СОВМЕСТНОЕ РЕШЕНИЕ CHECK POINT SOFTWARE TECHNOLOGIES И POSITIVE TECHNOLOGIES ДЛЯ ЗАЩИТЫ ПЕРИМЕТРА СЕТИ И ПРЕДОТВРАЩЕНИЯ АТАК ПРИКЛАДНОГО УРОВНЯ НА ВЕБ-РЕСУРСЫ ОРГАНИЗАЦИЙ

Сегодня веб-приложения — системы онлайн-банкинга, электронные торговые площадки, порталы государственных услуг, всевозможные бизнес-приложения — переживают взрывной рост. Многие компании активно внедряют интернет-технологии и разворачивают сложные системы защиты. Однако это совершенно не мешает злоумышленникам красть конфиденциальные данные и получать доступ к внутренним информационным системам компаний, эксплуатируя уязвимости конкретных веб-приложений. Статистика настораживает: по данным опросов Ponemon Institute, через веб-сервисы в 2015 году были скомпрометированы 78% компаний, а исследования Positive Technologies свидетельствуют, что 71% веб-приложений содержат критически опасные уязвимости.

Согласно данным Positive Research, вектор атак для проникновения злоумышленников во внутреннюю сеть компании преимущественно основывается на эксплуатировании уязвимостей в коде веб-приложений; это не позволяет традиционным системам ИБ эффективно противодействовать атакам. Для дополнительной защиты веб-сервисов рекомендуется использовать специализированный класс решений — межсетевые экраны прикладного уровня. Вместе с тем, несмотря на всю мощь механизмов сигнатурного анализа и эвристических алгоритмов поиска уязвимостей, применяемых в экранах уровня приложения, — подобные системы требуют сложной настройки, и не всегда результаты оправдывают ожидания. Поэтому в основе решений Positive Technologies лежат технологии машинного обучения, которые адаптируются к бизнес-логике конкретных веб-приложений и в комплексе с другими средствами защиты позволяют оперативно блокировать запросы злоумышленников, DDoS-атаки на приложения, выявлять уязвимости нулевого дня.

Эксперты Positive Technologies и Check Point Software Technologies считают крайне высокими риски информационной безопасности, связанные с веб-технологиями и доступом из интернета, поэтому компании решили объединить усилия и готовы предложить заказчикам интегрированное решение для защиты периметра организации и ее веб-ресурсов.

СТРАТЕГИЯ ЗАЩИТЫ

Применение комплексного подхода к обеспечению информационной безопасности позволяет существенно повысить степень защищенности организации и ее данных в динамичном информационном пространстве. Как правило, в операционном плане такой подход включает в себя несколько этапов — анализ активности, выявление аномального поведения, уведомление о нарушениях, блокировку источников — и работает на всех уровнях современной организации:

- на уровне пользователей,
- данных,
- приложений,
- инфраструктуры.

Доступные на сегодняшний день программные и аппаратные решения позволяют выстроить эффективную модель киберзащиты любой организации.

CHECK POINT SOFTWARE TECHNOLOGIES

Многоядерные процессоры, высокая плотность портов и дублированные компоненты — технологии, реализованные в устройствах Check Point Software Technologies для обеспечения максимального уровня защищенности. Интеграция с архитектурой программных блейдов позволяет просто наращивать функциональность системы защиты без необходимости замены самого устройства.

PT APPLICATION FIREWALL

PT Application Firewall (PT AF) — адаптивный защитный экран уровня приложений, предназначенный для выявления и блокирования атак на веб-порталы, ERP-приложения и системы интернет-банкинга. Совместная работа сканера уязвимостей и корреляционного механизма позволяет выявлять все этапы развития наиболее опасных атак и направлять на них максимум защитных ресурсов, которые в противном случае тратились бы на неактуальные попытки взлома.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Технологии PT AF:

- адаптация к объекту защиты за счет алгоритмов машинного обучения;
- интеллектуальный анализ для обнаружения аномальных запросов и поведения;
- приоритизация угроз и выстраивание цепочек связанных инцидентов, отслеживание развития атак;
- автоматическая генерация виртуальных патчей;
- защита от обхода межсетевого экрана;
- поведенческий анализ активности пользователей и приложений.

CHECK POINT SOFTWARE TECHNOLOGIES И PT APPLICATION FIREWALL

Безопасность веб-приложений — актуальный тренд, подкрепленный реальными случаями утечки данных, интернет-мошенничеством, атаками на отказ в обслуживании и другими действиями со стороны злоумышленников, способными повлиять на репутацию компании.

Сочетание опыта Check Point Software Technologies в сфере сетевой безопасности с технологиями обнаружения и устранения уязвимостей Positive Technologies в одном решении обеспечивает максимальную защиту наиболее важных веб-сервисов и приложений.

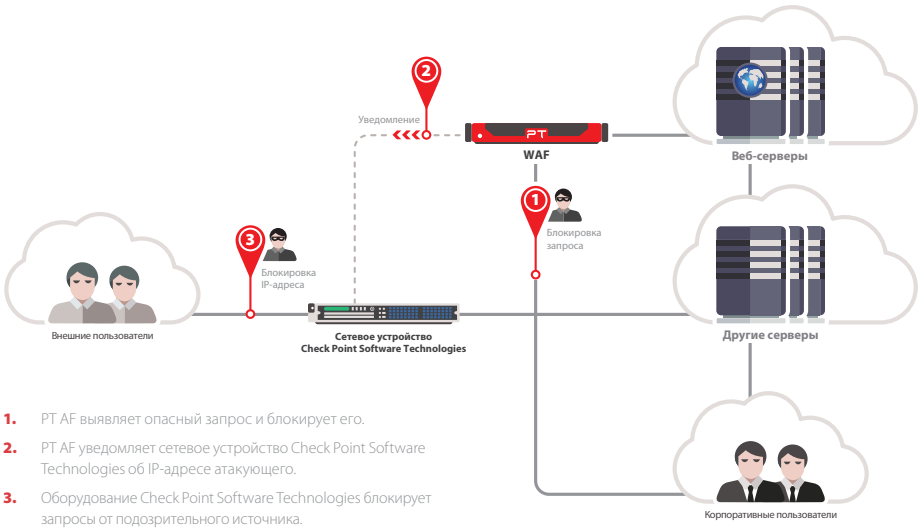
Преимущества предлагаемого решения:

- защита периметра и веб-приложений в режиме реального времени,
- автоматическое уведомление об инцидентах всех работающих в сети устройств Check Point Software Technologies,
- защита от атак нулевого дня благодаря механизмам машинного обучения,
- защита от DDoS-атак на приложения и выявление аномалий,
- широкие возможности для масштабирования,
- расширенные функции расследования инцидентов ИБ.

ТЕХНИКА ЗАЩИТЫ

I. Защита веб-ресурсов в режиме обратного прокси-сервера

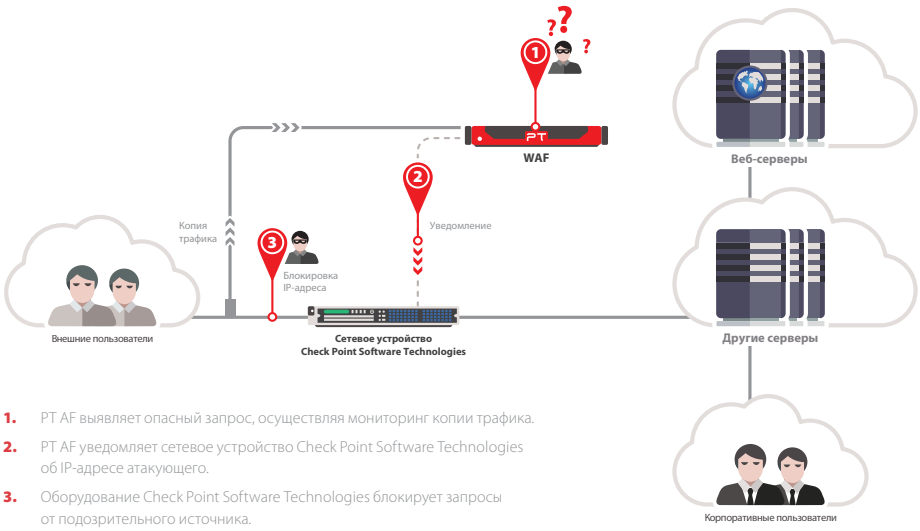
Благодаря интеграции PT AF с решениями Check Point Software Technologies при выявлении атак PT AF может уведомлять сетевые устройства Check Point Software Technologies об источнике атаки, сообщая IP-адрес злоумышленника и таймаут блокировки. Это позволяет оборудованию Check Point Software Technologies блокировать дальнейшие запросы с подозрительного адреса на сетевом уровне, тем самым снижая нагрузку на канал и PT AF.



1. PT AF выявляет опасный запрос и блокирует его.
2. PT AF уведомляет сетевое устройство Check Point Software Technologies об IP-адресе атакующего.
3. Оборудование Check Point Software Technologies блокирует запросы от подозрительного источника.

II. Защита веб-ресурсов в режиме мониторинга

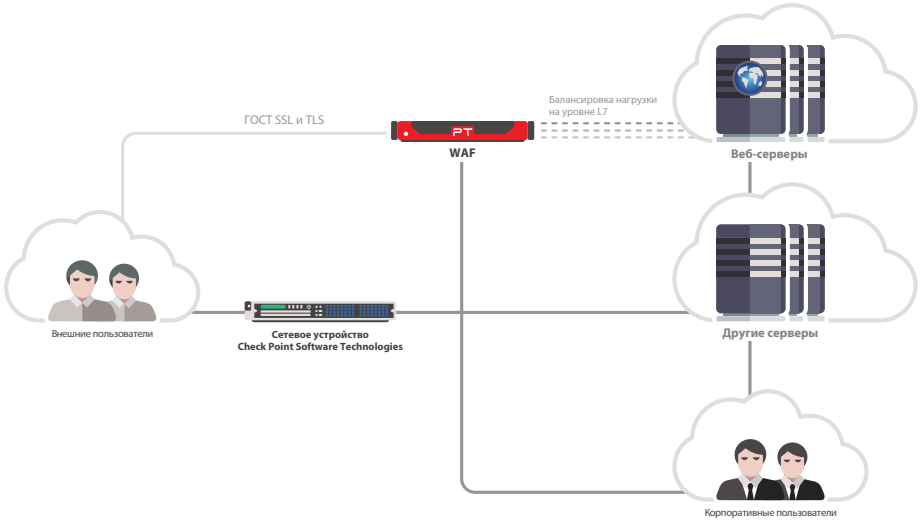
Передача данных об источнике атаки и таймаута блокировки подозрительного адреса на устройства Check Point Software Technologies может осуществляться и в ситуации, когда PT AF работает с копией трафика в режиме мониторинга (сниффера).



1. PT AF выявляет опасный запрос, осуществляя мониторинг копии трафика.
2. PT AF уведомляет сетевое устройство Check Point Software Technologies об IP-адресе атакующего.
3. Оборудование Check Point Software Technologies блокирует запросы от подозрительного источника.

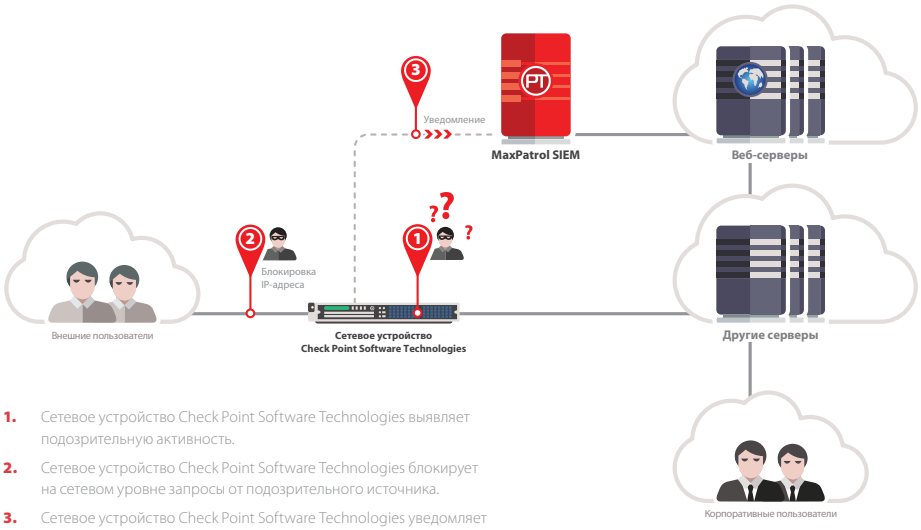
III. Защита передаваемых данных с использованием российских криптоалгоритмов

Данная интеграция может использоваться и для блокирования атак на веб-приложения, запросы к которым передаются по каналам, защищенным с использованием российских криптографических алгоритмов. Понимая контекст работы веб-приложения, PT AF способен осуществлять не только защиту, но и распределение запросов между группой серверов, обеспечивая высокий уровень доступности сервисов.



IV. Интеграция с MaxPatrol SIEM

Интеграция продуктов Check Point Software Technologies в MaxPatrol SIEM позволяет на основе правил корреляции с событиями других систем информационной безопасности, включая PT AF, выявлять и приоритизировать инциденты информационной безопасности в корпоративной сети.



1. Сетевое устройство Check Point Software Technologies выявляет подозрительную активность.
2. Сетевое устройство Check Point Software Technologies блокирует на сетевом уровне запросы от подозрительного источника.
3. Сетевое устройство Check Point Software Technologies уведомляет MaxPatrol SIEM о произошедшем событии.

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Check Point Software Technologies является ведущим в мире производителем ИБ-решений, специализирующимся исключительно на интернет-безопасности. Компания поставляет высокоэффективные решения в области информационной безопасности и обеспечивает клиентам защиту от кибератак с непревзойденным уровнем обнаружения вредоносного ПО и других видов угроз. Check Point Software Technologies предлагает полноценную архитектуру защиты корпоративных сетей и мобильных устройств, а также возможность всестороннего и наглядного управления безопасностью. По данным независимых аналитических агентств, таких как Gartner и IDC, компания Check Point Software Technologies неизменно входит в число лидеров рынка UTM-решений.

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». 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.ru
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays