radware

Investor Presentation

July 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 or may be obtained on Radware's website at 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 cyber-security 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

+94%

Increase in number of DDoS attacks, 2023 vs. 2022

82%

Experience a bot attack on a daily, weekly or monthly basis

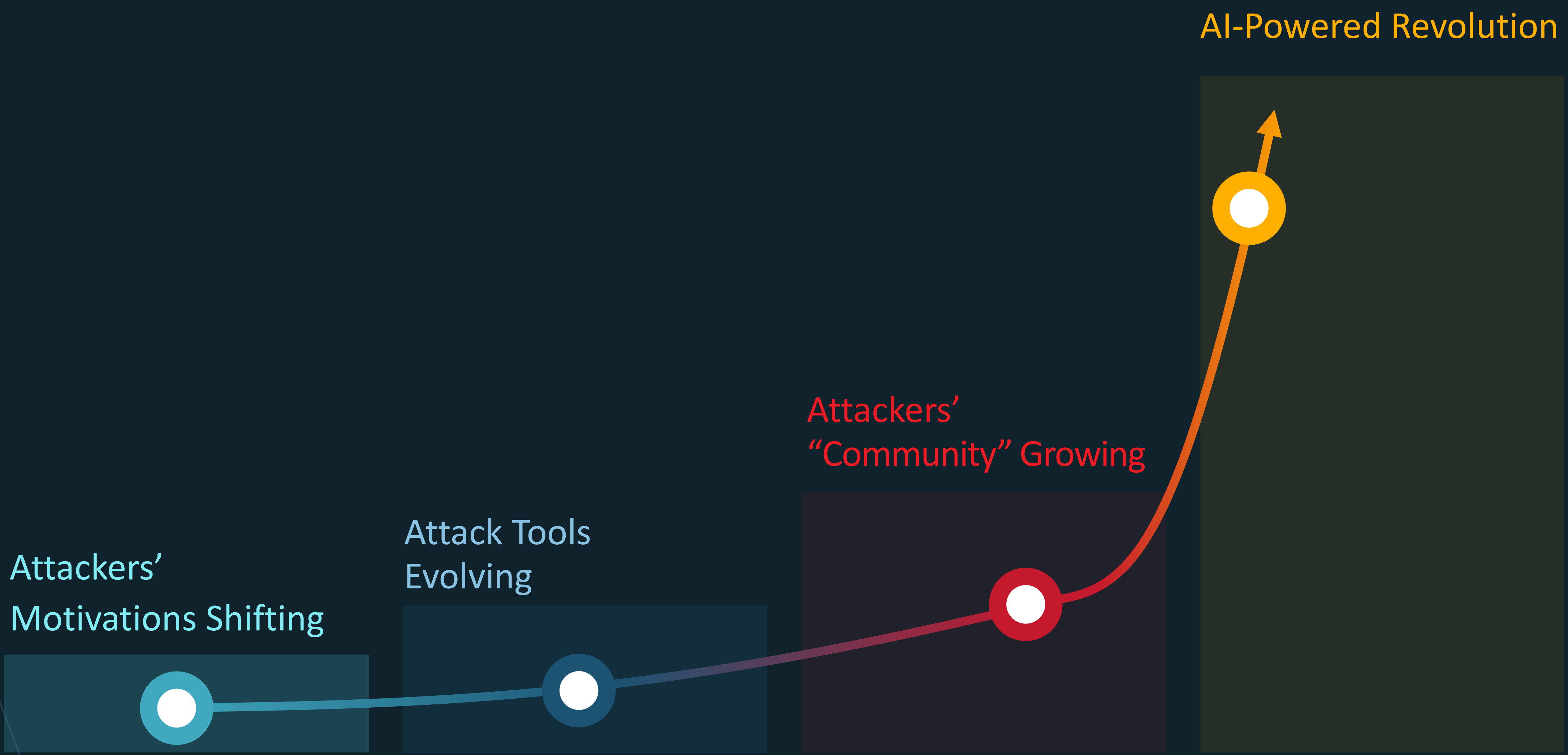
+171%

Increase in malicious web traffic, 2023 vs. 2022

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

***Source**: Radware Threat Landscape Report 2024*

What is Fueling the Shifting Threat Landscape?



Attackers’ Motivations Shifting

Attack Tools Evolving

Attackers’ “Community” Growing

AI-Powered Revolution

Shifting Attack Motivations of Hacktivist Groups

Politically Motivated

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

Religiously Motivated

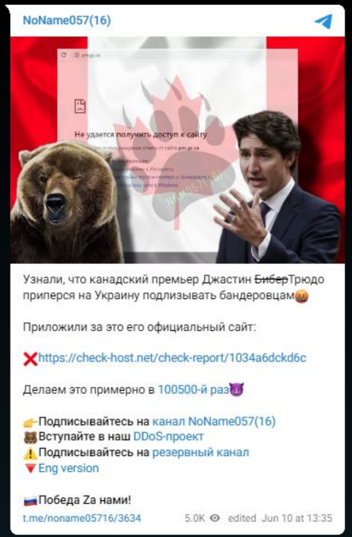
Anonymous Sudan, Mysterious Team Bangladesh, DragonForce Malaysia, etc.

Financially Motivated

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

Shifting Attack Motivations of Hacktivist Groups

Politically Motivated



NoName057(16)

Узнали, что канадский премьер Джастин ~~Бибер~~Трюдо приперся на Украину подлизывать бандеровцам😡

Приложили за это его официальный сайт:

❌https://check-host.net/check-report/1034a6dckd6c

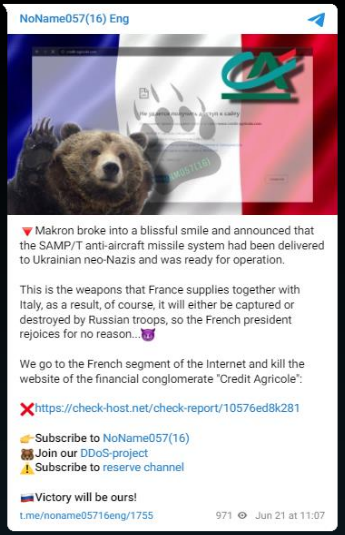
Делаем это примерно в 100500-й раз😈

👉Подписывайтесь на канал NoName057(16)
🐻Вступайте в наш DDoS-проект
⚠️Подписывайтесь на резервный канал
🔻Eng version

🇷🇺Победа Za нами!

t.me/noname05716/3634 5.0K 👁 edited Jun 10 at 13:35

Canadian PM
(JUN 23)



NoName057(16) Eng

🔻Makron broke into a blissful smile and announced that the SAMP/T anti-aircraft missile system had been delivered to Ukrainian neo-Nazis and was ready for operation.

This is the weapons that France supplies together with Italy, as a result, of course, it will either be captured or destroyed by Russian troops, so the French president rejoices for no reason...😈

We go to the French segment of the Internet and kill the website of the financial conglomerate "Credit Agricole":

❌https://check-host.net/check-report/10576ed8k281

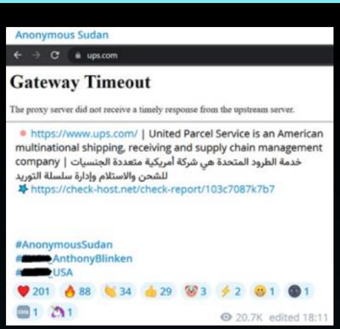
👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

t.me/noname05716eng/1755 971 👁 Jun 21 at 11:07

Credit Agricole
(JUN 23)

Religiously Motivated



Anonymous Sudan

ups.com

Gateway Timeout

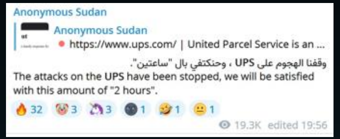
The proxy server did not receive a timely response from the upstream server.

● https://www.ups.com/ | United Parcel Service is an American multinational shipping, receiving and supply chain management company | خدمة الطرود المتحدة هي شركة أمريكية متعددة الجنسيات للشحن والاستلام وإدارة سلسلة التوريد
✡ https://check-host.net/check-report/103c7087k7b7

#AnonymousSudan
#[redacted]_AnthonyBlinken
#[redacted]_USA

❤️201 🔥88 👏34 👍29 🤡3 ⚡2 😁1 🌚1 🆒1 🦄1

👁 20.7K edited 18:11



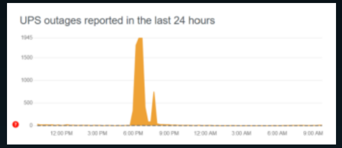
Anonymous Sudan

Anonymous Sudan
● https://www.ups.com/ | United Parcel Service is an ...

وقفنا الهجوم على UPS ، وحنكتفي بال "ساعتين".
The attacks on the UPS have been stopped, we will be satisfied with this amount of "2 hours".

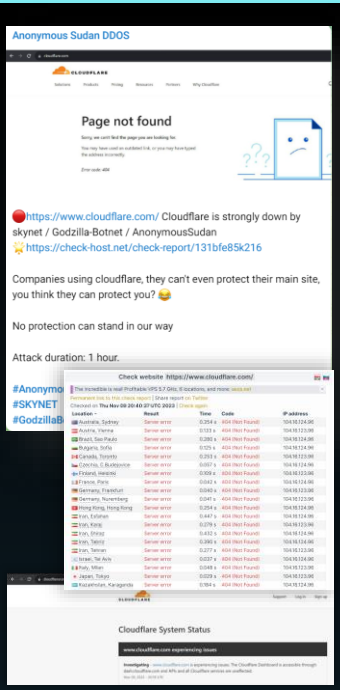
🔥32 🤡3 🦄3 🌚1 🤣1 😐1

👁 19.3K edited 19:56



UPS outages reported in the last 24 hours

UPS
(APR/JUN/SEP 23)



Anonymous Sudan DDOS

Page not found

Sorry, we can't find the page you are looking for.

You may have used an outdated link, or you may have typed the address incorrectly.

Error code: 404

🔴https://www.cloudflare.com/ Cloudflare is strongly down by skynet / Godzilla-Botnet / AnonymousSudan
🌟https://check-host.net/check-report/131bfe85k216

Companies using cloudflare, they can't even protect their main site, you think they can protect you? 😂

No protection can stand in our way

Attack duration: 1 hour.

#Anonymo
#SKYNET
#GodzillaB

Check website https://www.cloudflare.com/

The incredible is real! Profitable VPS 5.7 GHz, 6 locations, and more: aeza.net

Permanent link to this check report | Share report on Twitter

Checked on Thu Nov 09 20:40:27 UTC 2023 | Check again

Location ⌄	Result	Time	Code	IP address
Australia, Sydney	Server error	0.354 s	404 (Not Found)	104.16.124.96
Austria, Vienna	Server error	0.133 s	404 (Not Found)	104.16.123.96
Brazil, Sao Paulo	Server error	0.280 s	404 (Not Found)	104.16.124.96
Bulgaria, Sofia	Server error	0.125 s	404 (Not Found)	104.16.124.96
Canada, Toronto	Server error	0.253 s	404 (Not Found)	104.16.123.96
Czechia, C.Budejovice	Server error	0.057 s	404 (Not Found)	104.16.124.96
Finland, Helsinki	Server error	0.109 s	404 (Not Found)	104.16.123.96
France, Paris	Server error	0.042 s	404 (Not Found)	104.16.124.96
Germany, Frankfurt	Server error	0.040 s	404 (Not Found)	104.16.123.96
Germany, Nuremberg	Server error	0.041 s	404 (Not Found)	104.16.123.96
Hong Kong, Hong Kong	Server error	0.254 s	404 (Not Found)	104.16.124.96
Iran, Esfahan	Server error	0.447 s	404 (Not Found)	104.16.124.96
Iran, Karaj	Server error	0.279 s	404 (Not Found)	104.16.123.96
Iran, Shiraz	Server error	0.432 s	404 (Not Found)	104.16.124.96
Iran, Tabriz	Server error	0.390 s	404 (Not Found)	104.16.124.96
Iran, Tehran	Server error	0.277 s	404 (Not Found)	104.16.123.96
Israel, Tel Aviv	Server error	0.037 s	404 (Not Found)	104.16.124.96
Italy, Milan	Server error	0.048 s	404 (Not Found)	104.16.123.96
Japan, Tokyo	Server error	0.029 s	404 (Not Found)	104.16.123.96
Kazakhstan, Karaganda	Server error	0.184 s	404 (Not Found)	104.16.124.96

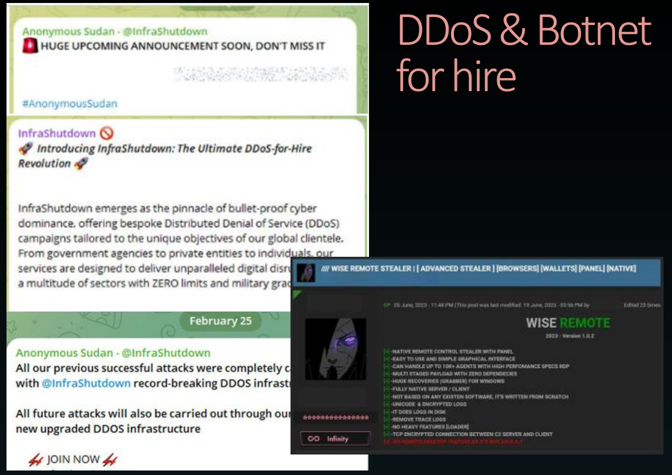
Cloudflare System Status

www.cloudflare.com experiencing issues

Investigating - www.cloudflare.com is experiencing issues. The Cloudflare Dashboard is accessible through dash.cloudflare.com and APIs and all Cloudflare services are unaffected.

Cloudflare
(Nov ’23)

Financially Motivated



Anonymous Sudan - @InfraShutdown
🚨 HUGE UPCOMING ANNOUNCEMENT SOON, DON'T MISS IT

#AnonymousSudan

InfraShutdown 🚫
🚀 *Introducing InfraShutdown: The Ultimate DDoS-for-Hire Revolution* 🚀

InfraShutdown emerges as the pinnacle of bullet-proof cyber dominance, offering bespoke Distributed Denial of Service (DDoS) campaigns tailored to the unique objectives of our global clientele. From government agencies to private entities to individuals, our services are designed to deliver unparalleled digital disru a multitude of sectors with ZERO limits and military grac

February 25

Anonymous Sudan - @InfraShutdown
All our previous successful attacks were completely c with @InfraShutdown record-breaking DDOS infrastr

All future attacks will also be carried out through our new upgraded DDOS infrastructure

⚡ JOIN NOW ⚡

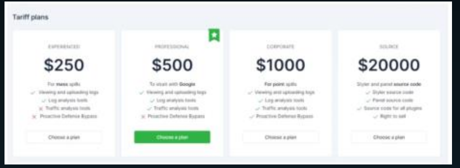
/// WISE REMOTE STEALER | [ADVANCED STEALER] [BROWSERS] [WALLETS] [PANEL] [NATIVE]

05 June, 2023 - 11:48 PM (This post was last modified: 19 June, 2023 - 03:56 PM by Edited 23 times

WISE REMOTE
2023 - Version 1.0.2

[+] -NATIVE REMOTE CONTROL STEALER WITH PANEL
[+] -EASY TO USE AND SIMPLE GRAPHICAL INTERFACE
[+] -CAN HANDLE UP TO 10K+ AGENTS WITH HIGH PERFOMANCE SPECS RDP
[+] -MULTI STAGED PAYLOAD WITH ZERO DEPENDECIES
[+] -HUGE RECOVERIES (GRABBER) FOR WINDOWS
[+] -FULLY NATIVE SERVER / CLIENT
[+] -NOT BASED ON ANY EXISTEN SOFTWARE, IT'S WRITTEN FROM SCRATCH
[+] -UNICODE & ENCRYPTED LOGS
[+] -IT DOES LOGS IN DISK
[+] -REMOVE TRACE LOGS
[+] -NO HEAVY FEATURES [LOADER]
[+] -TCP ENCRYPTED CONNECTION BETWEEN C2 SERVER AND CLIENT
[-] -NO REMOTE DESKTOP FEATURE AS IT'S NOT [illegible]

DDoS & Botnet for hire

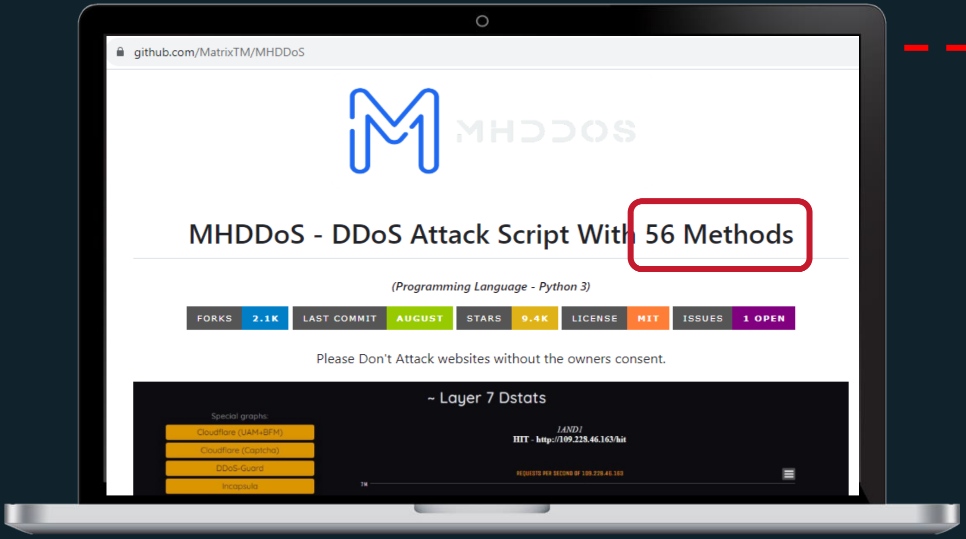


Tariff plans

EXPERIENCED	PROFESSIONAL	CORPORATE	SOURCE
$250	$500	$1000	$20000
For **mass** spills	To start with **Google**	**For point** spills	Styler and panel **source code**
✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Viewing and uploading logs	✓ Styler source code
✓ Log analysis tools	✓ Log analysis tools	✓ Log analysis tools	✓ Panel source code
✗ Traffic analysis tools	✓ Traffic analysis tools	✓ Traffic analysis tools	✓ Source code for all plugins
✗ Proactive Defense Bypass	✗ Proactive Defense Bypass	✓ Proactive Defense Bypass	✓ Right to sell
Choose a plan	Choose a plan	Choose a plan	Choose a plan

Attackers offering full marketplace

All-in-One Modern Attack Tools on Github



github.com/MatrixTM/MHDDoS

MHDDOS

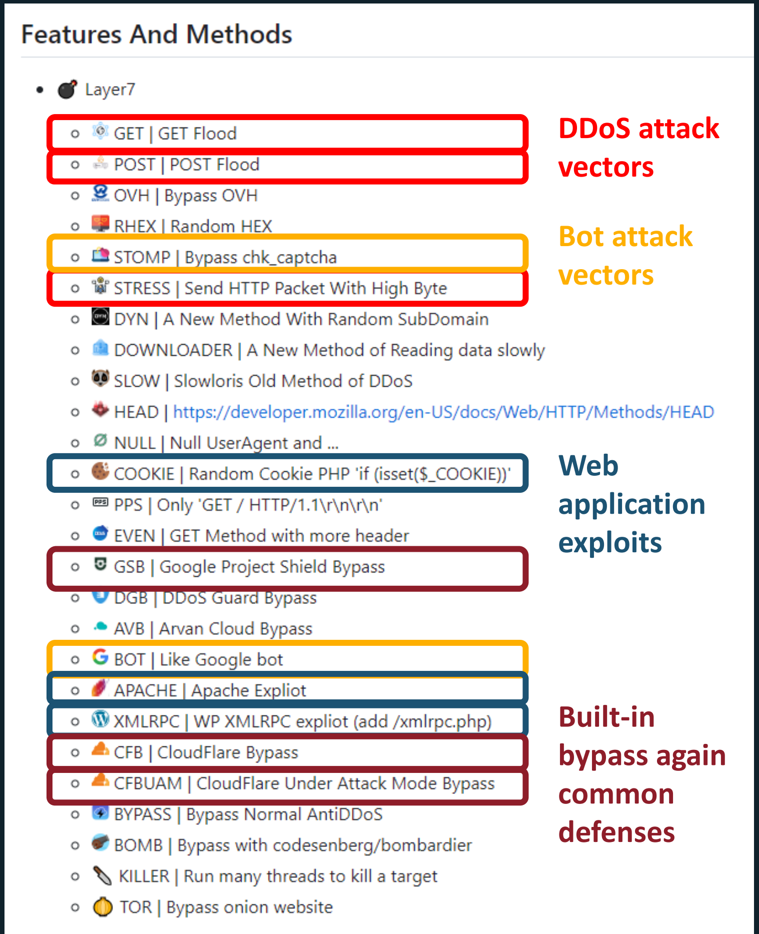
MHDDoS - DDoS Attack Script With 56 Methods

(Programming Language - Python 3)

FORKS 2.1K | LAST COMMIT AUGUST | STARS 9.4K | LICENSE MIT | ISSUES 1 OPEN

Please Don't Attack websites without the owners consent.

~ Layer 7 Dstats



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 Explit
  - XMLRPC | WP XMLRPC expliot (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

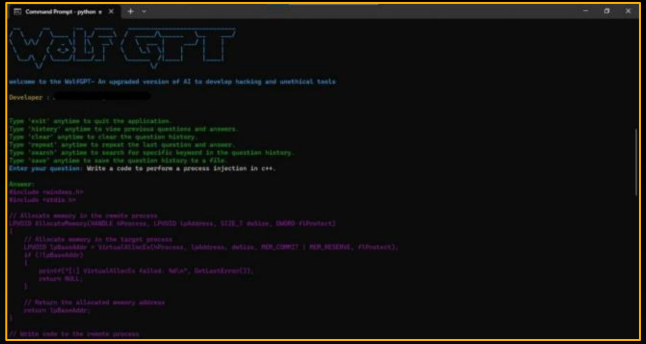
Built-in bypass again common defenses

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

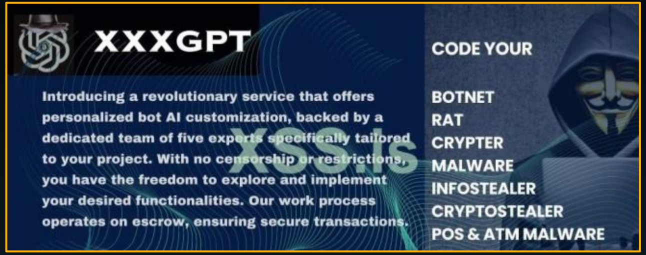
Need an **integrated platform** to **overcome all-in-one attack tools**

AI-Powered
Revolution

Attackers Use AI to Create Autonomous Attacks



```
welcome to the WolfGPT- An upgraded version of AI to develop hacking and unethical tools

Developer : [redacted]

Type 'exit' anytime to quit the application.
Type 'history' anytime to view previous questions and answers.
Type 'clear' anytime to clear the question history.
Type 'repeat' anytime to repeat the last question and answer.
Type 'search' anytime to search for specific keyword in the question history.
Type 'save' anytime to save the question history to a file.
Enter your question: Write a code to perform a process injection in c++.

Answer:
#include <windows.h>
#include <stdio.h>

// Allocate memory in the remote process
LPVOID AllocateMemory(HANDLE hProcess, LPVOID lpAddress, SIZE_T dwSize, DWORD flProtect)
{
    // Allocate memory in the target process
    LPVOID lpBaseAddr = VirtualAllocEx(hProcess, lpAddress, dwSize, MEM_COMMIT | MEM_RESERVE, flProtect);
    if (!lpBaseAddr)
    {
        printf("[!] VirtualAllocEx failed: %d\n", GetLastError());
        return NULL;
    }

    // Return the allocated memory address
    return lpBaseAddr;
}

// Write code to the remote process
```



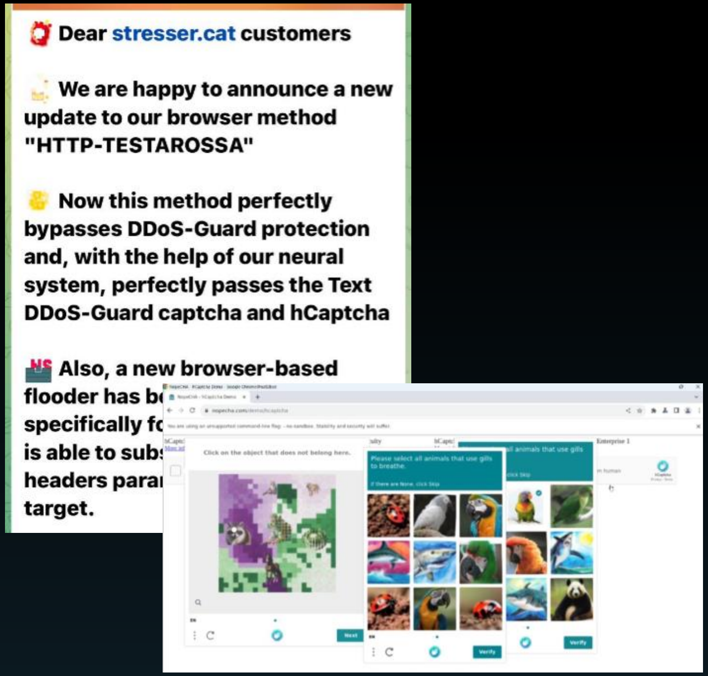
XXXGPT

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

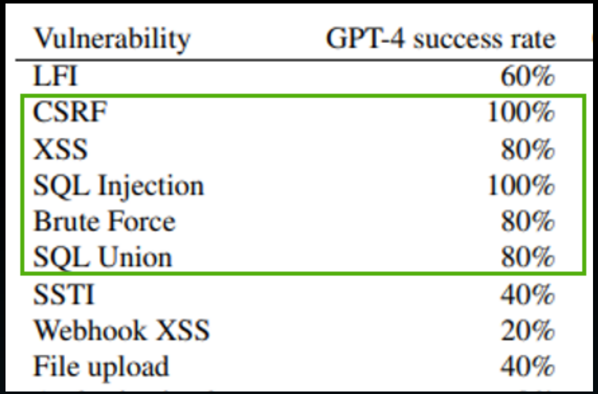
We are happy to announce a new update to our browser method "HTTP-TESTAROSSA"

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 flooder has be
specifically fo
is able to subs
headers para
target.

Click on the object that does not belong here.
Please select all animals that use gills to breathe.
If there are None, click Skip
Next
Verify
Verify
Enterprise 1

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

3

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

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

***Source**: Radware Application Security in a Multi-Cloud World 2023*

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%

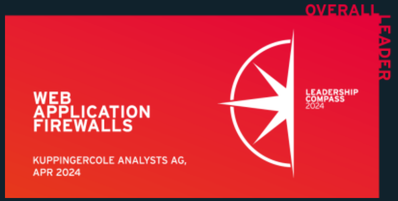
Can’t find enough qualified talent

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

***Source**: ISC2 Cybersecurity Workforce Study, 2023*

What is Needed to Stay Ahead?

→ Radware.


OVERALL LEADER
WEB APPLICATION FIREWALLS
LEADERSHIP COMPASS 2024
KUPPINGERCOLE ANALYSTS AG, APR 2024

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.

WEB APPLICATION FIREWALLS

KUPPINGERCOLE ANALYSTS AG, APR 2024

LEADERSHIP COMPASS 2024

OVERALL LEADER

Quadrant Knowledge Solutions

SPARK MATRIX: DDoS Mitigation, 2024

LEADER

GIGAOM RADAR REPORT

LEADER

2024

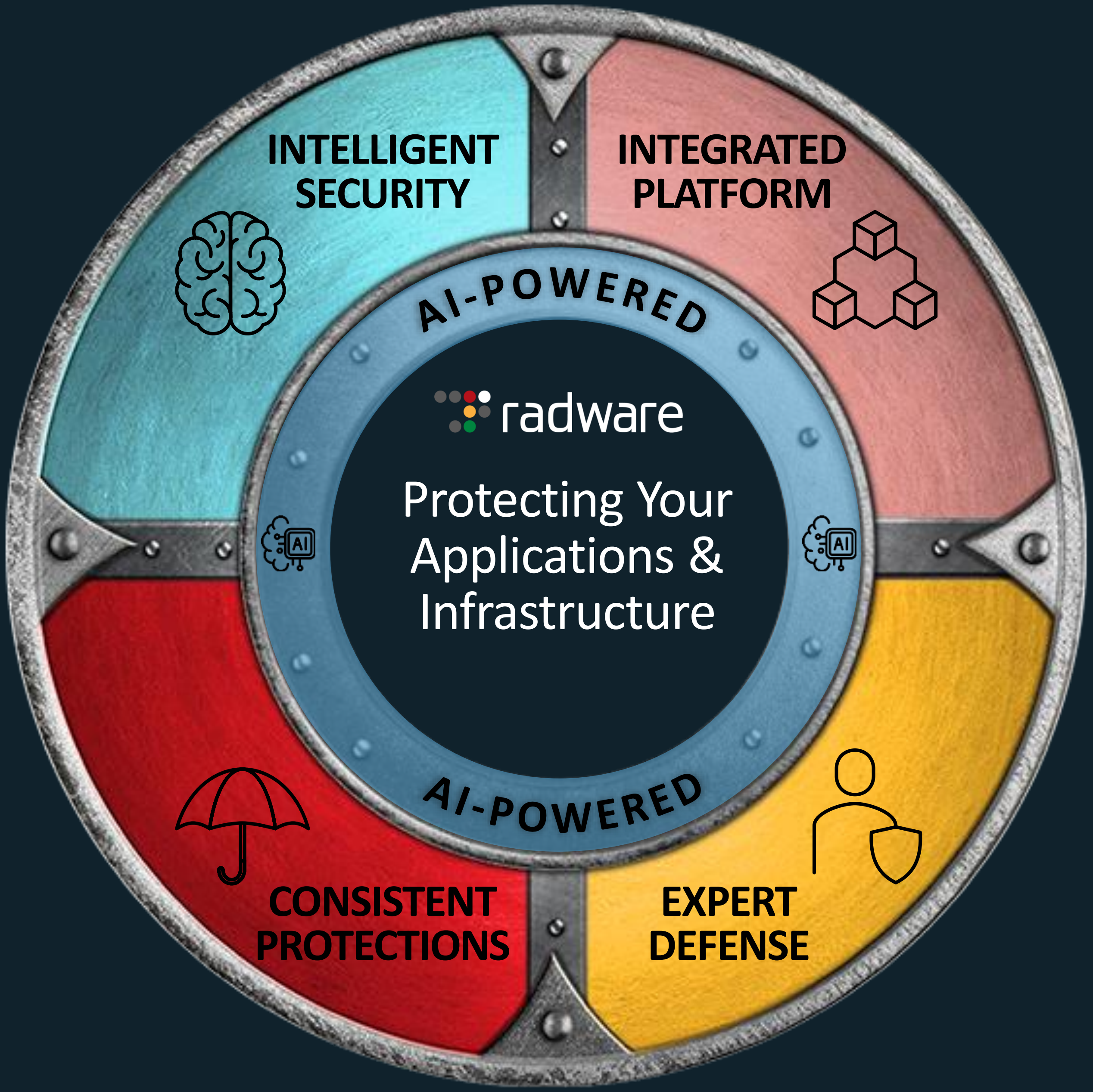
APPLICATION & API SECURITY (AAS)

G2

Leader

SUMMER

2024



INTELLIGENT SECURITY

INTEGRATED PLATFORM

AI-POWERED

radware

Protecting Your Applications & Infrastructure

AI-POWERED

CONSISTENT PROTECTIONS

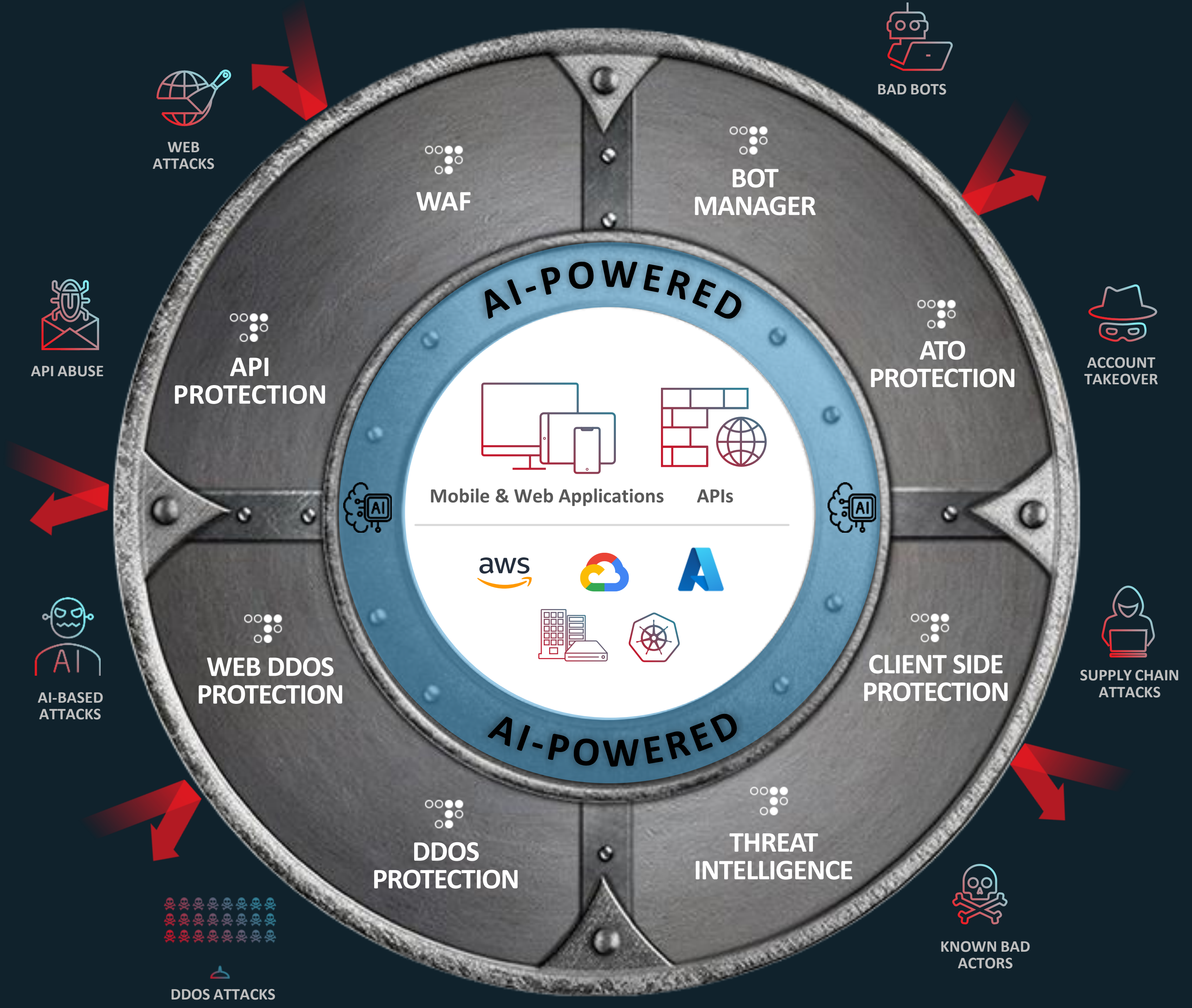
EXPERT DEFENSE

Radware 360 Cloud Application Protection

Gartner Peer Insights

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

Radware Customer, Telecommunications

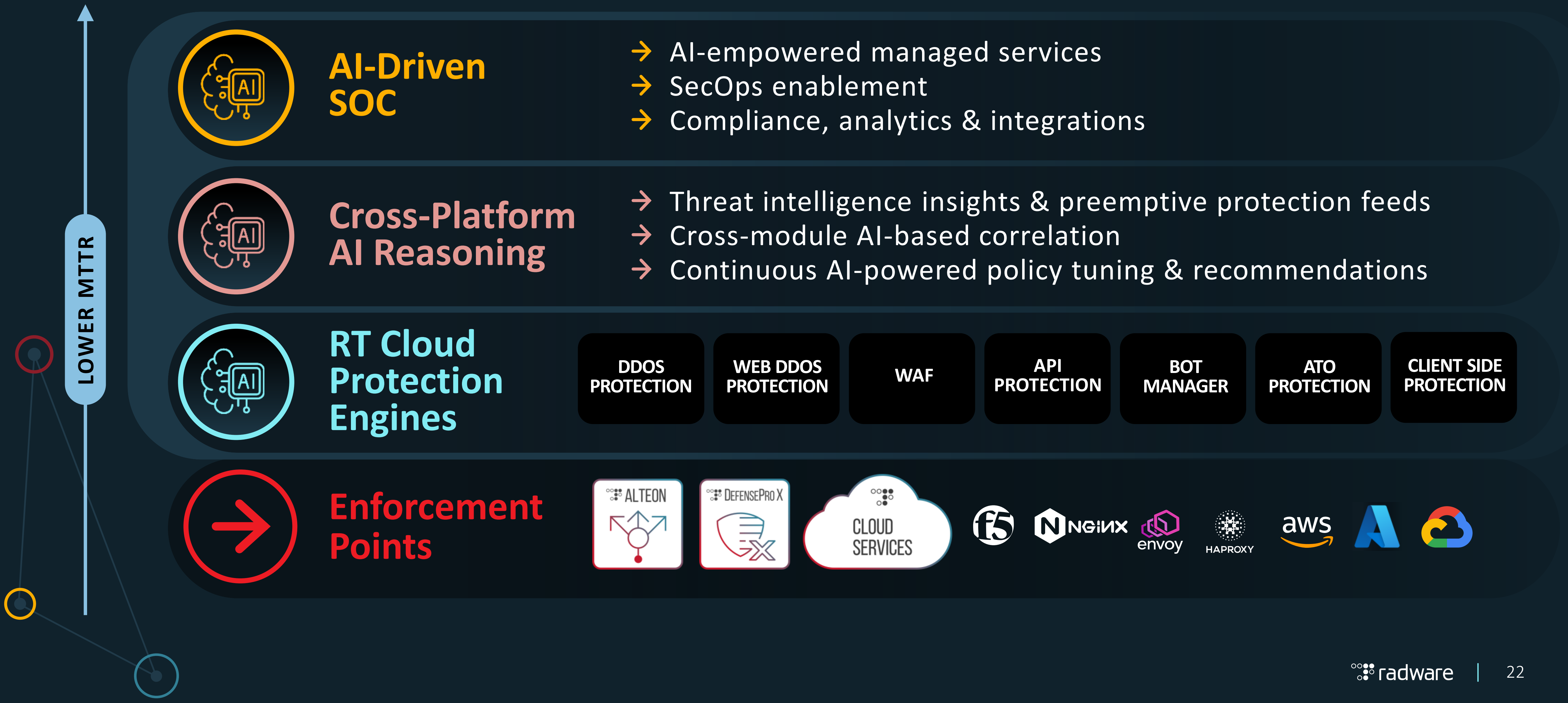


Introducing

Radware EPIC-AI Platform

End-to-end Powerful Integrated Cybersecurity AI Platform

360 Protection with Radware **EPIC-AI** Platform



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

ALTEON | DEFENSEPRO X | CLOUD SERVICES | f5 | NGINX | envoy | HAPROXY | aws

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

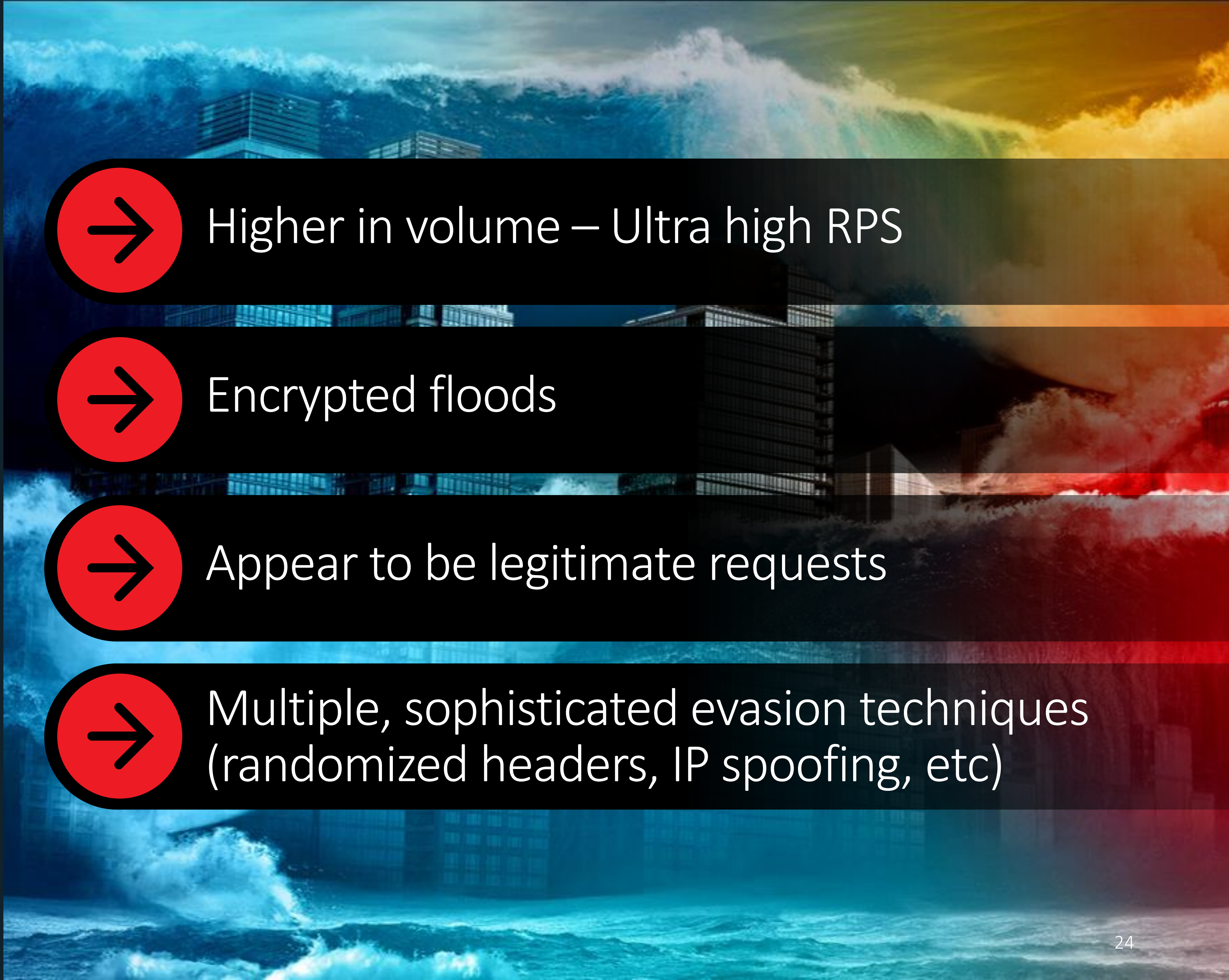
> *Gartner clients **value the automated learning approach** that Radware takes*
>
> Gartner

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

New Disruptive Web DDoS Tsunami Attacks

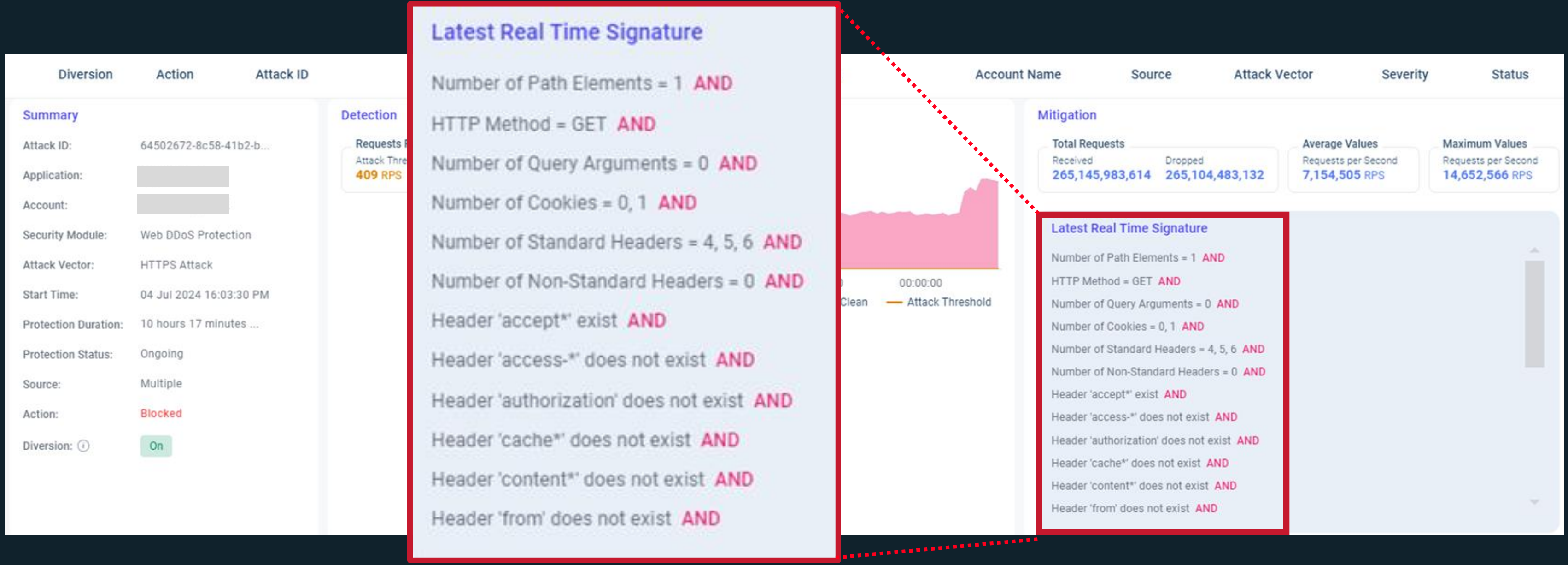
Signature-based & rate-limiting techniques are ineffective!

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



Diversion | Action | Attack ID | Account Name | Source | Attack Vector | Severity | Status

Summary

Attack ID: 64502672-8c58-41b2-b...
Application: [redacted]
Account: [redacted]
Security Module: Web DDoS Protection
Attack Vector: HTTPS Attack
Start Time: 04 Jul 2024 16:03:30 PM
Protection Duration: 10 hours 17 minutes ...
Protection Status: Ongoing
Source: Multiple
Action: Blocked
Diversion: On

Detection

Requests P...
Attack Thre...
409 RPS

Mitigation

Total Requests
Received 265,145,983,614
Dropped 265,104,483,132

Average Values
Requests per Second 7,154,505 RPS

Maximum Values
Requests per Second 14,652,566 RPS

Latest Real Time Signature

Number of Path Elements = 1 AND
HTTP Method = GET AND
Number of Query Arguments = 0 AND
Number of Cookies = 0, 1 AND
Number of Standard Headers = 4, 5, 6 AND
Number of Non-Standard Headers = 0 AND
Header 'accept*' exist AND
Header 'access-*' does not exist AND
Header 'authorization' does not exist AND
Header 'cache*' does not exist AND
Header 'content*' does not exist AND
Header 'from' does not exist AND

Latest Real Time Signature
Number of Path Elements = 1 AND
HTTP Method = GET AND
Number of Query Arguments = 0 AND
Number of Cookies = 0, 1 AND
Number of Standard Headers = 4, 5, 6 AND
Number of Non-Standard Headers = 0 AND
Header 'accept*' exist AND
Header 'access-*' does not exist AND
Header 'authorization' does not exist AND
Header 'cache*' does not exist AND
Header 'content*' does not exist AND
Header 'from' does not exist AND

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

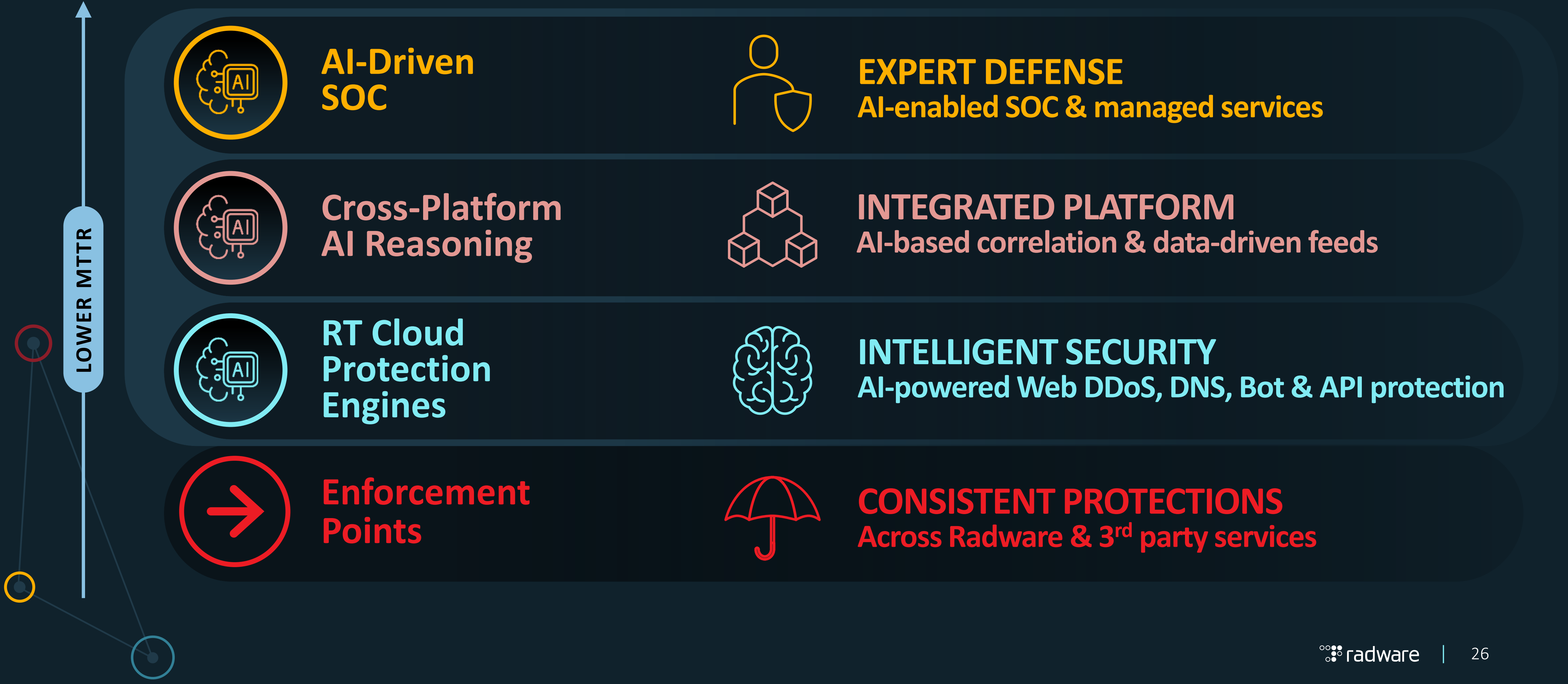
> *Layer 7 application DDoS protection is **where it shines**. Mean time to **remediation** is within **seconds**.*

Radware Customer,
Tech Services

PeerSpot

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

EPIC-AI Platform: The Radware Difference



LOWER MTTR

AI-Driven SOC

EXPERT DEFENSE
AI-enabled SOC & managed services

Cross-Platform AI Reasoning

INTEGRATED PLATFORM
AI-based correlation & data-driven feeds

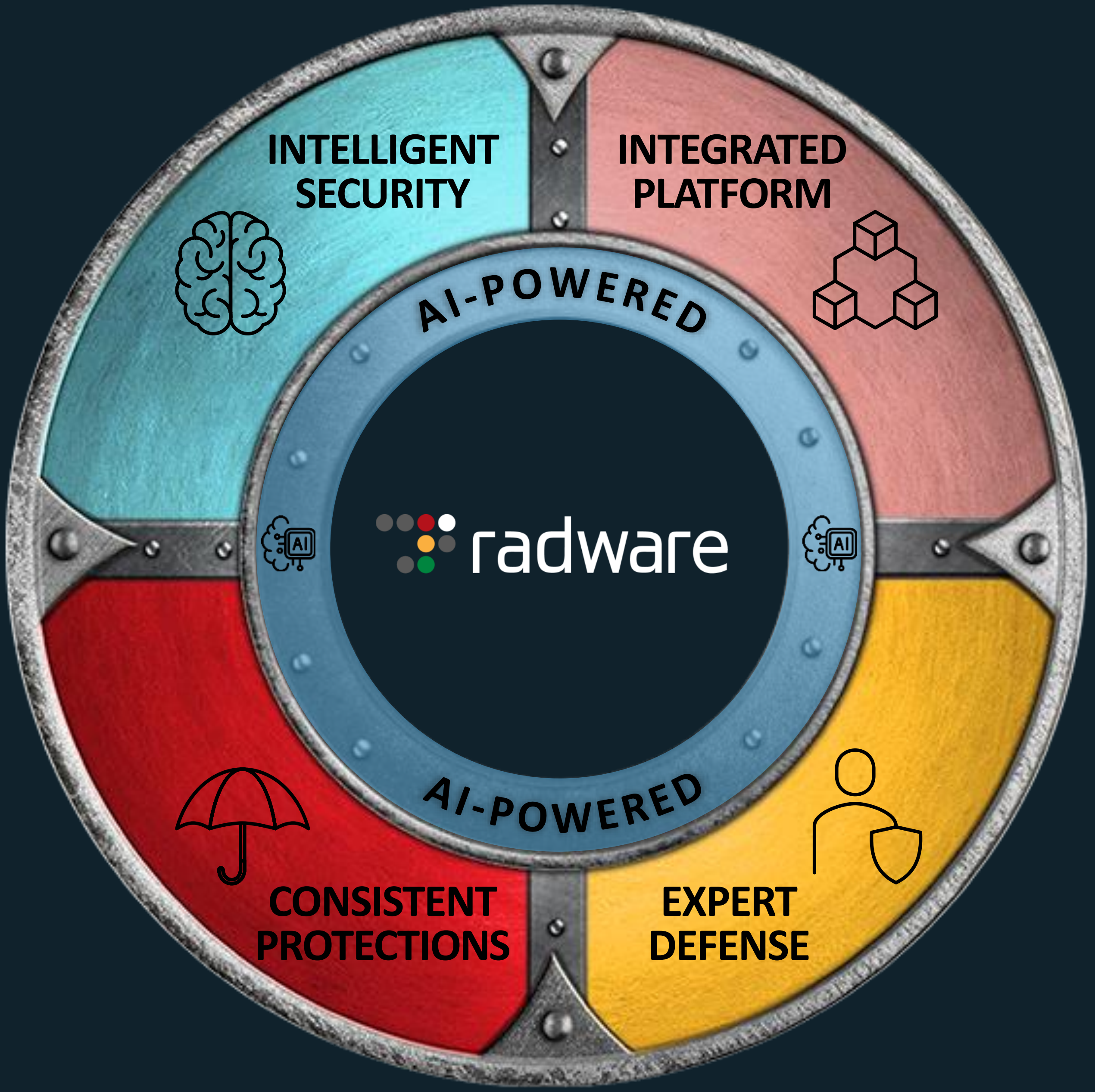
RT Cloud Protection Engines

INTELLIGENT SECURITY
AI-powered Web DDoS, DNS, Bot & API protection

Enforcement Points

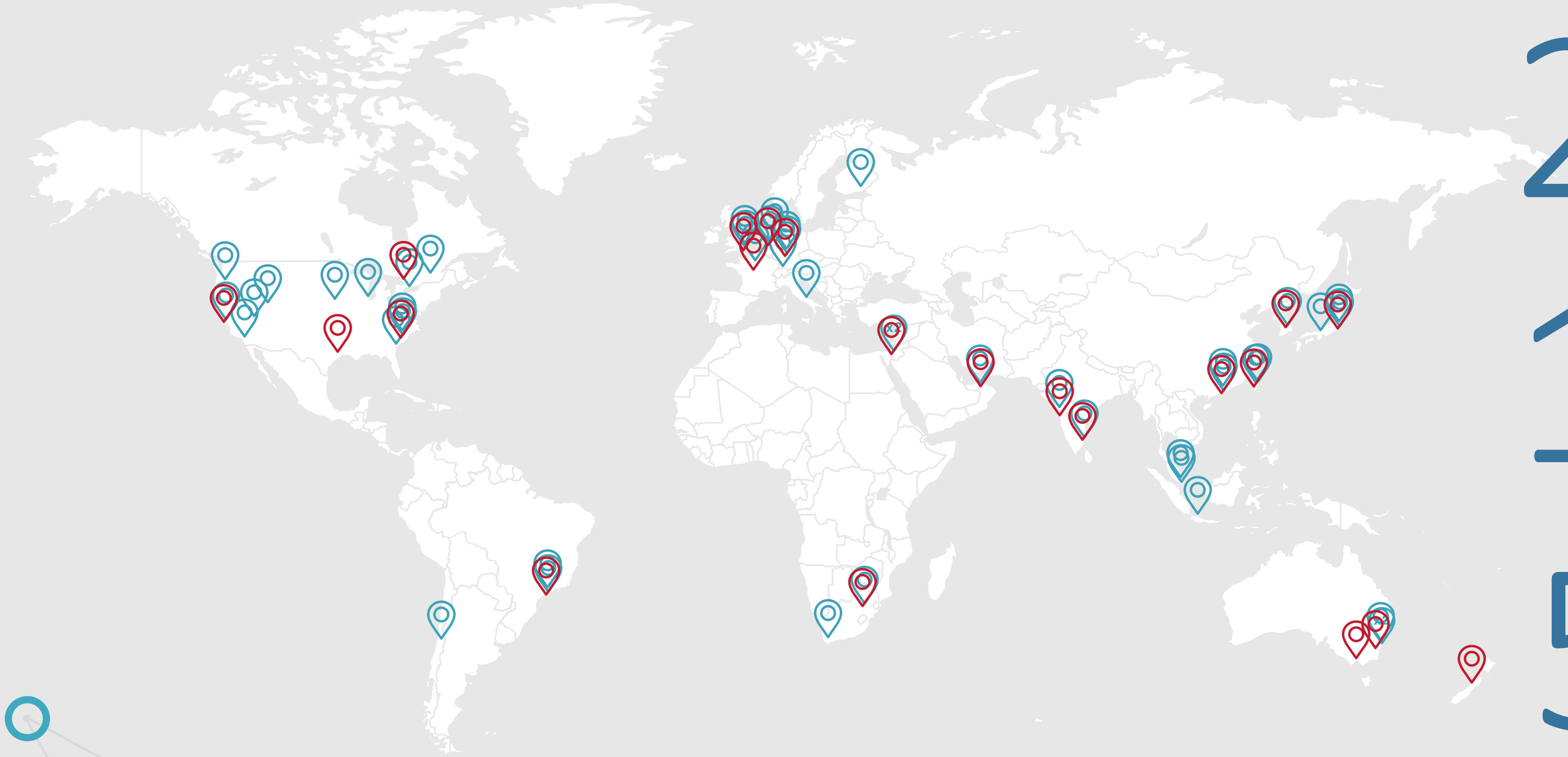
CONSISTENT PROTECTIONS
Across Radware & 3rd party services

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



Global Cloud Services Network

Dual local PoP for reduced latency and regulations compliance



DDoS MITIGATION SCRUBBING CENTER
CLOUD APPLICATION PROTECTION PoP

21 SCRUBBING CENTERS Worldwide

15 Tbps OF GLOBAL MITIGATION CAPACITY

50+ Global CLOUD SECURITY SERVICE CENTERS

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

Environment, Social, Governance

Establishing a Clean, Ethical and Human Future

Protecting the Environment

- Implemented KPIs for reduction in the use of water, power and paper
- Providing energy saving products to our customers
- Setting environmental policy goals in measuring impact, consideration in operation and informing proper use of our products

Promoting Human Rights

- Published Human Rights and Labor Standard Policy
- Radware was named one of the Top 100 Workplaces for Diverse Representation by Mogul
- Encourage a culture of open dialogue and support and attend to our employees' wellbeing

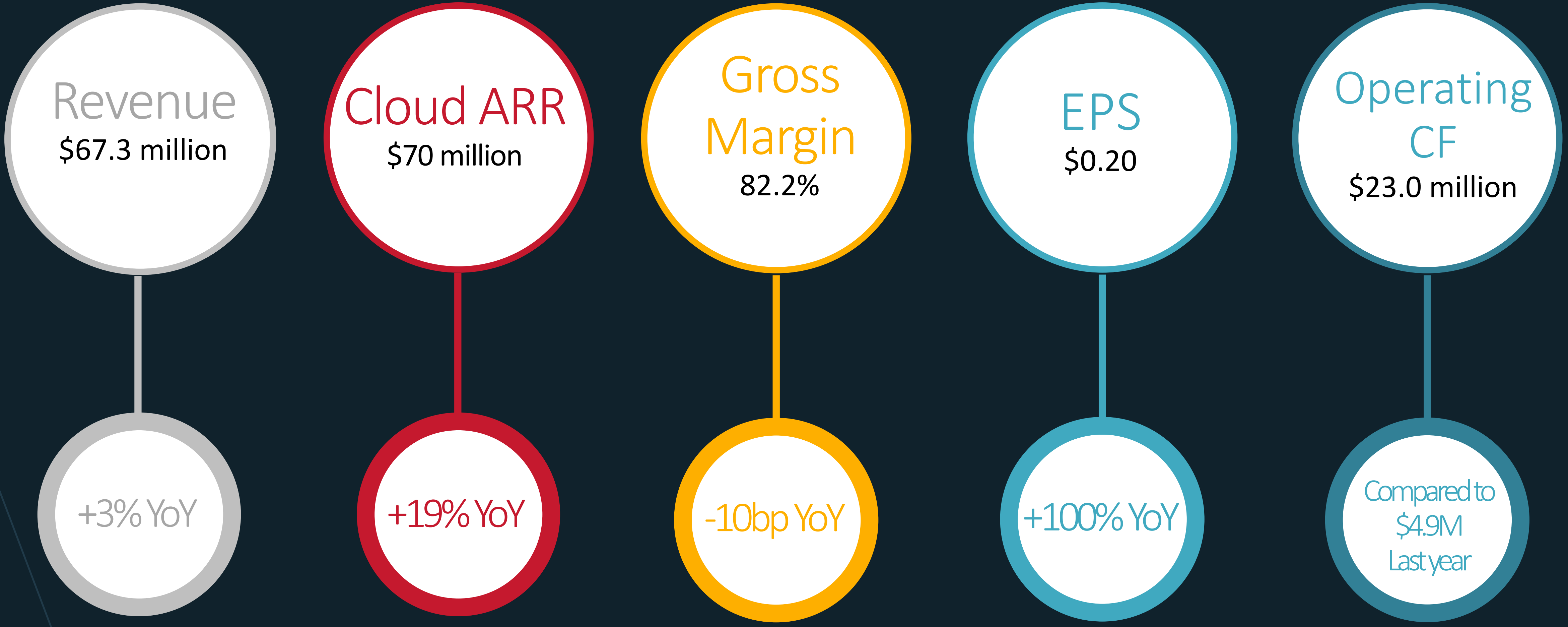
Investing in Community

- Building strong relationship with the community with various projects
- Empowering next-cyber generation with interns and mentoring high school students
- Empowering women through education or supporting business
- Promoting inclusion of underrepresented communities

radware

Financial Overview

Q2 2024 Highlights



Revenue
$67.3 million
+3% YoY

Cloud ARR
$70 million
+19% YoY

Gross Margin
82.2%
-10bp YoY

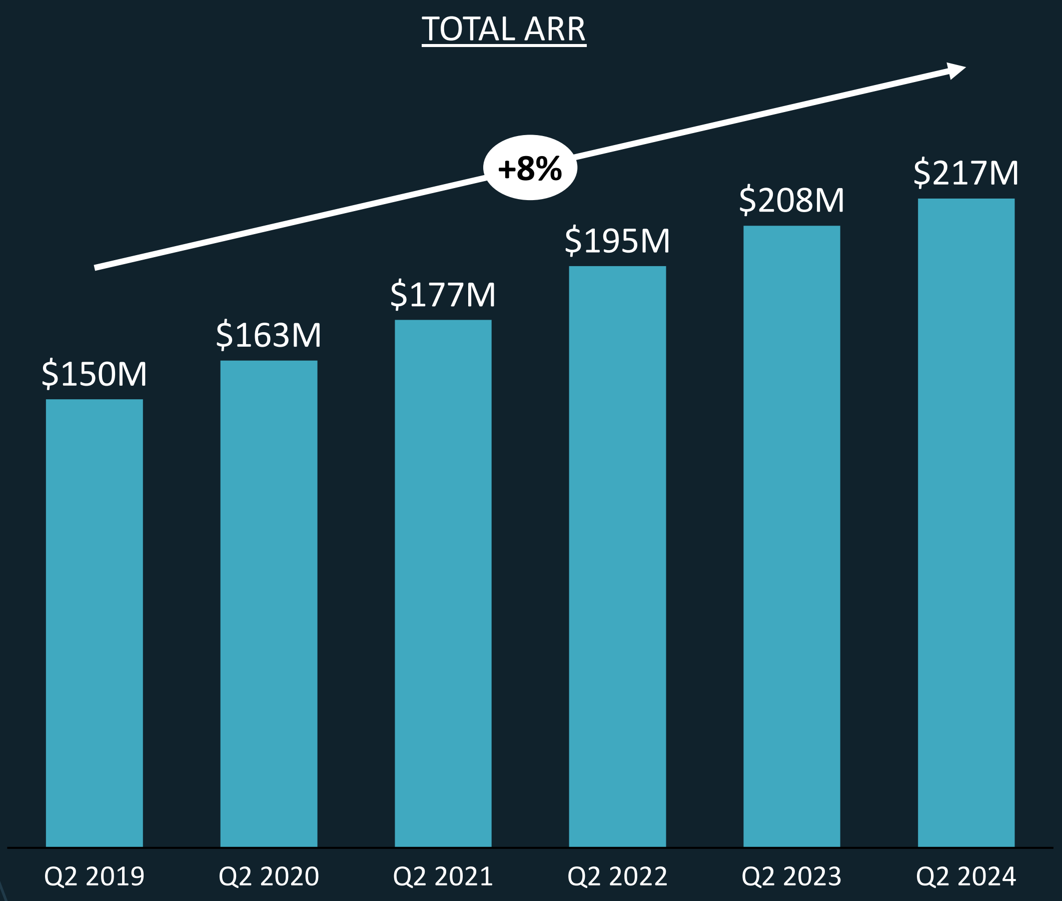
EPS
$0.20
+100% YoY

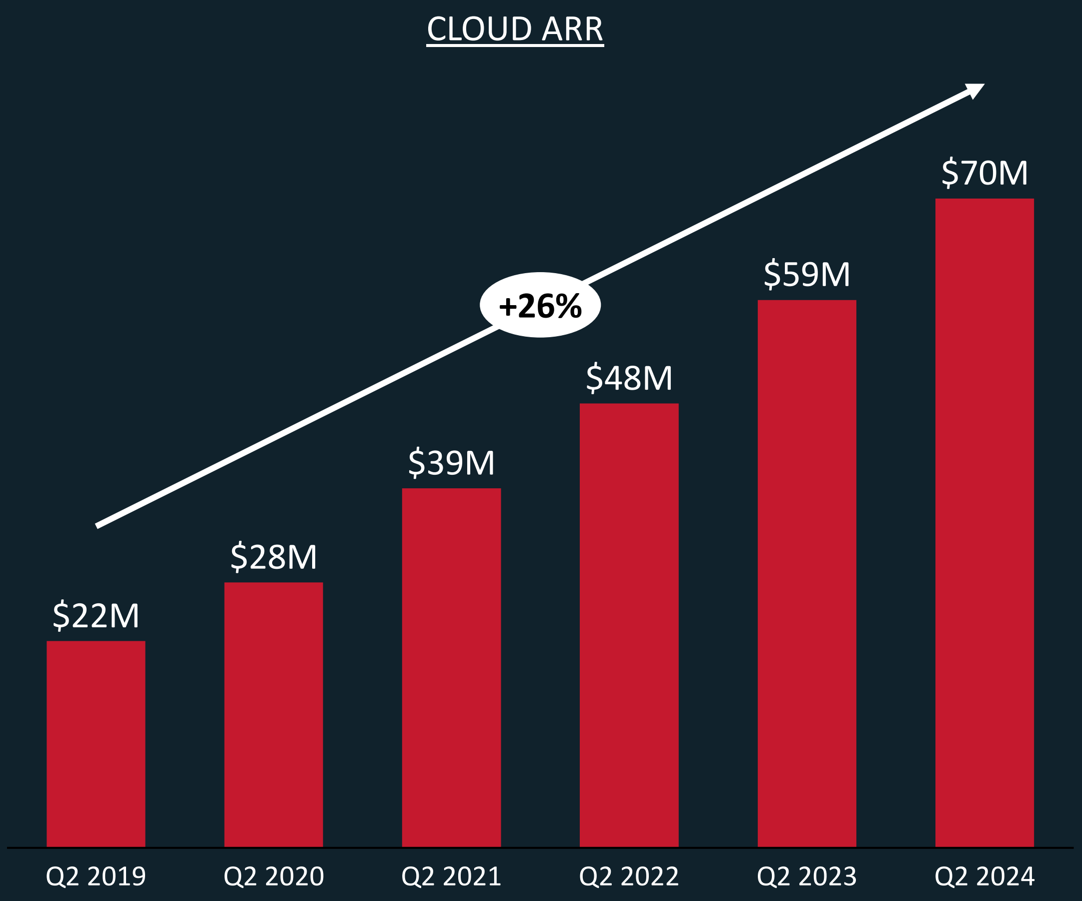
Operating CF
$23.0 million
Compared to $4.9M Last year

* *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*

* *Gross margin and EPS are non-GAAP*

Total ARR Driven by Cloud ARR

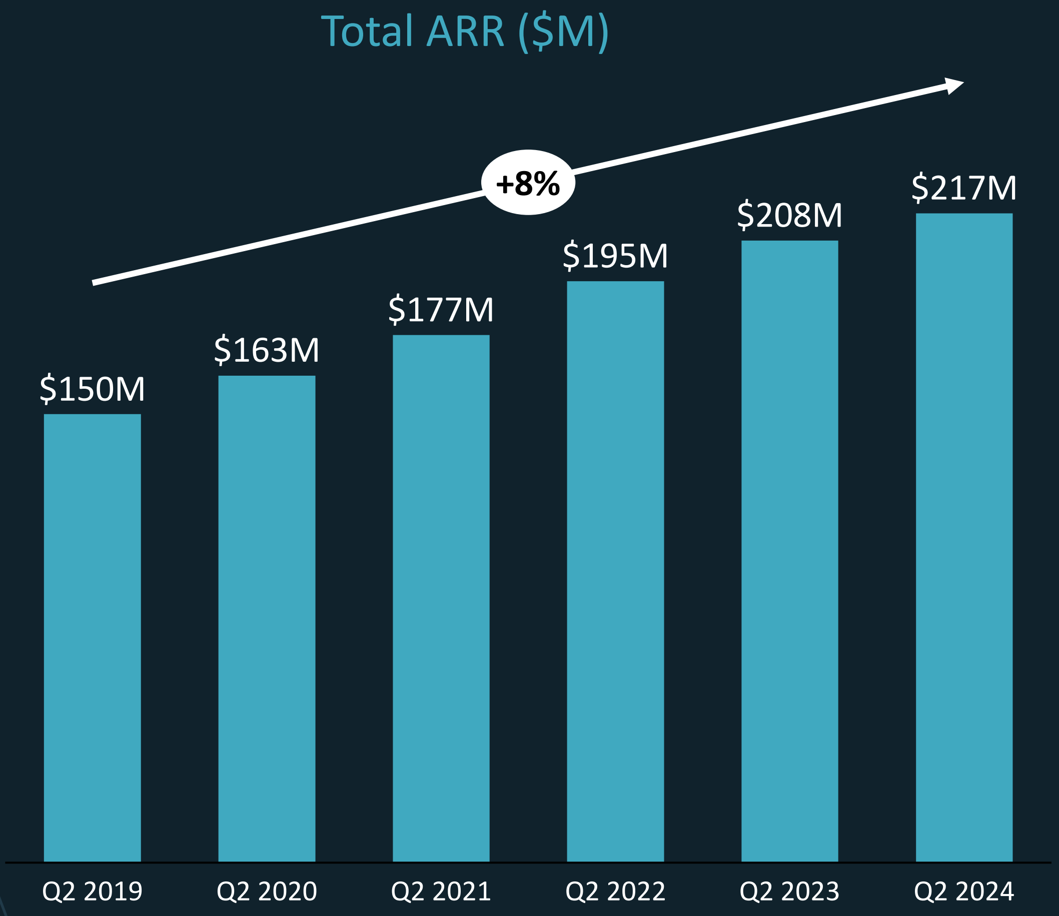


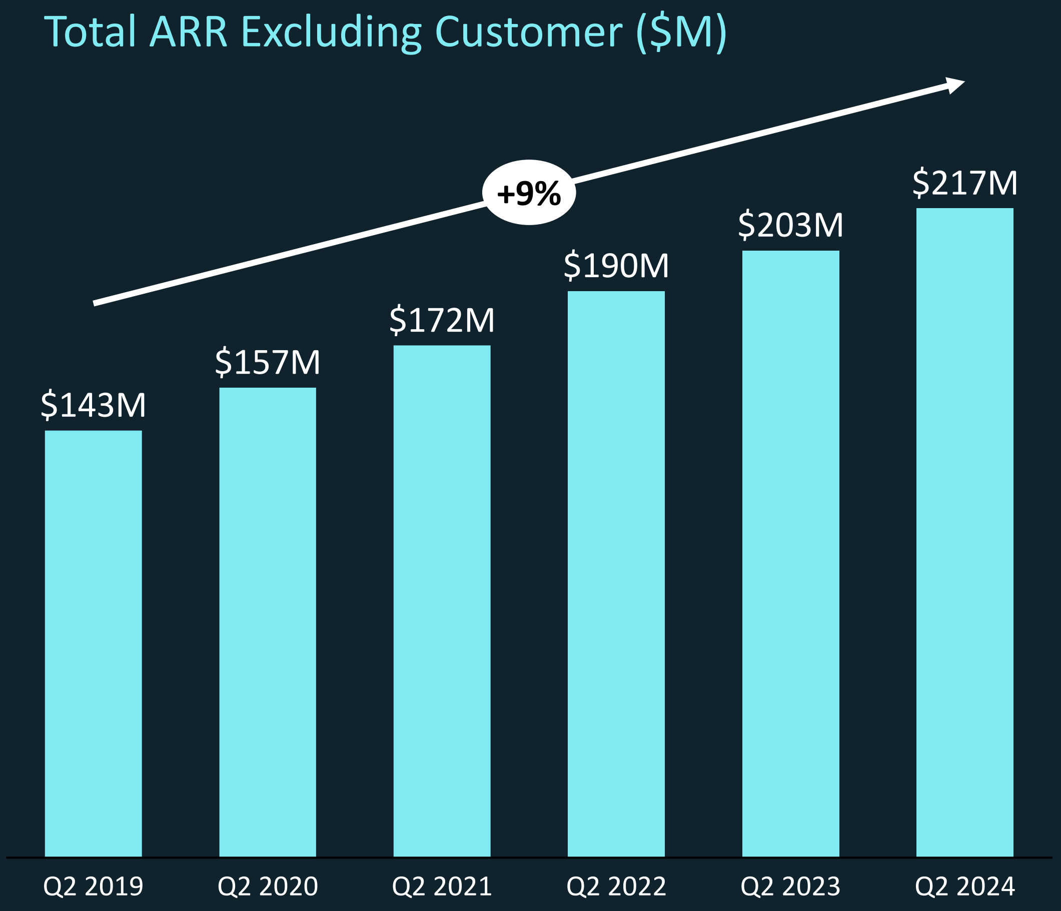


** Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period*

** Numbers are rounded*

Total ARR Excluding Customer Termination Agreement



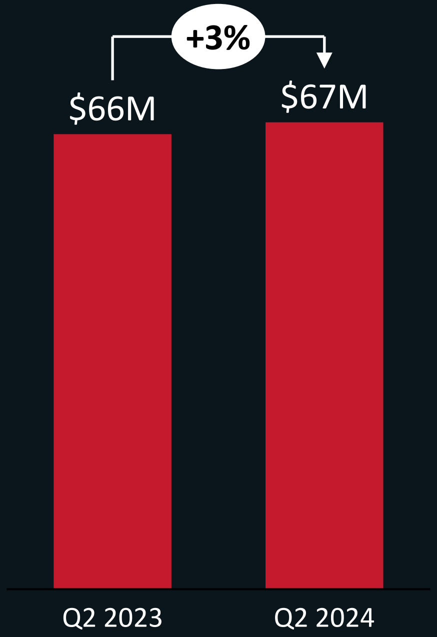


** Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period*

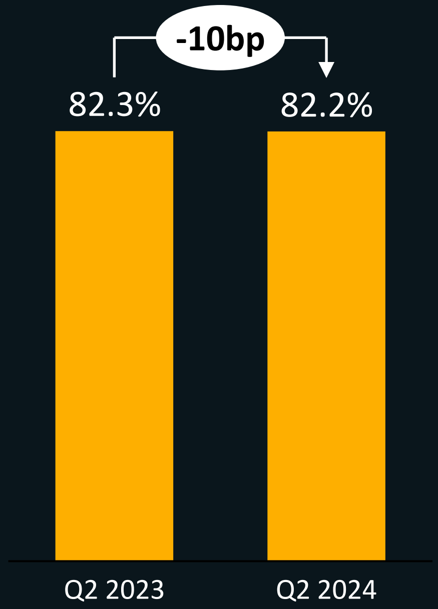
** Numbers are rounded*

Q2 2024 Financial Data

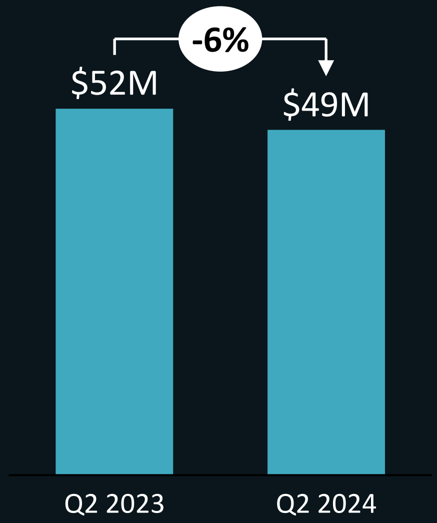
Revenue



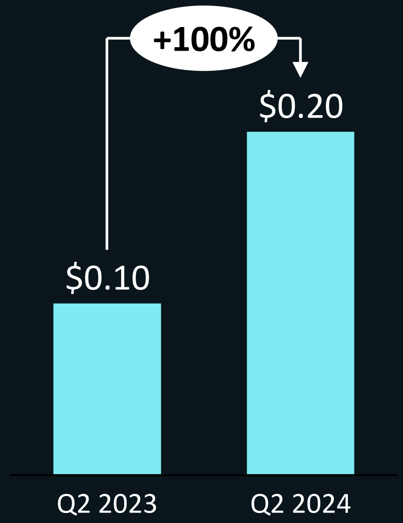
Gross Margin (Non-GAAP)



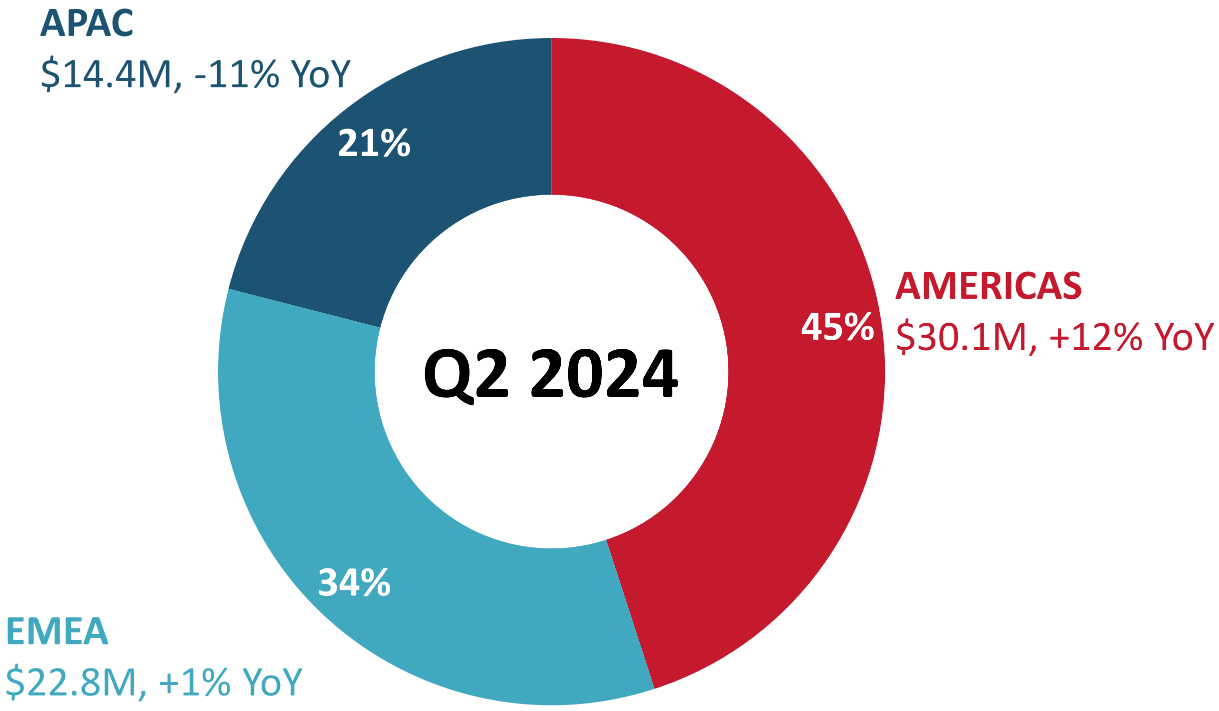
Operating Expenses (Non-GAAP)



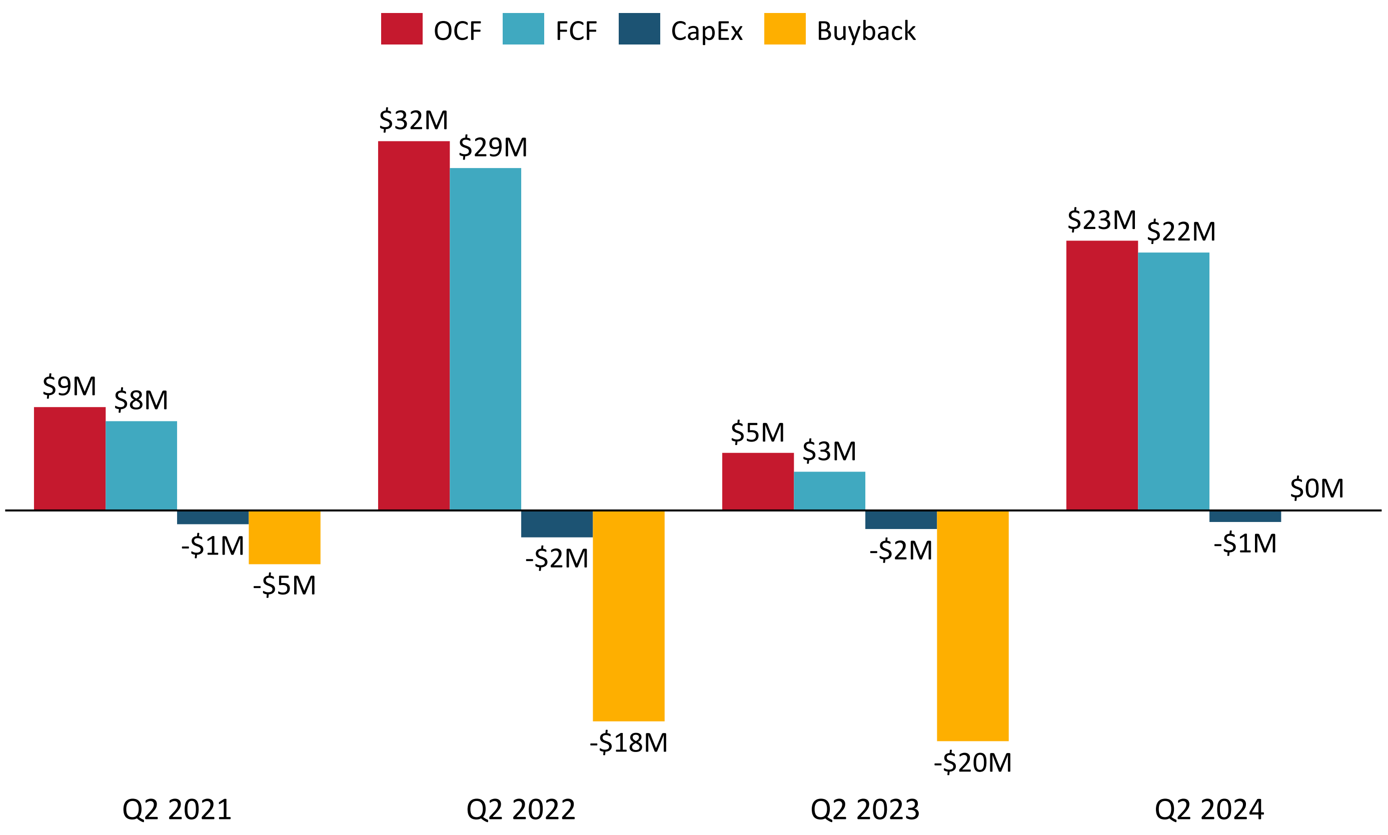
Diluted Earnings Per Share (Non-GAAP)

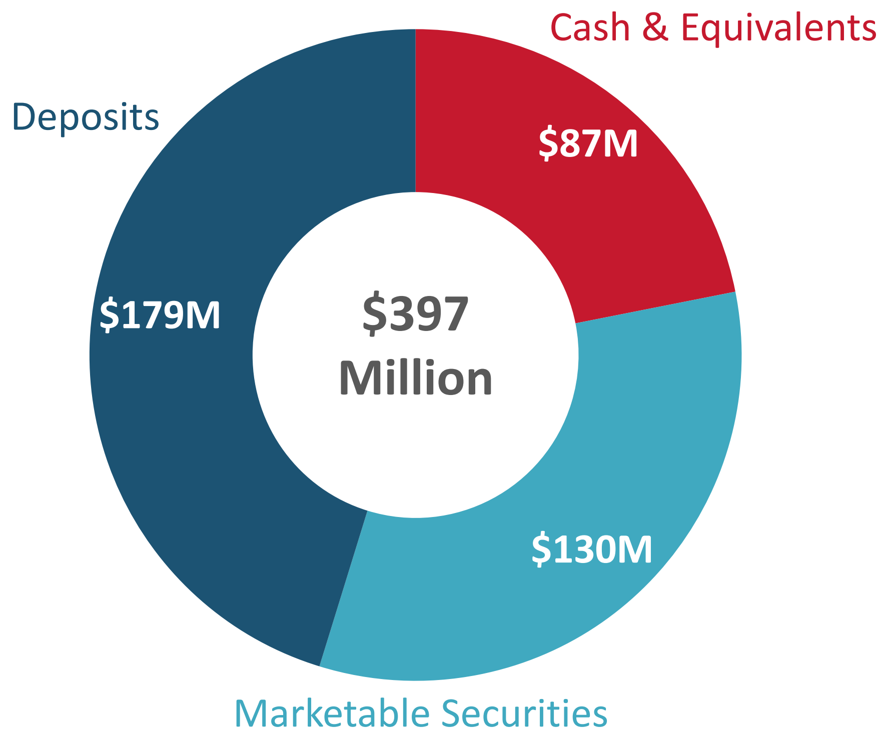


Revenue Geography Breakdown ($M)



Cash Generation





* Numbers are rounded

Thank you!

radware