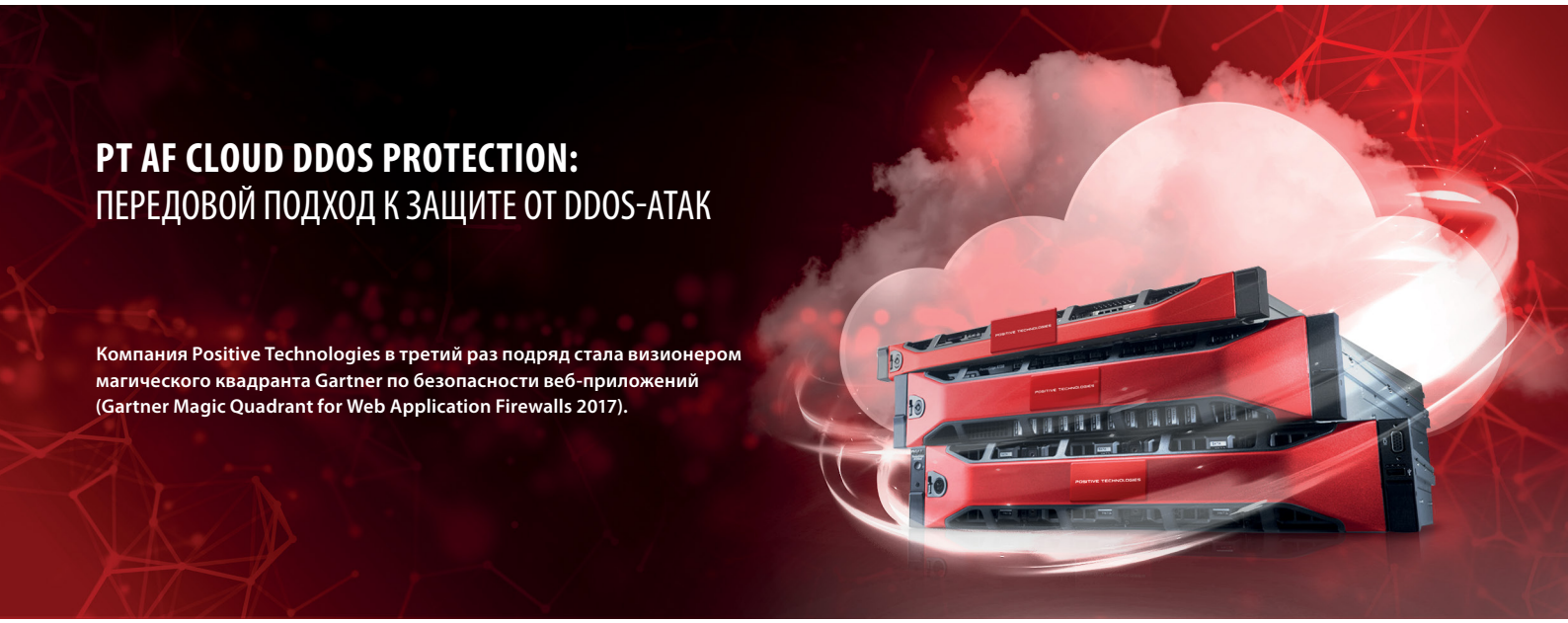
PT AF CLOUD DDOS PROTECTION:
ПЕРЕДОВОЙ ПОДХОД К ЗАЩИТЕ ОТ DDOS-АТАК



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

Решение для организаций, использующих веб-приложения в качестве одного из основных инструментов для реализации своей деятельности:

- банков,
- e-commerce,
- СМИ,
- госучреждений.

ПРЕИМУЩЕСТВА ДЛЯ БИЗНЕСА

- Приложение, доступное для легитимных пользователей — благодаря технологиям поведенческого анализа, позволяющим системе отличать хорошего пользователя от злоумышленника.
- Минимизация репутационных рисков благодаря сокращению времени простоя приложения.
- Увеличение прибыли за счет стабильной работы и непрерывной доступности веб-приложения, которые повышают лояльность существующих клиентов и привлекают новых.
- Снижение затрат на обслуживание за счет получения полнофункционального конечного продукта из одних рук.
- Выполнение требований регуляторов: РС БР ИББС-2.6-2014, приказов ФСТЭК № 17 и 21 и PCI DSS.

МАССИРОВАННЫЙ УДАР

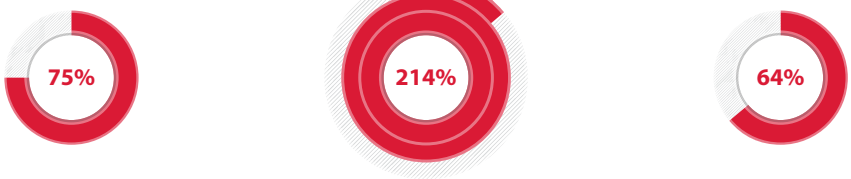
Один из самых распространенных приемов киберпреступников — проведение DDoS-атак, цель которых — сделать недоступными для пользователей веб-приложения и другие информационные системы организации. Подобные атаки популярны среди злоумышленников из-за невысокой стоимости их реализации и широкой доступности: быстро развивается направление «DDoS как услуга».

Ситуацию усугубляет то, что атаки становятся все мощнее, а их разновидностей больше. В целом типы DDoS можно разбить на несколько обширных классов в зависимости от объекта, на который они направлены:

- DDoS, нацеленные на канальную емкость,
- сетевую инфраструктуру,
- стек протоколов,
- приложение (L7).

Последний тип представляет наибольшую угрозу для бизнеса, так как данные атаки сложнее всего обнаружить — боты могут максимально копировать поведение пользователей, и тогда обычные методы обнаружения к ним неприменимы. При этом мощность атаки такого уровня в настоящее время может достигать десятков гигабит в секунду, что делает практически невозможной борьбу с ними своими силами.

На фоне роста количества и мощности DDoS-атак эксперты отмечают, что киберпреступники все чаще комбинируют методы нападения:



Рост числа DDoS-атак за первое полугодие 2016 года

Рост мощности атак за первое полугодие 2016 года

Доля комбинированных атак

В зависимости от реакции жертвы злоумышленники начинают моментально чередовать методы DDoS, одновременно добавляя к ним атаки, направленные на взлом веб-приложения и эксплуатацию его уязвимостей. Таким образом, для защиты ресурсов необходим комплекс специальных автоматизированных средств.

ЗАЩИТА НА НОВОМ УРОВНЕ: КОМПЛЕКСНЫЙ ПОДХОД

Эффективное противодействие угрозам возможно при объединении технологий облачной защиты от DDoS на всех уровнях и глубокой экспертизы в решениях противодействия комплексным атакам уровня приложений. Компания Positive Technologies в ответ на актуальные угрозы расширила возможности межсетевого экрана уровня приложений PT Application Firewall по блокировке DDoS-атак и представляет PT AF Cloud DDoS Protection.

PT AF Cloud DDoS Protection — инновационный сервис, основанный на облачных технологиях одного из ведущих лидеров в противодействии DDoS-атакам компании Qrator Labs и встраиваемого в инфраструктуру решения по противодействию веб-атакам и DDoS уровня L7 — PT Application Firewall. Сервис использует распределенную сеть фильтрации Qrator Labs, покрывающую США, Россию, Юго-Восточную Азию, Западную и Восточную Европу. Защита строится на взаимном обмене данными между системами: PT Application Firewall сообщает задействованные в атаке IP-адреса узлам очистки. Это обеспечивает проактивную автоматизированную защиту приложений даже от самого сложного комбинированного нападения.

ПРЕИМУЩЕСТВА КОМПЛЕКСНОЙ ЗАЩИТЫ ПРИЛОЖЕНИЙ

Благодаря объединению облачных технологий и частного (on-premise) решения вы получаете:

- **Сохранение приватности данных клиента.** Расширенные возможности PT Application Firewall для работы с SSL-трафиком позволяют настроить защиту таким образом, чтобы вся чувствительная информация (учетные данные, данные о сессии и о структуре приложения) не выходила за пределы периметра организации.
- **Легкую настройку защиты без влияния на работу приложения.** Это отличает PT AF Cloud DDoS Protection от других облачных сервисов, которые имеют ограничения по настройкам и требуют дополнительных изменений в конфигурации сети заказчика.
- **Предотвращение попыток обхода защитных средств.** Использование совместного решения позволит блокировать попытки обхода защитных механизмов и не использовать для этого выделенный канал от облака до оборудования клиента.
- **Мониторинг доступности защищаемого ресурса 24/7.** Клиент может настроить оповещения о любых проблемах с доступностью приложения, даже если DDoS-атака отсутствует.
- **Гибкую балансировку для обеспечения высокой доступности ресурса.** Распределение трафика происходит между основными и резервными веб-серверами клиента, с возможностью использования индивидуальных алгоритмов обращения к резервным серверам.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Помимо защиты от DDoS-атак, PT Application Firewall обеспечивает:

- **Автоматическую блокировку атак нулевого дня.** PT Application Firewall создает статистическую модель функционирования приложения и на ее основе выявляет аномальное поведение, что позволяет блокировать ранее неизвестные атаки.
- **Защиту от всех распространенных уязвимостей** по классификациям OWASP и WASC, включая SQLi, XSS и XXE, а также от популярных атак HTTP Request Splitting, Clickjacking.
- **Учет отраслевых особенностей.** PT Application Firewall защищает приложения любого масштаба с учетом специфики инфраструктуры заказчика: интернет-банкинг, ERP-системы (SAP и другие), веб-сервисы и корпоративные ресурсы (VMware, OWA, SharePoint).
- **Соответствие требованиям регулирующих организаций.** PT Application Firewall имеет сертификат ФСТЭК России (№ 3455 от 27.10.2015), сертификат Министерства обороны (№ 2619 от 21.07.2014), а также внесен в единый реестр российских программ для ЭВМ и баз данных. В 2016 году вышел приказ ФСТЭК № 9, в котором утверждены требования к межсетевым экранам. Документ вступил в силу с 1 декабря 2016 года. PT Application Firewall сейчас проходит сертификацию на соответствие новым требованиям.

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ PT APPLICATION FIREWALL

- Профилирование с использованием техник машинного обучения для обнаружения атак — система строит шаблоны поведения для групп пользователей, а также шаблоны поведения, характерного для злоумышленников.
- Мониторинг состояния приложения — непрерывно анализируя все входящие HTTP-запросы и ответы от сервера, PT Application Firewall проверяет состояние приложения и может прогнозировать тренд негативного влияния DDoS-атаки на показатели доступности приложения, а также оперативно информировать PT AF Cloud DDoS Protection.
- Защита от программ-роботов (сканеры, подбор паролей, фрод, бот-сети) — выявление аномалий в действиях пользователей средствами поведенческого анализа.
- Защита от XML DoS. Глубокий анализ и быстрая обработка XML/SOAP-данных позволяют снижать нагрузку на целевые системы, переложив часть операций по валидации полей на PT AF.

ПРЕИМУЩЕСТВА PT AF CLOUD DDOS PROTECTION

- Фильтрация DDoS в полностью автоматическом режиме.
- Сеть Qrator, на которой основано решение, полностью прозрачна для легитимных пользователей — при ее работе не используются CAPTCHA или другие неудобные проверки.
- Минимальное количество ложных срабатываний. 0% — без атаки. Не более 5% — под атакой.
- Используются собственные уникальные методики фильтрации, которые постоянно обновляются без участия клиента.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

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