Outsource iT .BY

Современные проблемы безопасности Веб-приложений и их решение

Максим Автоненко

ООО «Безопасные технологии и системы»

Radware@outsourceit.by

radware

В компаниях сейчас в приоритете

Проблемы обеспечения безопасности организаций

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

Сканируйте код, чтобы задать вопрос прямо сейчас или в процессе презентации

Растущий ландшафт угроз безопасности

1

Эксплуатация уязвимостей

100M Records
SERVER-SIDE REQUEST FORGERY
*$80M PENALTY

3.3M Records
DATA BREACH

Атаки ботов

10M Records
CREDENTIAL STUFFING

533M Records
SCRAPING BOTS

Абьюз API

200M Transactions
API EXPOSURE

18K Companies
UP TO $100B IN DAMAGES

Максимальная безопасность требует защиты от всех возможных угроз

Известные инциденты в Беларуси

1

> 100,000 записей

СОСЕДИ

> 620,000 записей

Остров чистоты и вкуса

. . .

PETITIONS.BY
УДОБНЫЙ ГОРОД

600,000 записей

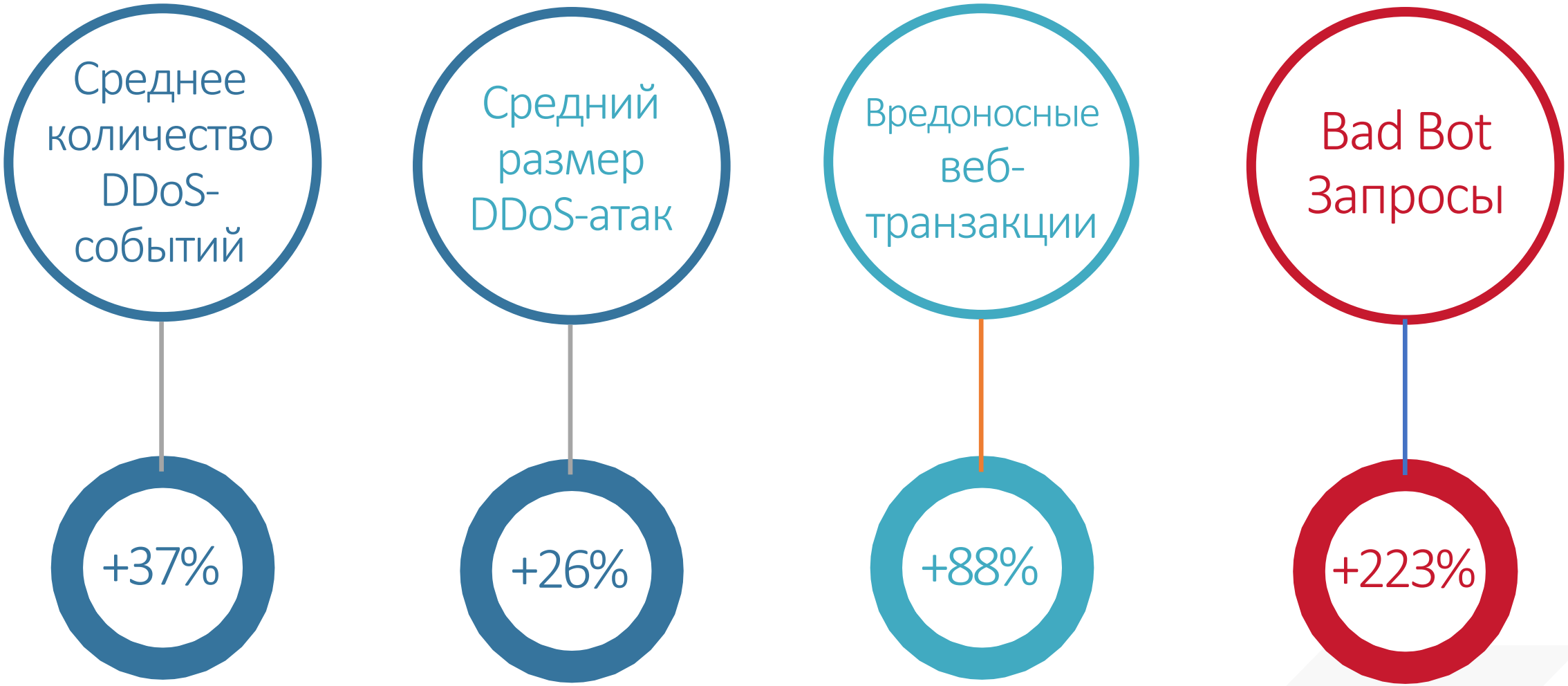
ilex

255GB данных

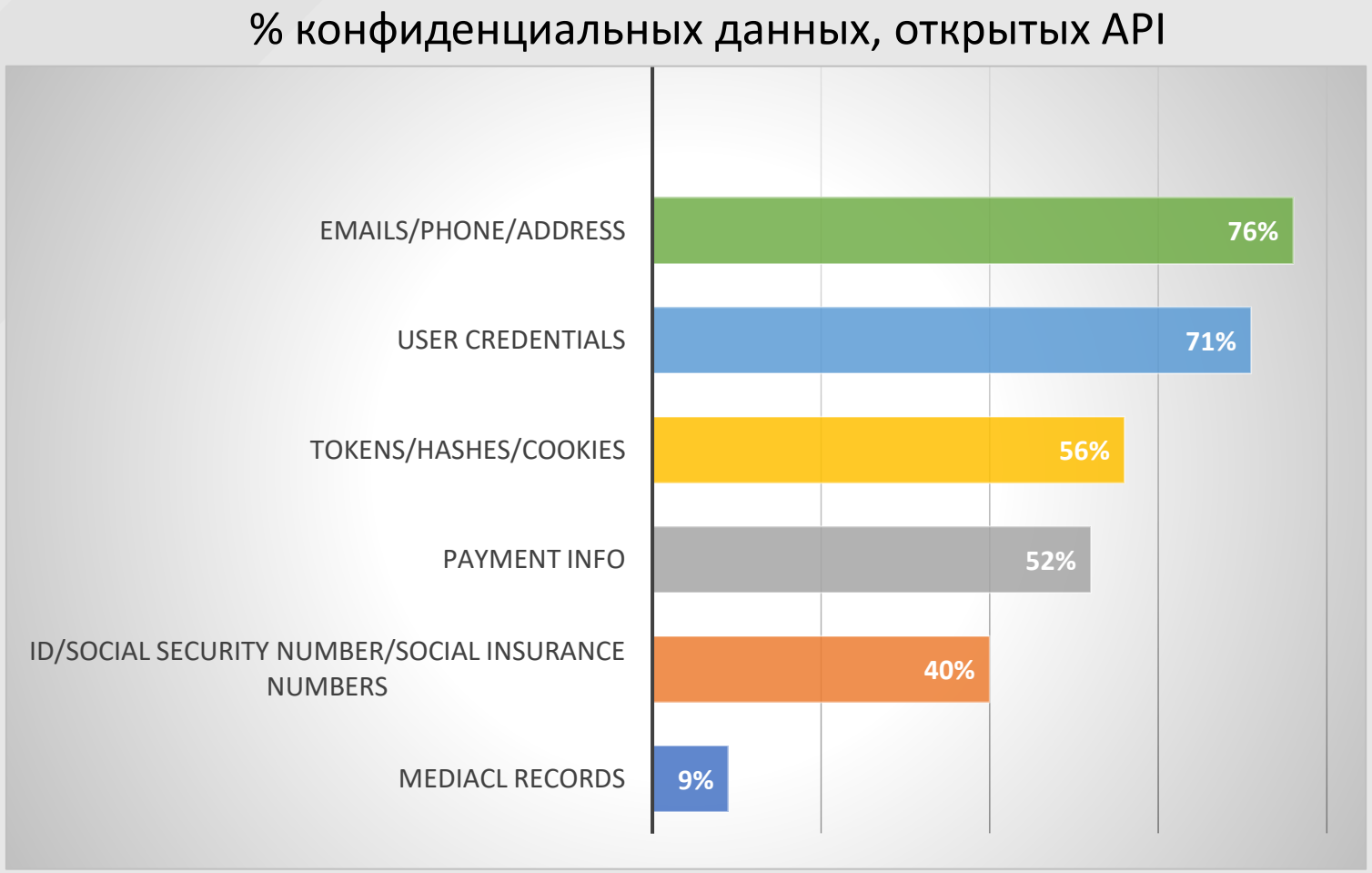
Максимальная безопасность требует защиты от всех возможных угроз

Интенсивность атак растет

Обзор 2022 года



ЗАЩИТА API — САМАЯ БЫСТРОРАСТУЩАЯ ЗАДАЧА



Угроза №1

61% СВЯЗАННЫЕ С НАРУШЕНИЯМИ ЭКСПЛУАТАЦИИ API

Приоритет №1

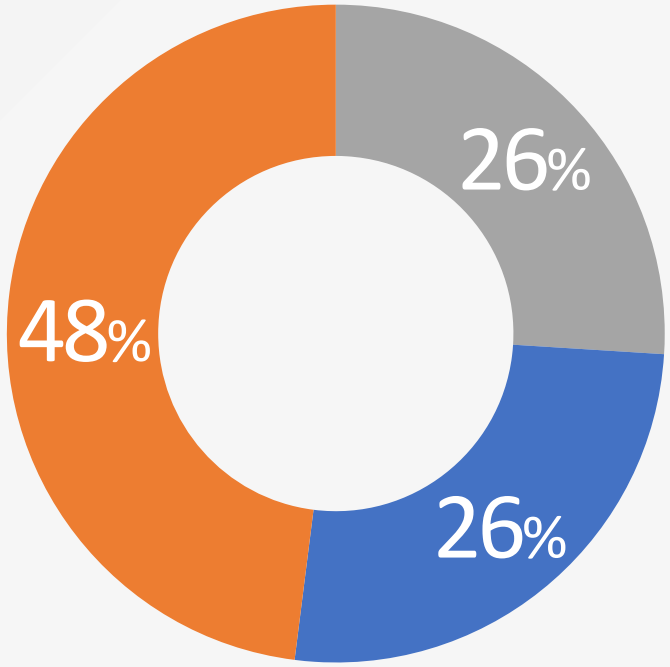
55% БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЯ И ИНФРАСТРУКТУРЫ API

#1 App-Sec

59% ТРЕБУЕЕТСЯ ИНВЕСТИРОВАТЬ В ЗАЩИТУ ПРИЛОЖЕНИЙ

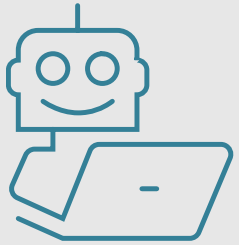
* Источник: Отчет о безопасности приложений Radware за 2021 г.

Боты захватывают Интернет



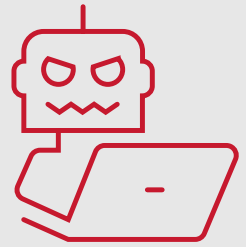
Что делают хорошие боты?

- 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 безопасности и навыков

3

+20%
спрос на специалистов по ИБ

~3M
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: 2021 (ISC)² Исследование и опрос рабочей силы в области кибербезопасности, проведенный Gaper ISSA/ESG.

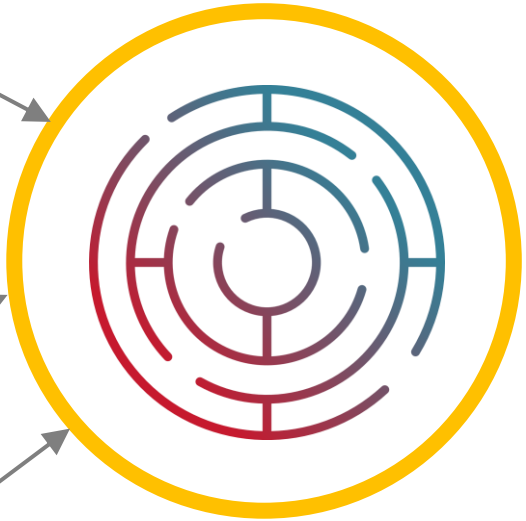
Растущая сложность

Среды и процессы разработки и доставки создают слепые зоны для ИБ

Непрерывная доставка

Распределенная информация

Частые изменения



Большая сложность

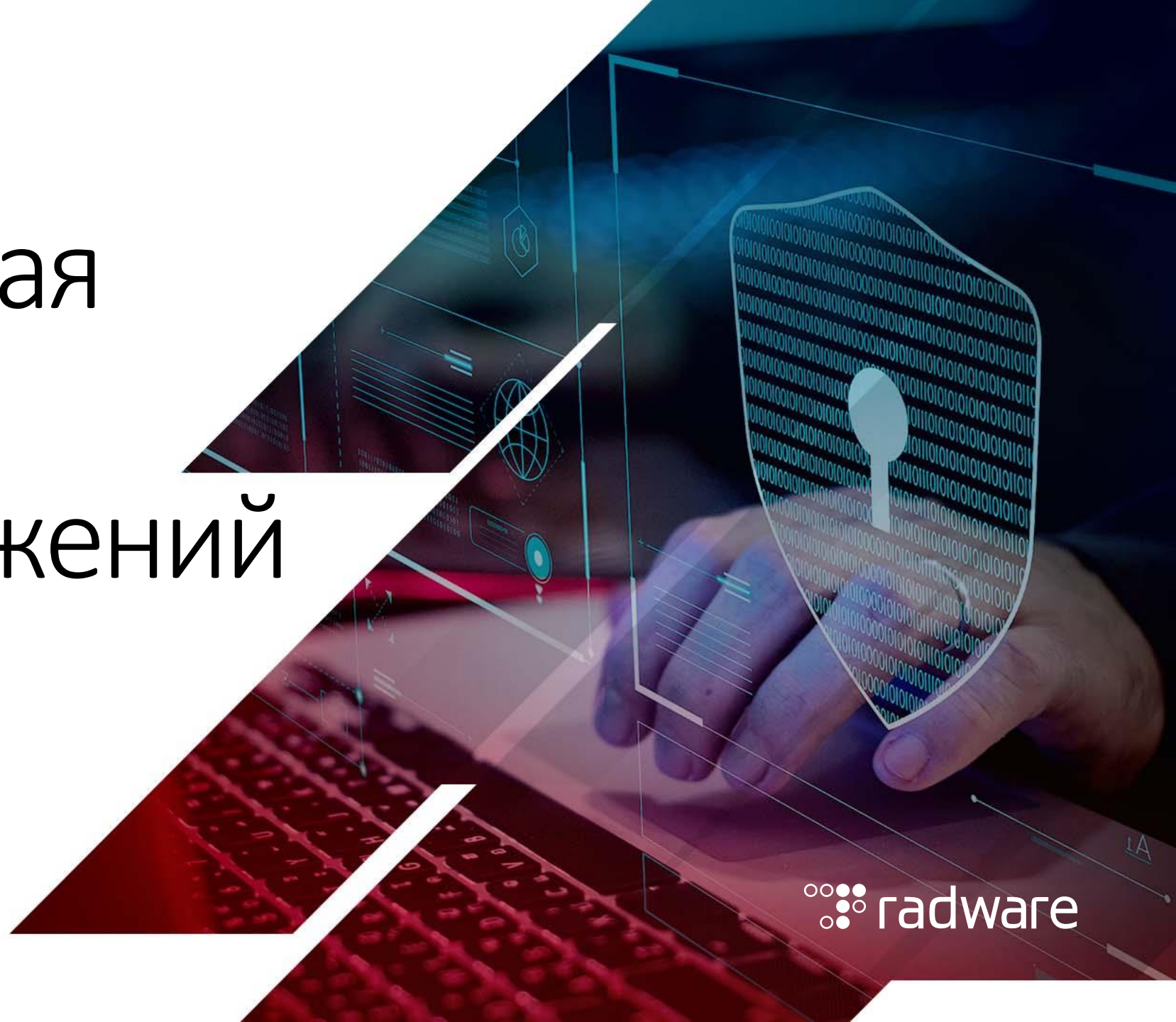
70% приложений еженедельно меняются

56% не интегрируют безопасность в конвейер CI/CD

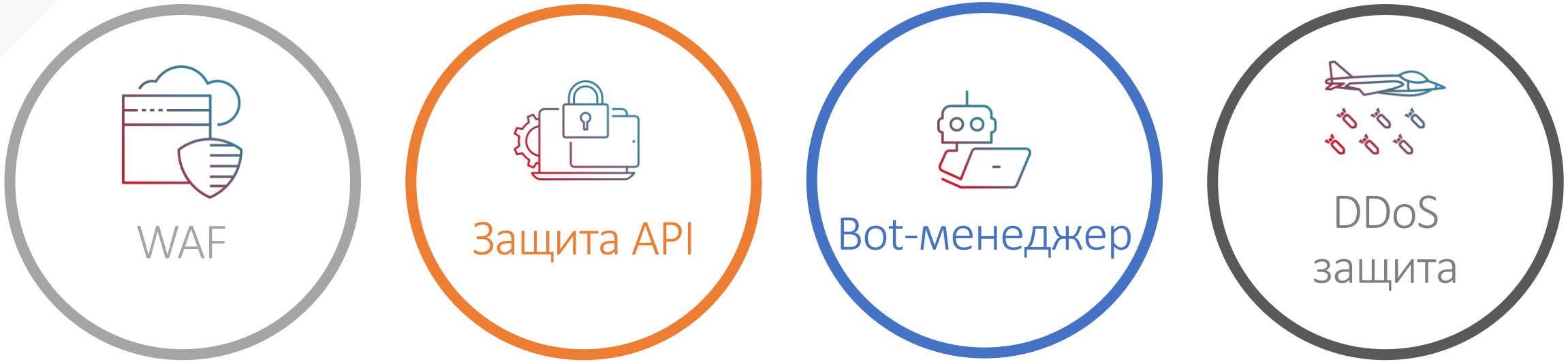
59% защита API - приоритет № 1 безопасности приложений на 2022 г.

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



Полная современная защита Веб-приложений

Защита цифровых активов и данных в любом месте

В дата-центре, частные и публичные облака, гибридные среды и Kubernetes

Защита от OWASP уязвимостей

Более 150 известных векторов атак на веб-приложения, ботов и API

Защита от атак нулевого дня

Снижает подверженность неизвестным угрозам и атакам нулевого дня на 99 %.

Детект, управление и устранение ботов

Различайте «хороших» и «плохих» ботов
Защита веб-сайтов, мобильных приложений и API

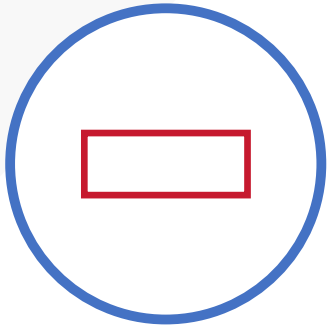
Обнаружение и защита API приложений

Узнайте, ЧТО защищать с помощью автоматического обнаружения API.
Применяйте глубокие меры безопасности

Смягчение DDoS-атак на уровне приложений

Кратчайшее время обнаружения и устранения HTTP DDoS-атак

Положительная + отрицательная модель безопасности для надежной защиты приложений



Отрицательная модель безопасности

- Стандарт для большинства облачных 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**

Полное покрытие 10 главных рисков OWASP для веб-приложений

- ✓ SQL иньекции
- ✓ Cross-site скриптинг (XSS)
- ✓ Подделка запроса на стороне клиента (CSRF)
- ✓ Атаки на протоколы
- ✓ Подделка запроса на стороне сервера (SSRF)
- ✓ Отказ в обслуживании (DoS)
- ✓ Cookie poisoning
- ✓ Zero-days
- ✓ Брутфорс-атаки
- ✓ LFI/RFI

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

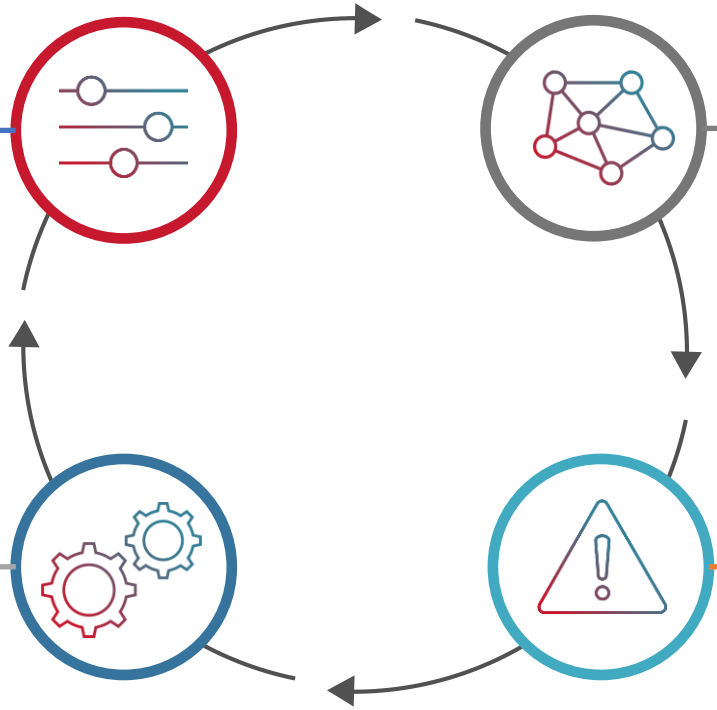
для обнаружения новых/изменений в веб-приложении

Автоматический анализ угроз

Охватывает ВСЕ Топ-10 OWASP и более 150 векторов атак

Генерация и оптимизация политик

для нестандартных правил, чтобы свести к минимуму ложные срабатывания



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

Практический пример: критическая уязвимость Log4Shell

CVE-2021-44228 в библиотеке Log4j

WAF

BGR

News Deals Tech Reviews Guides Best

Internet is scrambling to fix Log4Shell, the worst hack in history

threatpost

Robocalls More Than Doubled in 2021, Cost Victims $30B FBI: Anot

Conti Ransomware Gang Has Full Log4Shell Attack Chain

Hackers start pushing malware in worldwide Log4Shell attacks

WAF Radware обнаруживает и блокирует активность Log4Shell с **первого дня!**

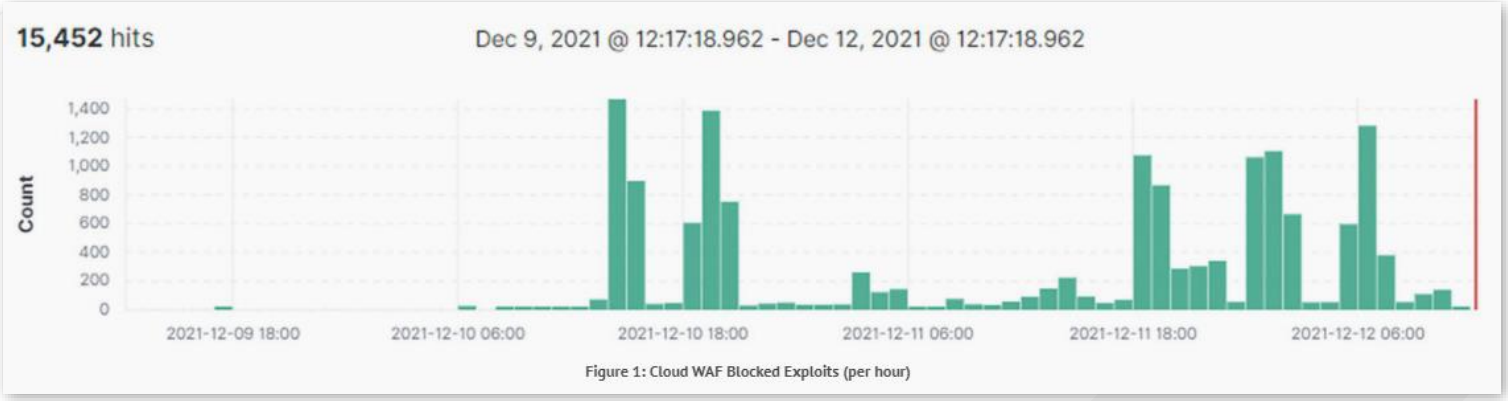


Figure 1: Cloud WAF Blocked Exploits (per hour)

Атаки на приложения всколыхнули Интернет

Spring4Shell
Критическая
Уязвимость

POSTED: 31 MAR, 2022 | 3 MIN READ | THREAT INTELLIGENCE

SUBSCRIBE FOLLOW

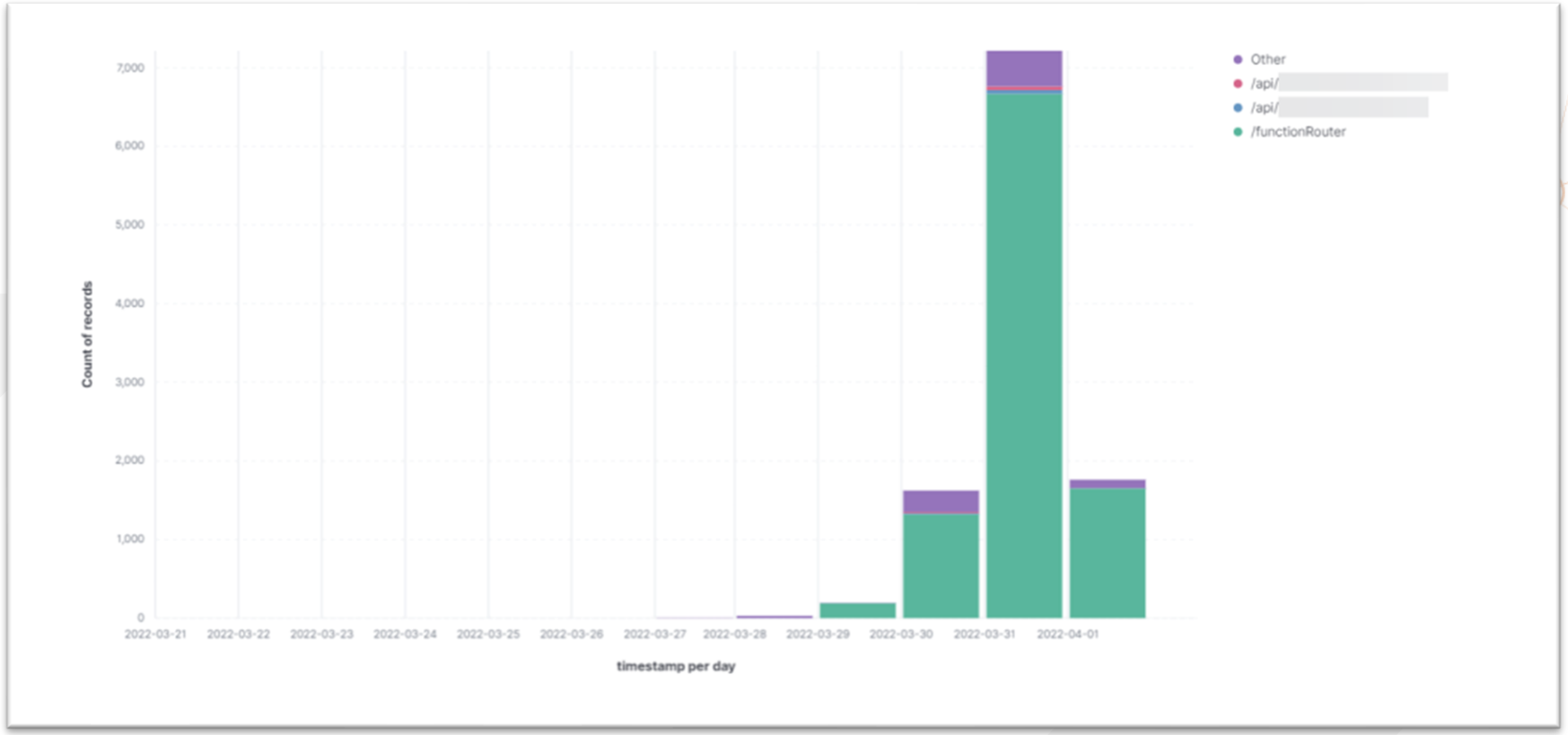
Spring4Shell: New Zero-day RCE Vulnerability Uncovered in Java Framework

Symantec products will protect against attempted exploits of Spring4Shell vulnerability.

UPDATE, April 1, 2022: *Updated with additional protection information*

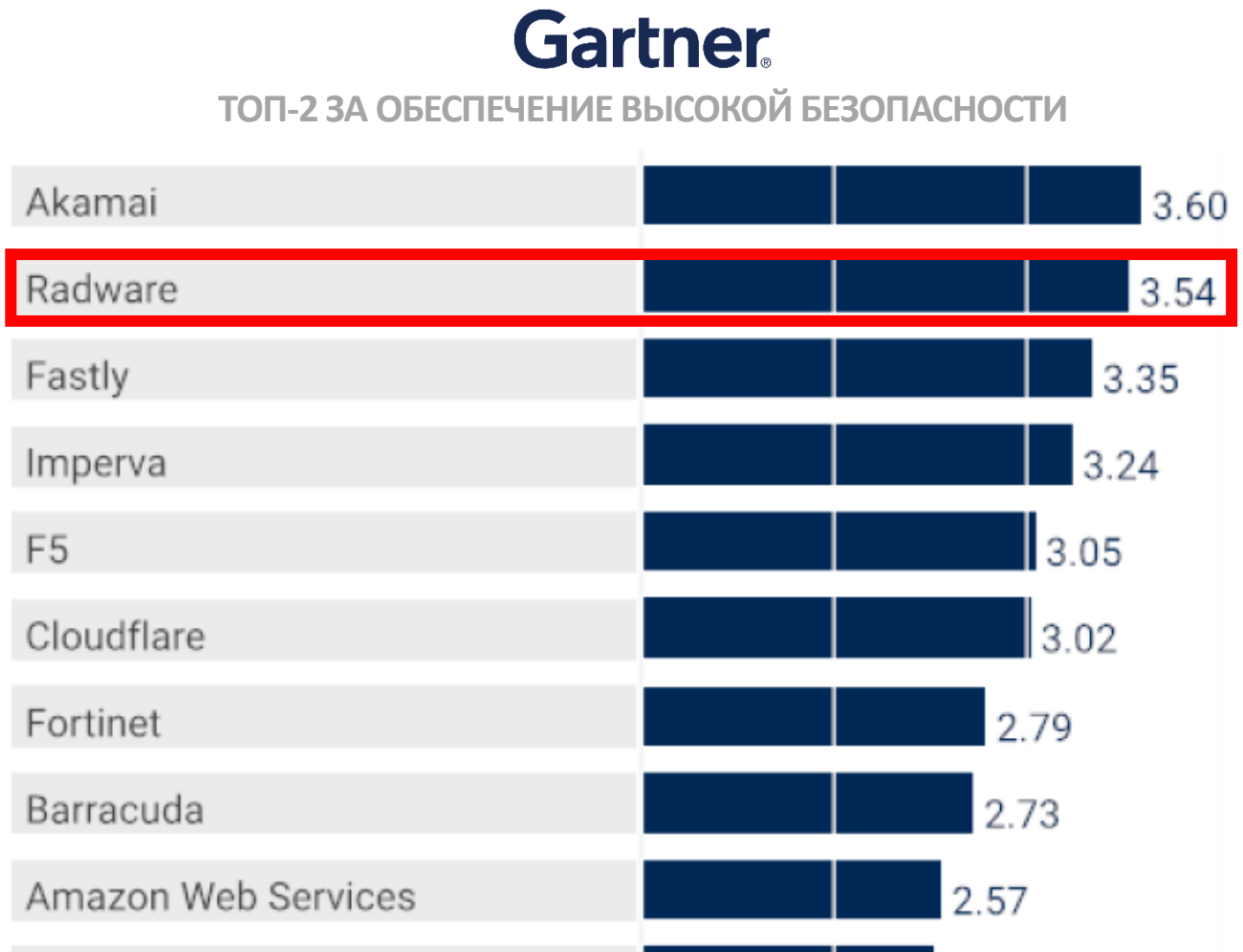
A zero-day vulnerability in the Spring Core Java framework that could allow for unauthenticated remote code execution (RCE) on vulnerable applications was publicly disclosed on March 30, before a patch was released. It was dubbed Spring4Shell.

WAF Radware блокирует Spring4Shell с первого дня!



Защита от уязвимостей Веб-приложений

Web Application Firewall (WAF)



Защищает веб-приложения

от взлома и эксплуатации уязвимостей

Полная защита OWASP Top 10

от взлома и эксплуатации

Позитивная модель безопасности

автоматически блокирует вредоносный трафик

Гибкие варианты развертывания

как управляемая облачная служба, виртуальное устройство, Kubernetes WAF или интегрированное с ADC

Что говорят о Radware клиенты

WAF

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

life:)

КЛИЕНТ №1 в Беларуси

Сертификация ОАЦ

Сертификация ОАЦ уже в процессе!

Ожидается получения сертификата уже в начале 2023 года.

Есть вопросы?
Хотите ДЕМО?

Пишите:

radware@outsourceit.by