# PT APPLICATION FIREWALL: ЗАЩИТА ВЕЩАНИЯ ВГТРК НА ОЛИМПИАДЕ 2014

*«Чтобы обеспечить круглосуточную защиту и доступность наших веб-ресурсов, нам нужен был инструмент, который умеет выявлять угрозы в режиме реального времени, работая с огромными потоками данных. Благодаря использованию PT Application Firewall все атаки были своевременно блокированы, а миллионы наших онлайновых зрителей и слушателей получили бесперебойную трансляцию Олимпийских игр».*

**Дмитрий Сафронов**
начальник отдела защиты информации
ВГТРК

VGTRK
TELEVISION AND RADIO

## ПРОФИЛЬ КОМПАНИИ

- **Отрасль:** СМИ
- **Компания:** ФГУП ВГТРК
- **Владелец:** Правительство РФ
- **География:** Россия, Украина, Белоруссия, Казахстан
- **Состав:** более 80 телеканалов и телерадиокомпаний
- **Аудитория интернет-вещания:** более 300 млн человек в год на десятках сайтов, в том числе с потоковым вещанием

- **Решение:** защита онлайн- и мобильных приложений
- **Масштаб:** более 20 веб-приложений, до 220 тыс. пользователей одновременно
- **Продукты:** PT Application Firewall

## ЗАДАЧА

Всероссийская государственная телевизионная и радиовещательная компания (ВГТРК), будучи ведущим СМИ страны-организатора зимних Олимпийских игр 2014 года, впервые предоставила зрителям возможность смотреть прямые трансляции всех соревнований не только по телевизору, но и через интернет.

В дополнение к существующим порталам холдинга было разработано более 20 веб-приложений для обеспечения трансляции на различные устройства, от мобильных телефонов до SmartTV. Обеспечение бесперебойной работы этих ресурсов требовало нового подхода к безопасности в непростых условиях:

- Большой интерес к Олимпиаде со стороны злоумышленников: приложения ВГТРК подвергались постоянному шквалу из тысяч различных атак, от спам-ботов и сканеров уязвимостей до попыток кражи персональных данных. В таком потоке событий оператору защитной системы легко потерять действительно актуальные срабатывания.
- Защита приложений, реализованных с помощью разных технологий: от информационных порталов и интерактивных социальных сервисов до XML-шлюзов и вещательных платформ. Большинство сайтов позволяли смотреть потоковое видео (Flash или HLS) в прямом эфире или в записи, адаптируясь под конкретные пользовательские устройства.
- Работа под высокой нагрузкой. Максимальная нагрузка сайтов ВГТРК была зафиксирована во время хоккейного матча 13 февраля, когда более 220 тысяч онлайн-зрителей одновременно наблюдали игру России и Словении.
- Защита в режиме реального времени не оставляет времени на «разбор полетов» и переписывание исходного кода; требуется проактивное выявление угроз и моментальное закрытие брешей.

## РЕШЕНИЕ

Для решения поставленной задачи ВГТРК обратилась к своему давнему партнеру, компании Positive Technologies. Эксперты компании предложили использовать межсетевой экран PT Application Firewall — как для защиты новых приложений, разработанных специально под Сочи-2014, так и для обеспечения безопасности уже существующих порталов, включая Sportbox.ru, Vesti.ru, новостной сайт «Россия-24» и веб-приложения центральных телеканалов «Россия-1» и «Россия-2».

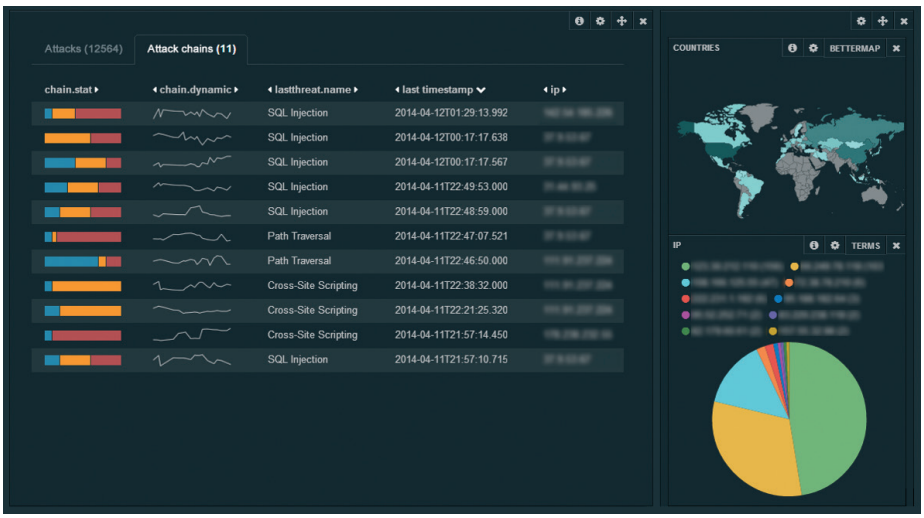
## КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Быстрое самообучение
- Высокая производительность
- Минимальный уровень ложных срабатываний
- Автоматическая верификация уязвимостей (DAST)
- Поддержка XML-приложений
- Корреляция событий и построение цепочек атак
- Широкие интеграционные возможности (SIEM и др.)
- Обратная связь для исправления уязвимостей

Интеллектуальные механизмы PT Application Firewall, включающие автоматическую верификацию уязвимостей и корреляционный анализ, позволили существенно снизить нагрузку на операторов защиты. Благодаря группировке сходных событий и выявлению цепочек развития атак, ИБ-эксперты ВГТРК смогли сконцентрировать внимание на самых важных происшествиях и оперативно реагировать на них.

Кроме собственных аналитических механизмов PT Application Firewall, в проекте были задействованы возможности интеграции межсетевого экрана с другими системами безопасности (SIEM), что позволило централизованно обрабатывать события из различных источников в рамках корпоративного Центра управления безопасностью (SOC).

«Раннее выявление угроз при помощи PT Application Firewall существенно повысило безопасность наших ресурсов, — говорит Дмитрий Сафронов, начальник отдела защиты информации ВГТРК. — У нас появилась возможность предотвращать атаки до того, как они приведут к серьезным последствиям. Мы планируем и дальше использовать продукты Positive Technologies для защиты приложений медиахолдинга».




## РЕЗУЛЬТАТ

Только за первый месяц работы на Олимпиаде межсетевой экран PT Application Firewall позволил своевременно обнаружить серьезные атаки на тринадцать веб-сайтов медиахолдинга: злоумышленники пытались нарушить работу пользовательских приложений или использовать их для проникновения во внутреннюю сеть компании ВГТРК. В частности, удалось предотвратить атаку, которая грозила закончиться утечкой большого объема конфиденциальных данных.

### О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована «Газпромом» и ФСТЭК. Более 3000 организаций из 30 стран 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 телекомов. В 2013 году компания заняла третье место на российском рынке ПО для безопасности и стала лидером по темпам роста на международном рынке систем управления уязвимостями. В 2015 году Gartner назвал Positive Technologies «визионером» в своем рейтинге Magic Quadrant for Web Application Firewalls.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.ru