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 — web application firewalls. 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 ИБ позволяют оперативно блокировать запросы злоумышленников, DoS-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 интернет, 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

Технологии Check Point Software Technologies:

- интеграция со сторонними серверами регистрации или серверами корреляции событий — благодаря Log Export API (OPSEC LEA), Event Logging API (ELA);
- механизм блокирования подозрительной активности Suspicious Activity Monitor (SAM).

PT APPLICATION FIREWALL

PT Application Firewall — 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 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 — против программ-роботов.

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:

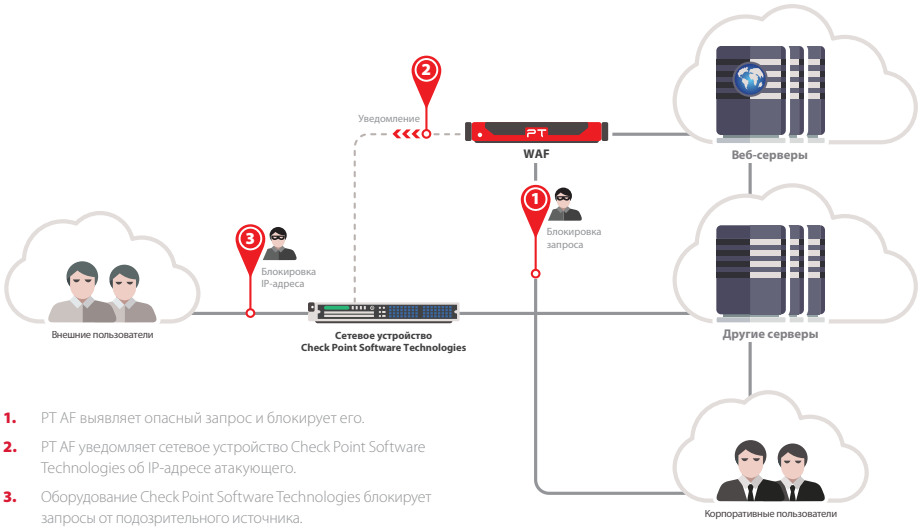
- защита периметра и веб-приложений в режиме реального времени,
- автоматическое уведомление об инцидентах всех работающих в сети устройств Check Point Software Technologies,
- защита от атак нулевого дня благодаря механизмам машинного обучения,
- защита от DoS-атак на приложения и выявление аномалий,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

ТЕХНИКА ЗАЩИТЫ

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

Оборудование Check Point Software Technologies защищает периметр сети и проксирует запросы к веб-приложениям на PT AF. PT AF используется для защиты веб-приложений и работает в режиме обратного прокси-сервера.

При выявлении атаки PT AF уведомляет сетевое устройство Check Point Software Technologies об источнике атаки, сообщая IP-адрес злоумышленника и таймаут блокировки. Оборудование Check Point Software Technologies на сетевом уровне блокирует дальнейшие запросы с подозрительного адреса.



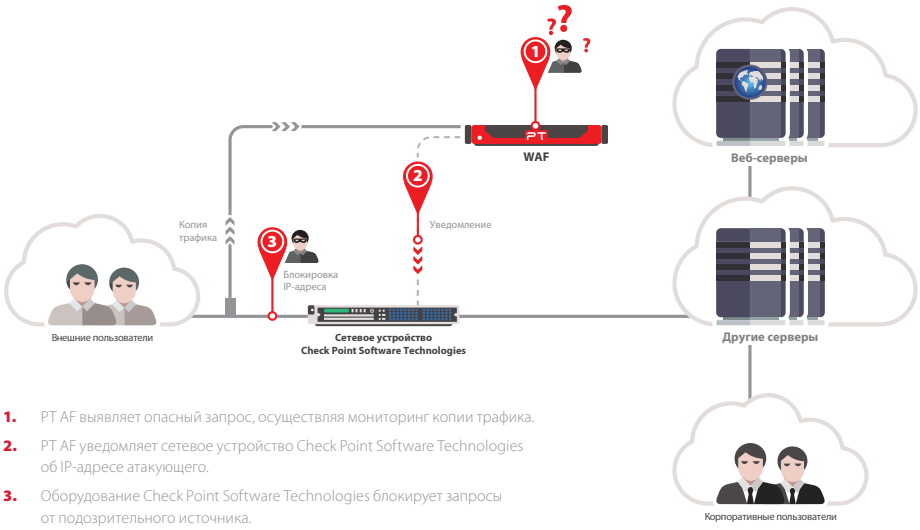
1. PT AF выявляет опасный запрос и блокирует его.
2. PT AF уведомляет сетевое устройство Check Point Software Technologies об IP-адресе атакующего.
3. Оборудование Check Point Software Technologies блокирует запросы от подозрительного источника.

2. Защита веб-ресурсов в режиме мониторинга

Внешние каналы терминируются на коммутаторе, сетевом брокере пакетов или используется ответвитель сетевого трафика. Цель — передача копии трафика веб-приложений на PT AF.

Оборудование Check Point Software Technologies защищает периметр сети. PT AF используется для защиты веб-приложений и работает в режиме сниффера для анализа копии трафика.

При выявлении атаки PT AF уведомляет сетевое устройство Check Point Software Technologies об источнике атаки, сообщая IP-адрес злоумышленника и таймаут блокировки. Оборудование Check Point Software Technologies на сетевом уровне блокирует дальнейшие запросы с подозрительного адреса.

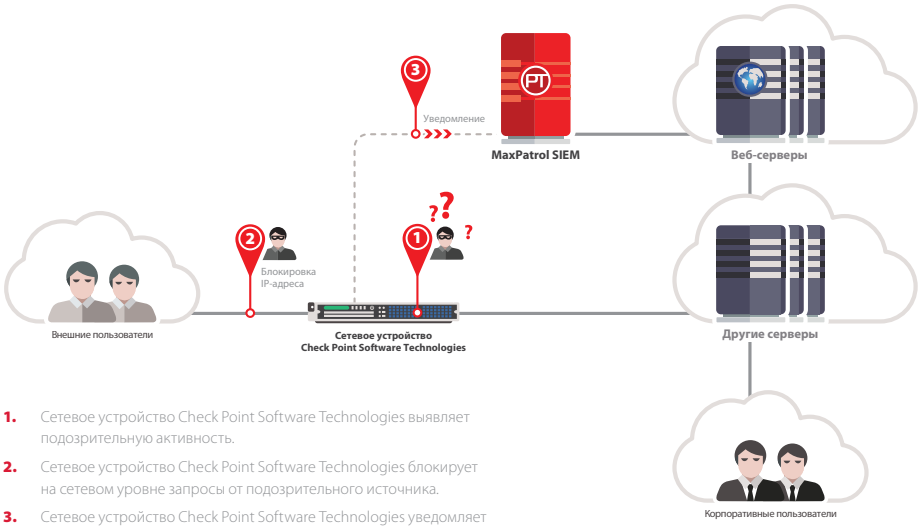


1. PT AF выявляет опасный запрос, осуществляя мониторинг копии трафика.
2. PT AF уведомляет сетевое устройство Check Point Software Technologies об IP-адресе атакующего.
3. Оборудование Check Point Software Technologies блокирует запросы от подозрительного источника.

3. Интеграция с MaxPatrol SIEM

Оборудование компании Check Point Software Technologies защищает периметр сети. При выявлении атак и иных подозрительных событий сетевое устройство Check Point Software Technologies уведомляет о них MaxPatrol SIEM.

MaxPatrol SIEM поддерживает большое число событий, которые генерирует оборудование Check Point Software Technologies, и имеет соответствующие правила корреляции.



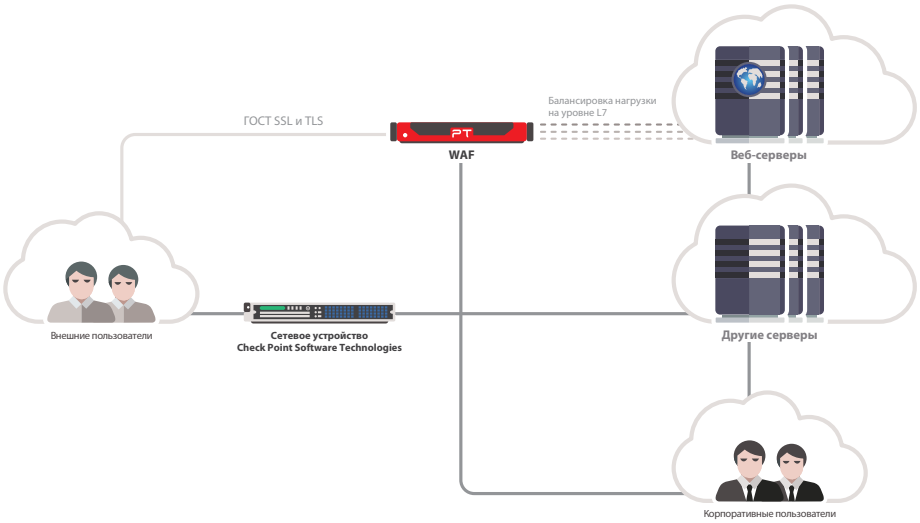
1. Сетевое устройство Check Point Software Technologies выявляет подозрительную активность.
2. Сетевое устройство Check Point Software Technologies блокирует на сетевом уровне запросы от подозрительного источника.
3. Сетевое устройство Check Point Software Technologies уведомляет MaxPatrol SIEM о произошедшем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

4. Защита трафика ГОСТ SSL

Оборудование компании Check Point Software Technologies защищает периметр сети и проксирует запросы к веб-приложениям. Веб-приложения защищены с помощью протоколов TLS/SSL с использованием алгоритмов ГОСТ (ГОСТ SSL).

PT AF используется для защиты веб-приложений и работает в режиме обратного прокси-сервера. Поддерживает работу с алгоритмами ГОСТ, способен расшифровать трафик и осуществить защиту веб-приложений в соответствии с политикой безопасности.

Понимая контекст работы веб-приложения, PT AF способен осуществить не только защиту, но и распределение запросов между группой серверов, обеспечивая высокий уровень доступности сервисов.



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 — 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