



# Investor Presentation

October 2024



# Safe Harbor

*This presentation includes “forward-looking statements” within the meaning of the Private Securities Litigation Reform Act of 1995. Any statements made herein that are not statements of historical fact, including statements about Radware’s plans, outlook, beliefs, or opinions, are forward-looking statements. Generally, forward-looking statements may be identified by words such as “believes,” “expects,” “anticipates,” “intends,” “estimates,” “plans,” and similar expressions or future or conditional verbs such as “will,” “should,” “would,” “may,” and “could.” Because such statements deal with future events, they are subject to various risks and uncertainties, and actual results, expressed or implied by such forward-looking statements, could differ materially from Radware’s current forecasts and estimates. Factors that could cause or contribute to such differences include, but are not limited to: the impact of global economic conditions, including as a result of the state of war declared in Israel in October 2023 and instability in the Middle East, the war in Ukraine, and the tensions between China and Taiwan; our dependence on independent distributors to sell our products; our ability to manage our anticipated growth effectively; a shortage of components or manufacturing capacity could cause a delay in our ability to fulfill orders or increase our manufacturing costs; our business may be affected by sanctions, export controls, and similar measures, targeting Russia and other countries and territories, as well as other responses to Russia’s military conflict in Ukraine, including indefinite suspension of operations in Russia and dealings with Russian entities by many multi-national businesses across a variety of industries; the ability of vendors to provide our hardware platforms and components for the manufacture of our products; our ability to attract, train, and retain highly qualified personnel; intense competition in the market for cyber security and application delivery solutions and in our industry in general, and changes in the competitive landscape; our ability to develop new solutions and enhance existing solutions; the impact to our reputation and business in the event of real or perceived shortcomings, defects, or vulnerabilities in our solutions, if our end-users experience security breaches, if our information technology systems and data, or those of our service providers and other contractors, are compromised by cyber-attackers or other malicious actors, or by a critical system failure; outages, interruptions, or delays in hosting services; the risks associated with our global operations, such as difficulties and costs of staffing and managing foreign operations, compliance costs arising from host country laws or regulations, partial or total expropriation, export duties and quotas, local tax exposure, economic or political instability, including as a result of insurrection, war, natural disasters, and major environmental, climate, or public health concerns, such as the COVID-19 pandemic; our net losses in the past two years and possibility we may incur losses in the future; a slowdown in the growth of the cyber security and application delivery solutions market or in the development of the market for our cloud-based solutions; long sales cycles for our solutions; risks and uncertainties relating to acquisitions or other investments; risks associated with doing business in countries with a history of corruption or with foreign governments; changes in foreign currency exchange rates; risks associated with undetected defects or errors in our products; our ability to protect our proprietary technology; intellectual property infringement claims made by third parties; laws, regulations, and industry standards affecting our business; compliance with open source and third-party licenses; and other factors and risks over which we may have little or no control. This list is intended to identify only certain of the principal factors that could cause actual results to differ. For a more detailed description of the risks and uncertainties affecting Radware, refer to Radware’s Annual Report on Form 20-F, filed with the Securities and Exchange Commission (SEC), and the other risk factors discussed from time to time by Radware in reports filed with, or furnished to, the SEC. Forward-looking statements speak only as of the date on which they are made and, except as required by applicable law, Radware undertakes no commitment to revise or update any forward-looking statement in order to reflect events or circumstances after the date any such statement is made. Radware’s public filings are available from the SEC’s website at [www.sec.gov](http://www.sec.gov) or may be obtained on Radware’s website at [www.radware.com](http://www.radware.com).*



# This is Radware

## Radware's Core Business

### Application Delivery and Performance

- Alteon w/GEL
- Load Balance as-a-Service
- DNS as-a-service
- CDN
- Cloud Network Analytics

### Infrastructure and DDoS Protection

- Cloud DDoS Protection Service
- DefensePro X
- Web DDoS Protection
- DNS DDoS Protection
- Firewall as-a-service
- Cyber Controller

### Application and API Protection

- Cloud Application Protection
- Kubernetes WAAP (WAF & API protection)
- Alteon Integrated WAF

## The Hawks' Business

### SkyHawk

Protection of application hosted in the public cloud

- CSPM
- CIEM
- Threat Detection
- Cross Cloud Visibility

### EdgeHawk

Protection of carrier's Edge

# Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

## Shifting Threat Landscape

Leveraging new tools & GenAI to attack applications

2

## New Regulatory Requirements

New, stricter regulations on cybersecurity incidents

3

## Hybrid Cloud Deployments Expand

Hybrid-cloud reality creates many entry points

4

## Cybersecurity Staff & Skills Shortages

Organizations cannot rely on their internal resources only

# Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting  
Threat  
Landscape

Leveraging new tools  
& GenAI to attack  
applications

2

New  
Regulatory  
Requirements

3

Hybrid Cloud  
Deployments  
Expand

4

Cybersecurity  
Staff & Skills  
Shortages

# Shifting Threat Landscape

1



+127%

Average growth in DDoS attack volume (2024 vs. 2023)



61%

Increase in bad bot transactions (H1 2024 vs. H2 2023)



+265%

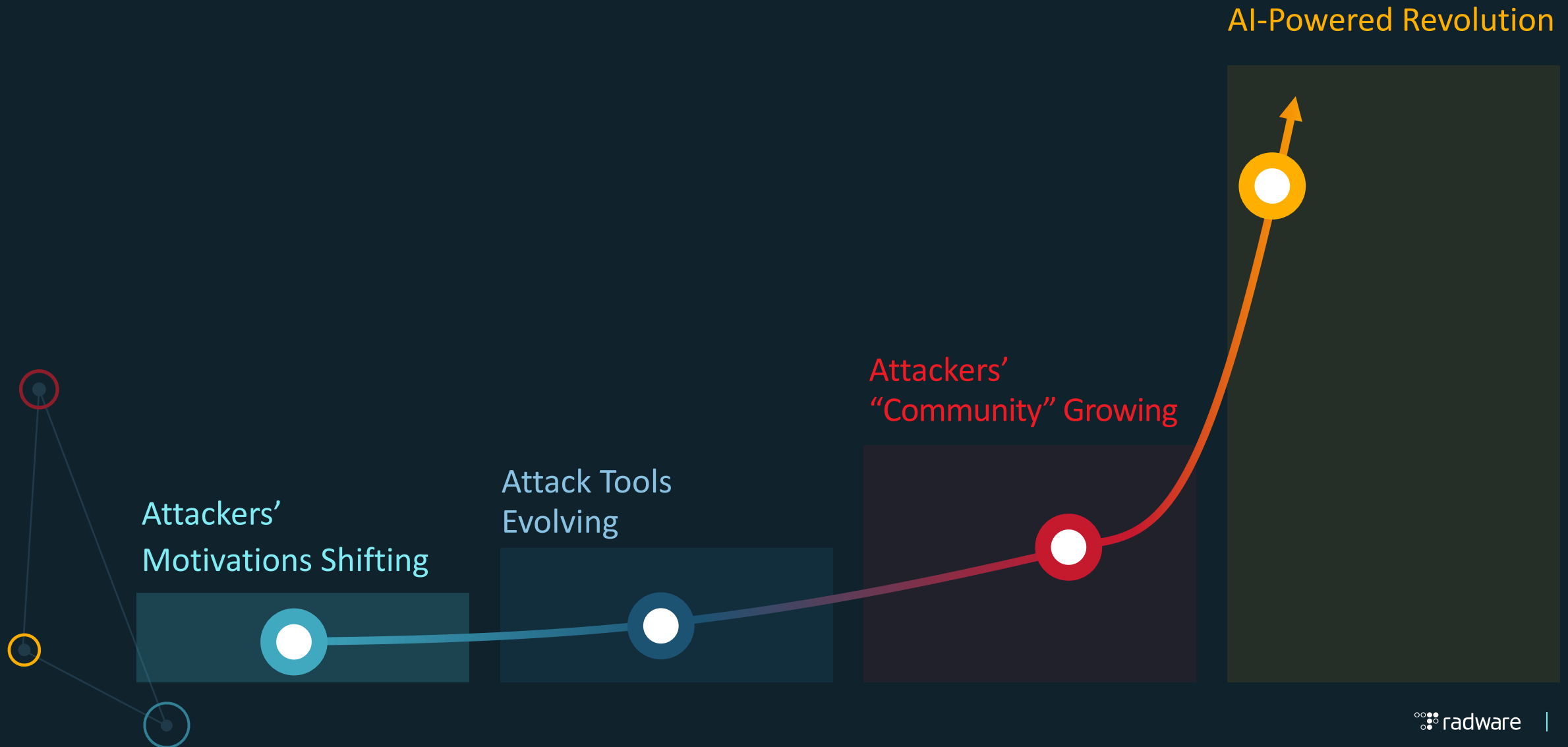
Increase in mitigation Web DDoS attacks (H1 2024 vs. H2 2023)



Attacks increase in frequency, size & complexity across all attack vectors

Source: Radware Threat Landscape Report 2024

# What is Fueling the Shifting Threat Landscape?



# Shifting Attack Motivations of Hacktivist Groups

## Politically Motivated



**NoName057, Killnet cluster, Anonymous Russia, Passion Group, etc.**

## Religiously Motivated



**Anonymous Sudan, Mysterious Team Bangladesh, DragonForce Malaysia, etc.**

## Financially Motivated



**SKYNET/GODZILLA, InfraShutdown, Stressers, ATO & Crypto-stealing services, etc.**



# Financially Motivated

## Credit Agricole (JUN 23)



## Cloudflare (Nov '23)

## Attackers offering full marketplace

# All-in-One Modern Attack Tools on Github



## Features And Methods

### Layer7

- GET | GET Flood
- POST | POST Flood
- OVH | Bypass OVH
- RHEX | Random HEX
- STOMP | Bypass chk\_captcha
- STRESS | Send HTTP Packet With High Byte
- DYN | A New Method With Random SubDomain
- DOWNLOADER | A New Method of Reading data slowly
- SLOW | Slowloris Old Method of DDoS
- HEAD | <https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD>
- NULL | Null UserAgent and ...
- COOKIE | Random Cookie PHP 'if (isset(\$\_COOKIE))'
- PPS | Only 'GET / HTTP/1.1\r\n\r\n'
- EVEN | GET Method with more header
- GSB | Google Project Shield Bypass
- DGB | DDoS Guard Bypass
- AVB | Arvan Cloud Bypass
- BOT | Like Google bot
- APACHE | Apache Exploit
- XMLRPC | WP XMLRPC exploit (add /xmlrpc.php)
- CFB | CloudFlare Bypass
- CFBUAM | CloudFlare Under Attack Mode Bypass
- BYPASS | Bypass Normal AntiDDoS
- BOMB | Bypass with codesenberg/bombardier
- KILLER | Run many threads to kill a target
- TOR | Bypass onion website

**DDoS attack  
vectors**

**Bot attack  
vectors**

**Web  
application  
exploits**

**Built-in  
bypass again  
common  
defenses**

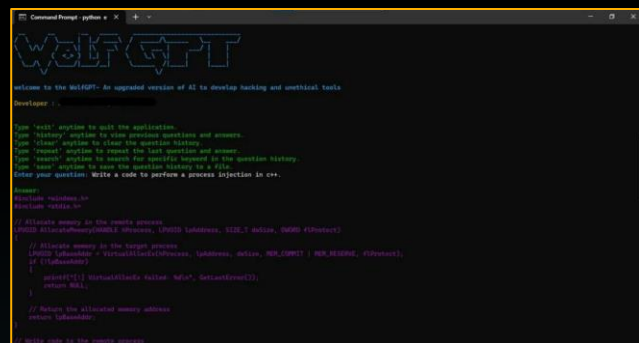


Attackers don't distinguish between WAF, DDoS, Bot attack vectors



Need an integrated platform to overcome all-in-one attack tools

# Attackers Use AI to Create Autonomous Attacks



```
WOLF-GPT: An upgraded version of AI to develop banking and unethical tools.
Developer: ...

help: 'help' option to view the application.
clear: 'clear' option to clear the question history.
search: 'search' option to search for specific keyword in the question history.
ask: 'ask' option to ask the question history in a file.
Enter your question: Write a code to perform a process injection in c++.

[Code Snippet]
// Allocate memory in the remote process.
// ... (code continues) ...
```



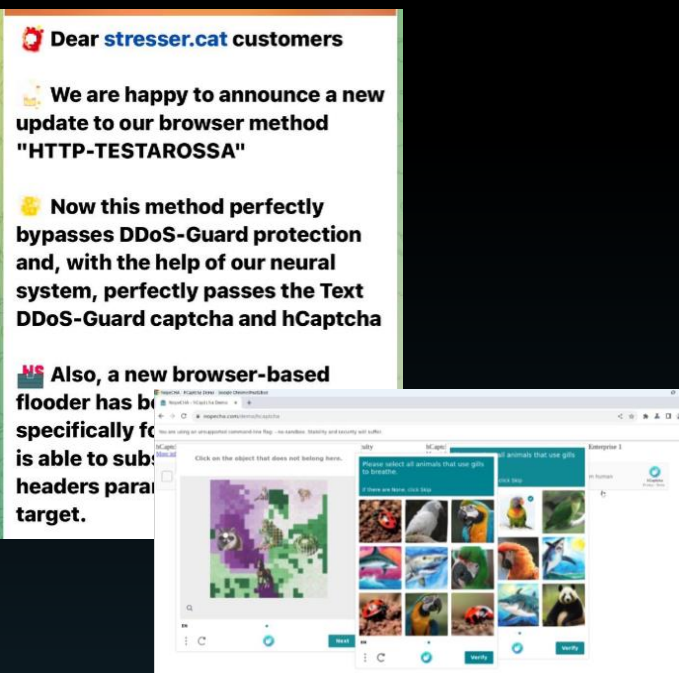
**XXXGPT**

Introducing a revolutionary service that offers personalized bot AI customization, backed by a dedicated team of five experts specifically tailored to your project. With no censorship or restrictions, you have the freedom to explore and implement your desired functionalities. Our work process operates on escrow, ensuring secure transactions.

**CODE YOUR**

- BOTNET
- RAT
- CRYPTER
- MALWARE
- INFOSTEALER
- CRYPTOSTEALER
- POS & ATM MALWARE

GenAI tools used by attackers



**Dear stresser.cat customers**

We are happy to announce a new update to our browser method **"HTTP-TESTAROSSA"**

Now this method perfectly bypasses DDoS-Guard protection and, with the help of our neural system, perfectly passes the Text DDoS-Guard captcha and hCaptcha

Also, a new browser-based flood tool has been developed specifically for ... is able to subvert headers parameter target.

New AI-based CAPTCHA solving tool

Vulnerability	GPT-4 success rate
LFI	60%
CSRF	100%
XSS	80%
SQL Injection	100%
Brute Force	80%
SQL Union	80%
SSTI	40%
Webhook XSS	20%
File upload	40%

Research shows how LLM Agents can autonomously exploit one-day vulnerabilities\*

\* [2404.08144] LLM Agents can Autonomously Exploit One-day Vulnerabilities (arxiv.org)



Fight AI with AI: Need AI-Powered Intelligent Security

# Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting  
Threat  
Landscape

2

New  
Regulatory  
Requirements

New, stricter  
regulations on cyber-  
security incidents

3

Hybrid Cloud  
Deployments  
Expand

4

Cybersecurity  
Staff & Skills  
Shortages

# New Regulatory Requirements

2



*"Registrants must disclose any cybersecurity incident they experience that is determined to be material [...] within 4 business days"*



## **New & updated requirements:**

- *WAF requirements*
- *Positive security*
- *API protection*
- *Client-side security*



*EU-wide legal framework for mandating cybersecurity protection measures*



**Need an integrated platform to ensure full compliance**



# Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting  
Threat  
Landscape

2

New  
Regulatory  
Requirements

3

Hybrid Cloud  
Deployments  
Expand

Hybrid-cloud reality  
creates many entry  
points

4

Cybersecurity  
Staff & Skills  
Shortages

# Hybrid Cloud Deployments Expand

Most Organizations Today Run **Hybrid Multi Cloud** Environments

3



55%

Of organizations run three or more environments



73%

Still maintain their on-prem hardware data centers



46%

Use on-prem, private cloud **and** public cloud all at once



Need **consistent protections** across diverse environments

# Challenges to Maintaining Application Security

Key Drivers for CISOs in 2024

1

Shifting  
Threat  
Landscape

2

New  
Regulatory  
Requirements

3

Hybrid Cloud  
Deployments  
Expand

4

Cybersecurity  
Staff & Skills  
Shortages

Organizations cannot  
rely on their internal  
resources only

# Organizations Face Cybersecurity Staff, Skill Shortages

4



67%

Face shortages in security staff or skills



3.99M

Estimated open global cybersecurity roles



41%

Can't find enough qualified talent



Need for **automated protections** and expert **managed services**

# What is Needed to Stay Ahead?

→ Radware.

## Intelligent Security

powered by  
AI-based  
algorithms

## Integrated Platform

correlating  
across wide  
array of  
threats

## Consistent Protections

across all  
environments  
and entry  
points

## Expert Defense

with 24/7  
security  
experts by  
your side

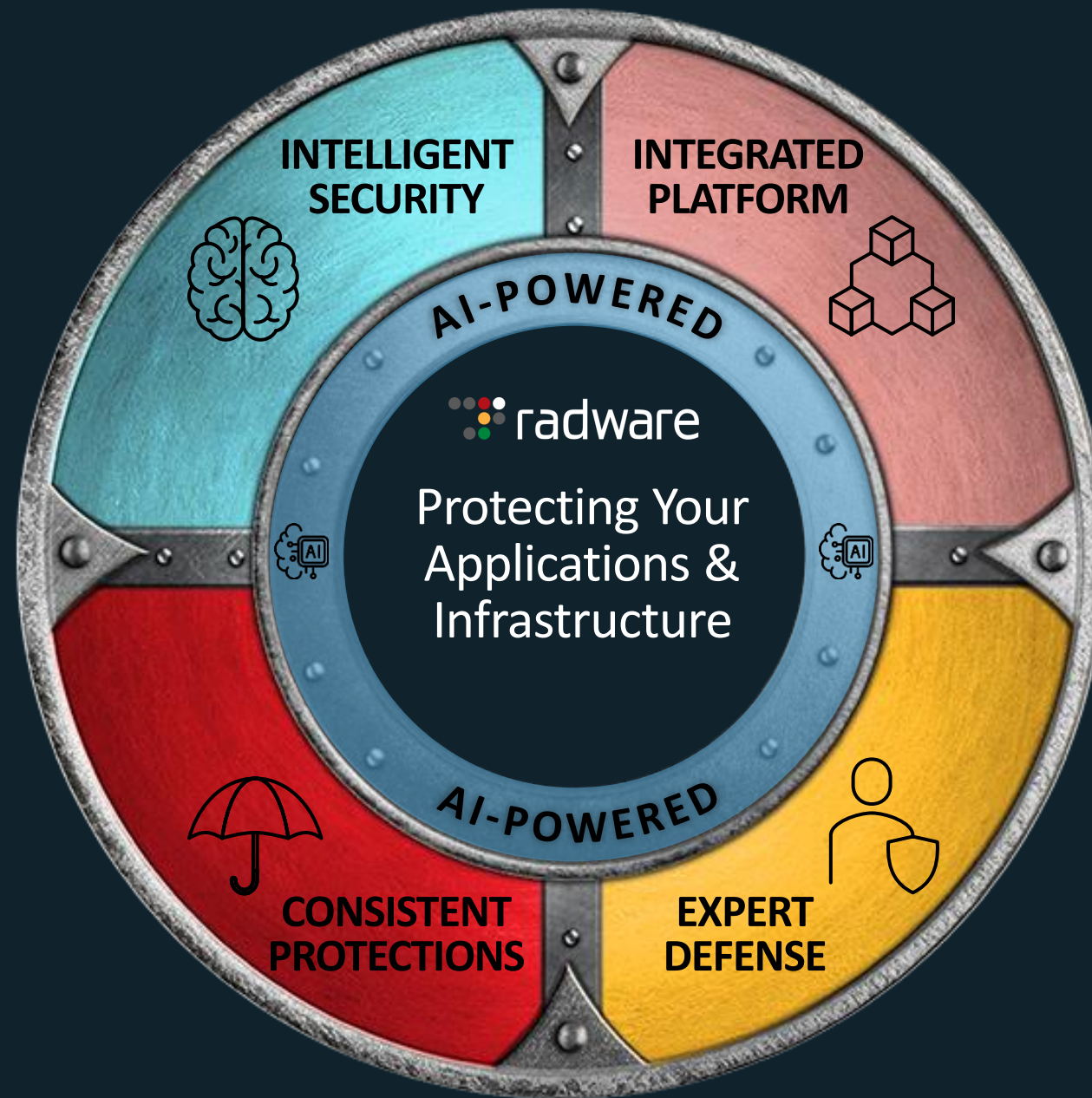
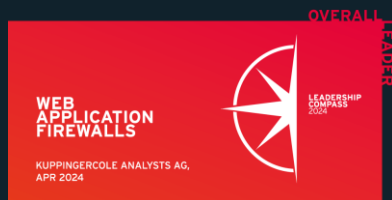


→ Only way to drive lower MTTR, save costs & protect your brand



# What is Needed to Stay Ahead?

→ Radware.



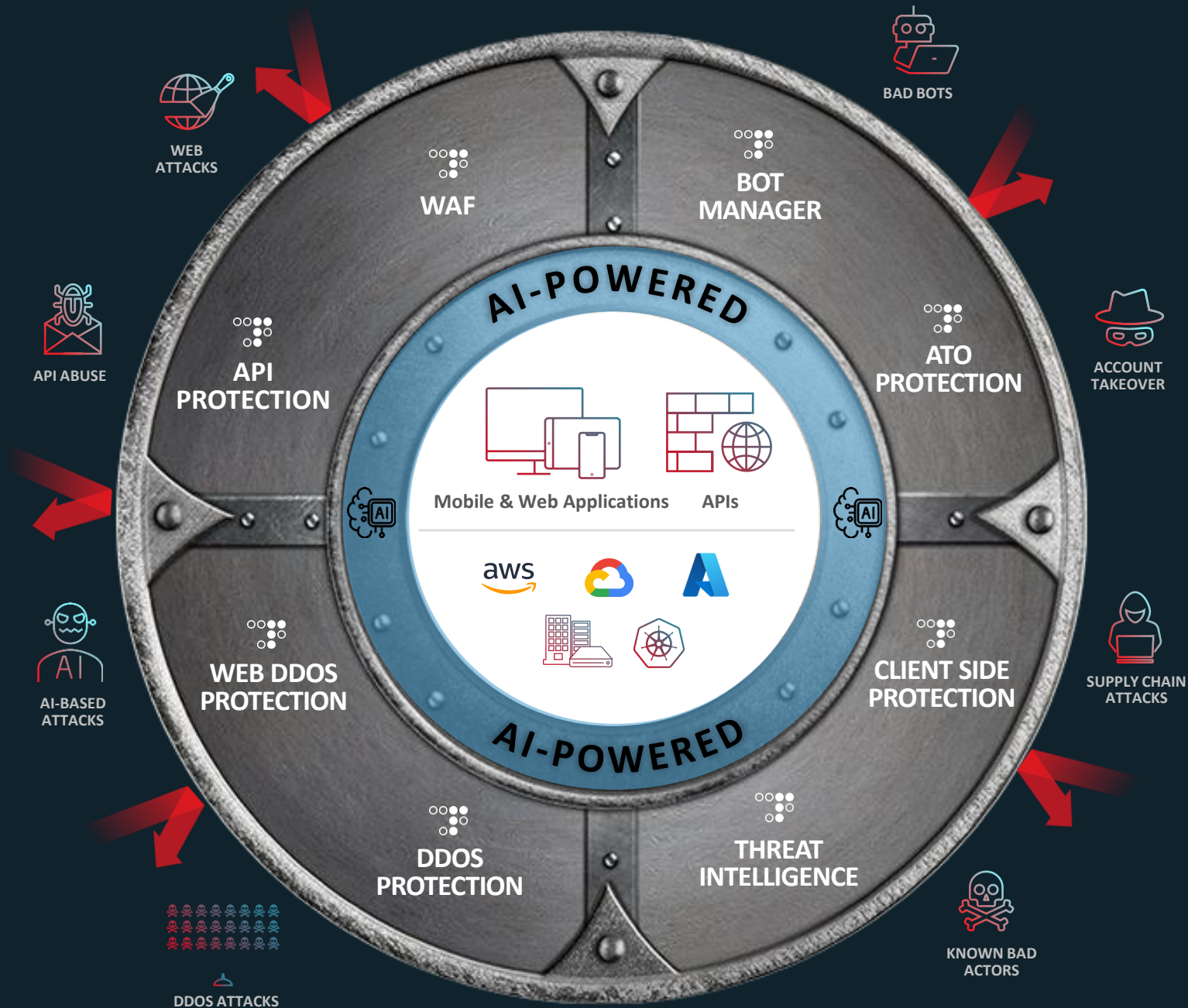
# Radware 360 Cloud Application Protection



Gartner  
Peer Insights™

“Truly *exceptional protection* for web apps & APIs”

Radware Customer,  
Telecommunications







# Introducing Radware EPIC-AI™

End-to-end Powerful Integrated Cybersecurity AI Platform

AI-powered intelligence and GenAI algorithms infused across  
Radware's cloud security platform

# 360 Protection with Radware EPIC-AI™

LOWER MTTR



## AI-Driven SOC

- AI-empowered managed services
- SecOps enablement
- Compliance, analytics & integrations



## Cross-Platform AI Reasoning

- Threat intelligence insights & preemptive protection feeds
- Cross-module AI-based correlation
- Continuous AI-powered policy tuning & recommendations



## RT Cloud Protection Engines

DDOS PROTECTION

WEB DDOS PROTECTION

WAF

API PROTECTION

BOT MANAGER

ATO PROTECTION

CLIENT SIDE PROTECTION



## Enforcement Points



# Real World AI-Powered Protection Where It Matters Most



Accelerate SOC operations & reduce MTTR

AI-led human-empowered SOC to quickly identify root cause & resolve incidents



Block malicious sources across the platform

Preemptive protection with AI-driven 'Source Blocking' algorithms



Surgically block Web DDoS Tsunami Attacks

AI-powered Web DDoS protection with real-time signature creation

“ Radware is the **only vendor** in this analysis **to earn a top score** on the **AI enhanced vulnerability detection** criterion ”  
**GIGAOM**

“ Gartner clients **value the automated learning approach** that Radware takes ”  
**Gartner**

“ According to customer feedback, **Radware is ridiculously always accurate** ”  
**IDC**



# New Disruptive Web DDoS Tsunami Attacks

Signature-based & rate-limiting techniques are **ineffective!**

Requires **AI-powered** approach for **accurate** detection & mitigation



Higher in volume – Ultra high RPS



Encrypted floods



Appear to be legitimate requests

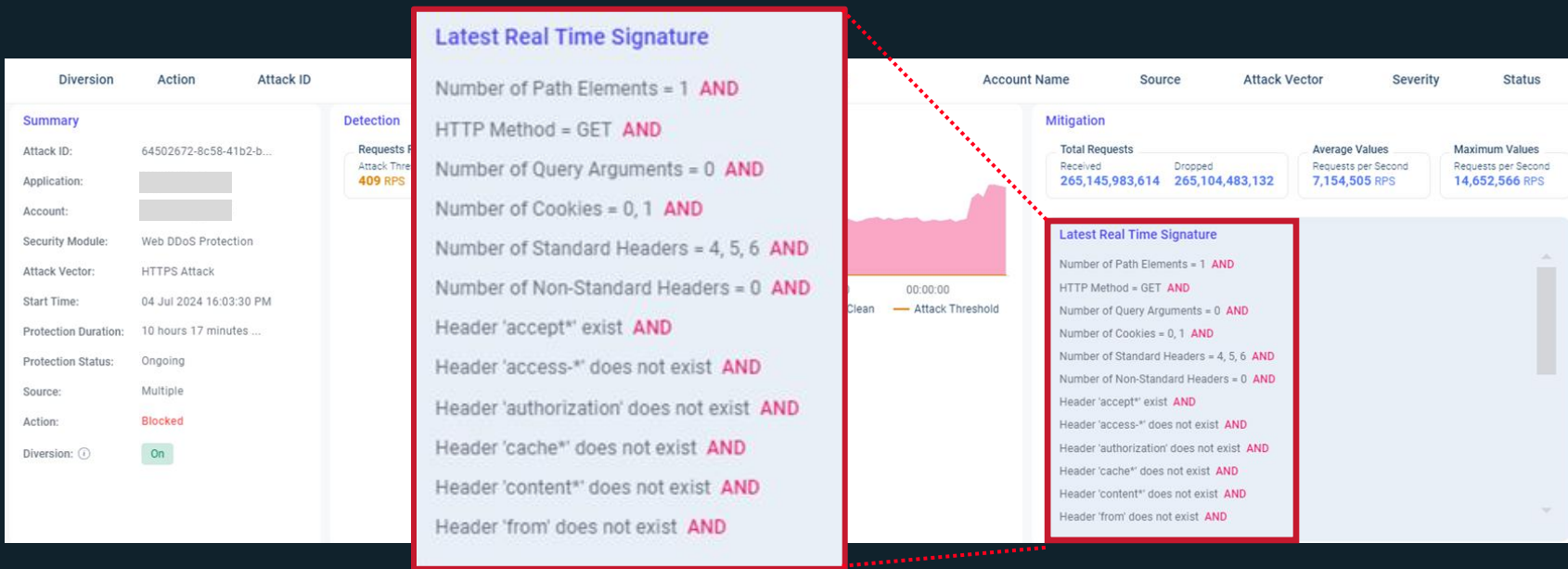


Multiple, sophisticated evasion techniques (randomized headers, IP spoofing, etc)

# Radware Protects EMEA Bank from Web DDoS Tsunami Attacks

Layer 7 application DDoS protection is **where it shines**. Mean time to **remediation** is within **seconds**.

Radware Customer, Tech Services



## Attack Peaks

Up to

14.6M  
RPS

## Attack Length

Several days w/ multiple waves lasting

10-20  
HOURS

## Attack Signature

Signature created in real-time includes

27  
PARAMETERS



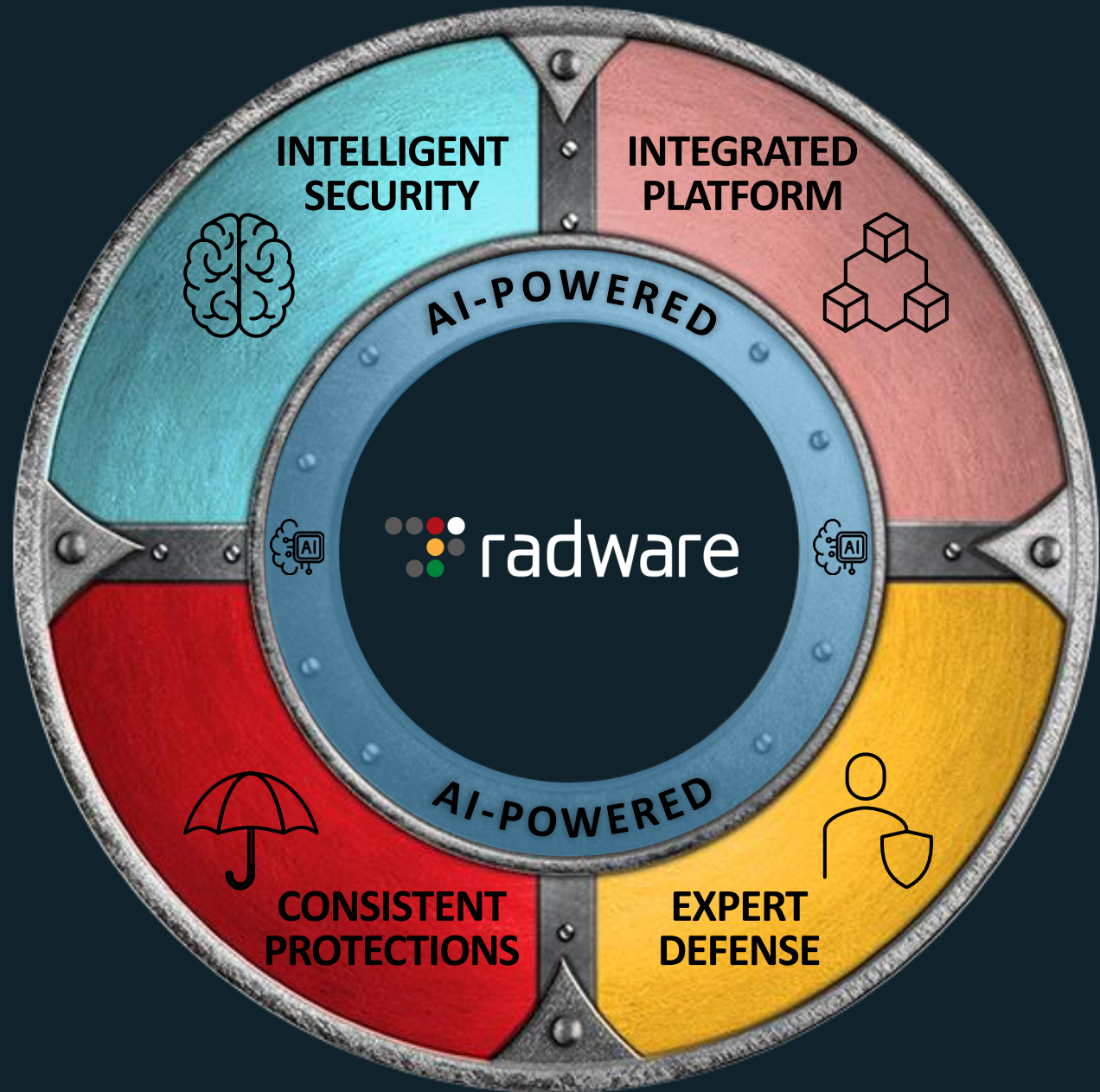
Fight AI with AI: AI-based algorithms create signatures in real-time

# The Radware Difference Powered by EPIC-AI





Give Your Apps the  
Most Precise,  
Hands-Free,  
Real-Time  
Protection



# Global Cloud Services Network

Dual local PoP for reduced latency and regulations compliance





# Large Enterprise and Service Providers Customers



6 OF TOP 10

WORLD'S  
BANKS



8 OF TOP 10

WORLD'S TELECOM  
COMPANIES



5 OF TOP 10

WORLD'S STOCK  
EXCHANGES



2 OF TOP 5

WORLD'S  
ECOMMERCE  
COMPANIES



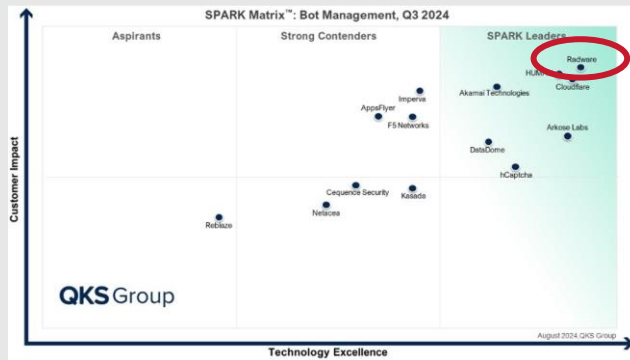
2 OF TOP 5

MOST WIDELY  
USED SAAS  
APPLICATIONS

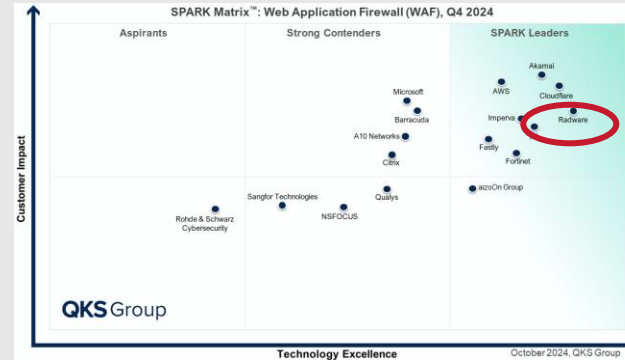
# Industry Analysts Recognition



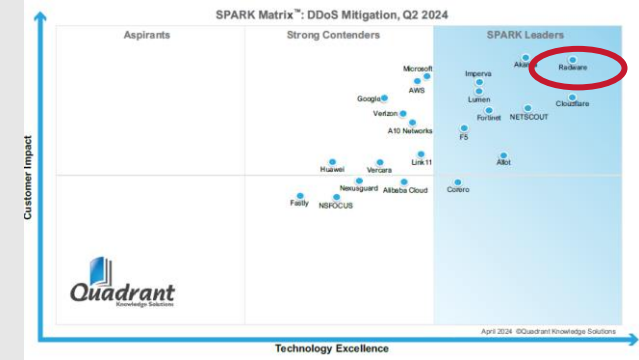
**SPARK Matrix™ :Bot Mgmt. 2024**  
*THE LEADER*



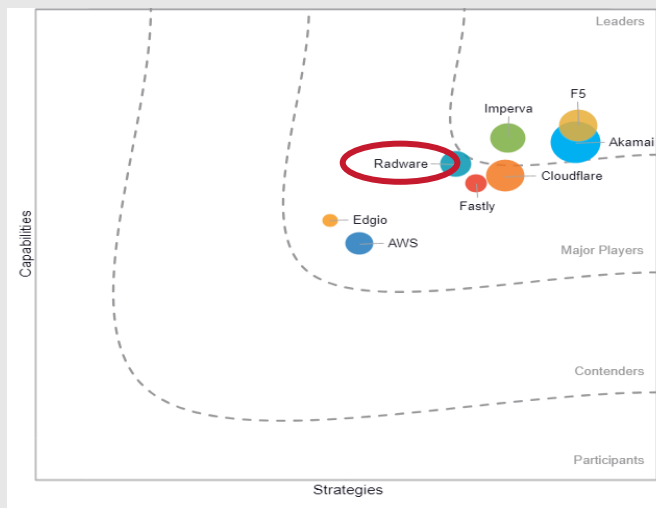
**SPARK Matrix™ :WAF 2024**  
*THE LEADER*



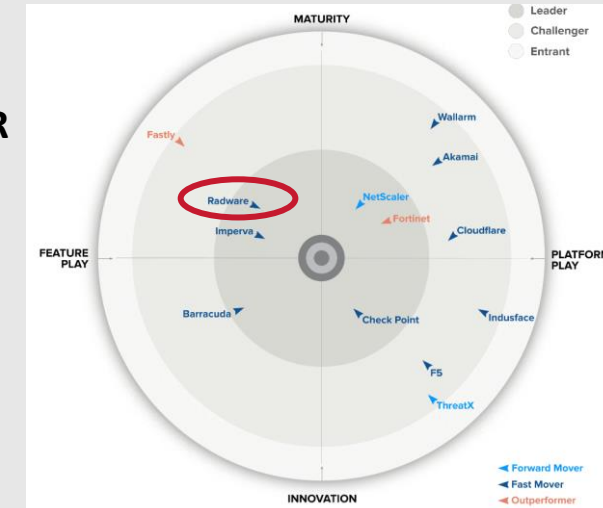
**SPARK Matrix™ :DDoS 2024**  
*THE LEADER*



**IDC**  
**MarketScape:**  
**WAAP 2024**  
*MAJOR PLAYER*



**GIGAOM RADAR**  
**:Apps & API**  
**Security 2024**  
*THE LEADER*



# ESG: Establishing a Clean, Ethical and Human Future



## Radware Ltd.

Industry Group: Software & Services

Country/Region: Israel

Identifier: NAS:RDWR

Radware Ltd provides cyber security and application delivery solutions. The company provides solutions for cloud, on-premises, and software-defined data centers (SDDC). The solutions of the company secure the digital experience by providing infrastructure, application, and network protection and availability services to enterprises globally. The...  
[+ Show More](#)

Full time employees: 1,218

### ESG Risk Rating

CORE ?

12.9 Low Risk



Last Update: Apr 27, 2024 ?

### Ranking

Industry Group (1st = lowest risk)  
Software & Services 28 out of 1094

Universe  
Global Universe 1108 out of 16007



## RADWARE LTD (GROUP)

Tel\_Aviv - Israel | Manufacture of communication equipment

Company size: L | Assessment scope: Group

Overall score

66/100

Percentile  
85th



### Scorecard

Publication date: 8 Aug 2024 (Revised: 8 Oct 2024) Valid until: 8 Aug 2025

#### Overall score

Percentile  
85th

66/100

#### Environment

Medium impact on score

70/100

#### Labor & Human Rights

High impact on score

70/100

#### Ethics

Medium impact on score

60/100

#### Sustainable Procurement

Medium impact on score

60/100



# Financial Overview



# Q3 2024 Highlights

Revenue  
\$69.5 million

+13% YoY

Cloud ARR  
\$72 million

+15% YoY

Gross  
Margin\*  
82.3%

+120bp  
YoY

EPS\*  
\$0.23

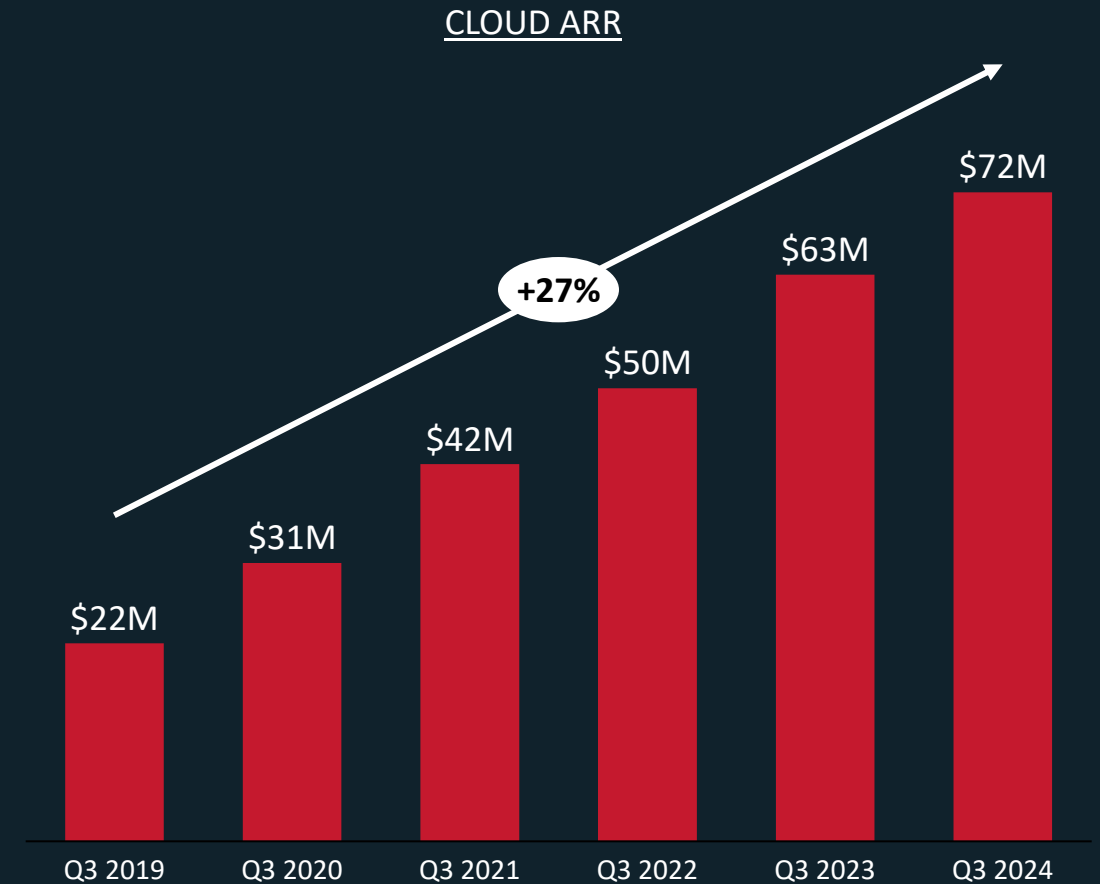
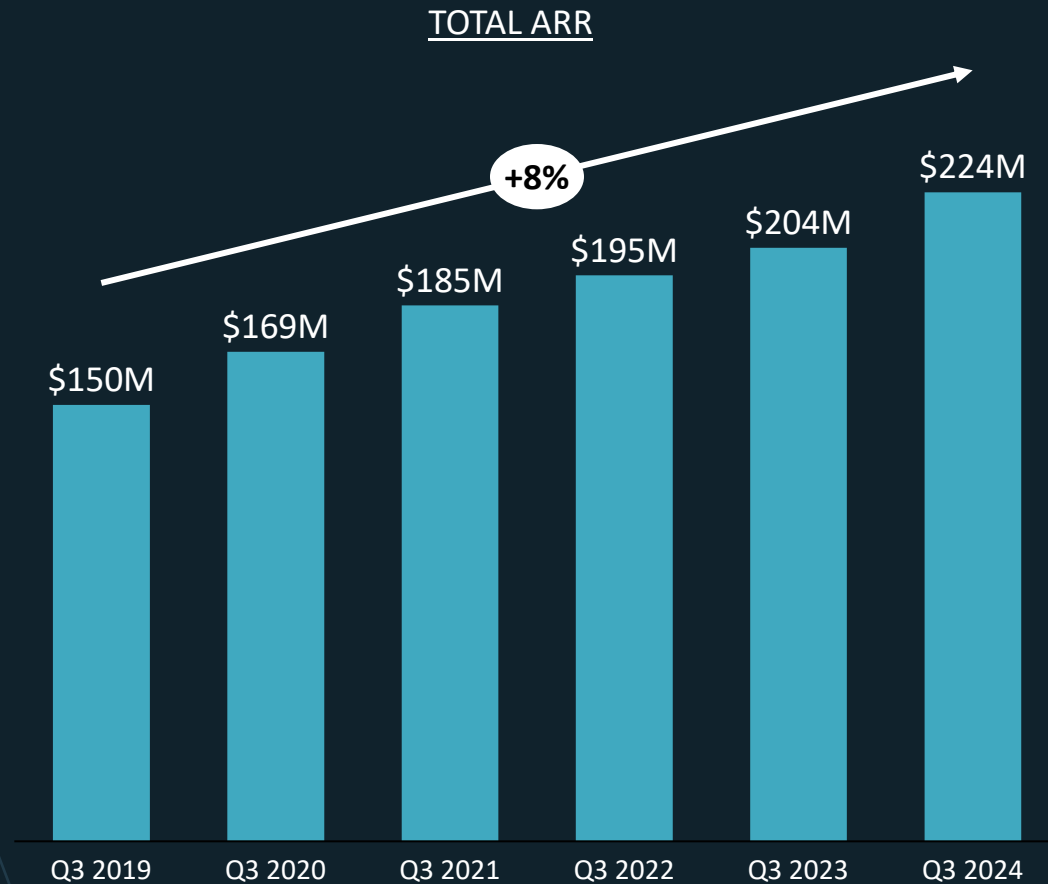
+229% YoY

Operating  
CF  
\$15 million

Compared to  
-\$10M  
Last year

\* Gross margin and EPS are non-GAAP

# Total ARR Driven by Cloud ARR



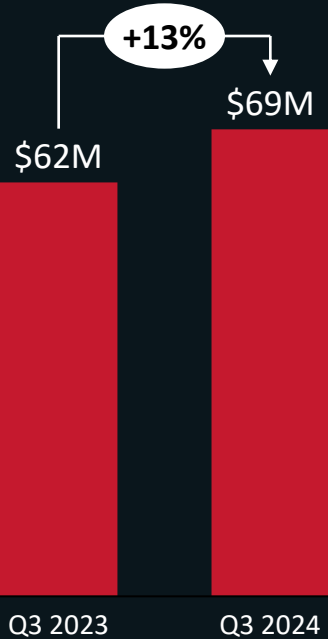
\* Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period

\* Numbers are rounded



# Q3 2024 Financial Data

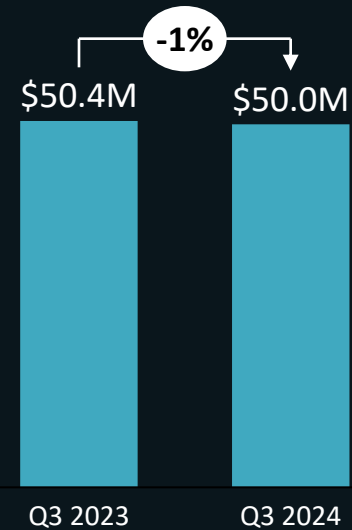
## Revenue



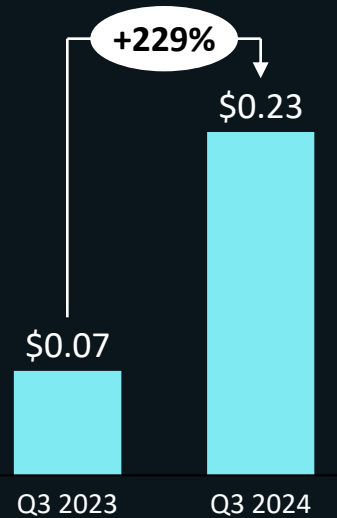
## Gross Margin (Non-GAAP)



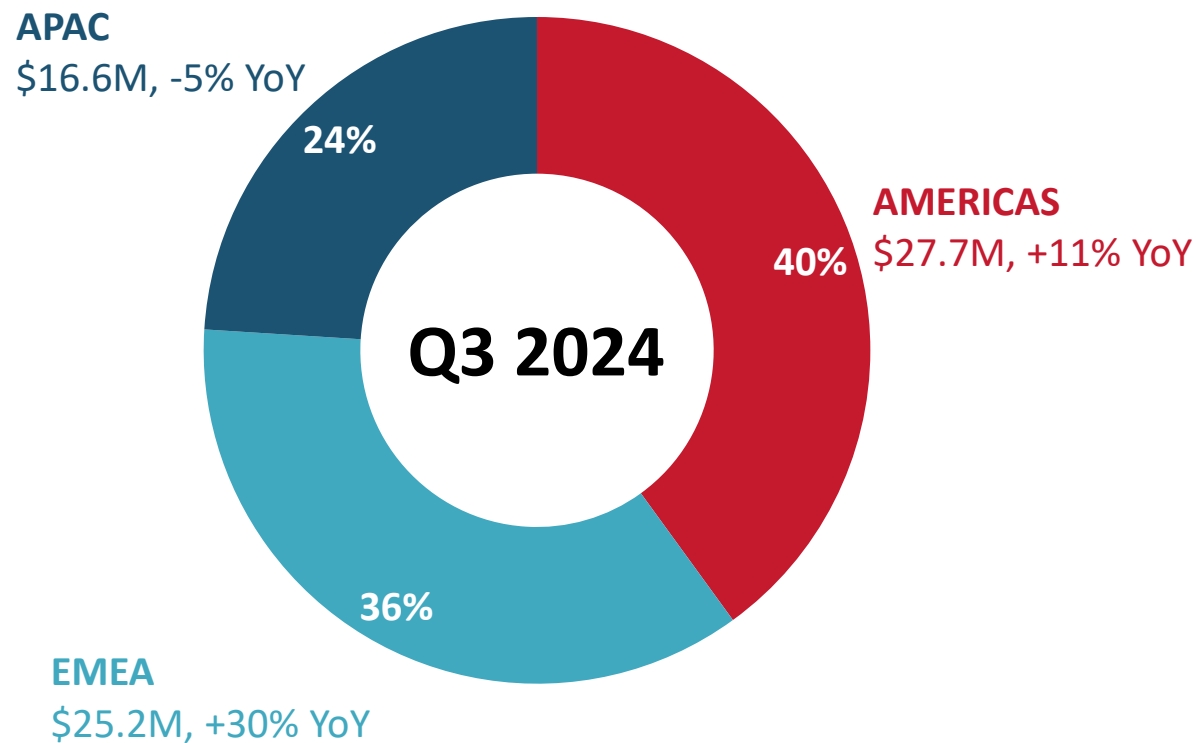
## Operating Expenses (Non-GAAP)



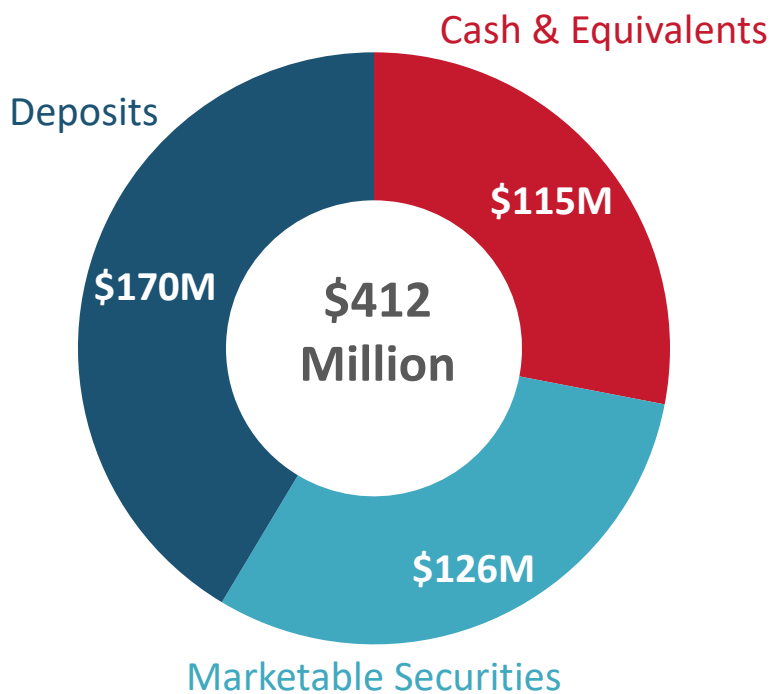
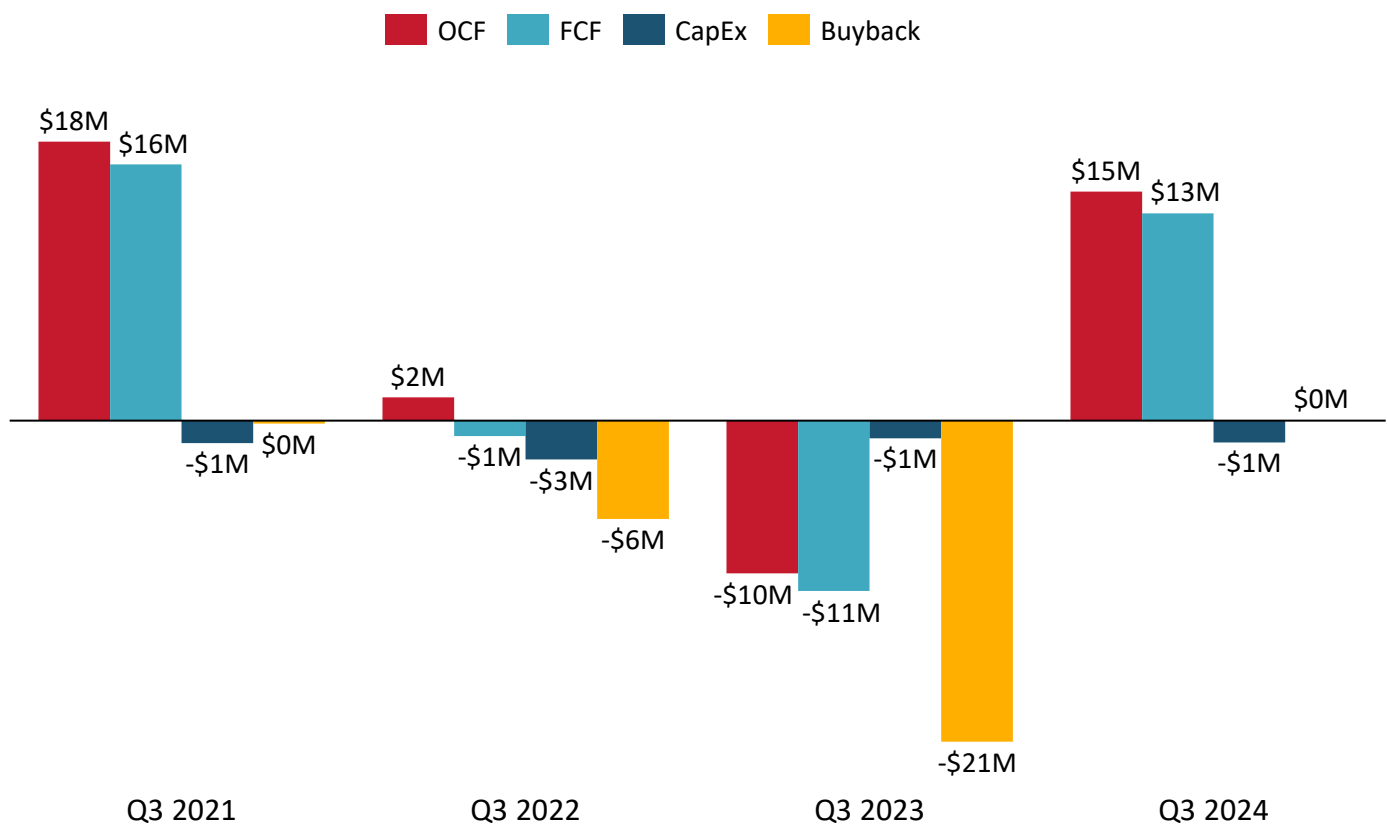
## Diluted Earnings Per Share (Non-GAAP)



# Revenue Geography Breakdown (\$M)



# Cash Generation



\* Numbers are rounded



Thank you!

