

PT Application Firewall PRO

**Высокопроизводительный межсетевой экран
для непрерывной защиты веб-приложений
(как сайтов-визиток, так и высоконагруженных
enterprise-порталов) и их API от внешних киберугроз**



Выявляет сложные
многоступенчатые атаки



Предотвращает загрузку ВПО



Противодействует вредоносным ботам



Поддерживает приложения с NLTМ



Блокирует атаки нулевого дня



Обнаруживает аномальное поведение трафика
и позволяет задавать правила обработки (L7)



Предоставляет аналитику
в режиме реального времени



Защищает API веб-приложений



Ключевые возможности



Мультитенантность

Изолированное пространство (тэнант) обеспечивает возможность независимой работы, настройки и доступа к защищаемым приложениям с использованием одного и того же продукта без взаимного влияния. Для каждого пространства выделяются индивидуальные обработчики трафика. Контейнерная архитектура позволяет изолировать кластеры физически, что выгодно отличается от изоляции на уровне логики



Поддержка full proxy HTTP/2

PT Application Firewall PRO поддерживает сквозной HTTP/2 – современный протокол передачи данных, который позволяет существенно ускорить обработку трафика. Благодаря ему функционирование защитной системы практически не отражается на скорости работы приложения, что напрямую влияет на восприятие сервиса пользователями



Автоскашивание ресурсов

При возрастании трафика добавляются новые обработчики, что помогает выдерживать всплески нагрузки (например, в случае DDoS-атаки или органического роста трафика в «черную пятницу»). Кроме того, контейнерная архитектура позволяет менять количество используемых в кластерах серверов, если в моменте не хватает мощности оборудования



Несколько типов развертывания

Можно выбрать один из вариантов установки:

- локальное развертывание – когда все данные хранятся в вашем периметре, а для полноценной защиты не нужна связь с интернетом;
- подключение нескольких площадок – за счет использования агентов либо дополнительных серверов обработки трафика;
- установка отдельного модуля, взаимодействующего с облачным PT AF, – если необходимо снизить затраты на инфраструктуру

Экспертиза «под капотом»

PT Application Firewall PRO содержит сильнейшую на российском рынке экспертизу по обнаружению и блокировке целенаправленных атак, основанную на собственном опыте проведения пентестов, а также на данных исследовательской группы Positive Research и экспертного центра безопасности Positive Technologies.

Технологии машинного обучения

PT Application Firewall PRO использует ML-модули для выявления:



подозрительной пользовательской активности



содержимого с признаками веб-шеллов
в загружаемых файлах

В отличие от сигнатурного анализа, который способен обнаруживать только известные веб-шеллы, ML-модель в PT AF PRO выявляет поведенческие паттерны, указывающие на вредоносное содержимое файлов. Это позволяет принять решение о блокировке даже ранее неизвестных угроз. Эффективность метода была неоднократно доказана в ходе международной кибербитвы Standoff, где ML-модели безошибочно обнаруживали подобные атаки.

2000+

клиентов за 10+ лет

Стабильная работа
в высоконагруженных
инфраструктурах

от **150 000 RPS**

Защита от угроз
из **OWASP Top 10**
и **OWASP API Security Top 10***

Защита от **5000+**
известных уязвимостей

PT Application Firewall PRO зарегистрирован
в реестре отечественного ПО
как программное обеспечение,
относящееся к сфере
искусственного интеллекта



Подробнее
о продукте



Тест-драйв
продукта



Наши
партнеры

