



## PT APPLICATION FIREWALL ЗАЩИЩАЕТ ОНЛАЙНОВЫЕ СЕРВИСЫ «МЕГАФОНА»

*«В мире онлайн-сервисов появляется все больше угроз, и мы должны быть уверены, что наши клиенты и веб-ресурсы надежно защищены. Мы изучили продукты различных компаний, включая лидеров зарубежного рынка, но предпочли российское решение PT Application Firewall. Мы давно сотрудничаем с Positive Technologies, и нам нравится то, что делают коллеги. Есть понимание, что их продукты будут развиваться и удовлетворять наши новые потребности. Мы находимся в постоянном диалоге, всегда получаем необходимую поддержку, и для нас очень важно, что наш партнер нас слышит».*

### Сергей Химаныч

ведущий специалист отдела информационной безопасности  
ОАО «МегаФон»

### ПРОФИЛЬ КОМПАНИИ

- + Отрасль:**  
Телекоммуникации
- + Компания:**  
ОАО «МегаФон»
- + Основные акционеры:**  
AF Telecom, TeliaSonera
- + География:**  
83 субъекта РФ
- + Клиенты:** 70 млн абонентов
- + Выручка за 2013 год:**  
297 млрд руб.

- + Решение:** защита онлайн- и мобильных приложений
- + Масштаб:** 12 ключевых систем на двух региональных площадках, до 60 000 пользовательских запросов в секунду
- + Продукты:** PT Application Firewall, PT MaxPatrol

### ЗАДАЧА

Компания «МегаФон», один ведущих российских операторов связи, делает свои сервисы максимально удобными и доступными для клиентов. В современном мире, где все активно пользуются Интернетом, системы самообслуживания реализуются в виде веб- и мобильных приложений.

Одним из ключевых требований бизнеса является высокая скорость внедрения новых сервисов, что приводит к применению гибких методик разработки — DevOps, Agile и др. При таком подходе остается слишком мало времени на анализ кода и другие элементы безопасной разработки (Secure SDL), а обнаруженные уязвимости устраняются слишком долго. Бизнес не готов ждать.

Кроме того, в процессе роста компания приобретает новые активы: часто требуется защита чужого или наследуемого кода, который невозможно кардинально исправить.

Другая проблема — защита клиентов от онлайн-фрода: взламывая домашние компьютеры или смартфоны, злоумышленники используют полученные пароли для манипуляций с личными счетами и кражи денег.

В рамках развития СУИБ компании «МегаФон» было принято решение внедрить систему защиты онлайн-приложений. Ключевые требования к системе:

- +** высокая производительность и поддержка отказоустойчивых конфигураций;
- +** быстрая адаптация к изменениям в защищаемых приложениях;
- +** работа в территориально-распределенных системах и интеграция с существующими средствами защиты;
- +** устранение уязвимостей разработки без внесения изменений в исходный код;
- +** выявление нетипового поведения пользователей и приложений.

### РЕШЕНИЕ

На основании заданных критериев для реализации системы защиты была сформирована программа испытаний, в рамках которой протестированы решения ведущих производителей — как с точки зрения функциональных возможностей, так и по эффективности анализа данных. По результатам тестов выбран межсетевой экран PT Application Firewall, в котором механизмы самообучения позволяют избежать значительного количества ложных срабатываний,

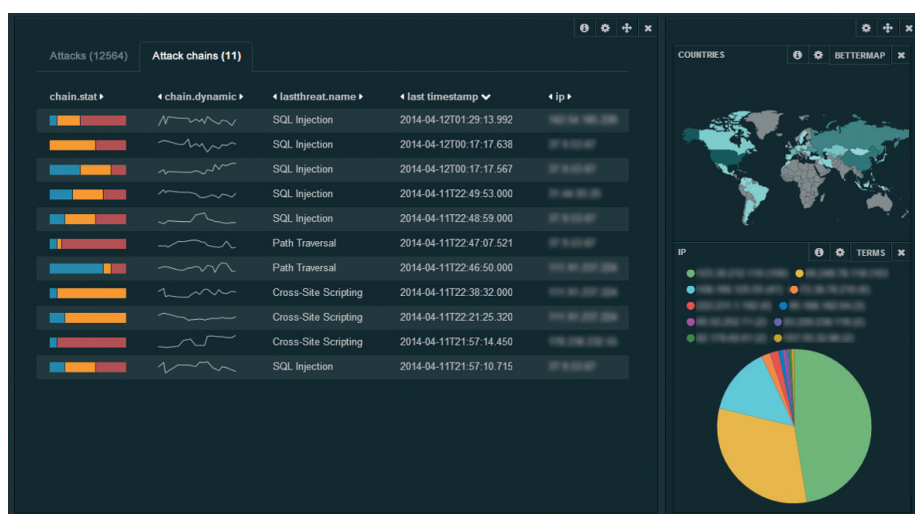
**КЛЮЧЕВЫЕ  
ВОЗМОЖНОСТИ**

- + 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

а функция автоматической верификации атак и уязвимостей в комбинации со встроенными механизмами корреляции дает возможность ИБ-специалистам сконцентрироваться на наиболее существенных событиях безопасности, снижая затраты на ручную обработку результатов.

Задача интеграции решена с использованием коннекторов к системам класса SIEM, используемых в компании «МегаФон», а также функции виртуального патчинга для интеграции с системами статического и динамического анализа защищенности приложений, включая систему контроля уязвимостей MaxPatrol. Этот же механизм применяется для проактивного блокирования атак на уязвимости, выявленные в ходе анализа защищенности, а также для защиты устаревших приложений, исправление которых невозможно.

Кроме того, механизм выявления веб-фрода позволяет своевременно отслеживать нехарактерную активность клиентов и несанкционированную деятельность сетевых «роботов», а гибкая модель поставок в виде виртуального или аппаратного решения позволила оптимизировать процесс внедрения для различных приложений телеком-оператора.

**РЕЗУЛЬТАТ**

Реализованная система защиты на основе PT Application Firewall обеспечивает своевременное обнаружение атак на онлайн- и мобильные приложения, а также проактивное выявление уязвимостей и устранение угроз до исправления ПО, включая защиту устаревших приложений. Комплекс успешно интегрирован в существующую СУИБ ОАО «МегаФон».

«Не секрет, что как любая большая компания, мы являемся большой мишенью: постоянно происходят попытки взломать наши веб-сервисы, получить доступ к личным кабинетам абонентов, к их персональным данным и счетам. Сейчас, благодаря PT AF, мы можем отслеживать и блокировать эти атаки в реальном времени, поддерживая высокий уровень безопасности для миллионов наших абонентов», — говорит Сергей Химаныч, ведущий специалист отдела информационной безопасности ОАО «МегаФон».

**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 «Газпром» 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.