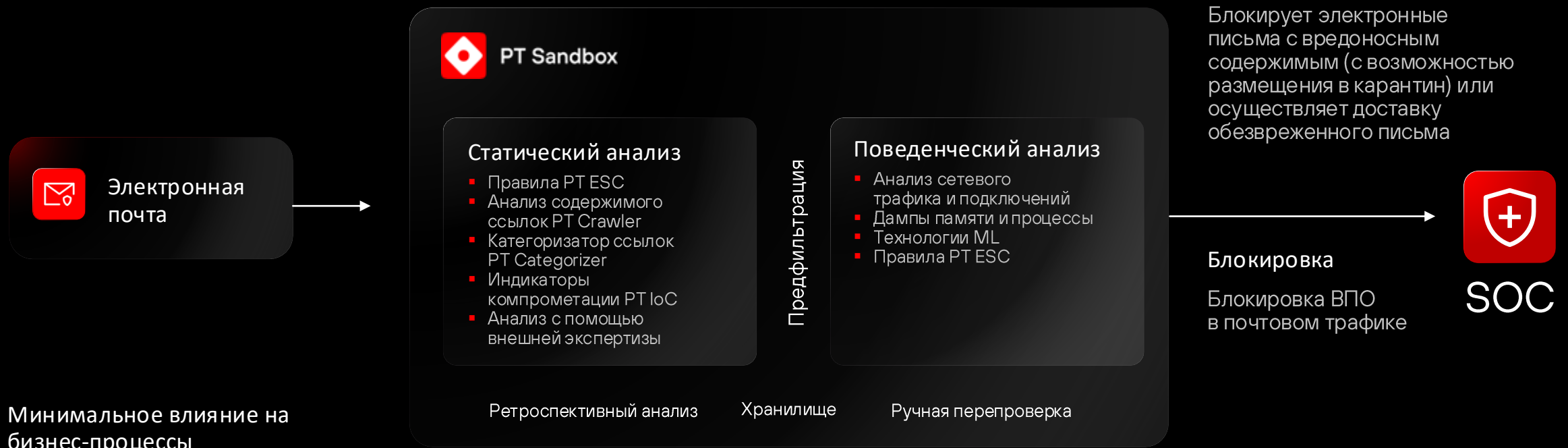


Anti-evasion-защита от популярных техник обхода виртуальных сред

PT Email Security. Блокировка ВПО в почтовом трафике



PT Email Security обрабатывает трафик от шлюза электронной почты, проверяет письма, определяет в них файлы и ссылки, осуществляет статический и динамический анализ объектов



Уникальность PT Email Security



Защита почты
и инфраструктуры
одним решением



Единая система для проверки
электронной почты и объектов
из других систем

Приманки
в песочнице



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

Экспертиза в ВПО и
почтовых угрозах



Доставка знаний о новых угрозах
за 2,5 часа, собственный
антиспам и антифишинг

Защита от
обнаружения



Обнаруживает все
популярные техники
обхода песочниц



Работает
на результат

Однозначно выявляет
вредоносное ПО
и оперативно блокирует
актуальные угрозы

ИНТЕГРАЦИЯ С ПРОДУКТАМИ POSITIVE TECHNOLOGIES И ДРУГИМИ СИСТЕМАМИ



Возможности интеграции PT Email Security



MaxPatrol SIEM

Выявление инцидентов ИБ



PT NAD

Анализ сетевого трафика



MaxPatrol EDR

Защита конечных точек



PT NGFW

Защита периметра сети



PT Application Firewall

Защита веб-приложений

PT Email Security передает
в MaxPatrol SIEM полную
информацию об угрозах,
обнаруженных в объектах,
с использованием
протокола **syslog**

Возможности интеграции PT Email Security



MaxPatrol SIEM

Выявление инцидентов ИБ



PT NAD

Анализ сетевого трафика



MaxPatrol EDR

Защита конечных точек



PT NGFW

Защита периметра сети



PT Application Firewall

Защита веб-приложений

Анализирует файлы,
извлекаемые из сетевого
трафика сенсором PT NAD.
Вердикт из PT Email Security
возвращается в PT NAD
автоматически

Возможности интеграции PT Email Security



MaxPatrol SIEM

Выявление инцидентов ИБ



PT NAD

Анализ сетевого трафика



MaxPatrol EDR

Защита конечных точек



PT NGFW

Защита периметра сети



PT Application Firewall

Защита веб-приложений

PT Email Security выполняет поведенческий анализ объектов, которые обнаруживают агенты MaxPatrol EDR на конечных точках.

Для повышения качества анализа используется информация о свойствах узла с агентом MaxPatrol EDR



Результат анализа
доступен на всех агентах

Возможности интеграции PT Email Security



MaxPatrol SIEM

Выявление инцидентов ИБ



PT NAD

Анализ сетевого трафика



MaxPatrol EDR

Защита конечных точек



PT NGFW

Защита периметра сети



PT Application Firewall

Защита веб-приложений

PT Email Security
анализирует файлы,
извлекаемые из сетевого
трафика, защищаемого
PT NGFW



Поддерживает работу
интеграции в режиме блокировки

Возможности интеграции PT Email Security



MaxPatrol SIEM

Выявление инцидентов ИБ



PT NAD

Анализ сетевого трафика



MaxPatrol EDR

Защита конечных точек



PT NGFW

Защита периметра сети

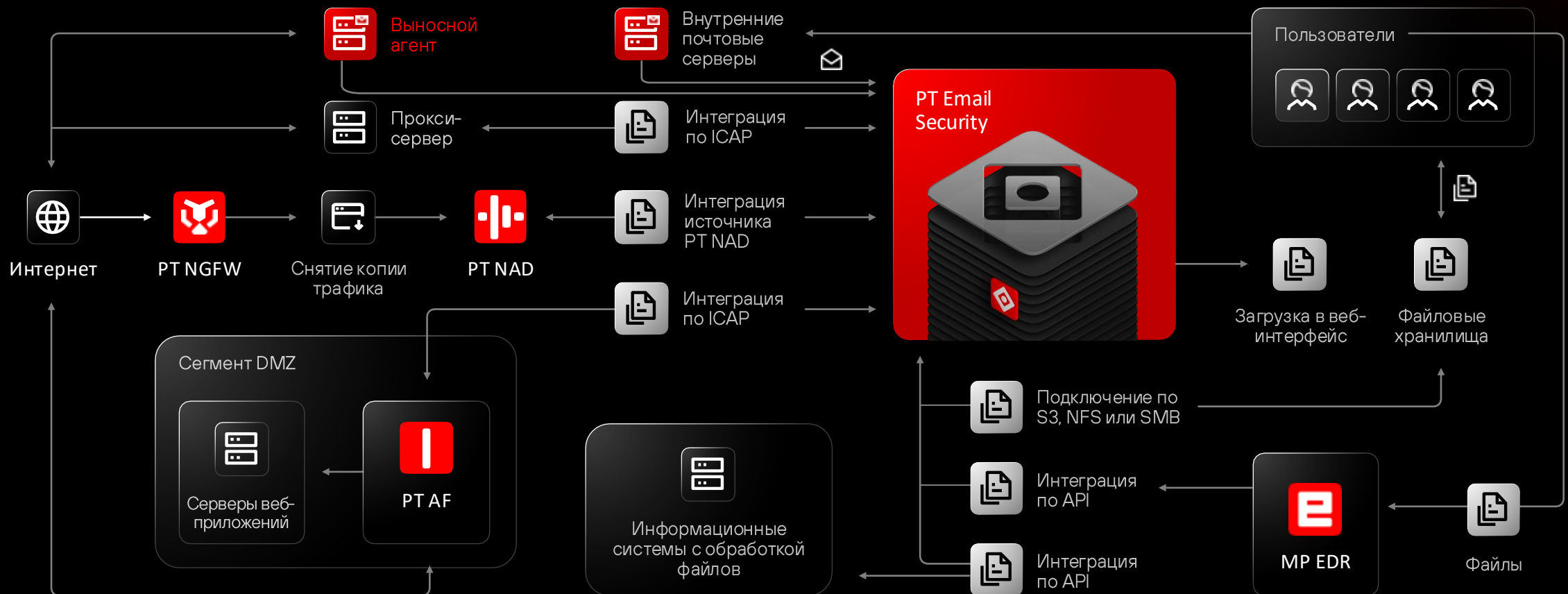


PT Application Firewall

Защита веб-приложений

PT Email Security анализирует
файлы, извлекаемые из трафика
веб-приложений, защищаемых
PT Application Firewall

PT Email Security в инфраструктуре



ЛИЦЕНЗИРОВАНИЕ И ВАРИАНТЫ ВНЕДРЕНИЯ



Варианты поставки PT Email Security с объединенными лицензиями



ПОСТАВКА

1 На аппаратной платформе

Все узлы PT Email Security разворачиваются на аппаратной платформе

2 Совмещенное размещение

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

ГОДОВОЕ ЛИЦЕНЗИРОВАНИЕ

1 Объединенная лицензия

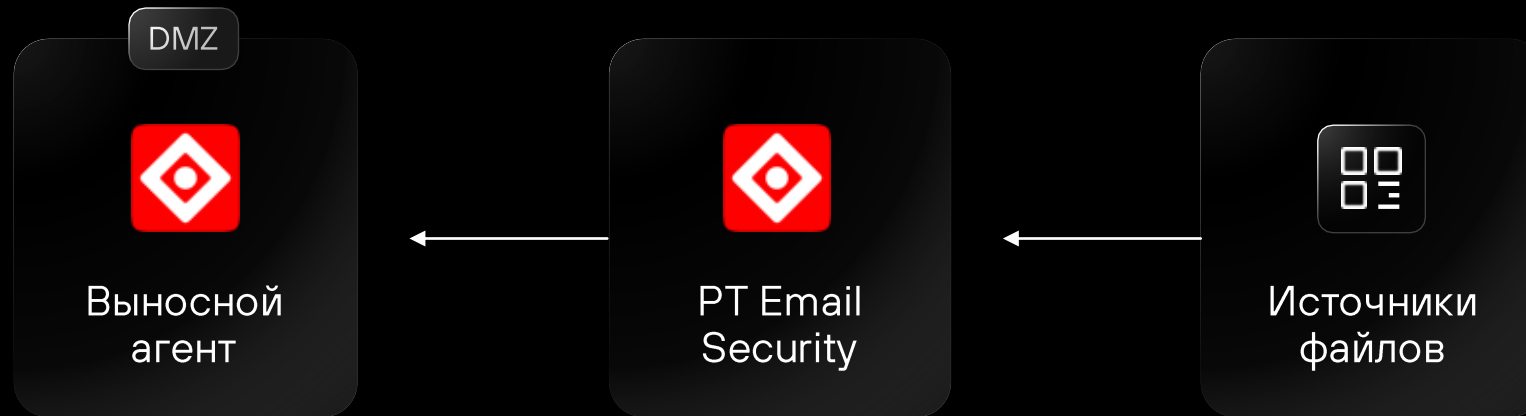
Включает лицензируемые компоненты:

- основного серверного узла
- дополнительных серверных узлов и отказоустойчивого кластера
- источников для приема анализируемых объектов

2 Метрика лицензирования

- От 1000 до 100 000 почтовых ящиков, с возможностью комбинирования
- в лицензии также включаются метрики лицензирования источников для анализа объектов из сетевого трафика, API-источников и файловых хранилищ

Минимальный вариант поставки PT Email Security



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

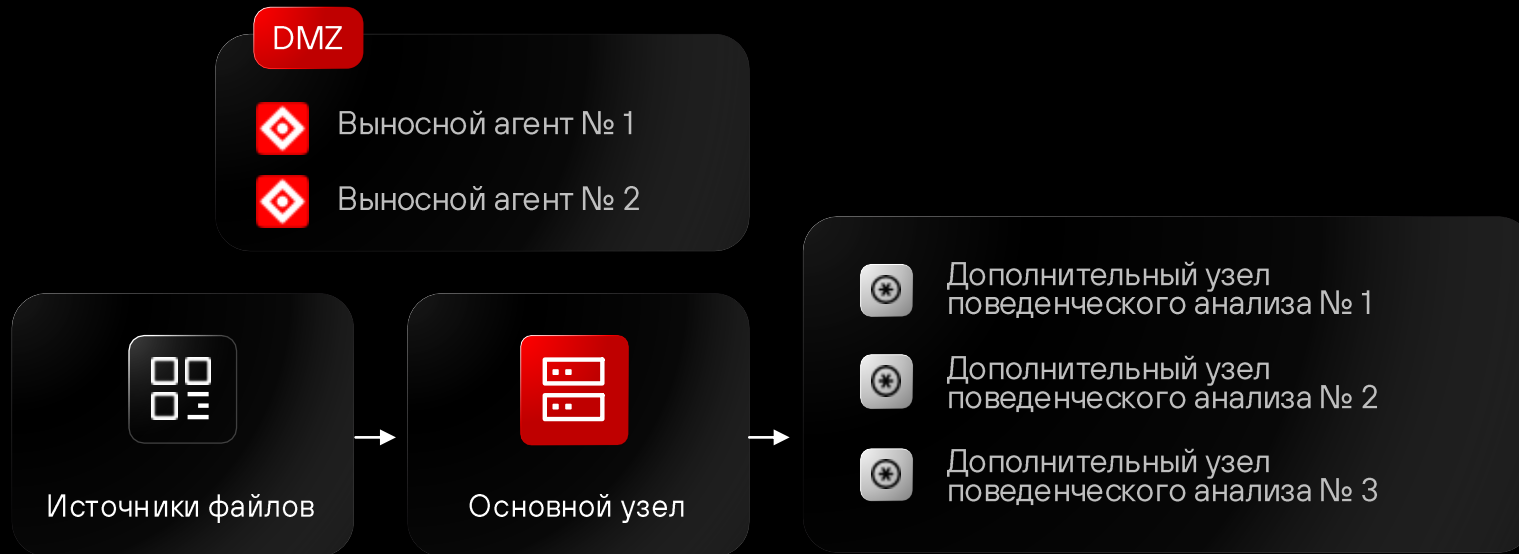
1

Размещение основного узла и узла поведенческого анализа на одной аппаратной платформе. Выносной агент находится на отдельном сервере в ДМЗ

2

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

Рекомендуемый вариант поставки PT Email Security



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

1

Добавление дополнительных узлов поведенческого анализа для повышения суммарной производительности. Добавление выносных агентов для обеспечения отказоустойчивости

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 Email Security



1

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

2

Рекомендовано при использовании PT Email Security в блокирующем режиме работы источников

КАК НАЧАТЬ РАБОТУ С PT EMAIL SECURITY



Провести пилотный проект PT Email Security



Оставить заявку
на демонстрацию



Сертификаты



PT Email Security внесен в реестр
российского ПО (запись №33012 от
17.04.2026г)



Позволяет выполнять требования
приказов ФСТЭК России
от 25.12.2017 № 239, от 18.02.2013
№ 21 и от 11.02.2013 № 17.



Полезные ссылки



Телеграм-чат
о PT Email Security
и PT Email Gateway



Каталог расширений Positive
Technologies



pt@ptsecurity.com

ptsecurity.com



Спасибо!