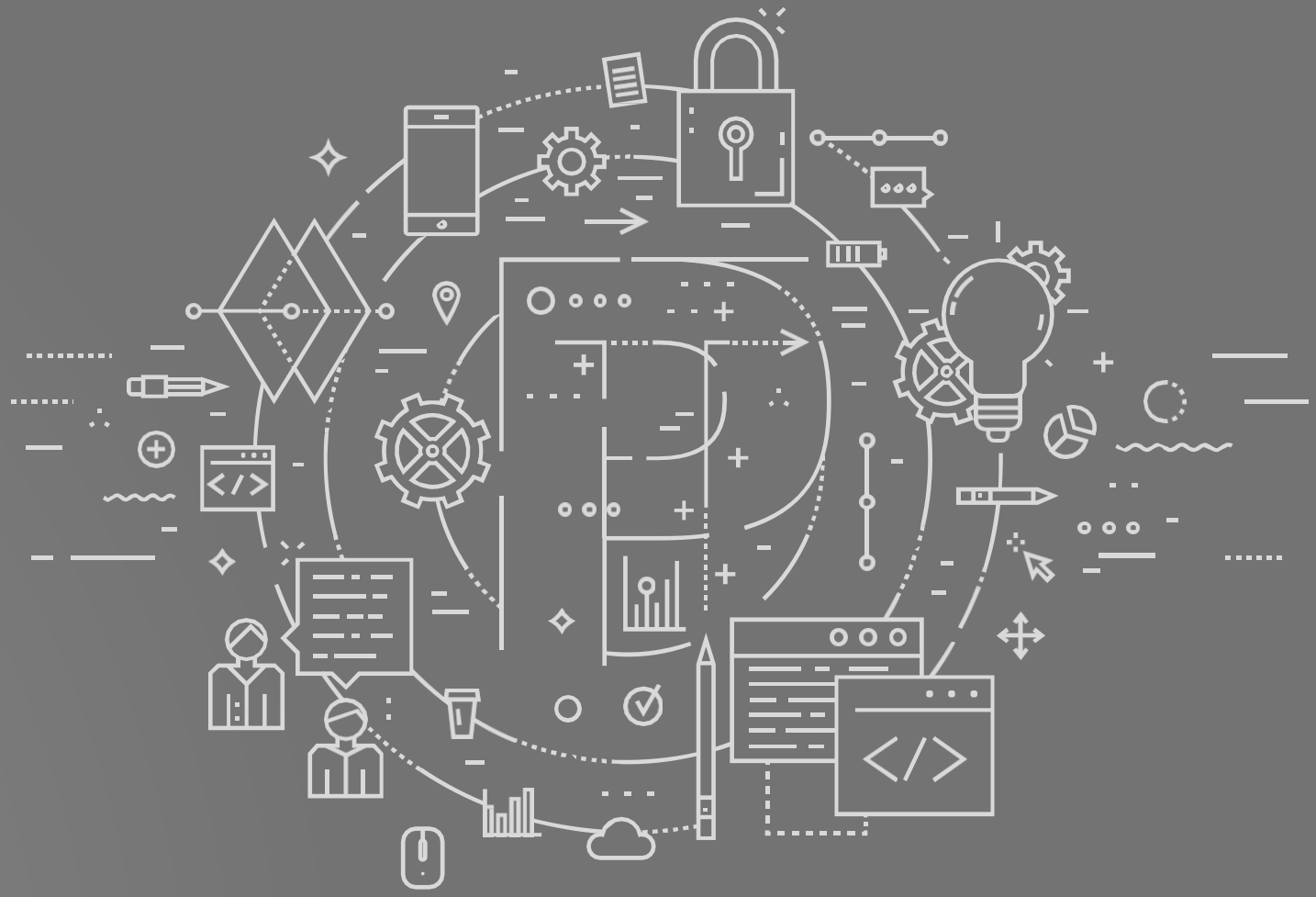
Защита от ботов с PT Application Firewall

Докладчик: Бозоров Сухроб

Содержание

- Коротко о PT
- Про боты
- Защита от ботов с PT Application Firewall
- Пара слов о ботах на мобильных приложениях
- Как обеспечить всестороннюю защиту: представляем новое интеграционное решение



О компании

15+ лет опыта

250+ экспертов по защите ERP, SCADA, банков и телекомов, веб- и мобильных приложений

Члены OWASP, WASC, CIS, CEH, ISACA

Каждый год они проводят **200+** аудитов безопасности: банки, веб- и мобильные приложения, телекомы, блокчейн и смарт-контракты, ICS/SCADA, ERP.

1000+ клиентов по всему миру

700+ сотрудников

Крупнейший в Европе исследовательский центр

Каждый год они находят **1500+** уязвимостей в корпоративных системах;

180+ уязвимостей в банковских системах;

200+ уязвимостей нулевого дня.

150+ партнеров – ведущих интеграторов ИТ и ИБ, производителей ПО и оборудования

Спикеры международных конференций Defcon, CCC, Black Hat.

В залах славы Google, Apple, Adobe

Боты: качество и количество

Более 50% посетителей вебсайтов — боты.

Соотношение между «хорошими» и «плохими» ботами — примерно 50 на 50

Monitoring Uptime Robot, Pingdom, mon.itor.us	**Impersonators** Fake user agents, Headless browsers
Crawlers AddThis, archive.org, Dataminr	**Scrapers** Dlvr.it, eCommerceBot, Buzzbot
Search Engines Google, Yandex, Bing, Yahoo	**Spammers** Godzilla, S.T.A.L.K.E.R., w0000t, EmailSpider
Feed Fetchers Feedly, Inoreader, NewsBlur	**Hackers Tools** Havij, sqlmap, brutus, DirBuster

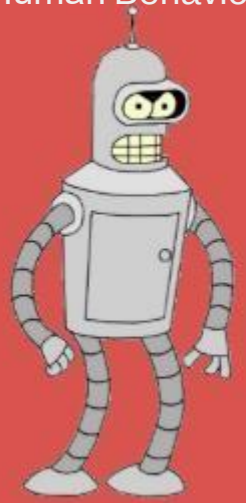
Чем опасны «плохие» боты

- Эксплуатация уязвимостей
- Атаки и подготовительные сканы
- Ложные заказы
- Накрутки бонусов, голосований
- Пустые «полки» онлайн-магазинов
- «Заспамленные» комментарии и форумы
- Перебор паролей и блокировка учетных записей

- Сбор информации о пользователях
- Копирование сайтов, контента
- Отказ в обслуживании
- Недоступность API-сервисов
- Финансовые потери
- Увеличение оплаты CPU/RAM/Bandwidth
- Снижение удовлетворенности легитимных посетителей

Эволюция ботов

Отсутствующие возможности

− Human Behavior − Browser Behavior − Java Script −Headers and Cookies	− Human Behavior − Browser Behavior − Java Script	− Human Behavior − Browser Behavior	− Human Behavior
			

Этапы эволюции

Сложность исполнения ↑ ●●● Возможности обнаружения ↓

Роль IoT

Table 1: IoT Units Installed Base by Category (Millions of Units)

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Source: Gartner (January 2017)

Sweet, vulnerable IoT devices compromised 6 min after going online

Gone in 360 seconds, says researcher

By John Leyden 17 Oct 2016 at 13:26 25 SHARE ▼

The unpatched Windows XP problem that spawned the Blaster and Sasser worm a decade ago is being replicated on a different platform by hackers exploiting IoT devices to launch denial of service attacks.

https://www.theregister.co.uk/2016/10/17/iot_device_exploitation/

Роль IoT

Table 1: IoT Units Installed Base by Category (Millions of Units)

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Source: Gartner (January 2017)

Sweet, vulnerable IoT devices compromised 6 min after going online

Gone

By John

The unp
Sasser
hackers

https://

It Still Takes 2 Minutes to Have Vulnerable IoT Devices Compromised Online

By Catalin Cimpanu

August 30, 2017 06:15 AM 0

Almost a year after the emergence of the Mirai botnet, smart devices are still facing a barrage of credential attacks, and a device left connected to the Internet with default credentials will be hijacked in about two minutes.

https://www.bleepingcomputer.com/news/security/it-still-takes-2-minutes-to-have-vulnerable-iot-devices-compromised-online/

Как бороться с «плохими» ботами

Firewall

NGFW

IPS/IDS

UTM

Sandbox

Endpoint AV

Anti DDoS

WAF

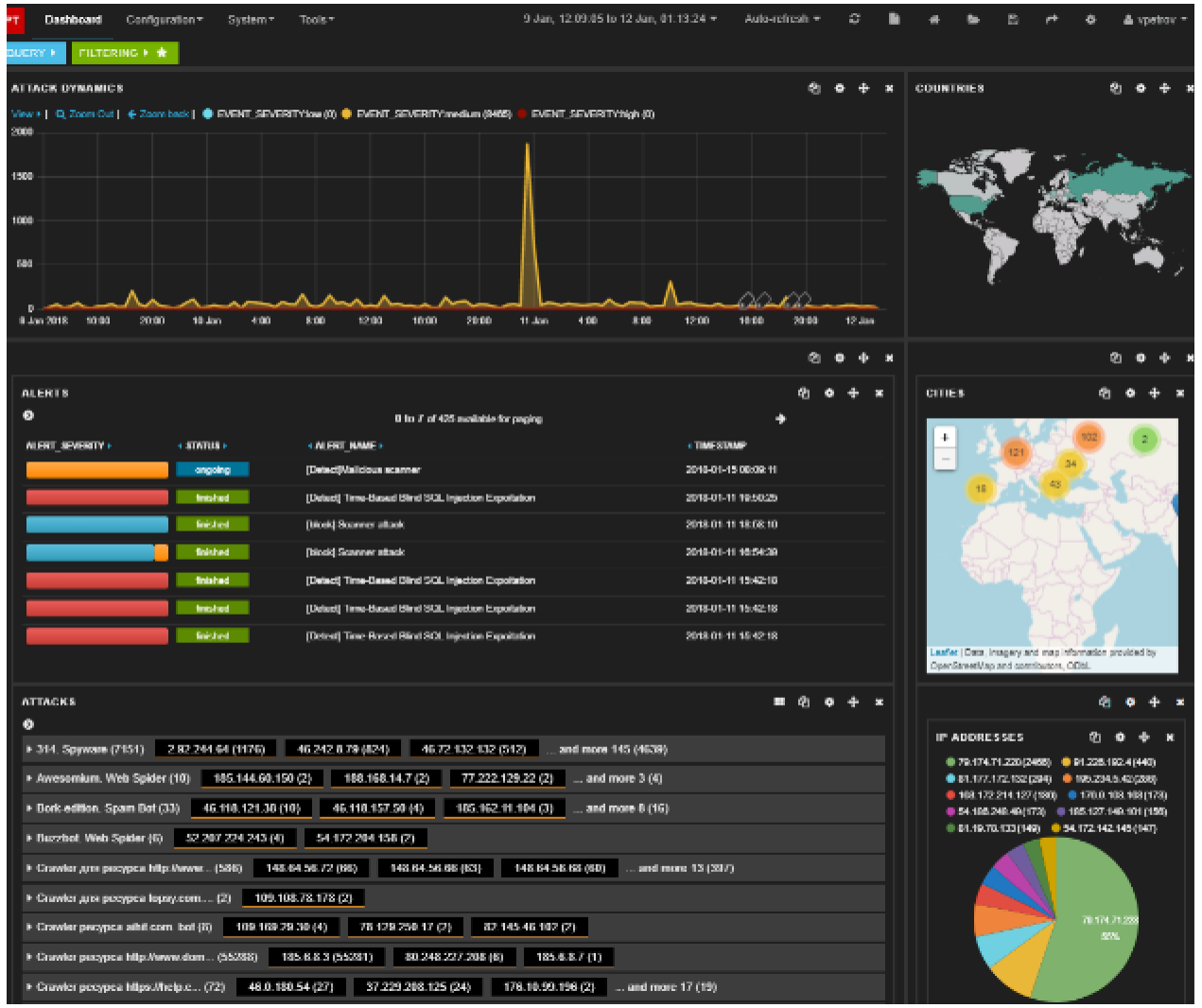
Представляем решение

PT Application Firewall (PTAF)

решение, которое PT создавали на базе инновационных технологий и постоянно улучшает, чтобы проактивно защищать приложения, пользователей и инфраструктуру от эволюционирующих угроз, включая ботов

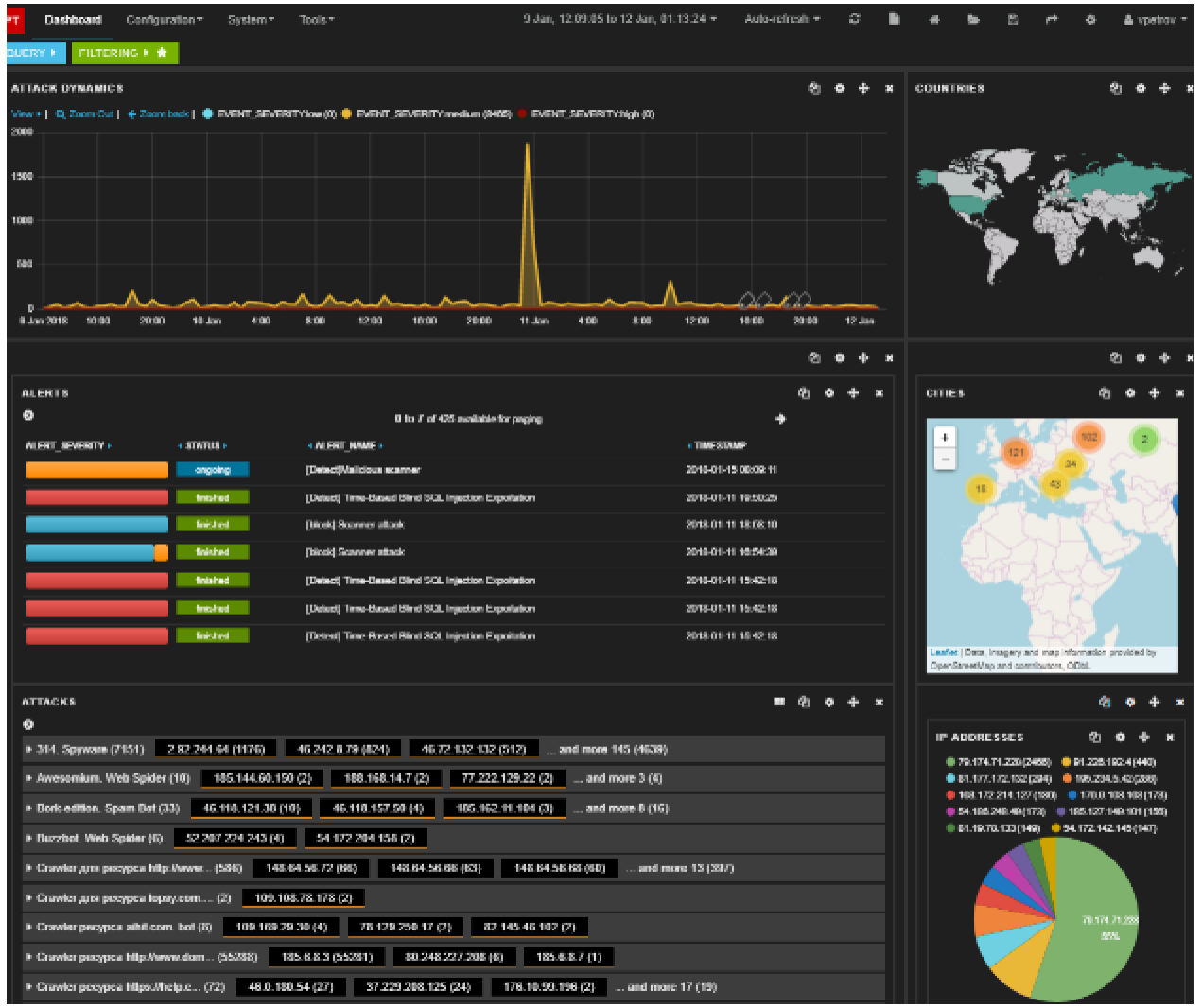
PT AF: ключевые возможности

- Обнаружение даже самых «умных» ботов благодаря непрерывному поведенческому анализу
- Защита от DDoS-атак
- Блокировка спам-ботов
- Защита серверного API
- Выявление прочих атак на защищаемое приложение (в том числе атак на уязвимости нулевого дня)



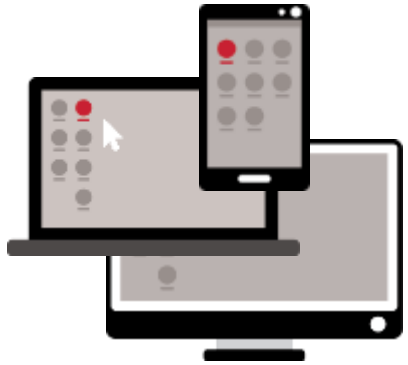
PT AF: ключевые возможности

- Контроль «хороших»/«плохих» ботов (без влияния на работу «хороших» ботов)
- Классификация ботов, включая возможность составления своих правил классификации и блокировки
- Управление бот-трафиком
- Улучшение работы веб-приложений за счет высвобождения ресурсов



PT AF против ботов: как это работает

Механизмы защиты



Посетитель

Приложение

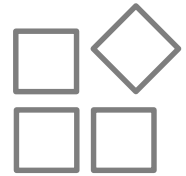
- Активность мышки
- Рендеринг страниц
- Выявление хакерских утилит
- Обнаружение средств автоматизации
- Инспектирование DOM

Клиентские проверки

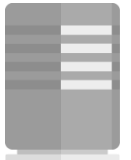
- Блокировка брутфорса
- Сигнатурный анализ
- Выявление bot-like поведения
- Корреляция событий
- Белые списки «хороших» ботов

Серверные проверки

Cloud



Containers

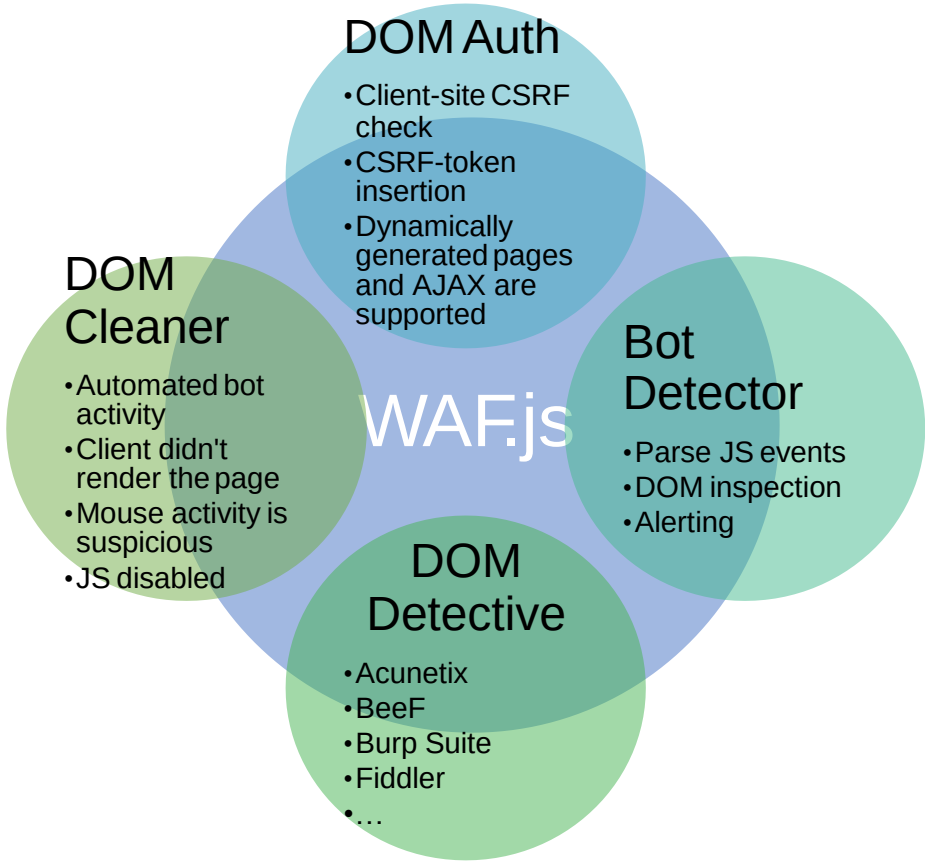


Virtual

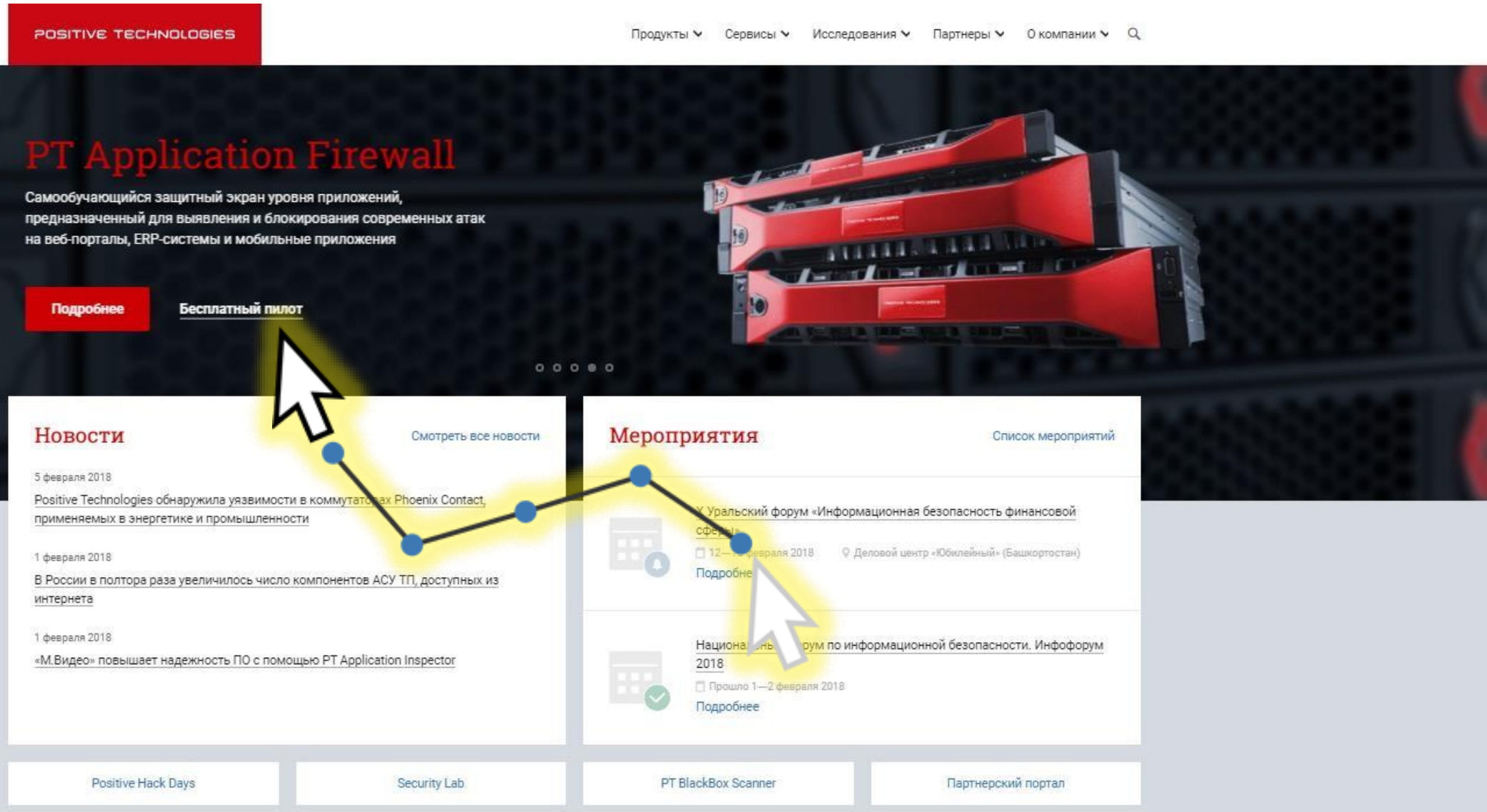
Bare Metal

Проверки на клиентской стороне

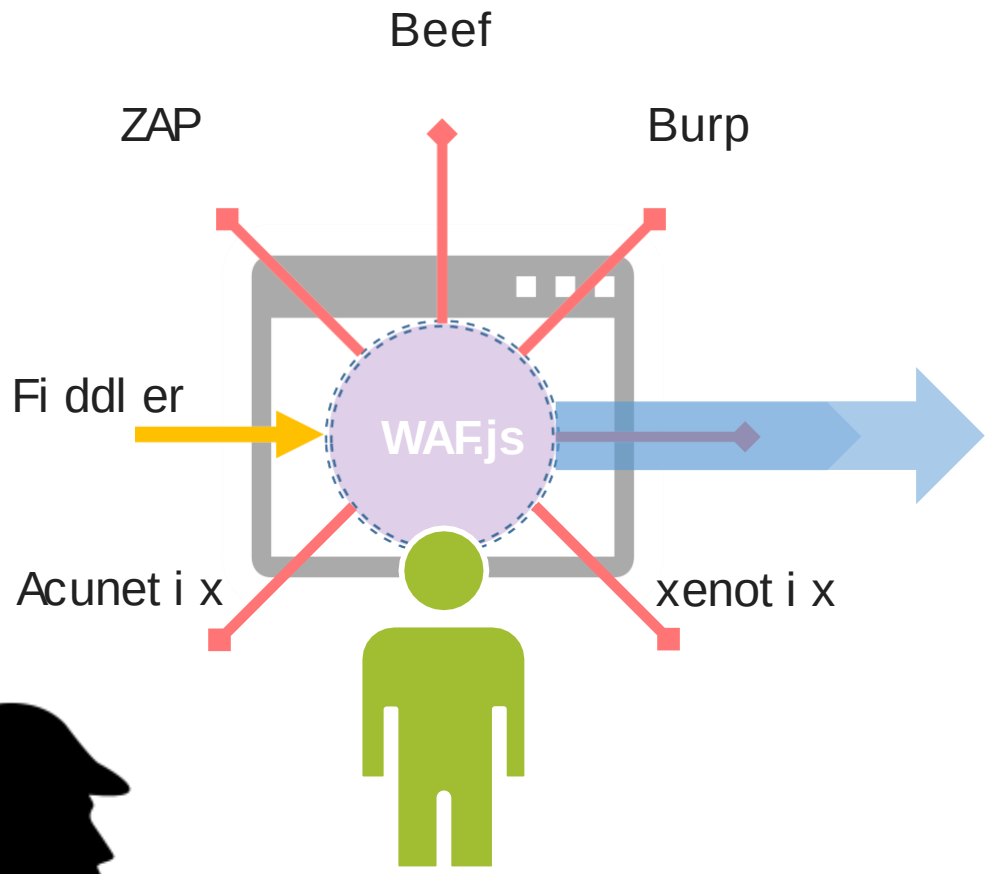
+ Анализ окружения браузера
+ Обнаружение средств автоматизации
+ Выявление хакерских утилит
+ Обнаружение DOM-based XSS атак



Отслеживание активности указателя



Выявление хакерских утилит



/ event s_col l ect or

Request blocked

Hacking tool has been detected:
Tool: ***Fiddler***
Open Port: ***8888***

Правильные фиды

Benign Bot Activity. Search Engine.

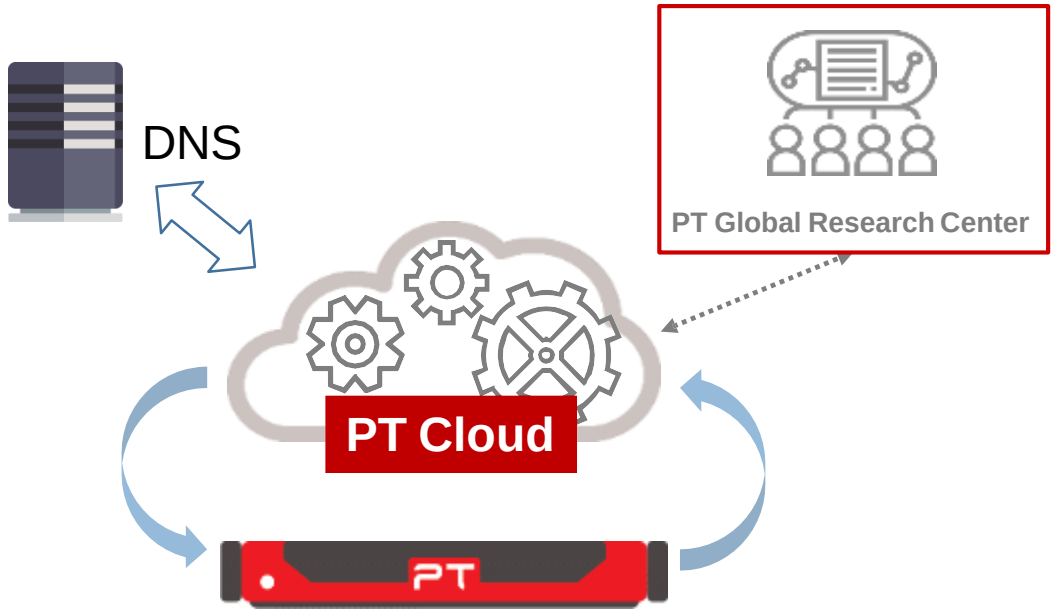
User-Agent: Googlebot/2.1 (+http://www.google.com/bot.html)

IP: 66.249.64.94

Malicious Bot Activity. Spam Bot.

User-Agent: Googlebot/2.1 (+http://www.google.com/bot.html)

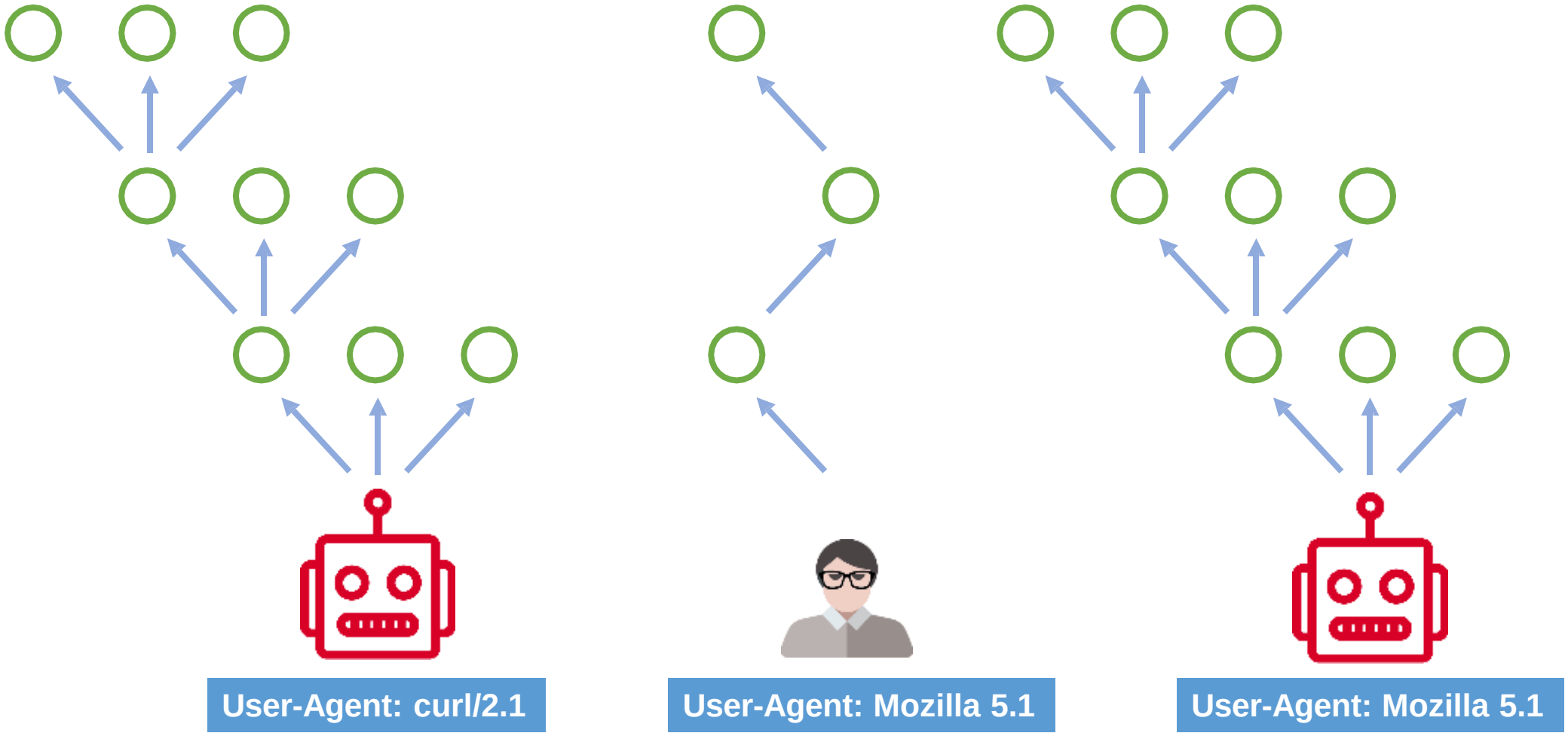
IP: 31.44.93.2



Преобразование ip-адресов в DNS имена может замедлить работу пользователя с приложением

Регулярные обновления от PT Global Research Center загружаются автоматически, что дает возможность блокировать «плохие» источники еще до того, как они попадут в ваше приложение

Выявление bot-like поведения

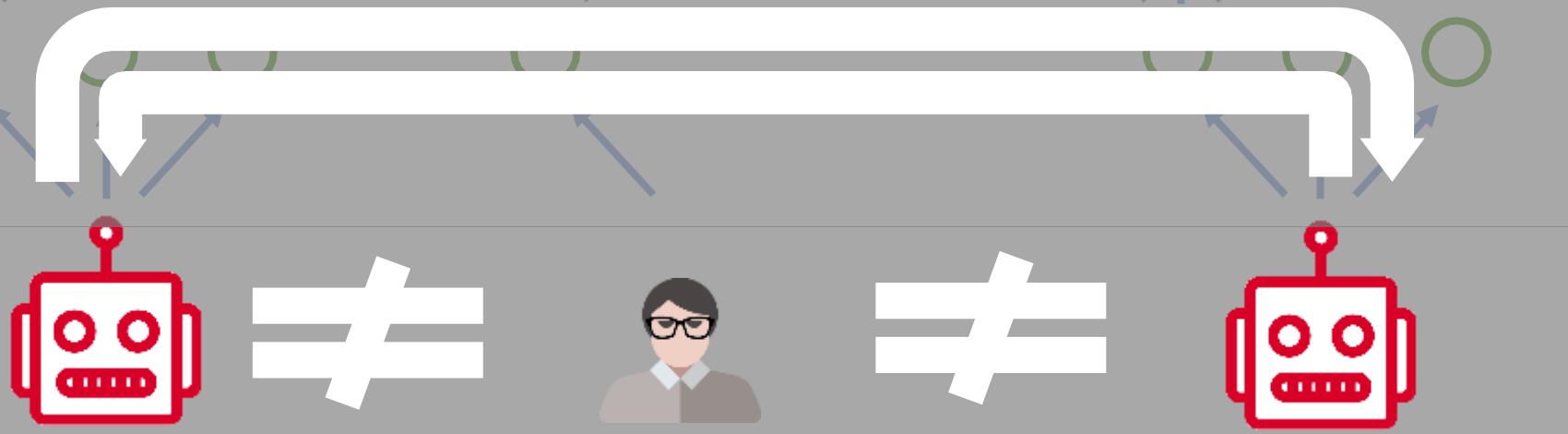


Выявление bot-like поведения

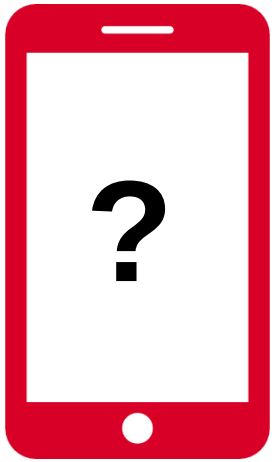
PT Application Firewall снабжен базой известных ботов

Встроенный алгоритм изучает поведение известных ботов

Каждая новая сессия сравнивается с изученной ранее

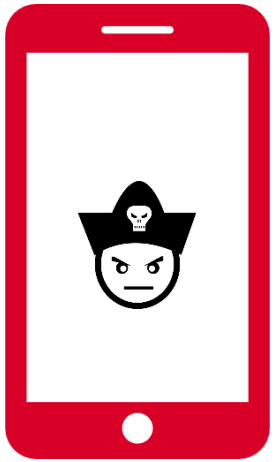


За пределами веб-приложений



Как насчет атак с мобильных приложений?

Немного статистики



Незаконные источники генерируют 10-15% трафика в среднем мобильном API.*

Немного о нашем новом партнере

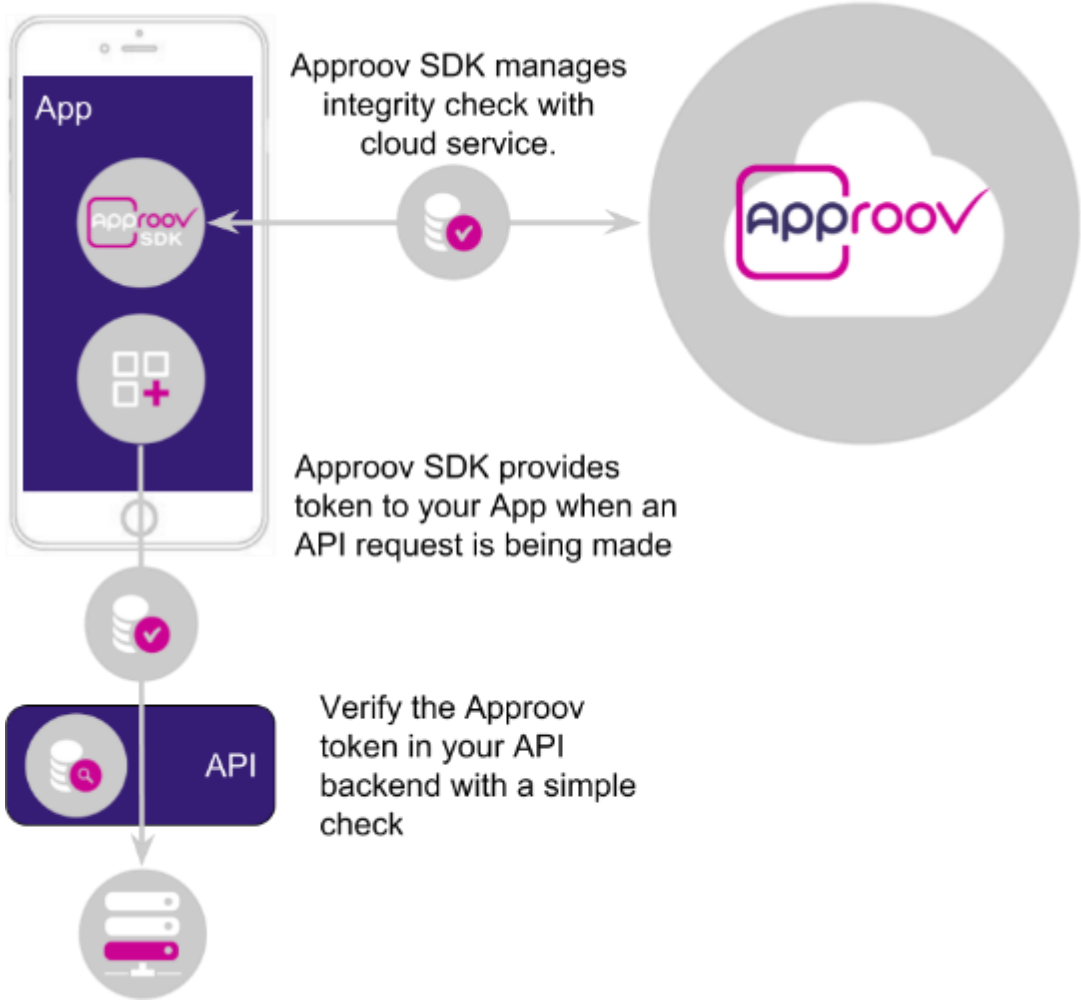
Approov — современное решение, которое защищает мобильные приложения от воздействия ботов без вреда реальным пользователям и приложениям.

Approov: как это работает

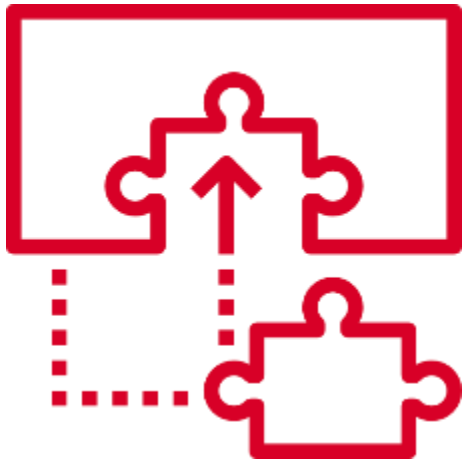
Approov проводит аутентификацию программного обеспечения, вызывающего ваш API, и блокирует:

- Трафик, созданный без присутствия мобильного приложения (ботов)
- Трафик от поддельных («фейковых») приложений

пропуская запросы только от реальных пользователей и легальных приложений.



Почему PT решили рассказать вам про Approov



Представляет совместный проект для комплексной защиты инфраструктуры
— PT Application Firewall + Approov

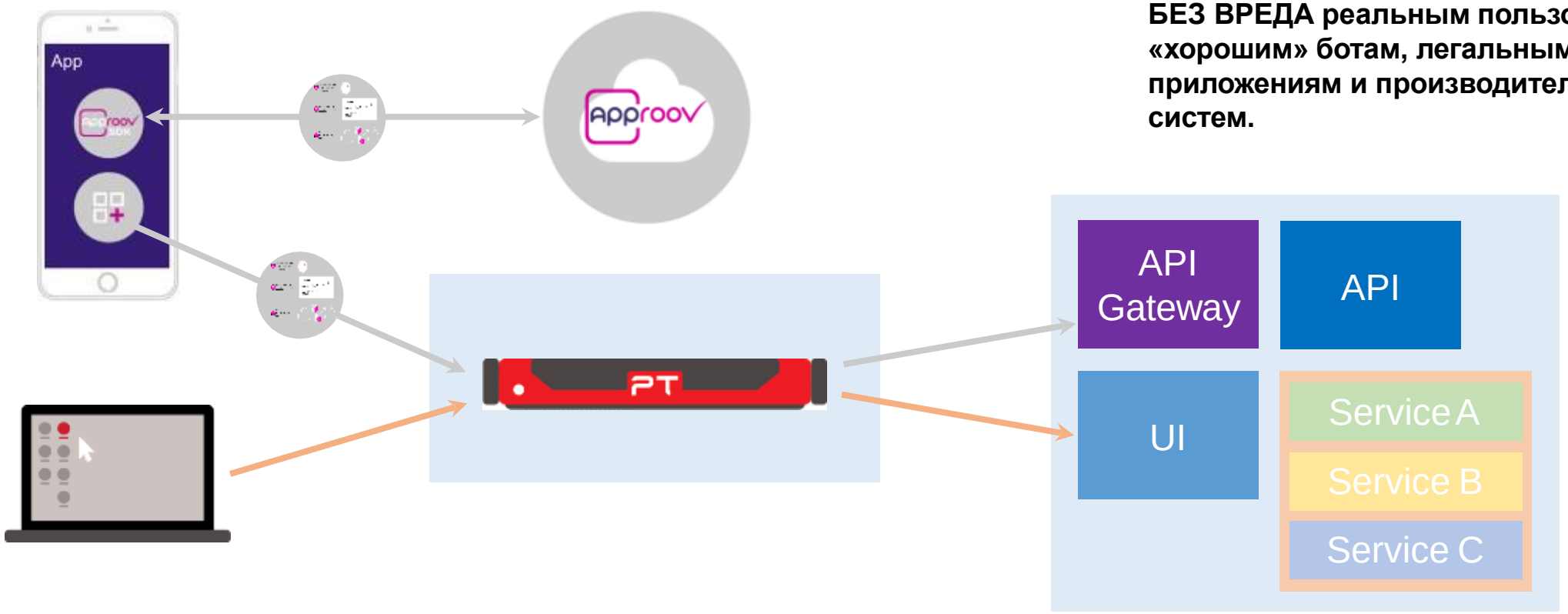
PT AF + Approov: как это работает

Задачи	
Approov	• Проверка подлинности приложения • Проверка источника запроса
PT AF	• Проверка достоверности токена и дальнейшая обработка запроса • Защита приложения от прочих веб-угроз

Выгоды:

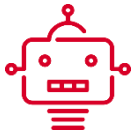
- Комплексная защита ваших веб- и мобильных приложений от ботов
- Защита от современных веб-атак

БЕЗ ВРЕДА реальным пользователям, «хорошим» ботам, легальным приложениям и производительности систем.



Ключевые моменты

>50% трафика в веб-приложениях создается ботами



50% всех ботов — «плохие»

«Плохие» боты могут привести к негативным последствиям, включая перебои в работе приложения или полный отказ в обслуживании

PT Application Firewall эффективно борется с «плохими» ботами без вреда пользователям и «хорошим» ботам, требует минимум трудозатрат благодаря высокому уровню автоматизации

Интеграционное решение PT AF и Approov позволяет обеспечить комплексную защиту веб- и мобильных приложений

Спасибо!