
radware
Radware Application Protection
Cloud WAF, Bot, API, and DDoS Protection Services

About Radware

Frictionless Security at the Pace of Innovation

Over 12,500 Customers

Bank of America, E*TRADE, ING, Wells Fargo, ebay, STAPLES, Samsung SDS, Carlsberg Group, salesforce, twitter, SAP, AT&T, CATERPILLAR, verizon, Tech Mahindra

Analysts Praise Us

IDC Analyze the Future
DDoS MarketScape
#1 Leader

Gartner
#2 API & High Security
WAF Peer Insights
Customer Choice

FORRESTER
DDoS Wave Leader

Quadrant Knowledge Solutions
Bot Management **Leader**
DDoS Protection **Leader**

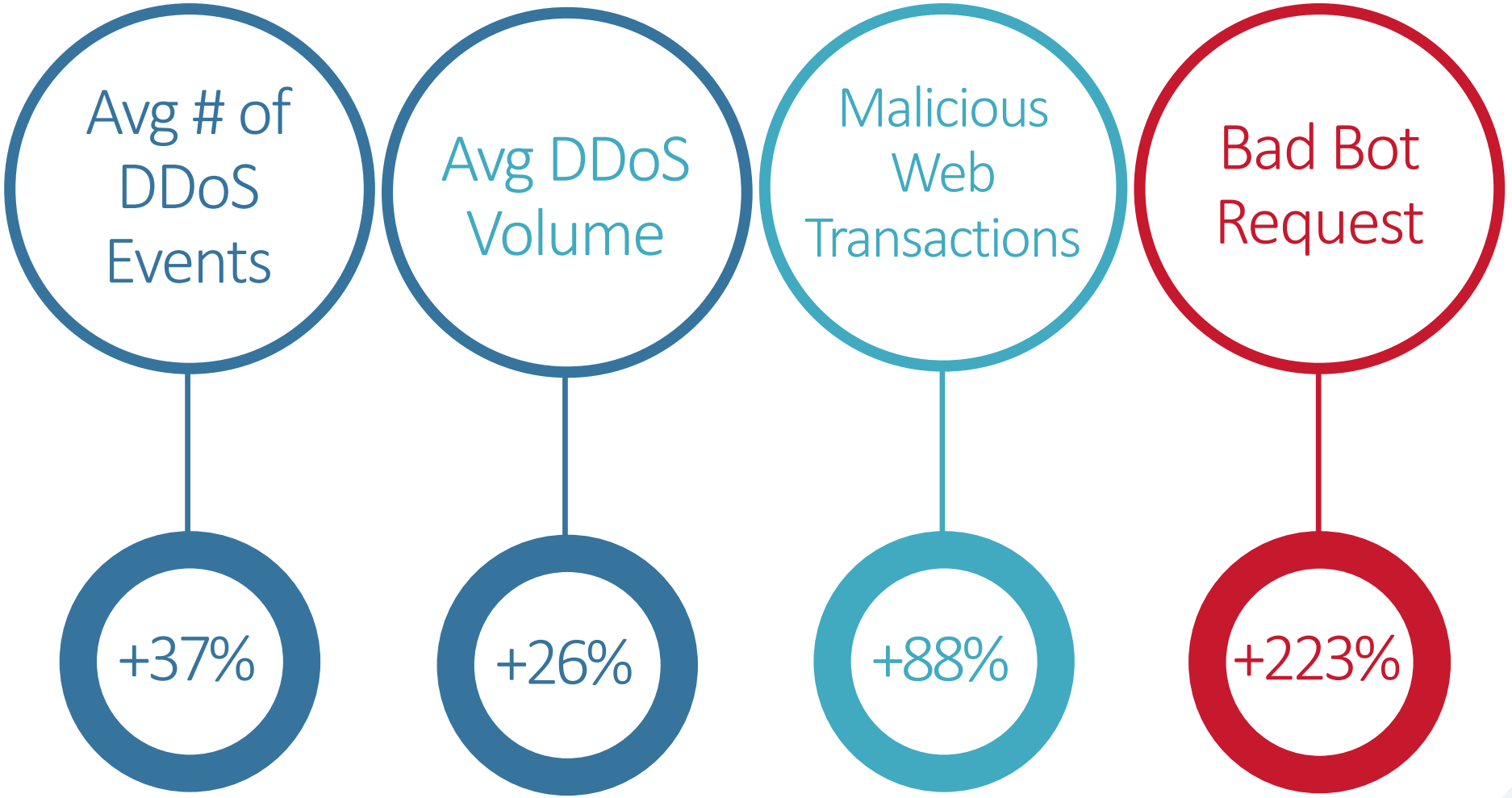
Our Partners

CISCO, CHECK POINT, NOKIA, aws, Microsoft Azure

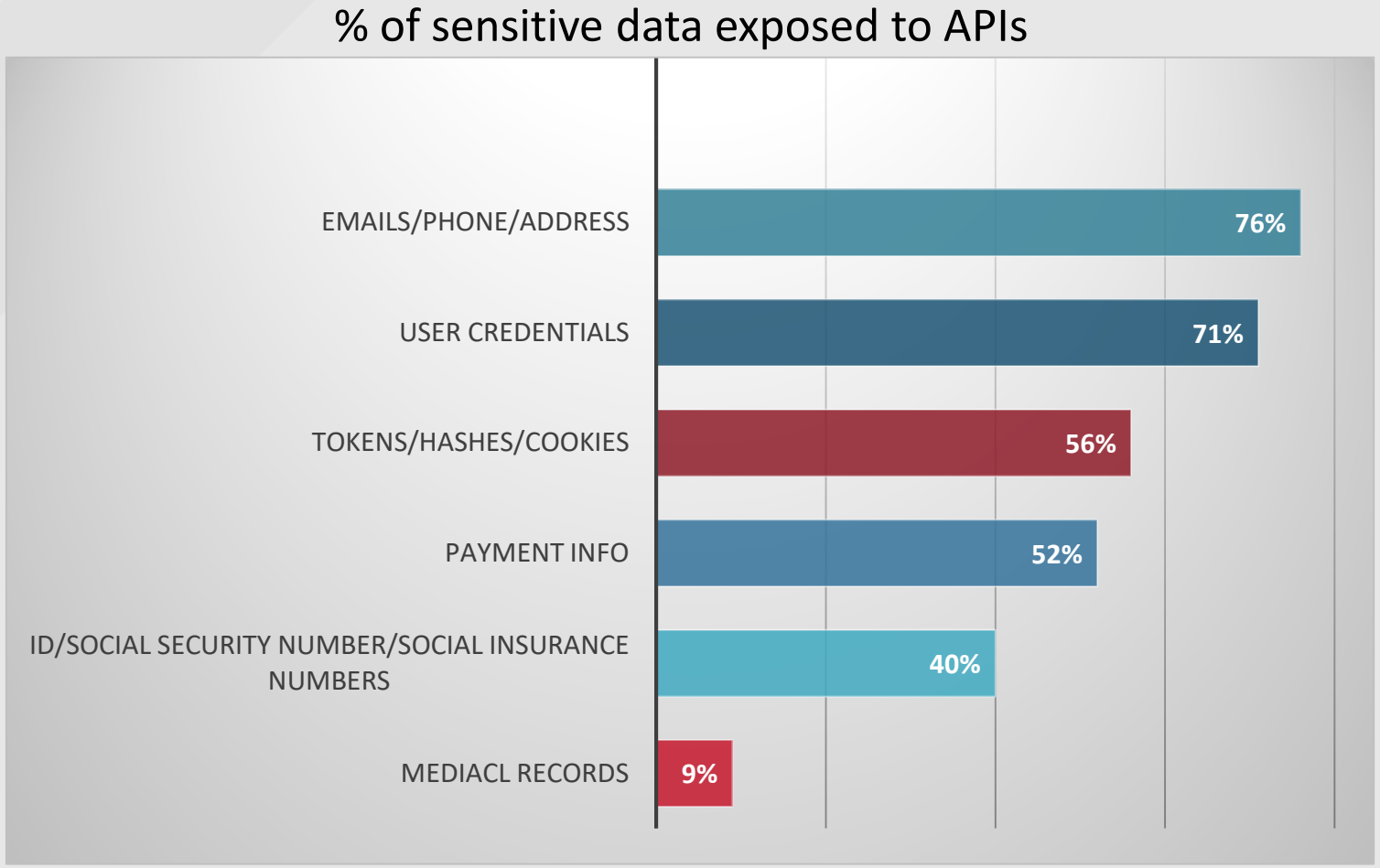
Application Security Challenges Are Growing

Attack Intensity Grows

2021 Year In Review



API PROTECTION – FASTEST GROWING CHALLENGE



** Source: Radware 2020-2021 Application Security Report*

#1 Threat

61% CONCERNED WITH BREACHES FROM APIS

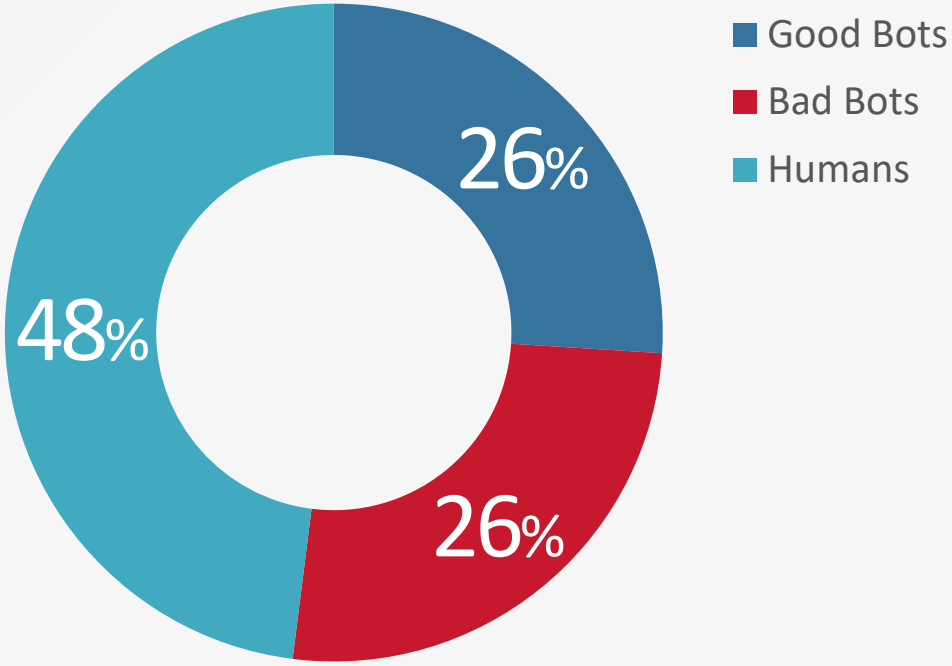
#1 Priority

55% SECURE THE APPLICATION AND API INFRASTRUCTURE

#1 App-Sec

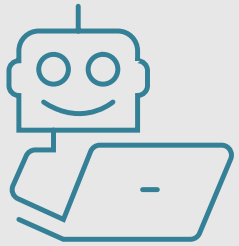
59% INVESTMENT AREA

Bots Are Taking Over the Internet



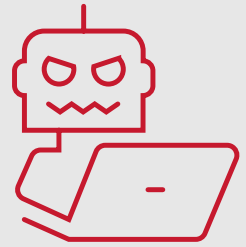
What Do Good Bots Do?

- Search engines
- Pricing services
- Web crawlers
- Fetchers



What Do Bad Bots Do?

- Web scraping
- Account takeover
- DDoS attacks
- Inventory holdups



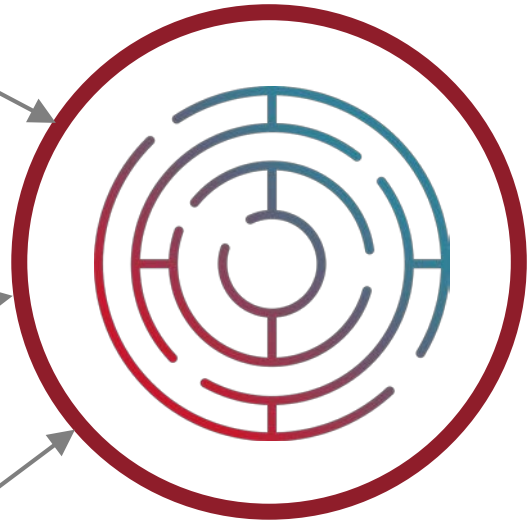
26% of the internet traffic is generated by **bad** bots

4 IN 5 orgs cannot distinguish between ‘good’ & ‘bad’ bots

Growing Complexity

Development and Delivery environments and processes create blind spots

- Continuous Delivery
- Distributed Information
- Frequent Changes



Greater Complexity

70% of applications undergo changes on a weekly basis

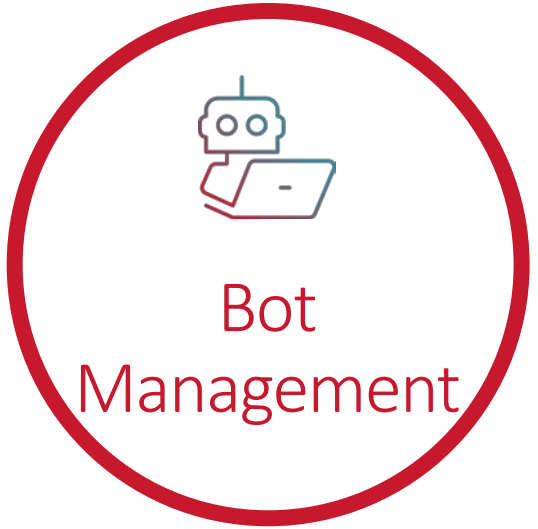
56% do not integrate security into their CI/CD pipeline

59% rank API protection as #1 app-sec priority for 2021

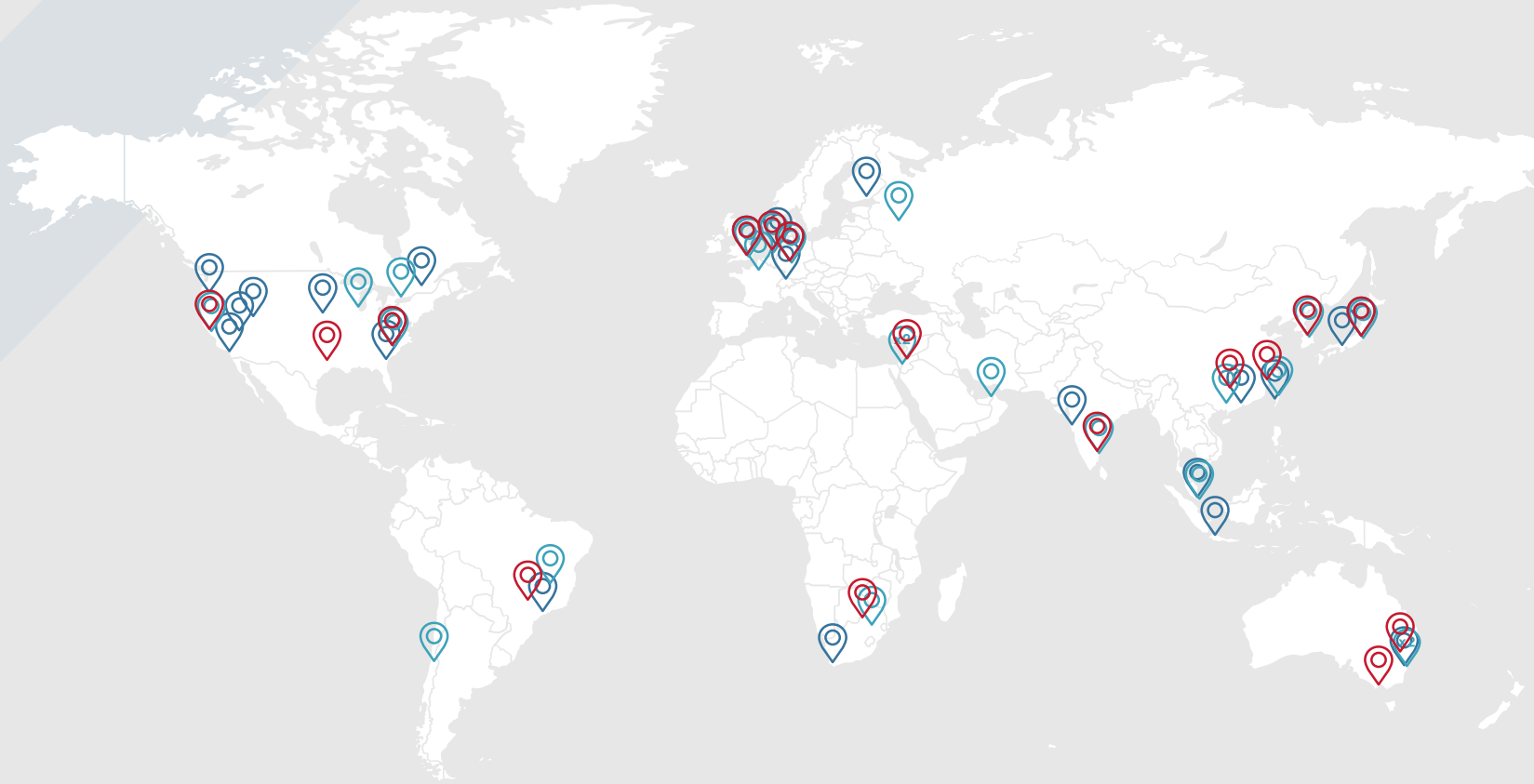
2/3 say the need for consistency and visibility are top concerns

Radware's State-of-the-Art, Frictionless Solution

One-Stop-Shop for All Your Application Security Needs



Global Cloud App Protection Network



16 SCRUBBING CENTERS Worldwide

10 Tbps OF GLOBAL MITIGATION CAPACITY

40+ AppSec PoPs WITH GLOBAL COVERAGE

DDoS MITIGATION SCRUBBING CENTER

CLOUD WAF PoP

BOT MANAGER SERVICE CENTER

Leading Global Service

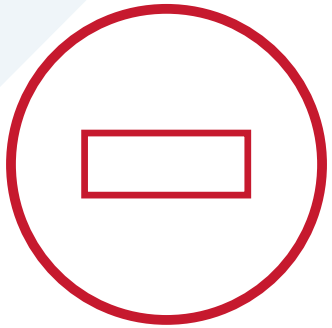
Fully Managed Security Service

Unmatched Compliance to Strictest Standards

Centralized Management with Actionable Analytics

Positive + Negative Security for Robust Application Protection

WAF



Negative Security Model

- Standard across most cloud WAF services and WAF technologies
- Blocks known attacks via known signatures and rules
- **Cannot provide FULL protection against OWASP TOP-10**
- **Cannot protect from unknown vulnerabilities: 0-day attacks**

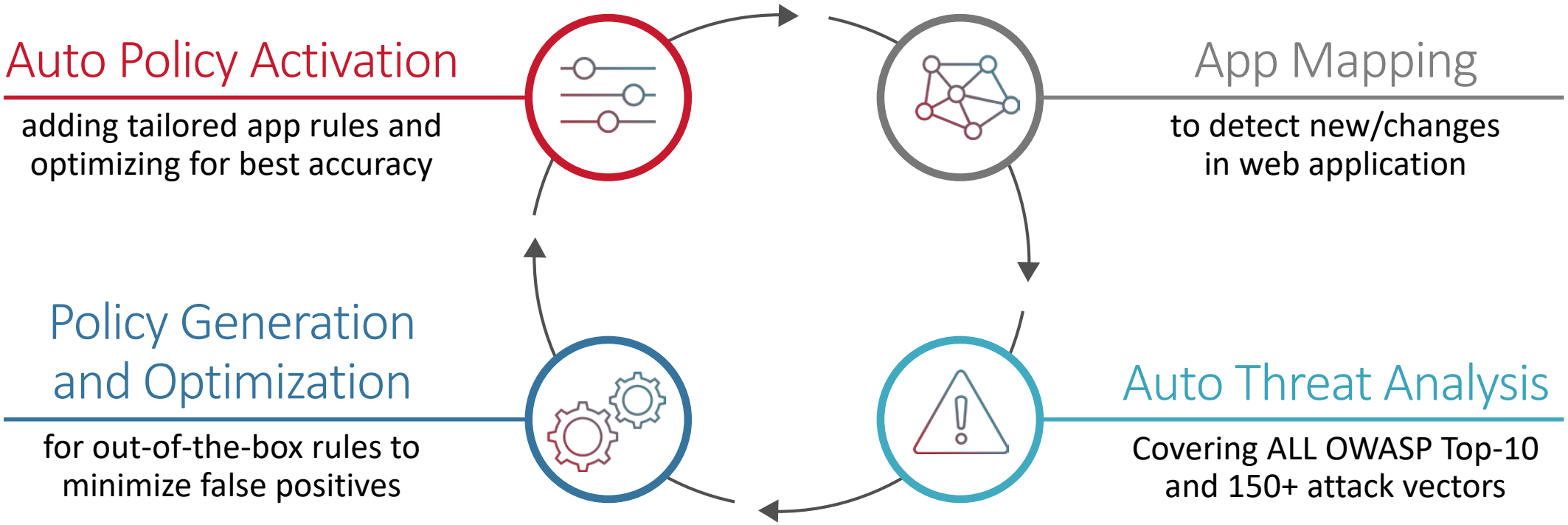
Positive Security Model

- Learns and defines what actions are legitimate traffic
- Blocks unauthorized access or actions that are not permitted
- **Uniquely protects from 0-day attacks and unknown vulnerabilities**
- **Higher layer of protection: FULL OWASP TOP-10 protection, minimum false-positives**

Automatic Policy Generation

Machine-learning Algorithms To Automatically Generate Policies

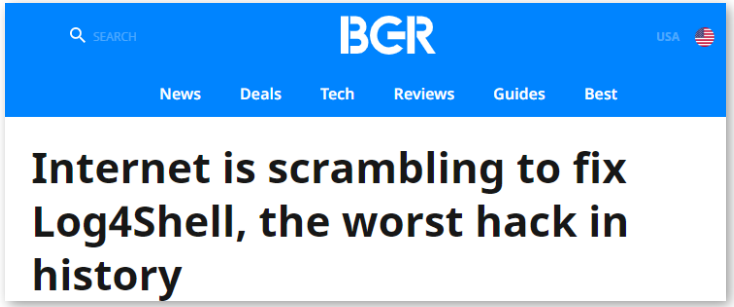
WAF



Continuously detect changes in the application and acceptable user behavior to keep protection current

Case study: Log4Shell Critical Vulnerability

CVE-2021-44228 in Log4j library



WAF

Radware WAF **DETECTS & BLOCKS** Log4Shell Activity **From Day 1**!

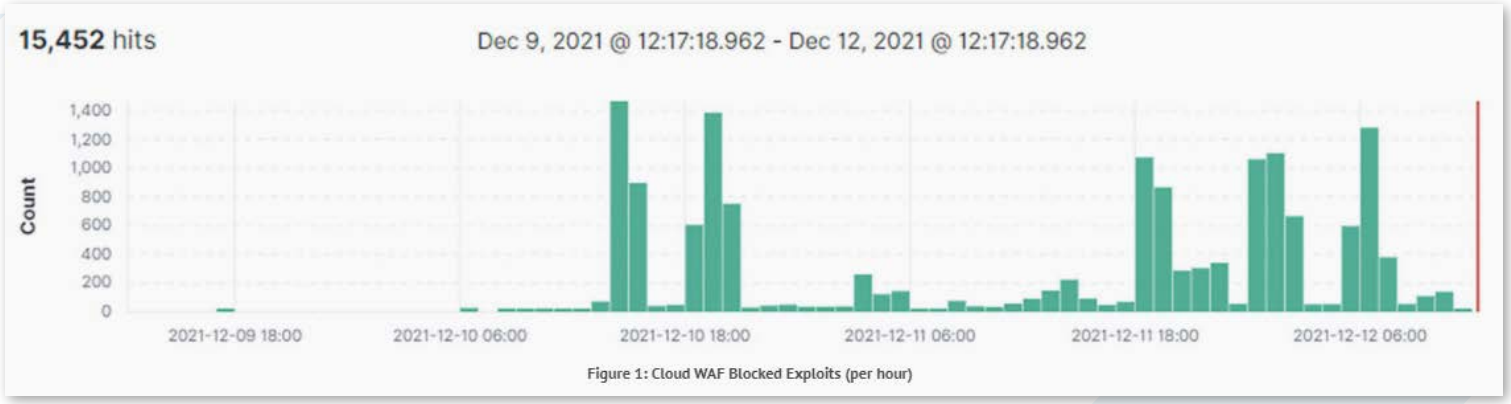


Figure 1: Cloud WAF Blocked Exploits (per hour)

Visibility: You Can Only Protect What You Know

API

APIs come in different forms

- Some APIs are documented
- Some APIs are undocumented
- Some APIs are from third parties
- Some APIs are unknown

- Is the Documentation accurate and up to date?
- How do you build protection rules for it?
- No documentation at all
- You are not even aware of this attack surface

OpenAPI Schema

API Discovery

Overcoming Challenges in Securing APIs

API

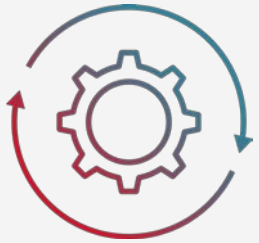
1

Visibility

Knowing what to protect

2

Automation



Updating and activating security policies

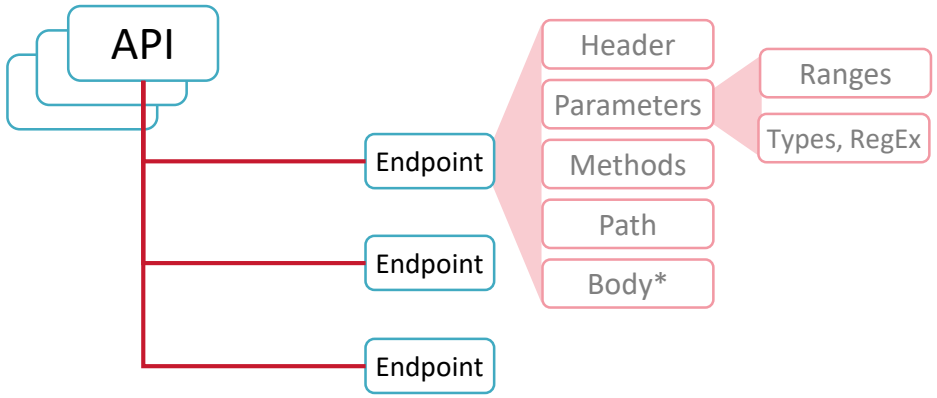
3

Protection

Protecting the entire API schema in all layers

Automation: From Discovery to Protection

Existence of APIs → Complete OpenAPI Schema File → Apply API Schema Protection



No Experts Required

END-TO-END AUTOMATION

Complete Protection Against API Attacks

Embedded Attacks

Discover API schema, and parse API calls to find embedded API attacks

BOT Attacks

Protect against ATO, scraping, and DDoS API bot attacks with Radware's Bot Manager

Zero-day Attacks

Positive security model enables protection against zero-day attacks

API Abuse

Manage quotas per API endpoint to ensure server resources aren't exhausted by malicious activities

Radware's Comprehensive API Protection Solution

Frictionless

No experts required
Easy onboarding
Easy ongoing maintenance

Complete

Protects the APIs you know & the APIs you don't know

Accurate

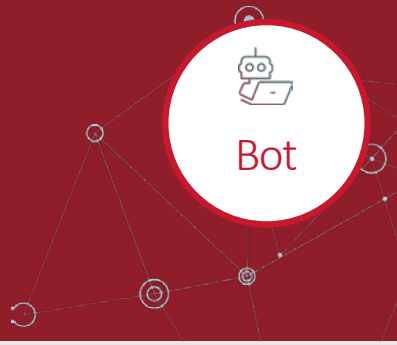
Auto discovery & schema file generation for protecting your entire API structure

Automated

Keeps up-to-date as your APIs evolve & when new APIs are added

Eliminating Bad Bots

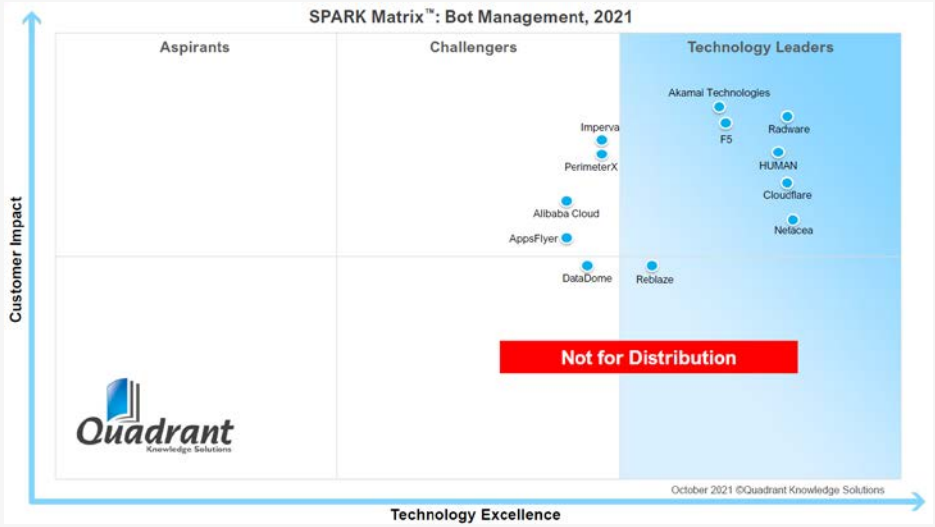
Bot Manager



Quadrant Knowledge Solutions

BOT MANAGEMENT, 2021

LEADER



Distinguishes between

Human and Bot Traffic

Protects Against Automated Attacks

such as web scraping, credential stuffing, and more

Improved detection with

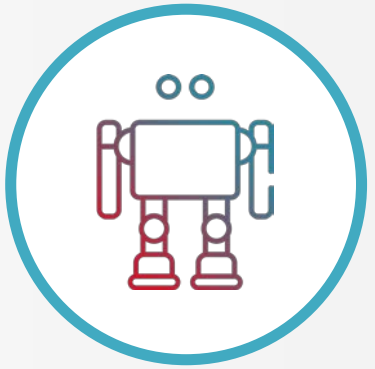
Semi-supervised Machine Learning

Flexible Deployment

as managed cloud service, local plugin,
or SDK plugin

Comparison of Bot Detection Capabilities

Bot

Bots	 Scripts	 Headless Browsers	 Human-like interaction	 Distributed attacks with advanced evasion
Technology	**Blacklists** IP, User Agent	**Device/Browser** Fingerprinting, JS, iFrame	**Interaction (shallow)** Behavioral Anomalies	**Intent (deep)** Correlation of Indicators based on big-data
				RADWARE

Protection from OWASP Automated Threats Top 21

Bot

ACCOUNT TAKEOVER

FAKE ACCOUNT CREATION

CARDING

GIFT CARD CRACKING

APPLICATION DDOS

DENIAL OF INVENTORY

AD FRAUD

API ABUSE

PRICE AND CONTENT SCRAPING

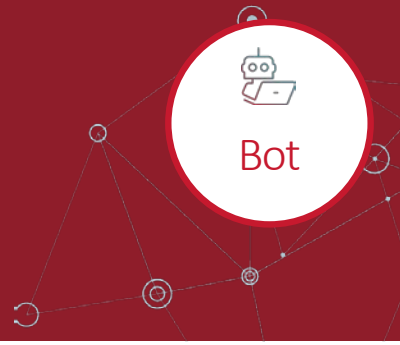
TICKET SCALPING

SKEWED ANALYTICS

FORM SPAM

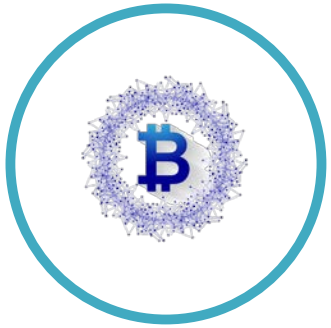
Best User Experience – CAPTCHA-less Bot Mitigation

Blockchain Crypto Challenge



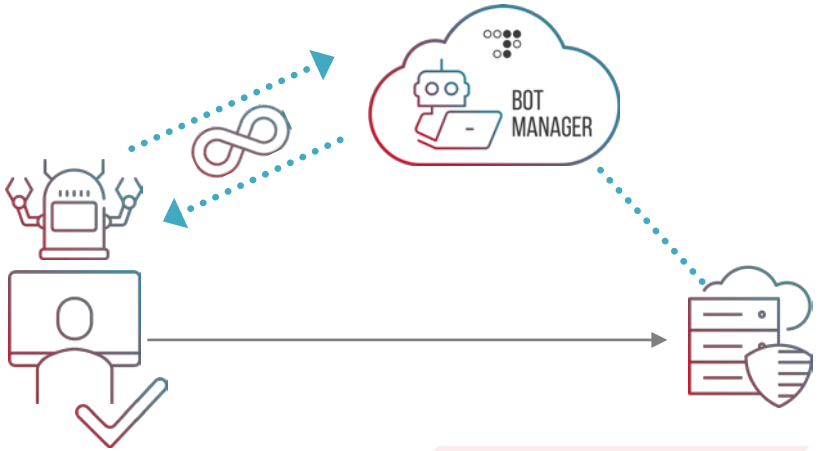
An Alternative to CAPTCHA – Why?

- Interactive challenge
- Binary determination
- Impact on UX
- CAPTCHA solving bots and CAPTCHA farms (e.g. 2captcha.com)



The Value of Blockchain

- No Impact on UX
- Continuous challenge, better protection
- Less frustration, less churn
- Keeps bots busy, makes them pay



Industry Leading Cloud DDoS Protection

DDoS

FORRESTER®

THE FORRESTER WAVE™
DDoS Mitigation
Solutions, Q1 2021

Behavioral-based Detection

distinguishes between legitimate and attack traffic

L7 DDoS Protection

against HTTPS floods, low-and-slow
and brute force attacks

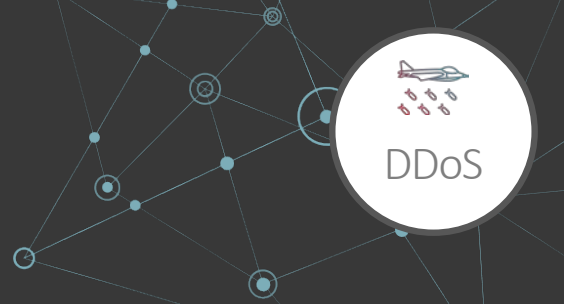
Flexible Deployment Options

as managed cloud service, virtual appliance,
or integrated with WAF

Industry-leading SLA

with 6 individual metrics

Protection Against Variety of L7 DDoS Attacks



HTTP/S Floods

SSL Negotiation Attack
(a.k.a. SSL Garbage Flood)

Slow HTTP/S
Read

Slow HTTP/S
Post

Bot / IoT
Attacks

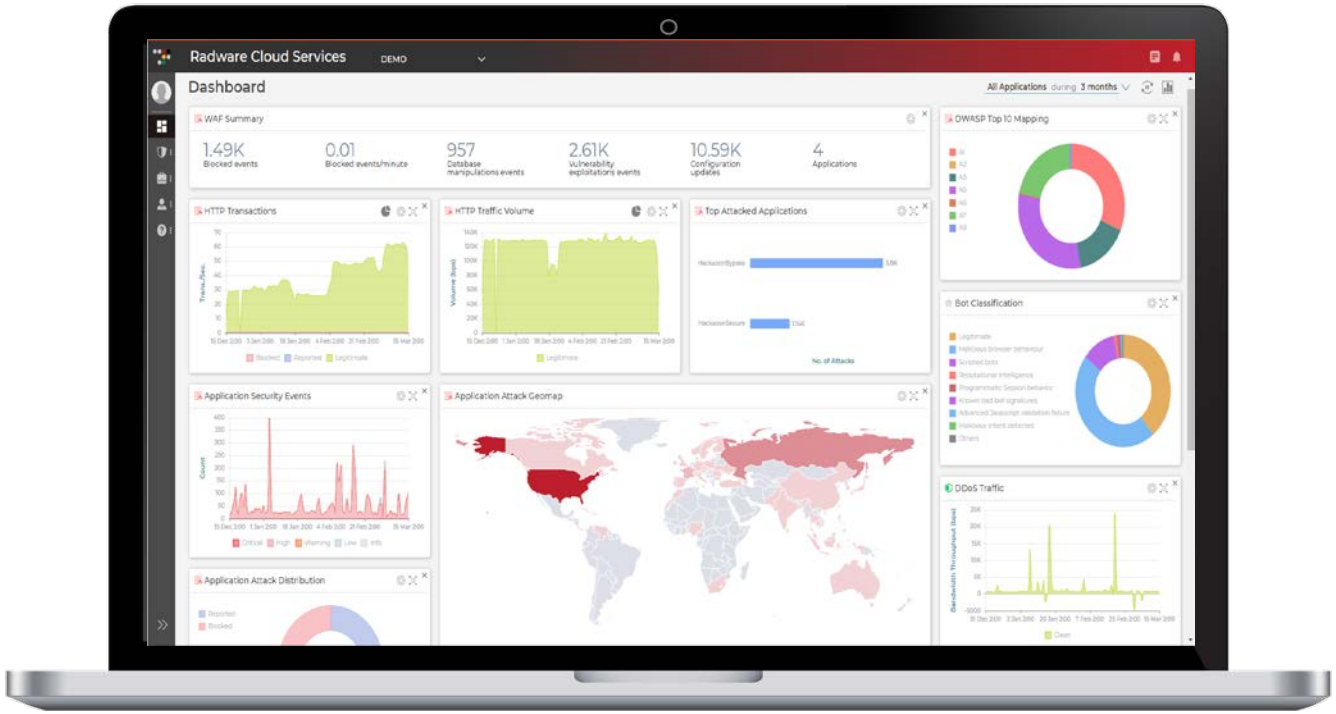
HTTP/S Bomb
(a.k.a. Large Payload Attack)

Large File Download
(a.k.a. Outbound Pipe
Saturation)

Application
Brute force

Centralized Cross-Cloud Visibility

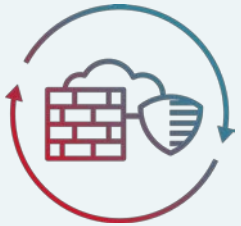
- Full visibility of all application security events, across all platforms
- Detailed reporting gives you full picture on every event
- Advanced analytics help you cut through the noise
- Single management interface for all applications regardless of where they are deployed



Summary

The Radware Advantage

Fully-Managed Cloud Web Application & API Protection Services



Complete Coverage

WAF, Bot Manager, API Protection & DDoS Mitigation

Faster Deployment

Automatic policy generation and optimization engine for continuous security

Reduced Overhead

Customer Success Management by application security experts

Greater Visibility

Advanced analytics & self-service capabilities

radware

Thank You!