КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

Мощная и надежная защита

- **Автоматическая блокировка атак нулевого дня.** Мощные алгоритмы машинного обучения позволяют определять известные и неизвестные атаки, включая атаки нулевого дня.
- **Точное выявление основных угроз.** Механизмы корреляции PT AF в разы уменьшают количество ложных срабатываний, идентифицируя самые важные инциденты. Возможность выстраивать цепочки атак также упрощает расследование инцидентов.
- **Мгновенная целевая защита.** Уникальный встроенный модуль анализа исходного кода P-Code обнаруживает уязвимости и мгновенно блокирует атаки на них. PT AF также может быть интегрирован с анализатором кода PT Application Inspector для обеспечения безопасного процесса разработки.
- **Расширенная защита от DDoS-атак уровня приложений.** С помощью машинного обучения PT AF выполняет непрерывное профилирование поведения пользователей. Это позволяет отслеживать аномальную активность, включая попытки DDoS-атак уровня приложений, и оперативно принимать меры для защиты.
- **Помощь с выполнением требований PCI DSS** и других международных, государственных и корпоративных стандартов безопасности.

Простой старт и адаптивность

- **Разные опции внедрения.** PT AF можно развернуть в любом из 5 режимов (сетевой мост L2, прозрачный прокси-сервер, обратный прокси-сервер, режим мониторинга или расследования).
- **Удобные настройки.** Мастер настройки системы, заранее подготовленные шаблоны политик безопасности, автоматическое определение ресурсов и готовая база правил позволяют легко и быстро настраивать PT AF.
- **Интеграция с другими решениями** — антивирусными, DLP, анти-DDoS, SIEM и IPS. Например, Check Point Security Gateway, Arbor Peakflow, Qrator, Array Networks, HP ArcSight, IBM QRadar, Zecurion Zgate. PT AF также интегрируется с решениями Positive Technologies: PT Application Inspector, PT MultiScanner и PT SIEM.
- **Автоматическая интеграция в инфраструктуру.** Благодаря поддержке Cisco ACI можно легко добавить PT AF в сети любого размера.

PT Application Firewall сертифицирован по новым требованиям ФСТЭК России.

PT APPLICATION FIREWALL: ИНТЕЛЛЕКТУАЛЬНАЯ ЗАЩИТА КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ

ПРОБЛЕМЫ РЫНКА

С каждым годом финансовые и промышленные предприятия, телекоммуникационные и IT-компании, СМИ и государственные учреждения все активнее используют интернет для автоматизации. Официальные сайты, электронные торговые площадки, системы документооборота, учета, дистанционного банковского обслуживания и другие приложения помогают упростить рабочие процессы. Однако в то же время эти технологии открывают новые возможности злоумышленникам.

В рамках исследования Positive Technologies, проведенного в 2016 году, в 77% случаев эксперты, действуя от лица злоумышленников, смогли получить доступ во внутреннюю сеть организаций и к конфиденциальной информации пользователей — за счет эксплуатации уязвимостей веб-приложений.

Большинство уязвимостей приложений вызваны ошибками разработчиков и не всегда могут быть выявлены обычными сканерами, системами обнаружения вторжений и межсетевыми экранами из-за ряда причин:

- Злоумышленники эксплуатируют уязвимости нулевого дня, что делает бесполезными сигнатурные методы анализа.
- Традиционные системы обнаружения и предотвращения вторжений (IDS/IPS) дают тысячи срабатываний на подозрительные события, которые нужно разбирать вручную, чтобы выявить реальную угрозу.
- Многие корпоративные сайты и онлайн-сервисы используют нестандартные решения, которые включают сторонние модули и имеют оригинальные уязвимости. Защита таких приложений требует глубокого анализа структуры, схем взаимодействия с пользователями и контекста эксплуатации.
- Даже известные уязвимости невозможно устранить сразу: исправление кода требует средств и времени, а зачастую и остановки важных бизнес-процессов, и все это время злоумышленники могут использовать уязвимость.
- Для защиты критически важных приложений необходимо учитывать их бизнес-логику и отделять реальные атаки от нормального функционирования приложения.

РЕШЕНИЕ: PT APPLICATION FIREWALL

Система Positive Technologies Application Firewall разработана в качестве ответа на самые современные вызовы, возникающие при защите веб-порталов, ERP-систем и мобильных приложений. PT AF обеспечивает непрерывную проактивную защиту веб-приложений от большинства атак, включая OWASP Top 10, WASC, автоматизированные атаки (включая скрапинг), атаки на стороне клиента и атаки нулевого дня.

Решение основано на мощных инновационных технологиях и исследованиях в сфере кибербезопасности, проводимых экспертами Positive Technologies уже более 15 лет.

Компания Positive Technologies в третий раз подряд стала визионером магического квадранта Gartner по безопасности веб-приложений (Gartner Magic Quadrant for Web Application Firewalls 2017).

Подробнее читайте на ptsecurity.com.

PT APPLICATION FIREWALL:
ИНТЕЛЛЕКТУАЛЬНАЯ ЗАЩИТА КОРПОРАТИВНЫХ ПРИЛОЖЕНИЙ

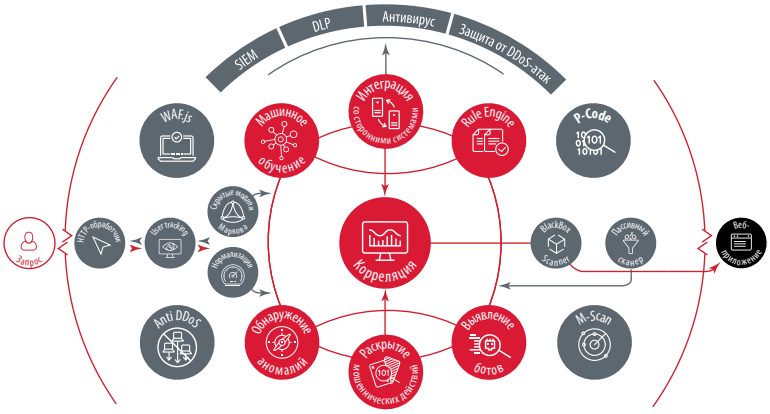
ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

- **Многоуровневая защита.** PT AF может быть интегрирован с системами безопасности сетевого уровня (Check Point, Arbor), что позволяет обеспечить защиту всей инфраструктуры организации.
- **Высокая эффективность.** Благодаря автоматизации PT AF позволяет экономить время и ресурсы. Среди возможностей переключение между режимами развертывания в один клик, удобная настройка политик безопасности, их сохранение и использование для новых ресурсов.
- **Еще больше защищенности благодаря пониманию бизнес-логики.** PT AF анализирует данные в различных форматах (XML, JSON и т. п.) и проверяет их на наличие фрагментов, потенциально опасных для бизнес-логики приложения. Это позволяет отличить атаки от обычных операций и своевременно их блокировать.
- **Максимальная конфиденциальность данных.** PT AF позволяет скрывать (маскировать) персональные данные конечных пользователей, такие как номера платежных карт или данные паспорта, от третьих лиц и даже от администраторов PT AF.
- **Доступность.** PT AF можно развернуть как аппаратное или виртуальное устройство. Продукт также полностью готов для работы в качестве облачного сервиса в моделях SaaS, VAS и MSS и доступен в облачной среде (Microsoft Azure).

ПРИНЦИП ДЕЙСТВИЯ: МОДУЛИ И МЕХАНИЗМЫ

PT Application Firewall использует всестороннюю схему защиты со множеством специализированных модулей и механизмов:

- **HMM** — самообучающийся модуль для блокировки атак нулевого дня и автоматизации работы приложения.
- **WAF.js** — модуль для защиты от атак на стороне клиента (XSS, DOM XSS, CSRF) и от программ-роботов разной степени сложности — даже от тех, которые могут исполнять JavaScript-код, эмулируя браузер. WAF.js также обнаруживает инструменты взлома, запущенные на стороне клиента в момент обращения к защищаемому приложению.
- Модуль **P-Code** выявляет уязвимости в исходном коде приложения и автоматически формирует правила для блокировки атак на эти уязвимости (виртуальные патчи).
- **Защита от программ-роботов** позволяет оперативно обнаруживать автоматизированные атаки, осуществляемые с целью кражи уникального контента или размещения несанкционированного контента на защищаемом сайте, при этом PT AF не оказывает влияние на активность «хороших» программ-роботов.
- **M-Scan** — модуль для автоматического сканирования загружаемых и скачиваемых пользователями файлов на антивирусных ядрах.
- **Пассивный сканер** идентифицирует компоненты приложений (CMS, фреймворки, библиотеки) для настройки модуля нормализации и обнаружения утечки данных, а также известных уязвимостей на базе словаря CVE.
- **BlackBox Scanner** осуществляет динамическое тестирование безопасности приложений (DAST): идентифицирует компоненты приложений, участвует в подготовке самообучающегося ядра и обнаружения уязвимостей в приложении.
- **Rule Engine** — механизм, который позволяет администратору самому создавать правила, в том числе для всех известных уязвимостей из словаря CVE.
- **SOA Firewall** — модуль анализа XML для противодействия атакам на распределенные веб-сервисы.



ЗАКАЖИТЕ БЕСПЛАТНЫЙ «ПИЛОТ» PT APPLICATION FIREWALL

Оставьте заявку на af.ptsecurity.ru!

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays