positive technologies

# PT Application Firewall PRO

**Высокопроизводительный межсетевой экран для непрерывной защиты веб-приложений и API**

- Защита современных веб-приложений и API
- Управление защитой из единого центра
- Обнаружение сложных и неизвестных атак с помощью ML
- Противодействие вредоносным ботам
- Предотвращение загрузки ВПО
- Блокировка DDoS-атак уровня L7

# Ключевые возможности

### Мультитенантность

Позволяет холдингам защищать десятки дочерних компаний в рамках одной системы. Контейнерная архитектура гарантирует, что нагрузка или атака на один филиал никак не повлияет на работоспособность других

### Единая консоль управления

Централизованное управление политиками и правилами защиты разнесенных инсталляций PT AF PRO значительно снижает риски взлома, повышает скорость реакции на инциденты и уменьшает операционные затраты на администрирование

### 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

### Автоскалирование 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

# 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.

**2000+**
клиентов

Работа
в инфраструктурах
от **150 000** RPS

# 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.

Защита от угроз
**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