

Компания Positive Technologies в третий раз подряд стала визионером магического квадранта Gartner по безопасности веб-приложений.

[Подробнее читайте в отчете Gartner Magic Quadrant for Web Application Firewalls 2017](#)

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Оптимальная защита

- + **Передовые техники машинного обучения** для точного обнаружения атак и высокого уровня автоматизации продукта
- + **Продвинутые механизмы корреляции** для своевременного обнаружения основных атак
- + **Технология виртуального патчинга** для целевой защиты в реальном времени
- + **Понимание бизнес-логики приложения** для максимальной точности и защиты от обхода
- + **Помощь в выполнении требований PCI DSS** и других международных, государственных и корпоративных стандартов безопасности

Непрерывность бизнес-процессов

- + **Быстрый запуск.** Простая установка в удобном интерфейсе с использованием готовых шаблонов политик безопасности
- + **Снижение вероятности человеческих ошибок и минимум ручного труда.** Множество автоматизированных функций, доступных в несколько кликов
- + **Экономия средств.** Интеграция с инструментами тестирования безопасности приложений (PT Application Inspector) для своевременного исправления ошибок

Отлично подходит для Microsoft Azure

- + **Доступен для быстрого развертывания** из Microsoft Azure Marketplace.
- + **Быстрая и удобная первичная настройка** с использованием шаблонов Azure Resource Manager.
- + **Высокая производительность** благодаря адаптивной настройке параметров и масштабируемости системы.
- + **Возможность гибридного развертывания** в Microsoft Azure и Azure Stack.



НАДЕЖНАЯ ЗАЩИТА ВЕБ-ПРИЛОЖЕНИЙ В ОБЛАКЕ MICROSOFT AZURE

Microsoft Azure позволяет без лишних затрат ускорить и оптимизировать процесс разработки и развертывания веб-приложений. Платформа доступна в любой момент и надежно защищена. Однако это относится только к самой инфраструктуре Azure, в то время как вопросы обеспечения безопасности данных, размещаемых в облаке, остаются актуальными.

Игнорируя эти вопросы, вы подвергаете свои данные риску атак, хищений, а также нарушения требований стандартов, включая PCI DSS. При этом вы рискуете потерять время, средства и ресурсы, сэкономленные благодаря переходу на использование облачной инфраструктуры. Более того, утечка данных и простои могут помешать нормальному функционированию бизнеса.

ПРЕДСТАВЛЯЕМ PT APPLICATION FIREWALL

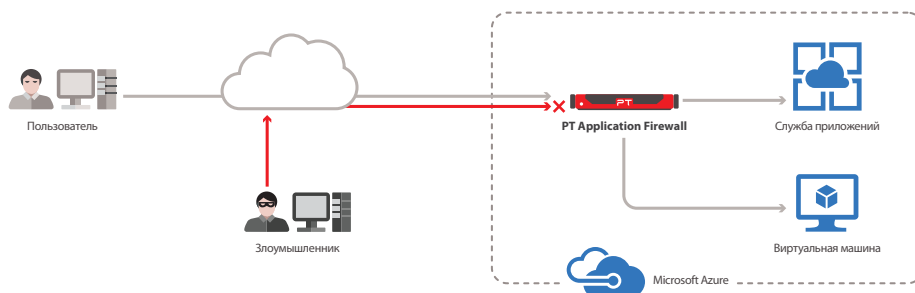
PT Application Firewall позволит вам безопасно работать в облачной среде Microsoft Azure, не подвергая свой бизнес угрозам.

Благодаря современным технологиям машинного обучения, передовым механизмам корреляции и самым свежим данным, полученным исследовательским центром Positive Technologies, PT Application Firewall автоматически блокирует большинство атак, включая OWASP Top 10, DDoS-атаки уровня приложений, атаки нулевого дня, автоматизированные атаки, специфичные для облачных приложений и сервисов EDoS-атаки (Economic Denial of Sustainability).

ПРЕИМУЩЕСТВА PT APPLICATION FIREWALL

- + **Непрерывная защита от эволюционирующих угроз.** Глобальный исследовательский центр Positive Technologies отслеживает и анализирует данные со всего мира в режиме реального времени. На основе этих данных продукт постоянно совершенствуется. Оптимальное сочетание подходов на основе черного и белого списков в совокупности с пониманием бизнес-логики защищаемого приложения способствует точному определению угроз. Кроме того, PT Application Firewall включает модуль P-Code, выявляющий уязвимости в исходном коде приложения и автоматически формирующий правила для блокировки атак на эти уязвимости (виртуальные патчи).
- + **Повышение эффективности бизнес-процессов.** Благодаря сочетанию инновационных технологий и подходов PT Application Firewall позволяет добиться непрерывности бизнес-процессов. Чтобы максимально соответствовать потребностям организации, продукт может быть интегрирован с SIEM- и DLP-системами, а также инструментами тестирования безопасности (включая собственную разработку Positive Technologies — PT Application Inspector). В отличие от других решений, PT Application Firewall обеспечивает высокий уровень автоматизации, что минимизирует ручной труд и повышает продуктивность процессов, связанных с обеспечением безопасности.
- + **Простота использования.** Подобно полностью готовой к использованию в инфраструктуре Microsoft Azure, PT Application Firewall может быть запущен быстро и легко. Это возможно благодаря простому развертыванию, удобной установке в интуитивно понятном интерфейсе и готовым шаблонам политик безопасности.

КАК ЭТО РАБОТАЕТ



ВОЗМОЖНОСТИ PT APPLICATION FIREWALL

Оптимальный уровень защиты

Инновационные технологии <ul style="list-style-type: none"> + обеспечение безопасности методами машинного обучения с использованием белых списков + виртуальный патчинг (SAST) с технологией P-Code + встроенный black-box scanner (DAST) + выявление клиентских атак (DOM-Based XSS) + блокировка атак нулевого дня 	Безопасность веб-приложений <ul style="list-style-type: none"> + защита от всех распространенных уязвимостей по классификации OWASP Top 10 + защита от подбора учетных данных + защита от замедляющих работу сети DoS-атак уровня приложений (slowloris, slow body и slow read) + встроенное антивирусное ядро + блокировка фишинговых атак + поддержка подписи cookie + защита статических и динамических HTML-форм от межсайтовой подмены запросов (CSRF) + защита HTML-форм + поддержка политики защиты контента (Content Security Policy) + эвристические алгоритмы блокировки межсайтового выполнения сценариев (XSS) и внедрения SQL-кода (SQLi) 	Защита от DDoS-атак уровня приложений <ul style="list-style-type: none"> + проверка соответствия HTTP-стандарту RFC + черный список программ-роботов + обнаружение программ-роботов на стороне клиента + обнаружение инструментов, используемых хакерами 	Предотвращение утечки конфиденциальной информации <ul style="list-style-type: none"> + фильтрация ответов + маскирование данных SOA Firewall <ul style="list-style-type: none"> + защита от DoS-атак (в частности, XML Bomb) + анализ соответствия XSD- и WSDL-схемам + поддержка GWT + поддержка JSON
--	---	---	--

Эффективный процесс управления

Варианты развертывания <ul style="list-style-type: none"> + построение кластера: Active/Active, Active/Passive, N+1 + балансировка нагрузки на сервер + SSL Bridging/SSL Offloading + RESTful API + режим обратного прокси-сервера 	Эксплуатация и техническое обслуживание <ul style="list-style-type: none"> + моментальный доступ к панели быстрого поиска + усовершенствованный механизм корреляции событий + группировка событий + наглядное представление развития векторов атаки Поддержка протоколов <ul style="list-style-type: none"> + полная поддержка протокола AMF + нормализация протокола HTTP + поддержка WebSockets 	Управление доступом <ul style="list-style-type: none"> + аутентификация с использованием клиентских SSL-сертификатов + поддержка LDAP-аутентификации + база данных геолокации + отслеживание сессий + отслеживание активности пользователей + политика управления доступом на основе ролей + черные списки узлов и IP-адресов 	Формирование отчетов по расписанию или по запросу <ul style="list-style-type: none"> + подробное описание атак + набор шаблонов для создания отчета + плановая отправка отчетов по электронной почте определенному кругу пользователей организации
--	--	---	--

Возможности интеграции и поддержки

Интеграция с внешними и внутренними системами <ul style="list-style-type: none"> + Check Point Security Gateway + HP ArcSight + IBM QRadar + Qrator Labs + PT SIEM, PT MultiScanner, PT Application Inspector + интеграция с антивирусным ПО по протоколу ICAP + SMTP, SNMP и т. п. 	Постоянная поддержка и выпуск обновлений <ul style="list-style-type: none"> + оказание технической поддержки на регулярной основе + автоматические обновления базы знаний
---	--

PT APPLICATION FIREWALL: РЕКОМЕНДАЦИИ ПО ВЫБОРУ ВИРТУАЛЬНОЙ МАШИНЫ MICROSOFT AZURE

PT Application Firewall доступен в рамках модели использования собственной лицензии (bring your own license, BYOL). Соответствие виртуальных машин Microsoft Azure производительности PT Application Firewall:

Минимальный размер виртуальной машины Microsoft Azure	F4	F8	F16
Производительность PT Application Firewall	1000 запросов в секунду	5000 запросов в секунду	10 000 запросов в секунду

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.