Outsource IT .BY

Современные проблемы безопасности Веб-приложений и их решение в 2024

ООО «Безопасные технологии и системы»

Radware@outsourceit.by

radware

В компаниях сейчас в приоритете

Проблемы обеспечения безопасности организаций

1. Растущий ландшафт угроз информационной безопасности
2. Ускорение цифровой трансформации
3. Нехватка специалистов по безопасности и навыков

Сканируйте код, чтобы задать вопрос прямо сейчас или после презентации

Растущий ландшафт угроз безопасности

Mercedes-Benz USA Says 1.6 Million Records Exposed

Notification Comes Shortly After a Similar Disclosure by Volkswagen

Jeremy Kirk (jeremy_kirk) • June 29, 2021

Twitter Facebook LinkedIn Credit Eligible Get Permission

The vendor notified Mercedes-Benz on June 11. The exposure, which occurred on a cloud storage platform, was discovered by an external security researcher, Mercedes-Benz says.

Photo: Daimler AG

Mercedes-Benz USA says one of its vendors exposed 1.6 million records that pertained to its customers and interested buyers.

See Also: Live Panel | Zero Trusts Given- Harnessing the Value of the Strategy

Most of the exposed records contained names, addresses, email addresses, phone numbers and possibly information about purchased vehicles. The data was collected on dealer and Mercedes-Benz websites between Jan. 1, 2014, and June 19, 2017, according to a news release.

Twitch Suffers Massive 125GB Data and Source Code Leak Due to Server Misconfiguration

October 06, 2021 Ravie Lakshmanan

The Amazon-owned service said it's "working with urgency to understand the extent of this," adding the data was exposed "due to an error in a Twitch server configuration change that was subsequently accessed by a malicious third party."

other internal tools.

The Amazon-owned service said it's "working with urgency to understand the extent of this," adding the data was exposed "due to an error in a Twitch server configuration change that w subsequently accessed by a malicious third party."

"At this time, we have no indication that login credentials have been exposed," Twitch noted in a post published late Wednesday. "Additionally, full credit card numbers are not stored by Twitch, so full credit card numbers were not exposed."

Aug 29, 2019, 05:45am EDT | 21,069 views

Capital One Hacker 'Breached 30 Organizations And Mined Cryptocurrency,' Claims DOJ

Thomas Brewster Forbes Staff Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

Listen to this article now -02:29

Powered by Trinity Audio

Thompson acquired access to company computer login details, pilfered from open Amazon servers, the government alleged. She would then abuse control over those computers to both steal data and use up processing power to mine cryptocurrency, according to the indictment. Such mining is often referred to as cryptojacking.

only hacking Capital One, but another 30 companies and in some cases using their servers to mine cryptocurrency.

Растущий ландшафт угроз безопасности

Эксплуатация уязвимостей

Capital One

100M Records

SERVER-SIDE REQUEST FORGERY

*$80M PENALTY

3.3M Records

DATA BREACH

Атаки ботов

DUNKIN' DONUTS

10M Records

CREDENTIAL STUFFING

533M Records

SCRAPING BOTS

Абьюз API

venmo

200M Transactions

API EXPOSURE

solarwinds

18K Companies

UP TO $100B IN DAMAGES

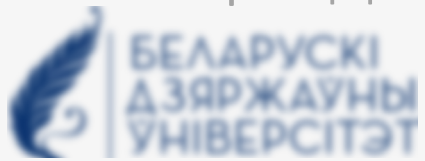
Максимальная безопасность требует защиты от всех возможных угроз

Известные инциденты в Беларуси

Регулярно подвергается атакам

и другие компании гос. сектора

Утечки перс. данных



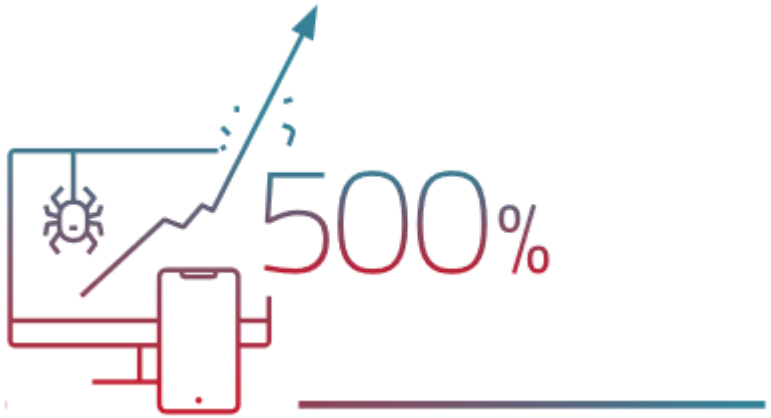
и другие...

Атакуют всех и бдительным нужно быть всегда

Интенсивность атак растет

Обзор 2023 года

Атаки на мобильные приложения



по сравнению с 2022 число атак в 2023 на мобильные приложения выросло на 500%

Увеличение активности Хактивистов

Biggest worry for western countries supporting Ukraine

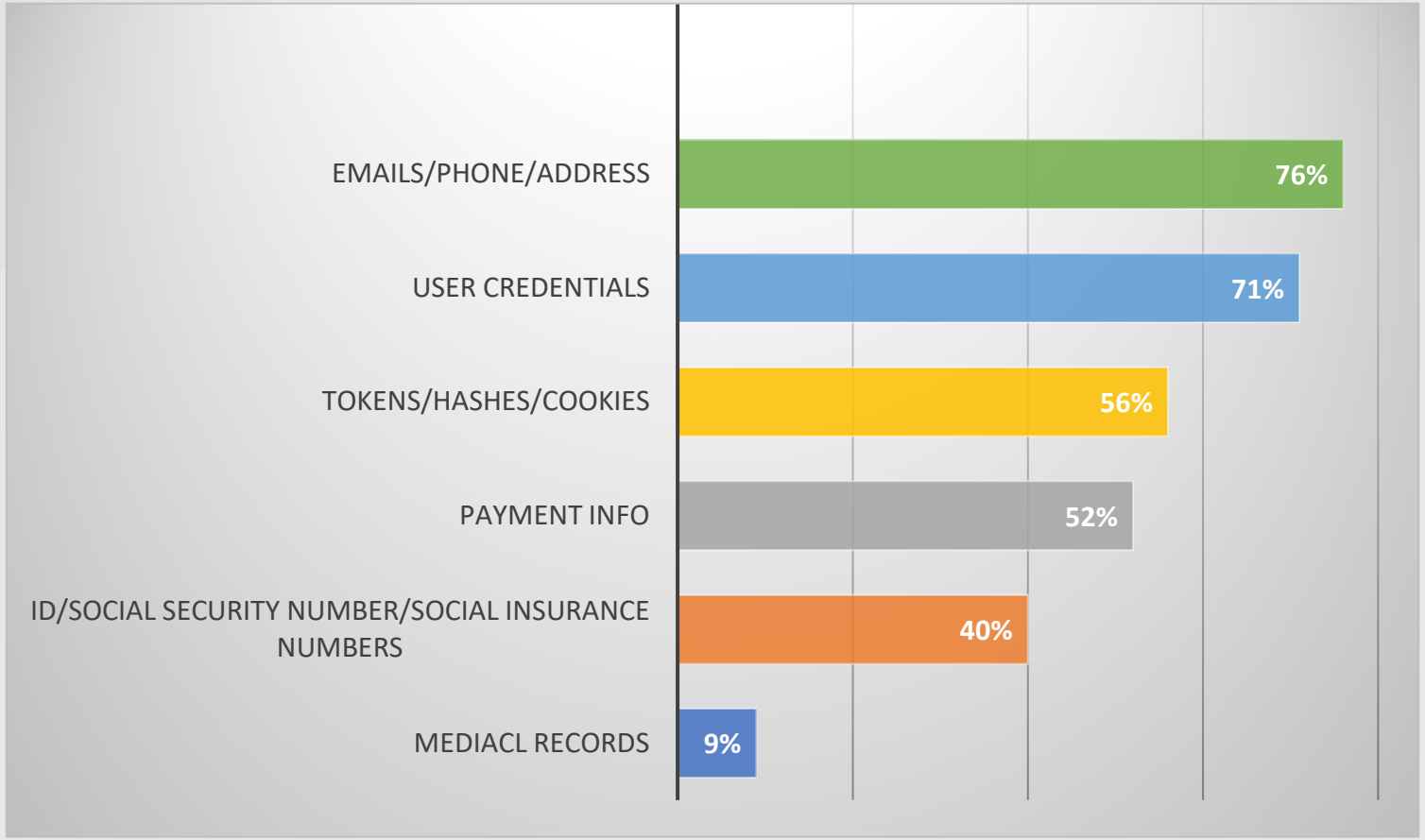
NoName057(16)

Anonymous Sudan found motivation in religion, politics and money

Killnet leader Killmilk became the most influential pro-Russian hacktivist

ЗАЩИТА API — САМАЯ БЫСТРОРАСТУЩАЯ ЗАДАЧА

% конфиденциальных данных, открытых через API



Угроза №1

61% СВЯЗАННЫЕ С НАРУШЕНИЯМИ ЭКСПЛУАТАЦИИ API

Приоритет №1

55% БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЯ И ИНФРАСТРУКТУРЫ API

#1 App-Sec

59% ТРЕБУЕЕТСЯ ИНВЕСТИРОВАТЬ В ЗАЩИТУ ПРИЛОЖЕНИЙ

* Источник: Отчет о безопасности приложений Radware.

Нарушения прав доступа

Неаутентифицированный доступ	• Authentication: OAuth2, JSON Web Token,… • Session Hijacking (e.g. steal token) • Token manipulation (e.g. privilege esc.)
Не авторизованный доступ	• IP, token or role-based access • Access to restricted APIs (temp/ test) • Excessive use (cost)
Захват аккаунта	• Credential Stuffing • Brute-force

Манипуляции API

Встроенные атаки

- SQL & Command Injections
- Cross-Site Scripting (XSS)
- Directory Traversal

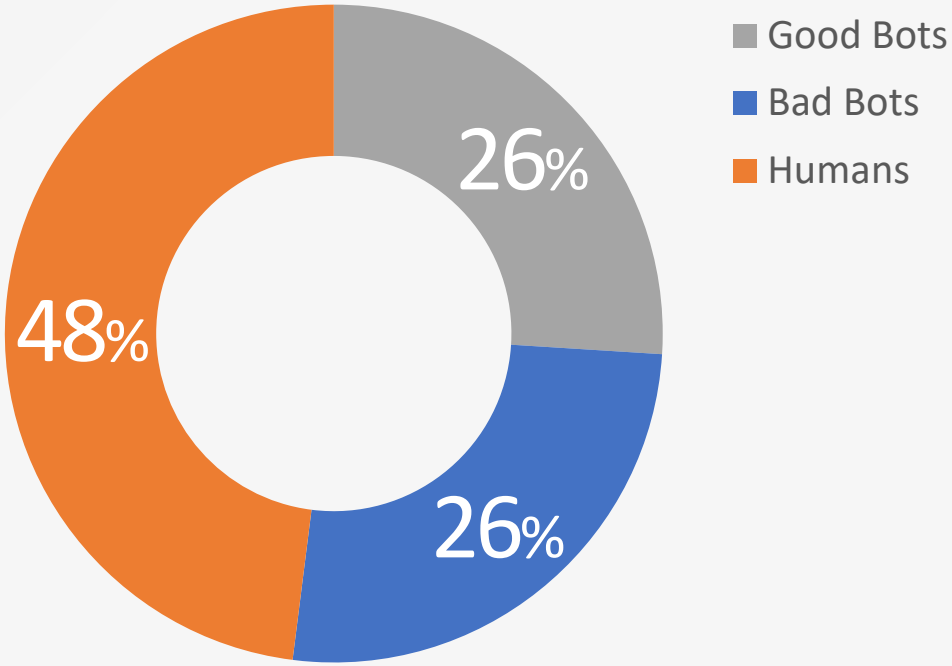
Абьюз API

- HTTP Method Abuse: DELETE vs. GET
- Unexpected JSON/XML Element Types
- Out of range JSON/XML Element Values

Утечка конфиденциальных данных

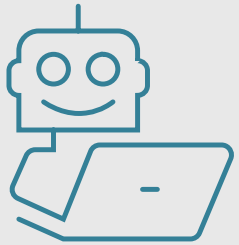
- Data Exposure (PII/CCN/SSN etc.)
- 5XX Internal Server Errors
- HTTP response headers

Боты захватили Интернет



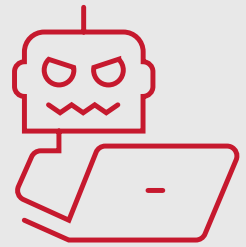
Что делают хорошие боты?

- Поисковые системы
- Сервисы сравнения цен
- Сборщики информации
- Загрузчики информации



Что делают плохие боты?

- Захваты аккаунта
- DDoS атаки
- Блокирование склада в e-commerce
- и другие вредоносные активности



26% интернет-трафика генерируют плохие боты

4 из 5 организации не могут отличить «хороших» от «плохих» ботов

Ускорение цифровой трансформация

Работа
из дома

Интернет-
потребление
товаров

Веб-приложения
в центре
бизнеса

Скорость и **гибкость** имеют решающее значение для сохранения конкурентоспособности

Нужна **стабильная безопасность**, которая **не снижает** вашей скорости

Нехватка специалистов по ИБ растет

+27%
спрос на специалистов по ИБ

~3,5M
открытые позиции по всему миру

85%
организаций сталкивается с нехваткой навыков

38%
сообщают о высоком уровне выгорания

Потребность в **автоматизированных средствах защиты** и **полностью управляемых сервисах ИБ**

* Источники: (ISC)² Исследование и опрос рабочей силы в области кибербезопасности, проведенный Gaper ISSA/ESG.

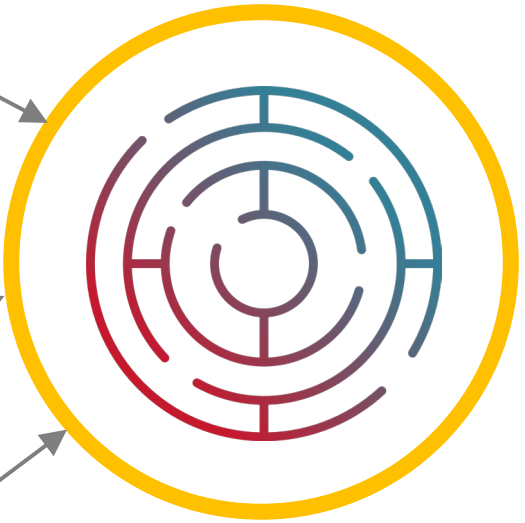
Растущая сложность

Среды и процессы разработки и доставки создают слепые зоны для ИБ

Непрерывная доставка

Распределенная информация

Частые изменения



Большая сложность

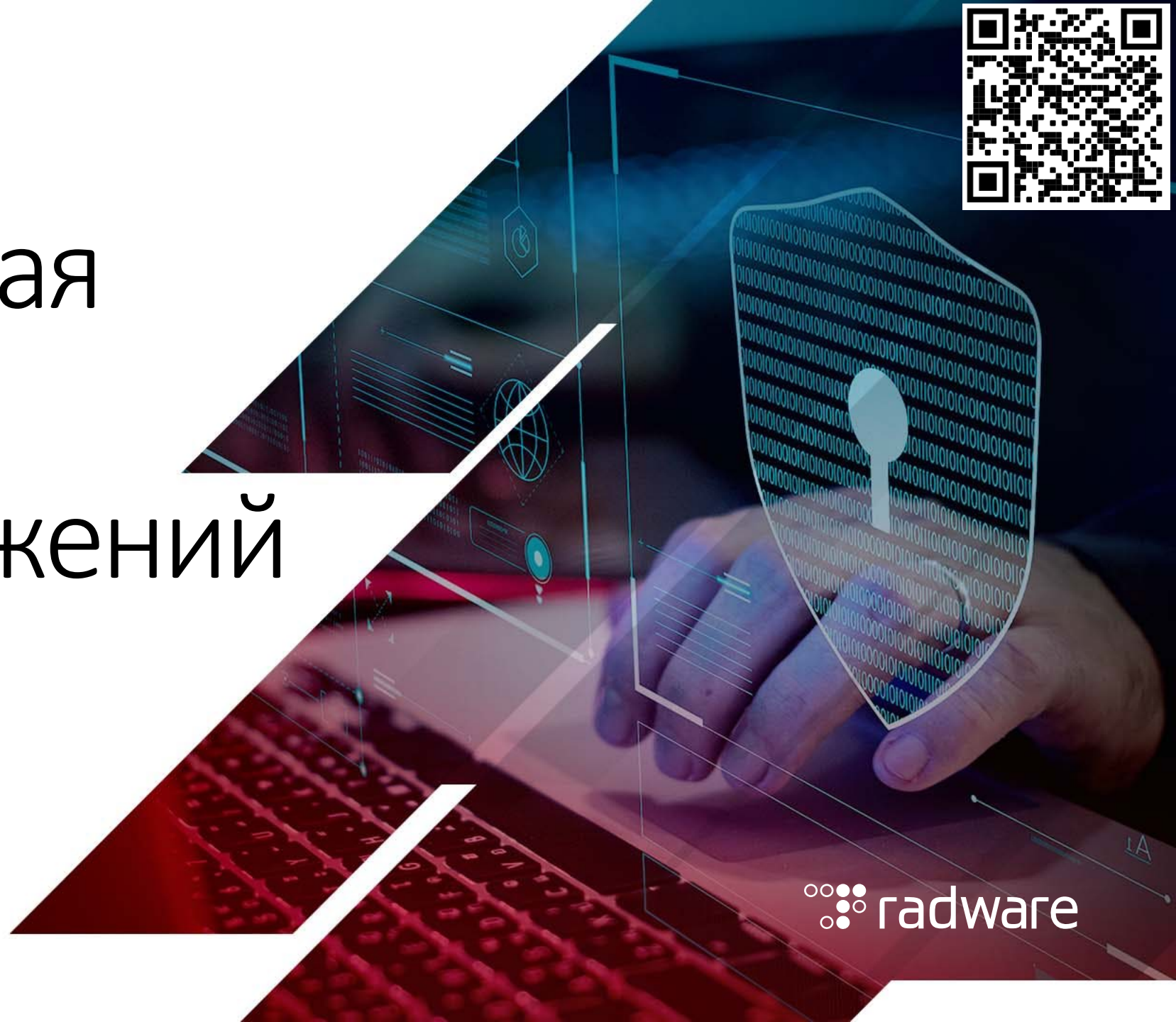
70% приложений еженедельно меняются

56% не интегрируют безопасность в конвейер CI/CD

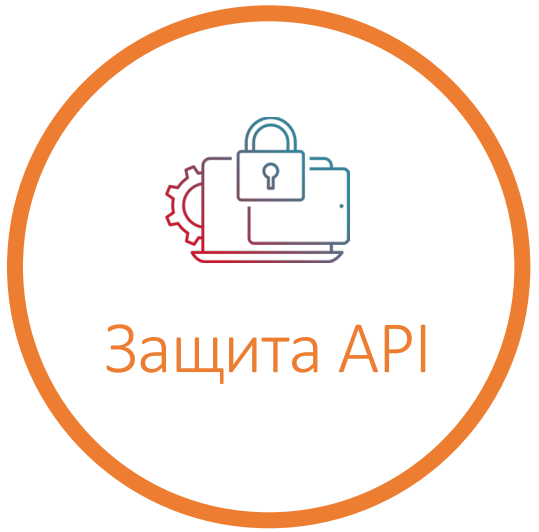
59% защита API - приоритет № 1 безопасности приложений на 2024 г.

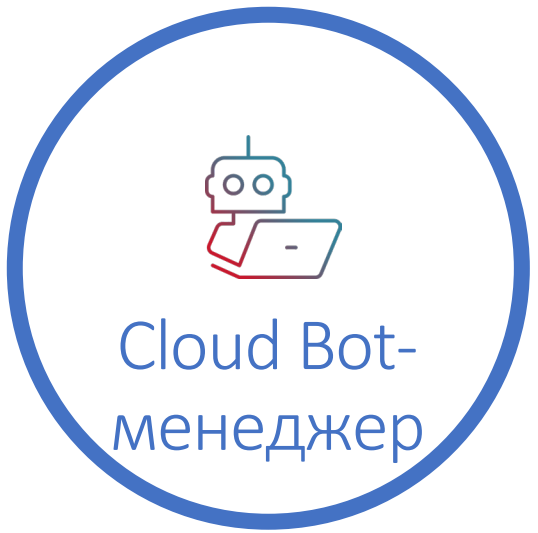
2/3 говорят, что потребность в последовательности и наглядности является главным вопросом

Комплексная защита Вэб-приложений Radware

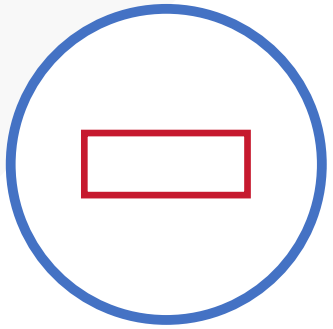


Универсальное решение для всех потребностей в безопасности приложений





Положительная + отрицательная модель безопасности для надежной защиты приложений



Отрицательная модель безопасности

- Стандарт для большинства сервисов WAF и технологий WAF
- Блокирует известные атаки с помощью известных сигнатур и правил
- **Не может обеспечить ПОЛНУЮ защиту от OWASP TOP-10**
- **Не может защитить от неизвестных уязвимостей: атаки нулевого дня**

Позитивная модель безопасности

- Изучает и определяет, какие действия являются законным трафиком
- Блокирует несанкционированный доступ или действия, которые не разрешены
- **Уникальная защита от атак нулевого дня и неизвестных уязвимостей**
- **Высокий уровень защиты: ПОЛНАЯ защита OWASP TOP-10, минимум ложных срабатываний**

Автоматическая генерация политик

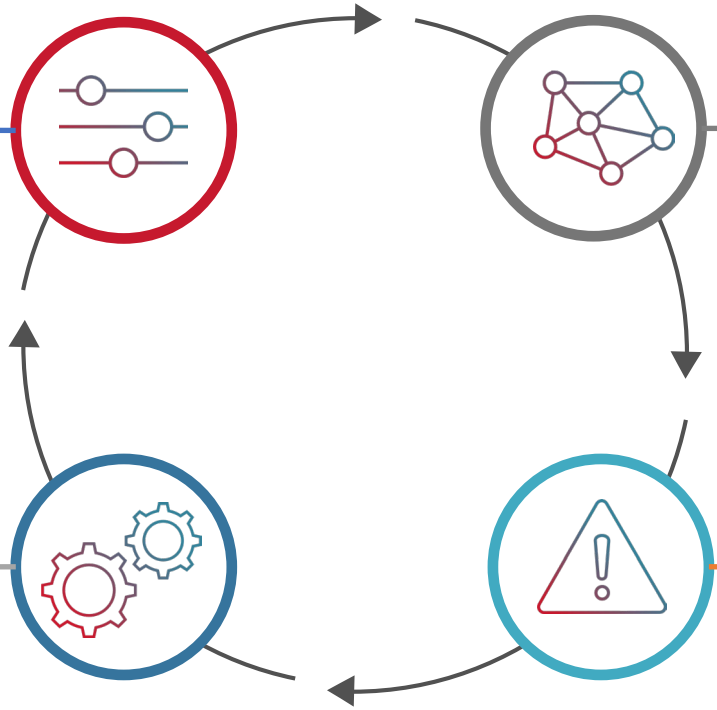
Алгоритмы машинного обучения для автоматического создания политик

Автоматическая активация политики

добавление адаптированных правил для приложений и оптимизация для максимальной точности

Сопоставление приложений

для обнаружения новых/изменений в веб-приложении



Генерация и оптимизация политик

для нестандартных правил, чтобы свести к минимуму ложные срабатывания

Автоматический анализ угроз

Охватывает ВСЕ Топ-10 OWASP и более 150 векторов атак

Постоянно следите за изменениями в приложении и приемлемом поведении пользователя, чтобы поддерживать защиту в актуальном состоянии.

Непрерывная оптимизация политик

Больше безопасности. Меньше работы.

МОДУЛЬ ОПТИМИЗАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ

Запатентованные алгоритмы машинного обучения

УТОЧНЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ

Более высокая эффективность

Точная и надежная защита

Меньше ложных срабатываний

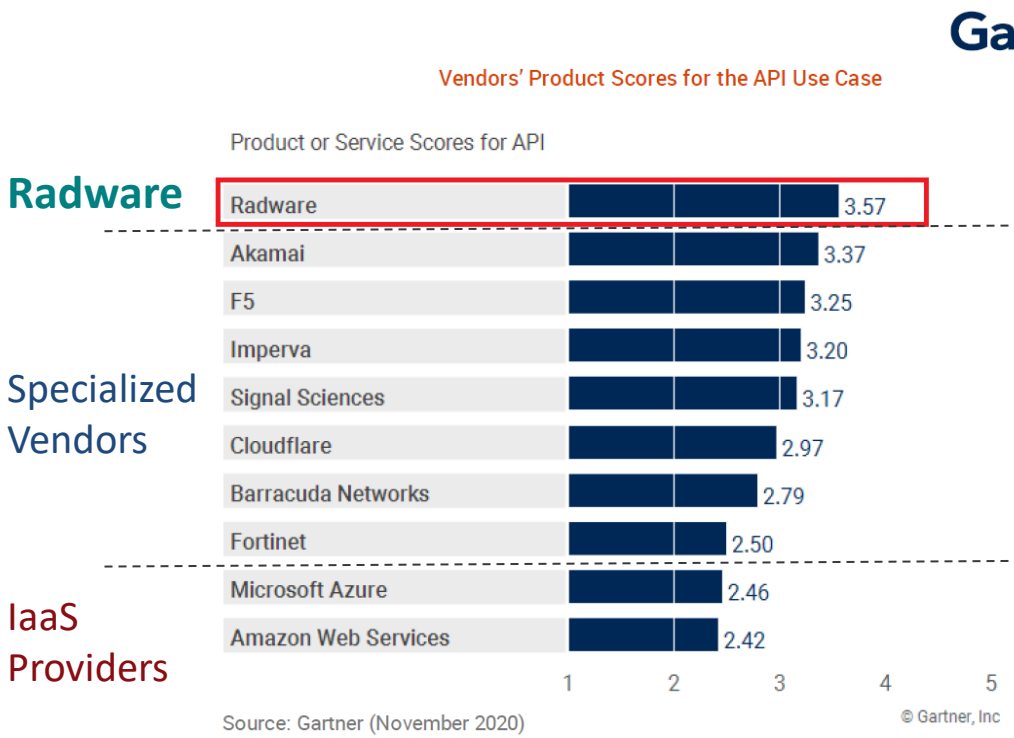
Защита от уязвимостей Веб-приложений и API

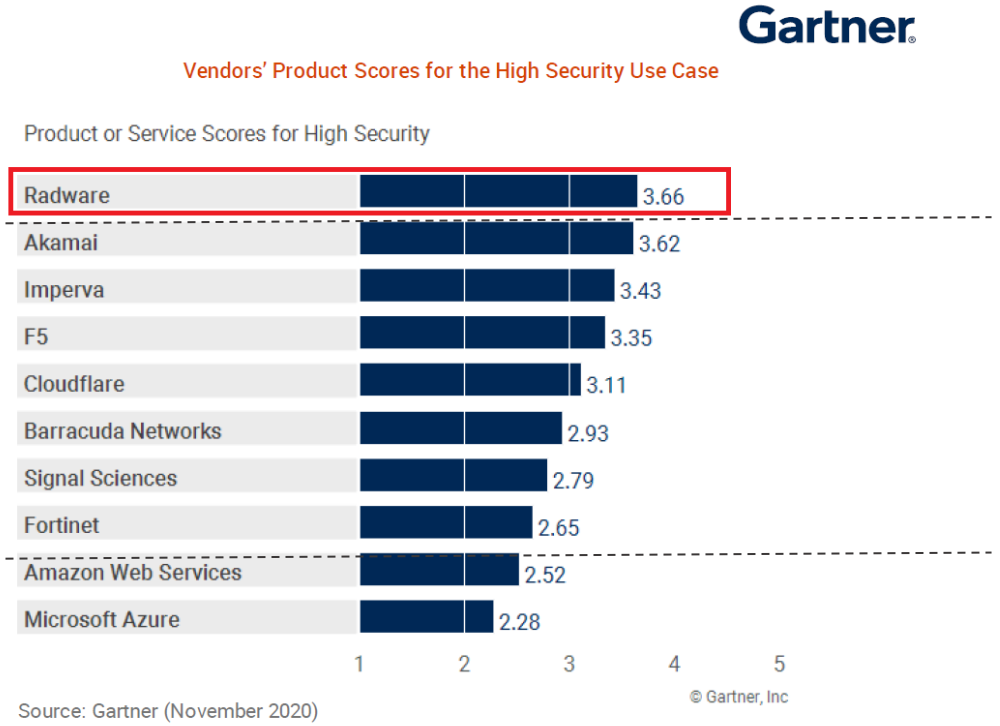
Web Application Firewall (WAF)

Radware

Specialized Vendors

IaaS Providers





Что говорят о Radware клиенты

Gartner peerinsights

Gartner peerinsights customers' choice 2021

90%

БУДУТ РЕКОМЕНДОВАТЬ
Radware WAF

#2

Radware WAF
ТОП #2 ПО МНЕНИЮ ПОЛЬЗОВАТЕЛЕЙ

★★★★★

Radware Bot Manager
в среднем 5-звезд по отзывам

в 2023 году в Беларуси WAF Radware покупали в банковском секторе и секторе телеком

Сертификация ОАЦ

СЕРТИФИКАТ СООТВЕТСТВИЯ

TP BY

Зарегистрирован в реестре **№ BY/112 02.02. TP027 036.01 00690**

Дата регистрации **21 февраля 2023 г.**

Заявитель Общество с ограниченной ответственностью «Безопасные технологии и системы», Республика Беларусь, 220053, г.Минск, ул.Нововиленская, д.38, каб.11, регистрационный номер в ЕГР – 193303745.

Изготовитель Компания «Radware Ltd.», 22 Raoul Wallenberg Street Tel Aviv, 6971917, Государство Израиль.

Продукция Программное обеспечение контроллера доставки приложений (ADC), балансировки сетевой нагрузки и защиты веб-приложений Radware Alteon Virtual Appliance версии 33.0.5.xx, партия продукции 20 шт. (s/n: 01 – 20; товарная накладная от 02.12.2022 № 0226820).

Код ОКП РБ 62.01.29.000
Код ТН ВЭД ЕАЭС 8523499101

соответствует требованиям ТР 2013/027/BY (СТБ 34.101.1-2014, СТБ 34.101.2-2014,

Есть Вопросы?
Нужно ДЕМО?

radware@outsourceit.by