

Защита приложений и API

Igor Kontsevoy

June 2021

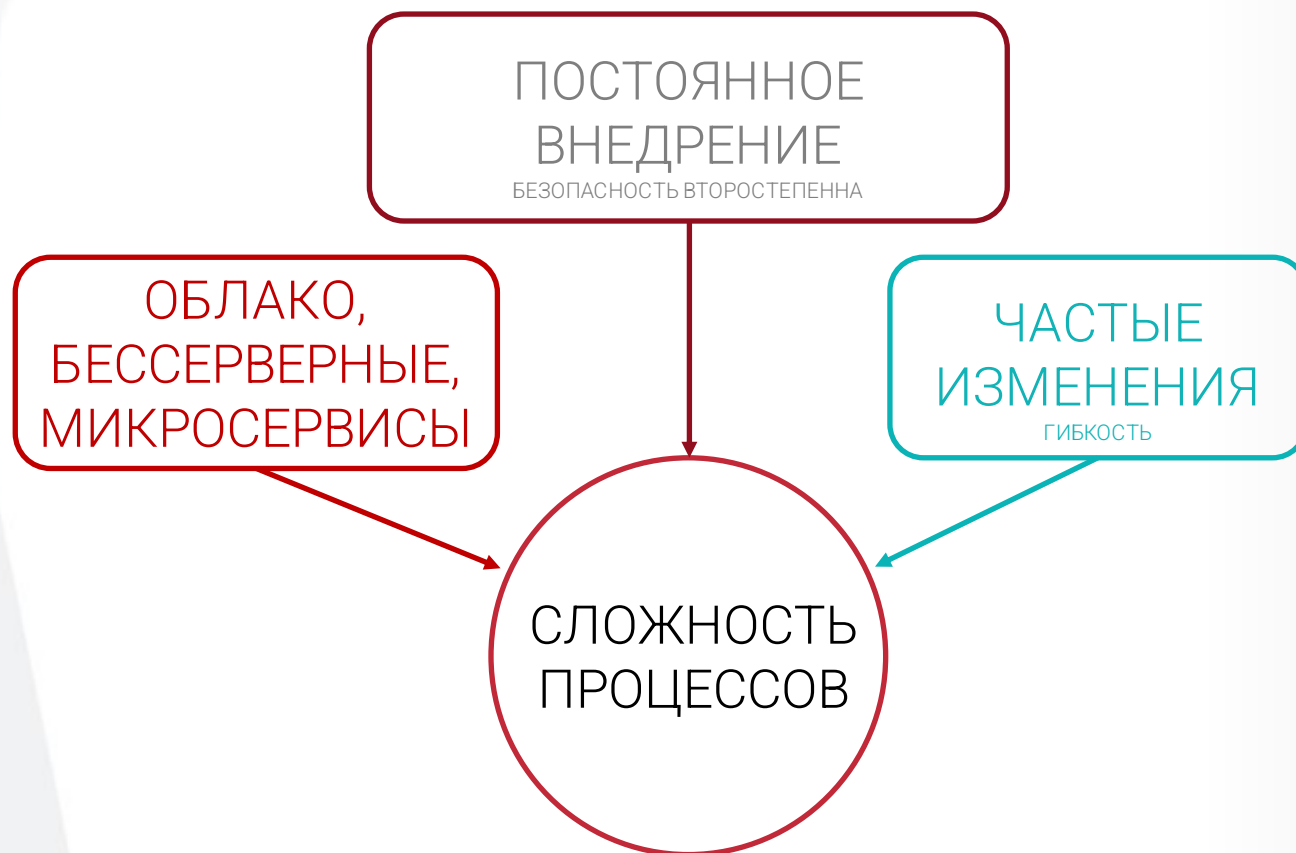


AGENDA

- Актуальные проблемы
- Обеспечение эффективной и комплексной защиты приложений и API
- Решение по управлению Ботами

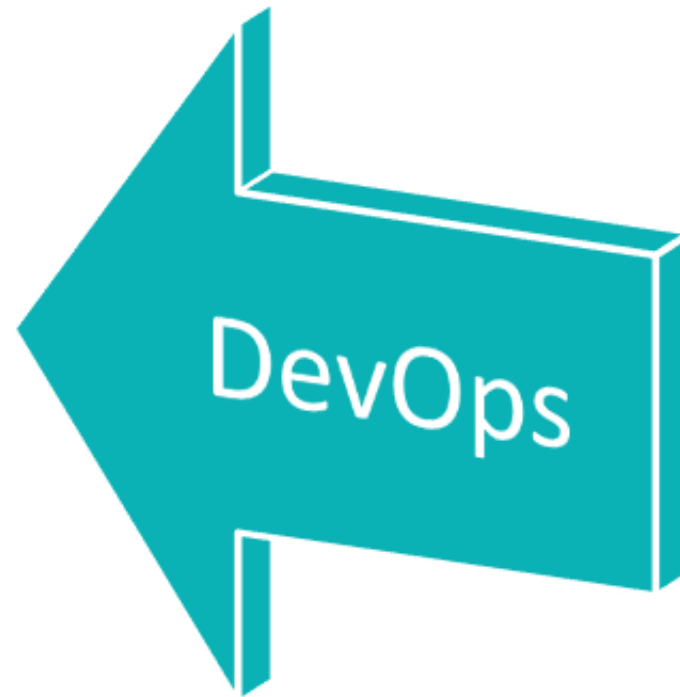
Современные приложения сложно защитить ?!

! Одновременные изменения окружения, парадигм и процессов, создают «СЛЕПЫЕ ЗОНЫ» в безопасности



- ❖ 70% претерпевают изменения еженедельно
- ❖ 56% не интегрируют безопасность в свой процесс CI/CD
- ❖ 53% связывают нарушение с конфликтом ответственности с облачным провайдером

Одна команда ... Конфликт интересов



Цель

Требования к
решению

- Минимизация рисков
- Защитить целостность данных
- Защитить доступность
- Эффективная безопасность
- Адаптивные политики и машинное обучение
- Видимость и аналитика

Цель

Требования к
решению

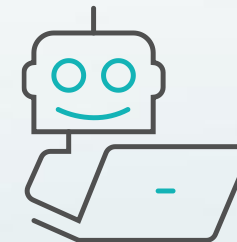
- Скорость
- Непрерывное внедрение
- Безопасность постфактум
- Автоматизация
- Эластичность и масштаб
- Визуализация

БОТЫ ЗАХВАТЫВАЮТ ИНТЕРНЕТ



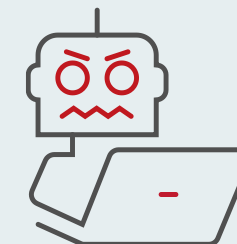
ЧТО ДЕЛАЮТ ХОРОШИЕ БОТЫ?

- Поисковые системы
- Ценообразование на услуги
- Веб-сканеры
- Сборщики



ЧТО ДЕЛАЮТ ПЛОХИЕ БОТЫ?

- Веб-скрапинг
- Захват аккаунта
- DDoS-атаки
- Замораживание активов



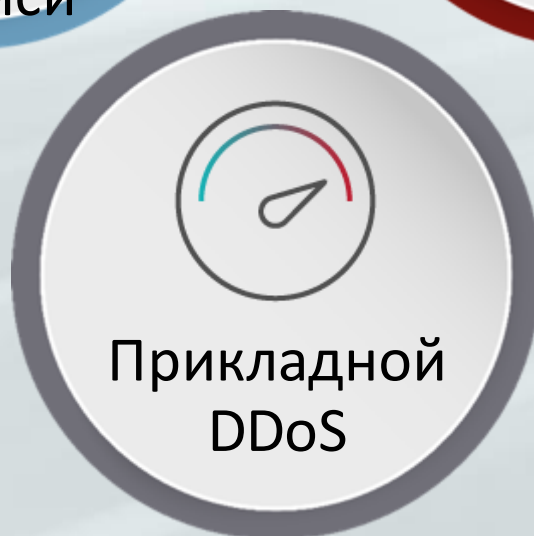
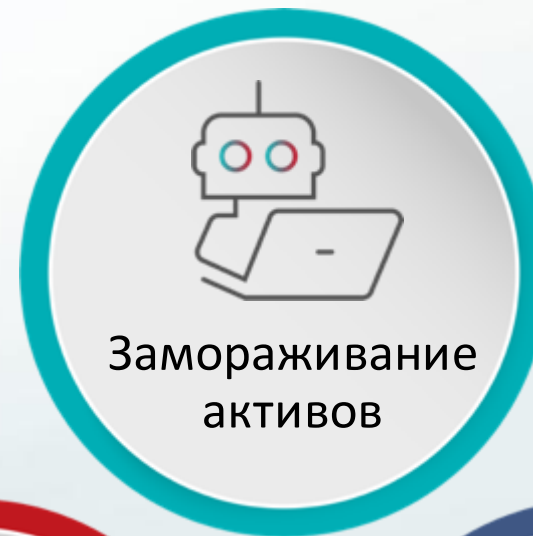
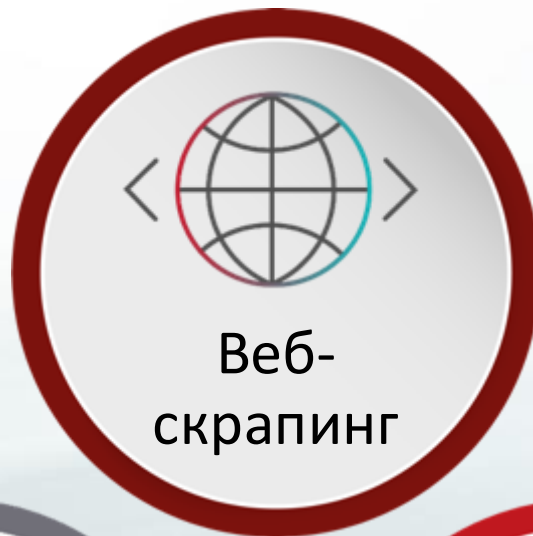
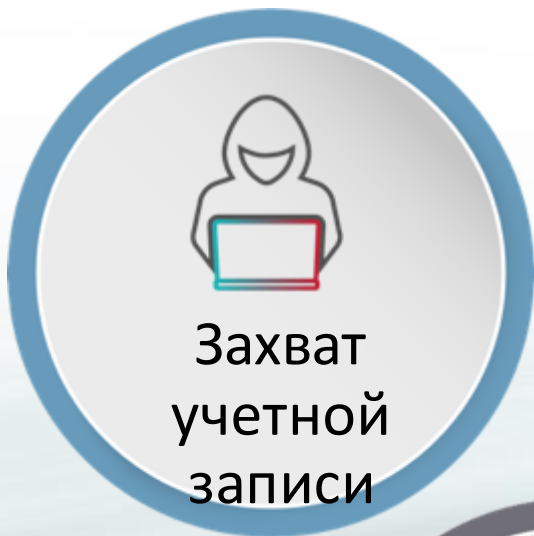
26%

Интернет-трафика генерируется **плохими** ботами

4 IN 5

организации не могут различить "хороших" и "плохих" ботов.

Распространенные атаки ботов

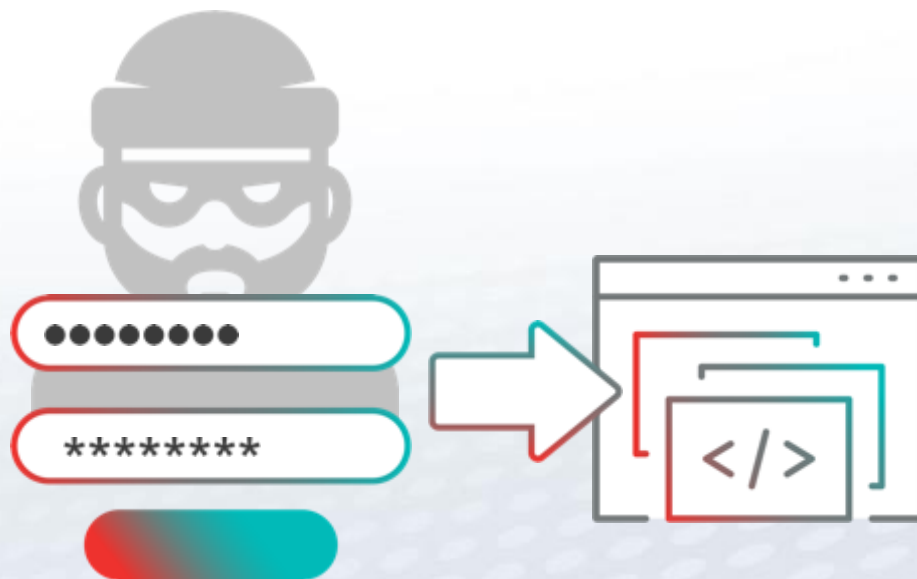


РИСК: Захват учетной записи



Использование информации учетной записи другого человека для получения продуктов и услуг

Как это работает?



Различные формы:



Кража данных



Потеря репутации



Финансовые потери

РИСК: Web-Scraping



Сбор данных, используемый для извлечения данных с веб-сайтов

Как это
работает?



Потери данных



Потеря дохода

50%

Bad bot traffic (of all traffic) to APIs
(2019)

50%

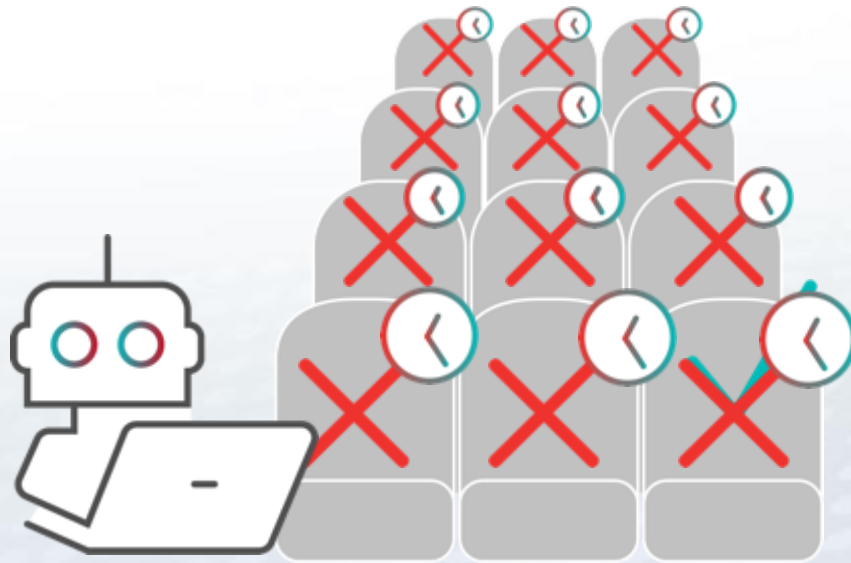
Increase in bad bot
traffic to APIs
(H1-2020 vs. H1-2019)

РИСК: УДЕРЖИВАНИЕ РЕСУРСОВ



Истощение запасов товаров или услуг, даже не завершив покупку или совершив транзакцию.

Как это работает?



45%

Удерживание ресурсов*

32%

Пострадал от удерживания *



Потеря клиентов



Потеря репутации



Потеря дохода

OWASP TOP-21 AUTOMATED THREATS



ACCOUNT TAKEOVER

- > Credential Cracking
- > Credential Stuffing
- > Account Creation
- > Account Aggregation
- > Token Cracking



AVAILABILITY OF INVENTORY

- > Denial of Inventory
- > Scalping
- > Sniping



ABUSE OF FUNCTIONALITY

- > Data Scraping
- > Skewing
- > Spamming
- > CAPTCHA Defeat
- > Ad Fraud
- > Expediting



PAYMENT DATA ABUSE

- > Carding
- > Card Cracking
- > Cashing Out



VULNERABILITY IDENTIFICATION

- > Fingerprinting
- > Footprinting
- > Vulnerability Scanning



RESOURCE DEPLETION

Denial of Service

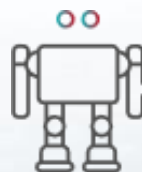


4 Поколения Ботов



Script Bots

Не умеет
хранить файлы
cookie или
выполнять JS



Headless Browsers

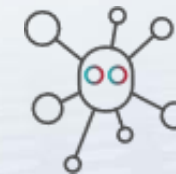
Умеет хранить
файлы cookie и
выполнять JS

Анализ поведения пользователей



Human-Like

Мимикрирует
основные
человеческие
взаимодействия

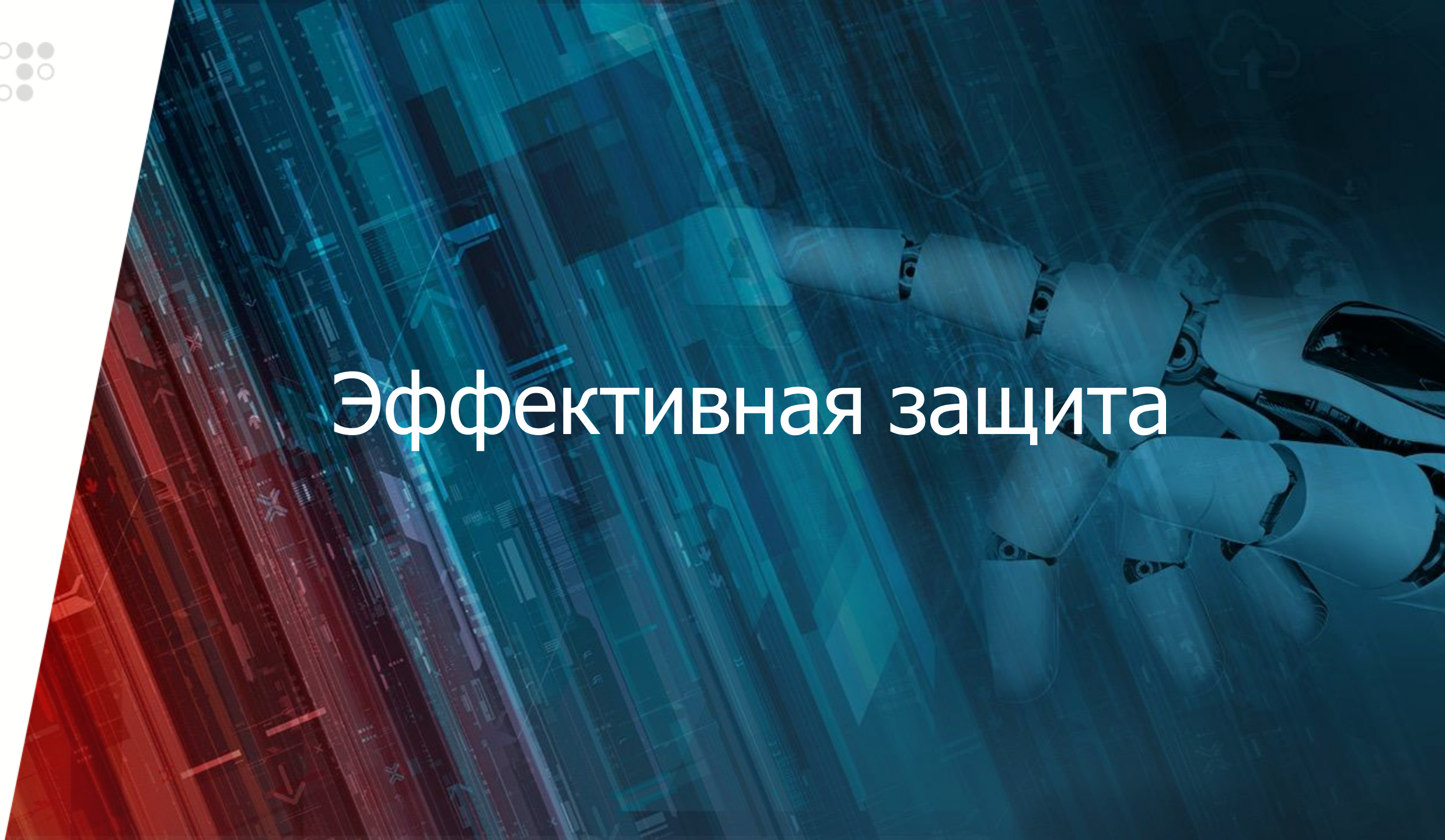


Distributed Mutating Bot

Расширенные
возможности
человекоподобного
взаимодействия



Эффективная защита





Можно ли защититься частично?

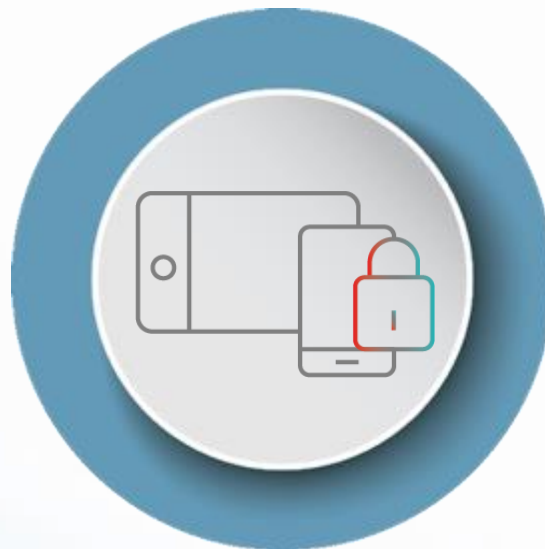




Защита всех каналов



Веб-сайт



Мобильные
приложения



API



'NO SILVER BULLETS' РЕШЕНИЯ RADWARE

Radware Cloud Security Services



2017 Wave
DDoS Leader



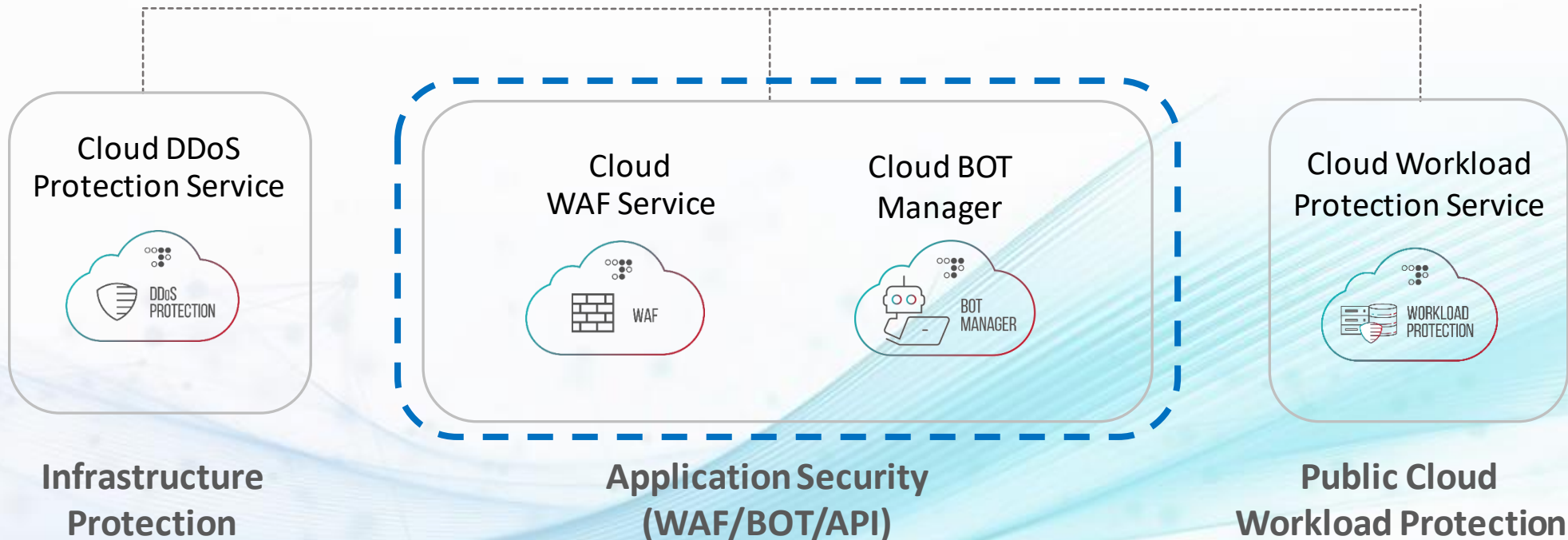
2018 WAF MQ
Visionary Vendor



2018 WAF Vendor
of the Year



Fully-managed **cloud security services**
that **protect from multi-vector threats**





Решения от компании Radware



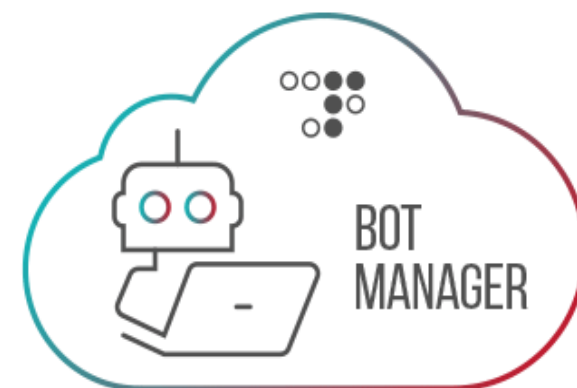
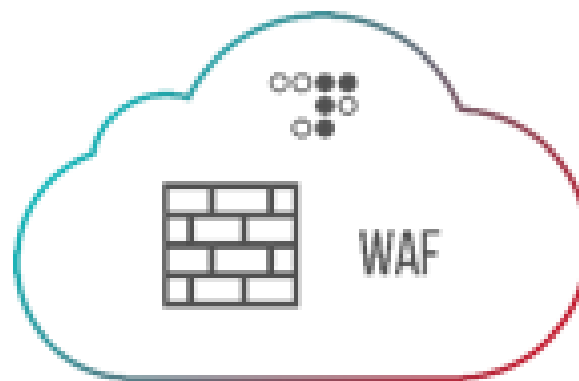
Локальные

&



Облачные

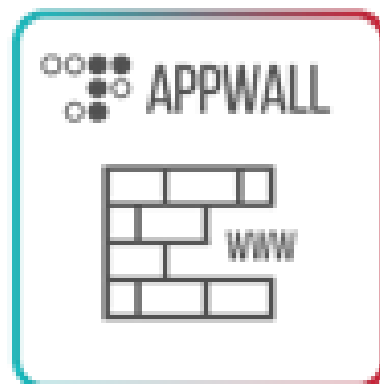
Облачные решения



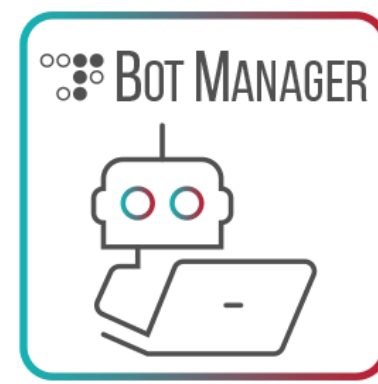
Локальные решения



DDoS



WAF



**Bot
Manager**

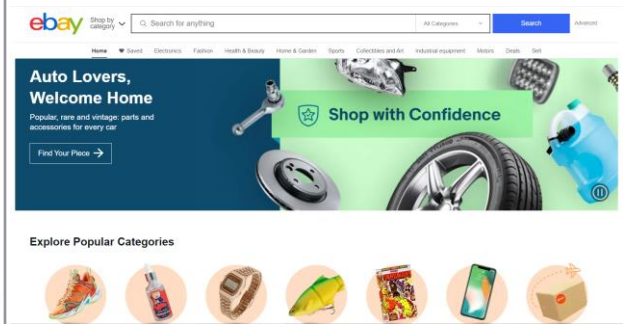


RADWARE BOT MANAGER

Пример: eBay



Одна из крупнейших в мире компаний электронной коммерции



Проблема ...?

- eBay сталкивается с серьезными проблемами со стороны вредоносных ботов: сбор данных, мошенничество с кардингом, атаки АТО и многое другое.



Почему выбрали Radware

- Продемонстрирована превосходная защита ботов
- Полное соответствие требованиям InfoSec и конфиденциальности данных



Что они искали?

- Ключевые требования: надежное предотвращение плохого трафика ботов с низким уровнем ложноположительных и ложноотрицательных результатов, соответствие InfoSec и конфиденциальности данных.



Конкуренция

- Akamai
- Imperva
- И другие

RADWARE BOT MANAGER



Полная защита

Захват учетной записи,
Веб-скрапинг, атаки на
инвентарь, DDoS и
другие
автоматизированные
угрозы



Заблаговременно остановите автоматические атаки

Запатентованная полу-
управляемая модель
глубокого обучения



Обширная база данных отпечатков ботов

Коллективная
информация об угрозах
из тысяч источников по
всему миру



«Ненавязчивый»

Подход на основе API, не
влияет на стек
приложений



ТЕХНОЛОГИИ БОТ-М

*Множественные механизмы идентификации и отслеживания
для максимальной точности*

Глубокий анализ
поведения на
основе намерений



Машинное
обучение для
определения новых
паттернов ботов



Анализ
поведения
пользователей



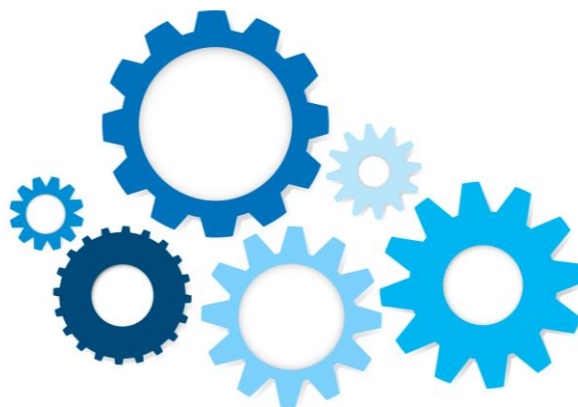
Динамические
тесты Тьюринга



Отслеживание
IP



Глобальная
корреляция
поведения БОТ-
ОВ

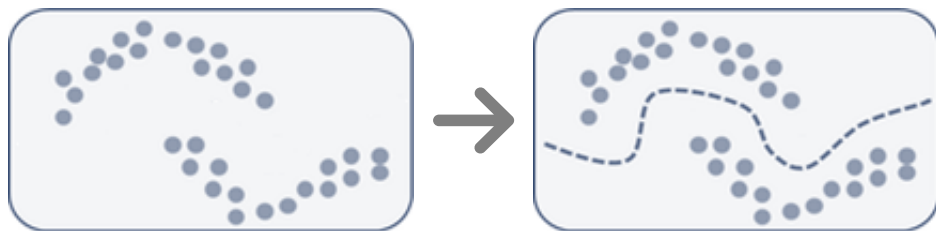


Уникальные
«отпечатки
пальцев» каждого
устройства



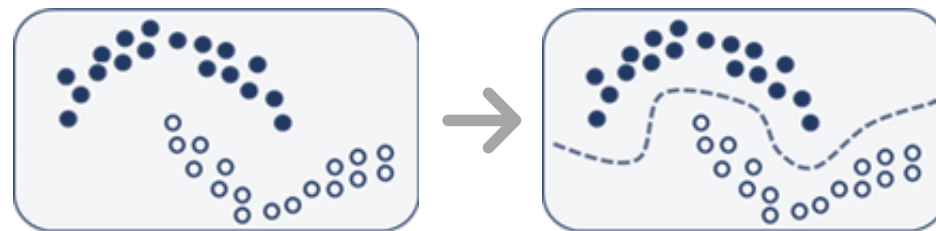
Запатентованное полу-управляемое обучение

БЕСКОНТРОЛЬНОЕ МАШИННОЕ ОБУЧЕНИЕ



- Кластеризация по общности
- Нет разделения на хорошее или плохое
- Риск → Высокий уровень **ложных срабатываний**

УПРАВЛЯЕМОЕ МАШИННОЕ ОБУЧЕНИЕ

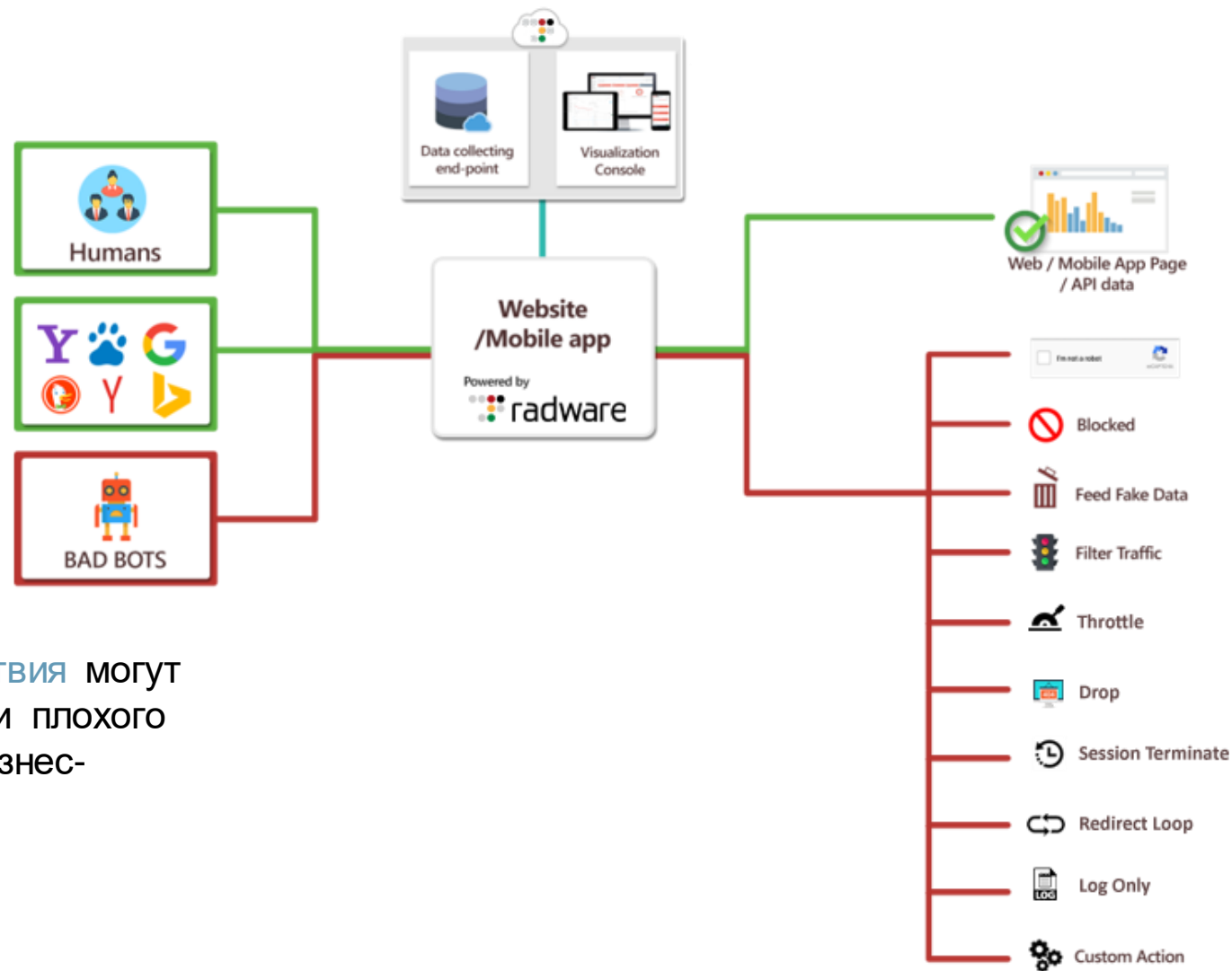


- Управляемая классификация на основе прошлого
- Новые образцы данных создают «шум»
- Риск → Высокий уровень **ложноотрицательных результатов**

Полу-управляемое: *комбинированный подход, обеспечивающий высочайшую точность*

Как Radware BOT-Manager защищает вас?

- REST API/JavaScript Tag фиксирует параметры посетителей и создает уникальный слепок
- Bot-Manager классифицирует каждого посетителя как человека, хорошего или плохого бота
- Гибко настраиваемые противодействия могут быть предприняты при обнаружении плохого трафика ботов в зависимости от бизнес-требований.



*Radware's JavaScript код и cookies добавляются в объект ответа.

Специализированное решение для API



Слепок для
коммуникации
M2M



ЗАЩИТА ВЕБ- И
МОБИЛЬНЫХ API



БЕЗОПАСНЫЙ IoT И
ПОДКЛЮЧЕННЫЕ
УСТРОЙСТВА



ПРЕДОТВРАЩЕН
ИЕ ЗАХВАТА
АККАУНТА

Radware на #1 в рейтинге Gartner по защите API Protection

*Отчет о критических возможностях облачных веб-приложений и защиты API, октябрь 2020 г.

РАЗВЕРТЫВАНИЕ RADWARE'S BOT MANAGER



Reverse Proxy

Web-server & CDN
plug-ins



Out of Path

Web & Mobile SDKs /
Javascript tag

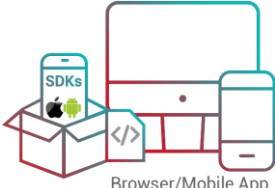


Cloud Managed Service

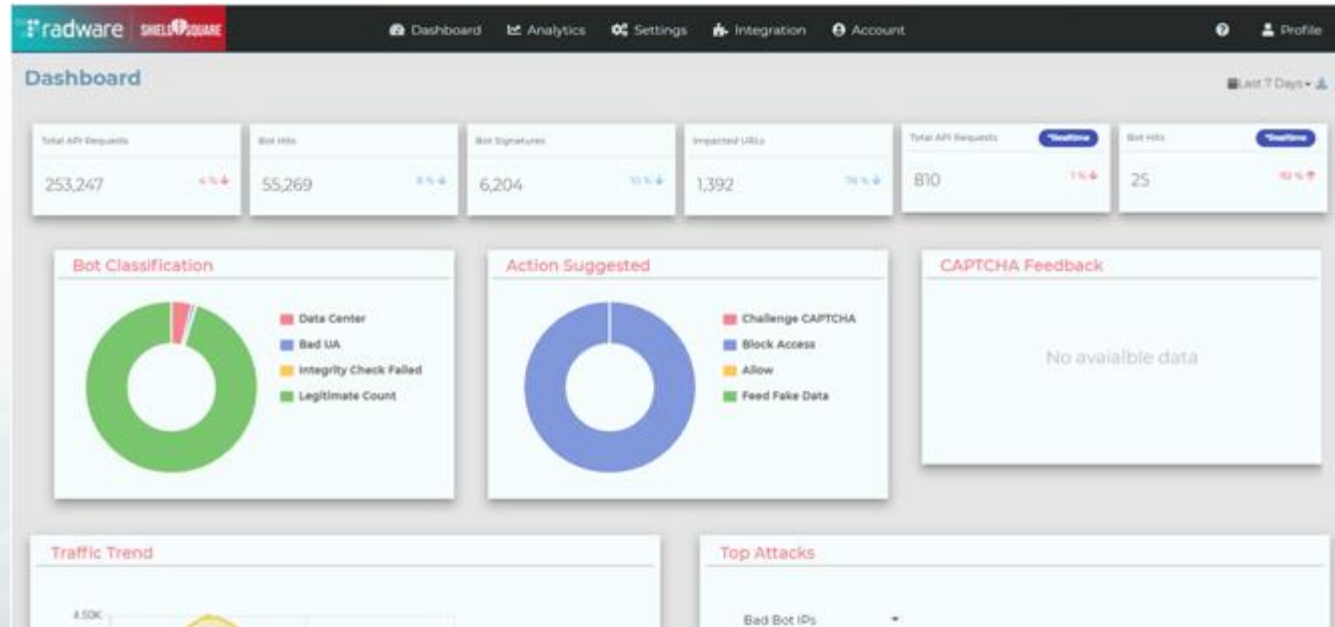


**Bot Manager
интегрирован в
Alteon**

Возможности интеграции

	
 Load Balancer	
 Web Server	
 Application Server	
 Browser/Mobile App	

Полная защита приложений



ПОЛНАЯ ДЕТАЛИЗАЦИЯ

- ✓ Выборки по типу ботов
- ✓ По «следам» и плохим IPs
- ✓ Измерение загрузки плохого трафика

ИНДИВИДУАЛЬНЫЕ ДЕЙСТВИЯ

- ✓ Блокирование
- ✓ Challenge (CAPTCHA)
- ✓ Подача поддельных данных
- ✓ «Снижение / растягивание»

Подавление / управление ботами

Bot Management

[Bot Management](#)[URL Management](#)[Block Country / ISP](#)

Bad Bot Response

Generation

▼ Gen 1

Scripted bots

Bot attacking from Public Cloud

Known bad bot signatures

Misbehaving legitimate bots

> Gen 2

> Gen 3

> Gen 4

Allow

Challenge CAPTCHA

Block Access

FeedFakeData

Complex JS

Throttle

Drop Request

Session Termination

Redirect Loop

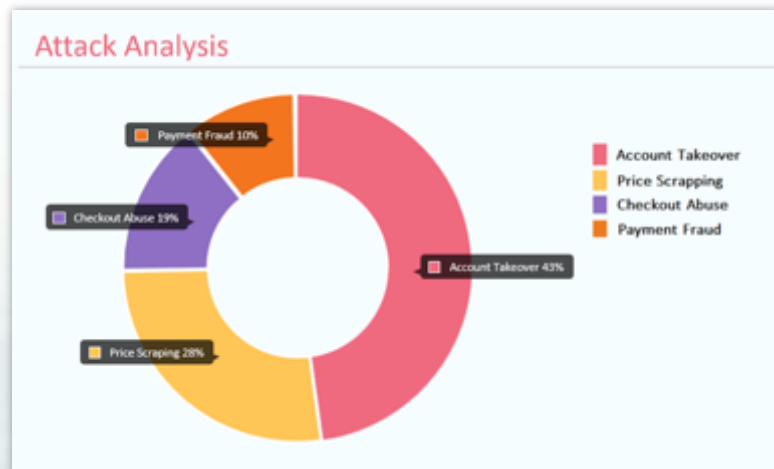
Log Only

Custom Response

Submit

Детализация и настройка для управления

INTENT ANALYSIS



NEW ATTACK RESPONSES

Gen 1

Scripted bots

Bot attacking from Public Cloud

Known bad bot signatures

Misbehaving legitimate bots

Gen 2

Gen 3

Allow

- Throttle
- Drop Request
- Session Termination
- Redirect Loop
- Log Only
- Custom Response

Challenge CAPTCHA

CAPTCHA DIFFICULTY

Bot Management

Bad Bot Response

Generation	Responses	CAPTCHA Difficulty
Gen 1	Challenge CAPTCHA	Basic
Gen 2	Challenge CAPTCHA	Advanced
Gen 3	Challenge CAPTCHA	Advanced
Gen 4	Challenge CAPTCHA	Adaptive

Submit

GOOD BOTS' VISIBILITY



РЕЗЮМЕ



ВСЕ ВИДЫ АТАК



ВСЕ ПОКОЛЕНИЯ



**ЛЮБЫЕ
КАНАЛЫ**



**МИНИМУМ
ЛОЖНЫХ
СРАБАТЫВАНИЙ**

АНАЛИЗАТОР ПЛОХИХ БОТОВ

БЕСПЛАТНАЯ ОЦЕНКА ТРАФИКА БОТОВ И АТАК БОТОВ



- ✓ Оцените объем плохого бот-трафика
- ✓ Получите полную информацию о попытках захвата, мошенничестве с платежами и веб-сканировании
- ✓ Протестируйте все каналы: веб-сайты, мобильные приложения и API
- ✓ Проанализируйте плохой трафик ботов по уровню сложности
- ✓ Получите советы и рекомендации

**Requires sharing access logs from web-server, CDN or WAF*

Thank You!