

PT Application Firewall

Межсетевой экран уровня веб-приложений
(web application firewall, WAF)

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Блокирует массовые и целевые атаки
- Быстро встраивается в инфраструктуру
- Адаптируется под защищаемые приложения

250+

клиентов уже используют PT Application Firewall

50%

рынка WAF в России занял PT AF в 2019 году²

40+

авторизованных партнеров³ внедряют PT AF в России и СНГ

Веб-приложения по-прежнему остаются популярной целью для злоумышленников. Как показали наши исследования¹, каждая пятая атака направлена на веб-ресурсы организаций, чаще всего — государственных и медицинских учреждений, онлайн-сервисов, организаций сферы науки и образования и IT-компаний.

PT Application Firewall защищает веб-приложения от внешних атак и не позволяет злоумышленникам эксплуатировать уязвимости. С помощью комбинации защитных технологий решение предотвращает как известные атаки, так и атаки нулевого дня.

Преимущества

Поддерживает непрерывность бизнес-процессов

PT Application Firewall защищает от DDoS-атак уровня приложений (L7), эксплуатации уязвимостей, связанных с ошибками в бизнес-логике приложений.

Минимизирует риск утечки информации

PT Application Firewall блокирует современные атаки на веб-приложения, включая те, что в списке OWASP Top 10 и классификации WASC, а также благодаря алгоритмам машинного обучения блокирует атаки нулевого дня.

Помогает выполнять требования стандартов

PT Application Firewall помогает соблюдать требования PCI DSS и других международных, государственных и корпоративных стандартов безопасности. Решение зарегистрировано в реестре российского ПО, имеет действующий сертификат ФСТЭК России и сертификат соответствия Республики Казахстан.

1 «Актуальные киберугрозы: итоги 2019 года», Positive Technologies: ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019/

2 «У рынка WAF хорошие перспективы», ComNews: comnews.ru/content/205891/2020-04-29/2020-w18/u-rynka-waf-khoroshie-perspektivy

3 Список партнеров Positive Technologies: ptsecurity.com/ru-ru/partners/auth-partners/



**СХЕМЫ
ВНЕДРЕНИЯ**

СНИФФЕР

Анализ копии трафика.
Трафик передается в PT AF
со SPAN-порта коммутатора

**ОБРАТНЫЙ
ПРОКСИ-СЕРВЕР**

Перехват и расшифровка трафика, блокирование атак

**ПРОЗРАЧНЫЙ
ПРОКСИ-СЕРВЕР**

Подключение «в разрыв» на пути трафика между клиентом и веб-сервером в качестве L2-моста

**УЗНАТЬ
ПОДРОБНЕЕ**

Больше информации о PT Application Firewall на странице продукта: ptsecurity.com/ru-ru/products/af



PT Application Firewall

	Выявляет сложные многофазные атаки		Защищает от DDoS-атак уровня приложений
	Автоматически выявляет уязвимости приложения		Защищает от атак на пользователей приложения
	Противодействует вредоносным ботам		Предотвращает загрузку вредоносного ПО
	Блокирует атаки нулевого дня		Выполняет виртуальный патчинг

Возможности интеграции

**С ПРОДУКТАМИ
POSITIVE TECHNOLOGIES**

- **MaxPatrol SIEM**
Передача событий веб-безопасности для их дальнейшей корреляции
- **PT Application Inspector**
Формирование виртуальных патчей для защиты от эксплуатации обнаруженных уязвимостей
- **PT MultiScanner или PT Sandbox**
Защита веб-порталов от загрузки вредоносного ПО

**С ДРУГИМИ
РЕШЕНИЯМИ**

- **Next Generation Firewalls (NGFW)**, например Check Point
- **Системы Anti-DDoS**, например NETSCOUT Arbor
- **DLP- и антивирусные системы** (по протоколу ICAP)
- **SIEM-системы** (по протоколу syslog)

Режимы работы

STANDALONE

Установка продукта на одной аппаратной или программной платформе.

CLUSTER

Установка продукта на две и более аппаратных или программных платформы

Поставка

HARDWARE APPLIANCE

Для развертывания на физическом сервере. Производительность до 40 000 RPS

VIRTUAL APPLIANCE

Для развертывания на виртуальной машине. Производительность до 10 000 RPS