positive technologies

PT Email Security

Система многоуровневой защиты корпоративной электронной почты

Ключевые возможности

- Защита от массовых атак (включая спам) и целевых атак с использованием ВПО (включая фишинг)
- Предотвращение проникновения ВПО в контур организации
- Проверка файлов и ссылок, поступающих из почтового и сетевого трафика, файловых хранилищ, а также любых других источников

PT Email Security

Электронная почта остается главным вектором кибератак на организации. Фишинг становится целенаправленным, письма маскируются под легитимную переписку, а вредоносные вложения и ссылки обходят традиционные средства защиты.

Классических антивирусных и антиспам механизмов уже недостаточно для выявления современных атак с использованием многоступенчатых сценариев и вредоносного ПО нулевого дня.

Решение

PT Email Security – комплексное решение для защиты электронной почты, объединяющее базовые и продвинутые механизмы выявления почтовых угроз в одном продукте.

PT Email Security построен на технологическом фундаменте PT Sandbox, экспертизе PT Expert Security Center (PT ESC), а также обладает функциями почтового шлюза и почтового транспортного агента.

PT Email Security

Отсеивает ненужное, защищает важное

Как работает PT Email Security

Получение писем

Система принимает почтовые сообщения через шлюз безопасности (SEG), либо через транспортный агент с внутренних почтовых серверов.

Фильтрация

Выполняется предварительная фильтрация писем и объектов

Статический анализ

Проводится статический анализ писем, файлов и ссылок

Песочница

Подозрительные объекты направляются в изолированную среду для анализа поведения

Вердикт

По результатам анализа формируется вердикт и применяется политика: блокирование с размещением в карантине, обезвреживание и доставка писем

Почему PT Email Security

Единое решение для комплексной защиты электронной почты

Обеспечивает защиту корпоративной почты от известных и неизвестных угроз, включая целевые атаки и новое вредоносное ПО

Сочетание методов статического, поведенческого и репутационного анализа

Позволяет достоверно выявлять ВПО и оперативно блокировать актуальные угрозы

Комплексная антивирусная проверка писем

Выполняется на основе постоянно обновляемой и разносторонней экспертизы PT с возможностью подключения дополнительной и пользовательской экспертизы

Карантин для писем с расширенным функционалом

Включает пересылку писем, добавление комментариев с расширенным логированием, отслеживанием действий и автоматическим сокрытием уже обработанных писем (подход «zero-inbox»)

Защищенная архитектура за счет использования выносного агента

Дает возможность опубликовать выносной агент PT Email Security в интернете, не выставляя серверы продукта в демилитаризованную зону

Неограниченные возможности интеграции

Осуществляет проверку объектов в информационных системах любой конфигурации

Поддержка отечественных ОС

Решение может быть установлено на Astra Linux и ОСнова, поддерживает виртуальные среды с Astra Linux, «РЕД ОС», ALT Linux

Интеграция с продуктами Positive Technologies

Бесшовно интегрируется с MaxPatrol SIEM, PT NAD, MaxPatrol Endpoint Security, PT NGFW, PT Application Firewall

Соответствие требованиям регуляторов

PT Email Security внесен в реестр российского ПО. Позволяет выполнять требования регуляторов: приказ ФСТЭК России № 117 и № 239, ГОСТ Р 57580.1-2017

Уникальные технологии

Собственный антиспам и антифишинг движок

Защита от массового спама и фишинга

Обновление экспертизы за 2,5 часа

Оперативная доставка обновленных наборов правил обнаружения от PT ESC

Глубокая кастомизация образов и приманок

Настройка среды эмуляции и приманок с учетом отраслевой специфики организации

Гипервизор с уникальными плагинами

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

Протестируйте PT Email Security

Хотите проверить работу продукта в условиях реальной эксплуатации?

Оставьте заявку на пилот PT Email Security — мы свяжемся с вами для обсуждения всех деталей.

PT_Email Security_A4.RUS.0002.24.APR.2026