radware

Investor Presentation

February 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 and volatility of the market for our products; the effects of the current attacks by the terrorist groups Hamas and Hezbollah, and the war between Israel and Hamas and Israel and Hezbollah; natural disasters and public health crises, such as the COVID-19 pandemic; 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; our ability to expand our operations effectively; timely availability and customer acceptance of our new and existing solutions; risks and uncertainties relating to acquisitions or other investments; the impact of economic and political uncertainties and weaknesses in various regions of the world, including the commencement or escalation of hostilities or acts of terrorism; intense competition in the market for cyber security and application delivery solutions and in our industry in general and changes in the competitive landscape; changes in government regulation; outages, interruptions or delays in hosting services or our internal network system; compliance with open source and third-party licenses; the risk that our intangible assets or goodwill may become impaired; our dependence on independent distributors to sell our products; long sales cycles for our solutions; changes in foreign currency exchange rates; real or perceived shortcomings, defects or vulnerabilities in our solutions or if we or our end-users experience security breaches; the availability of components and manufacturing capacity; our reliance on a single managed security service provider to provide us with scrubbing center services; the ability of vendors to provide our hardware platforms and components for our main accessories; our ability to protect our proprietary technology; intellectual property infringement claims made by third parties; changes in tax laws; our ability to realize our investment objectives for our cash and liquid investments; our ability to attract, train and retain highly qualified personnel; 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.](www.radware.com)

This is Radware

Radware's Core Business

Application Availability

Application delivery
- ↗ Alteon
- ↗ Alteon GEL

Application and Data Center Security

Mitigation of denial-of-service and application attacks
- ↗ DPX
- ↗ DefensePro
- ↗ Web DDoS Protection
- ↗ AppWall
- ↗ API Protection

Cloud Security As-a-Service

Mitigation of data centers, web applications, API and automated attacks
- ↗ Cloud DDoS
- ↗ Cloud Web DDoS Protection
- ↗ Cloud WAF
- ↗ Cloud API
- ↗ Bot Manager
- ↗ Client-Side Protection
- ↗ FWaaS

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

1

Shifting
Threat
Landscape

2

Adopting
Cloud

3

Lacking
Security
Skills

4

Accelerating
Risk
with AI

radware | 4

Challenges to Maintaining Application Security

1 **Shifting** Threat Landscape
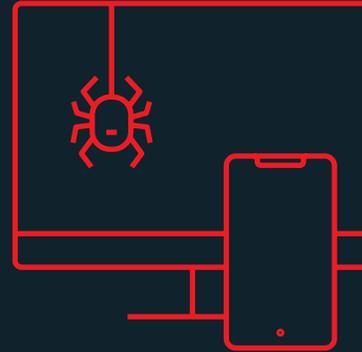
2 **Adopting** Cloud

3 **Lacking** Security Skills

4 **Accelerating** Risk with AI

Shifting Threat Landscape

Shift in
**Attackers'
Motivations**

Shift to
**Attacks on the
Application** Layer

Shift to
Automated Tools

radware | 6

Russian/Ukraine Conflict Ignites New Cyber War Era

Conflict extended beyond the two countries

Pro-Russian Hacktivist Groups

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

Attacking targets in countries that are supporting Ukraine

Religious Groups

Anonymous Sudan, Mysterious Team Bangladesh, DragonForce Malaysia, etc

Cyber attacks against targets who supposedly insulted Muslims

Global Attack Campaigns by Pro-Russian Hacktivists

Canadian PM
(JUN 23)

Credit Agricole
(JUN 23)

Orange Spain
(AUG 23)

Amazon Global
(JUN-SEP 23)

radware

New Disruptive Web DDoS Tsunami Attacks

Requires a behavioral-based 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)

Standard Protections are Not Effective

Network-Based DDoS protection cannot detect & mitigate L7 DDoS attacks

Standard WAF solutions look for vulnerability exploits

Rate-limiting techniques impact legit traffic

→ Available mitigation tools ineffective in detecting & mitigating HTTP/S floods **without impacting legitimate web traffic!**

Challenges to Maintaining Application Security

1

Shifting Threat Landscape

2

Adopting Cloud

3

Lacking Security Skills

4

Accelerating Risk with AI

Cloud Adoption Introduces Uncertainties

Multi-Cloud Creates New Security Risks

Azure

aws

Private Cloud

Legacy Data Center

Kubernetes

87% Use a combination of two or three types of environments

61% Think protection coverage between platforms is a problem

56% Think that security policy consistency is a problem

→ Need for **consistent security** across all clouds

Sources: Radware Market Report: Application Security in a Multi-Cloud World 2023

Challenges to Maintaining Application Security

1 **Shifting** Threat Landscape

2 **Adopting** Cloud

3 **Lacking** Security Skills

4 **Accelerating** Risk with AI

radware | 13

Lacking Security Skills

+18%
demand for cyber security experts

~4M
Workforce gap worldwide (+12.6% YoY)

67%
businesses are facing skill shortages

41%
can't find enough qualified talent

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

Sources: 2023 (ISC)² Cybersecurity Workforce Study & Survey by Gaper ISSA/ESG

Challenges to Maintaining Application Security

(1)

Shifting Threat Landscape

(2)

Adopting Cloud

(3)

Lacking Security Skills

(4)

Accelerating Risk with AI

Accelerating Risks with AI

Attackers & defenders become more powerful with Artificial Intelligence

→ AI-powered tools used to **craft automated & highly adaptive attacks**

→ AI helps identify and then **weaponize zero-day vulnerabilities**

→ AI-driven botnets used to **orchestrate massive DDoS attacks**

→ Fight AI with AI: Need **AI-powered, adaptive protections** to stay ahead.

Challenges to Maintaining Application Security

1 **Shifting** Threat Landscape

- DDoS shift to the Web
- Rise in web & bot based attacks
- More sophisticated, automated tools

2 **Adopting** Cloud

- Multi-cloud creates new security risks
- According to Radware's survey most of the respondents think there is no consistency in security policy

3 **Lacking** Security Skills

- Lack of security experience
- Underqualified & overwhelmed teams

4 **Accelerating** Risk with AI

- AI-powered tools to craft highly adaptive attacks
- AI used to quickly 'weaponize' 0-day vulnerabilities
- AI-driven botnets to generate DDoS attacks

radware | 17

radware

What is Needed to Stay Ahead?

What is Needed to Stay Ahead?

Intelligent Security

Automated, real-time protections based on AI + ML-based algorithms that evolve as the attacks morph

Consistent Protections

360-degree, consistent protection across all environments and entry points

Expert Defense

Access to security experts 24/7 during attack and in peacetime

Radware 360 Application Protection

Dedicated to Protecting Your Applications
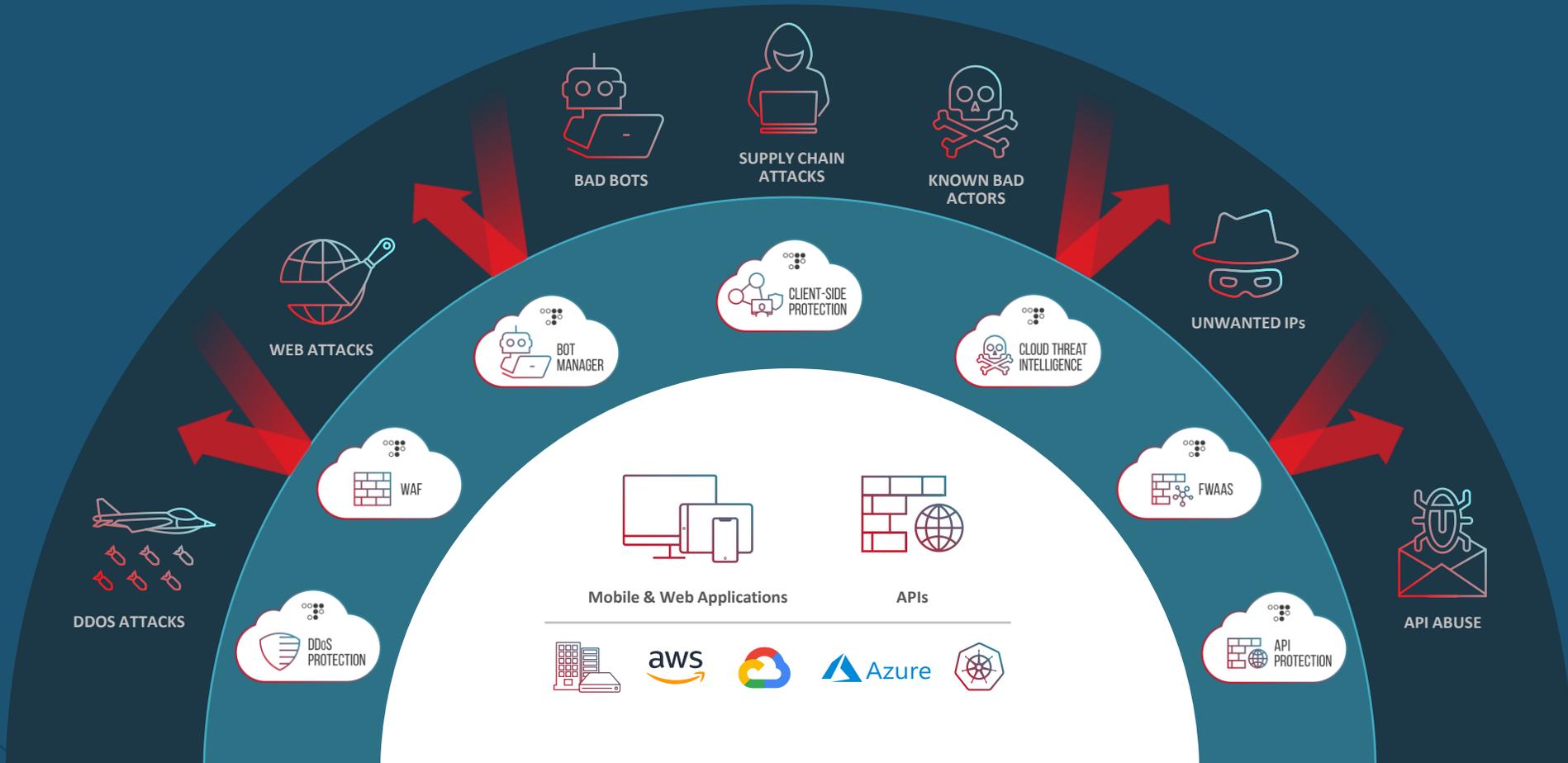
The Radware Difference

Intelligent Security, Consistent Protections, Expert Defense.

Intelligent Security

- Automated AI & ML based detection & mitigation
- Real-time, zero-day protection
- Adaptive & continuous learning
- No human intervention

Consistent Protections

- Any environment – on-prem, private and public clouds, K8S
- Web, mobile, API, server-side, browser-side, third party JS
- Single pane of glass

Expert Defense

- Managed services
- 24/7 ERT security experts
- Industry-leading SLA
- Reduce TCO

Global Cloud Services Network

Dual local PoP for reduced latency and regulations compliance
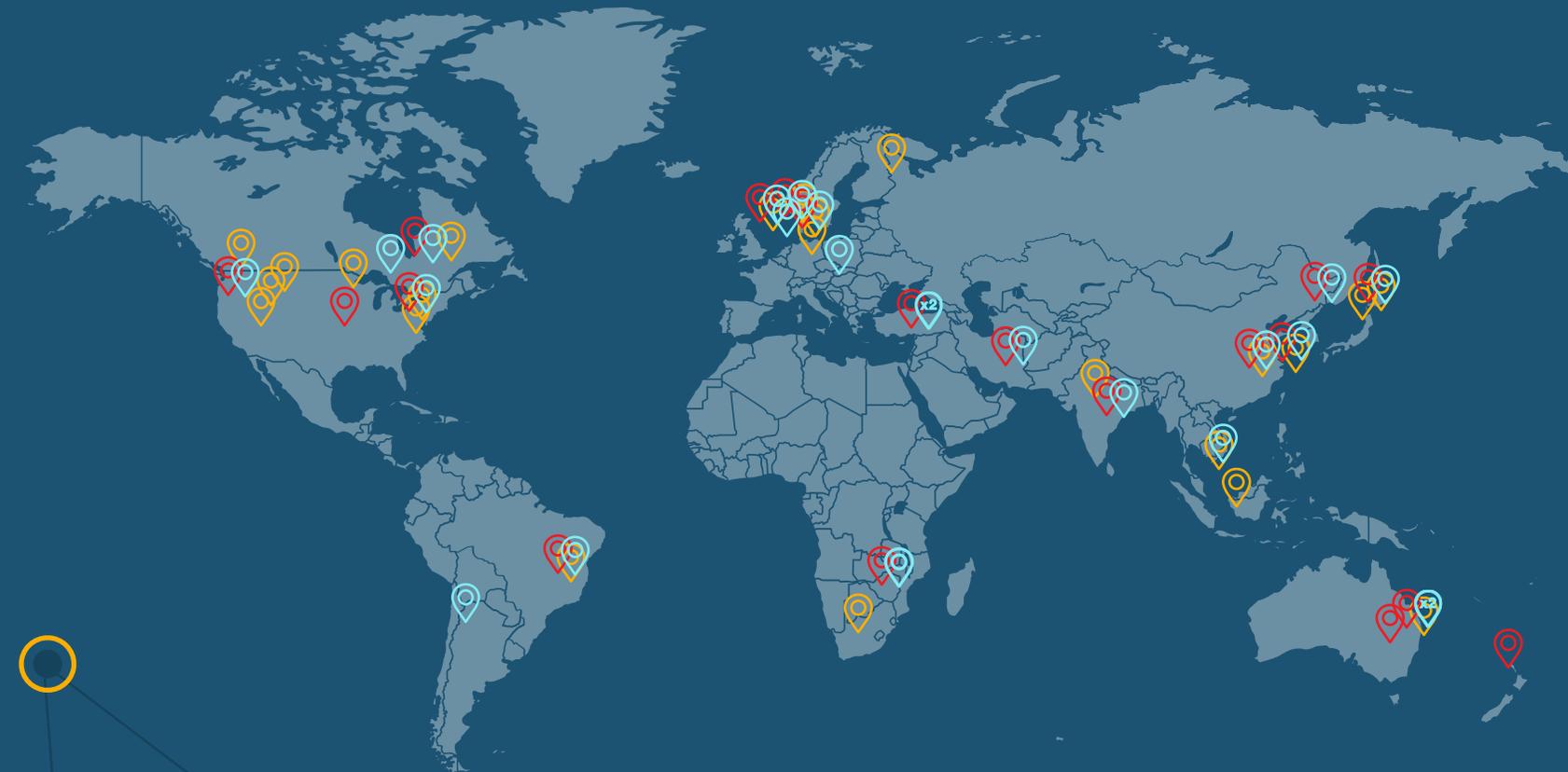
19 Scrubbing centers **Worldwide**

12 Tbps of global mitigation capacity

40+ **AppSec PoPs** With Global Coverage

DDoS MITIGATION SCRUBBING CENTER   CLOUD WAF PoP   BOT MANAGER SERVICE CENTER

radware | 22
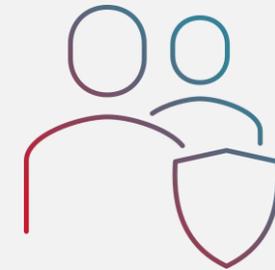
Reduce TCO With Fully Managed Services

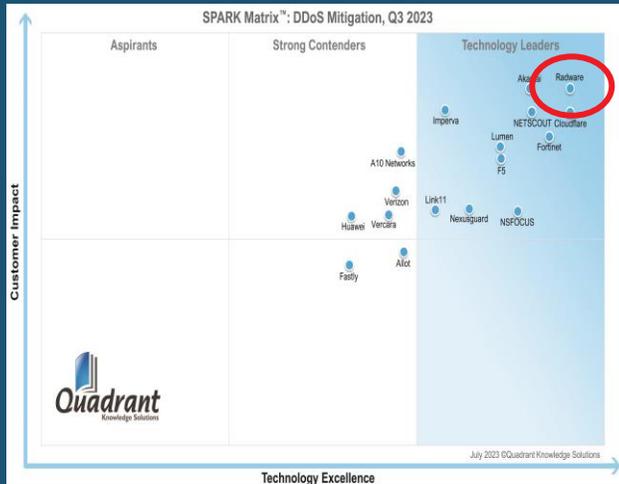Take the Burden Off Your Shoulders

Under Attack Immediate Service 24/7

Security Policy Configuration & Tuning

Outsource to Radware's Security Experts

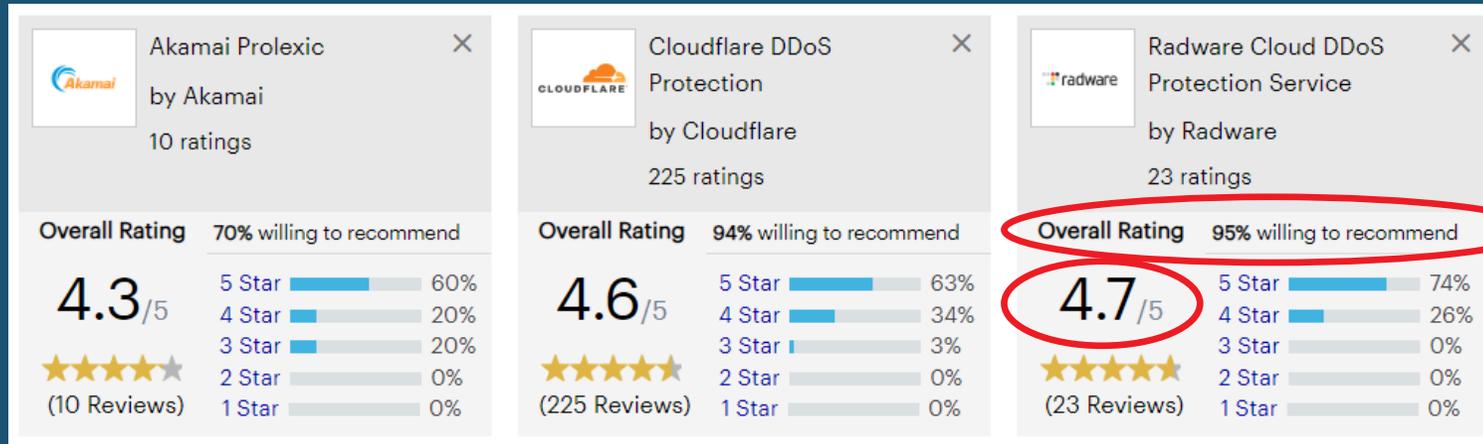# Winning Industry Recognition 2023

DDoS Mitigation 2023
LEADER

Bot Management 2023
LEADER
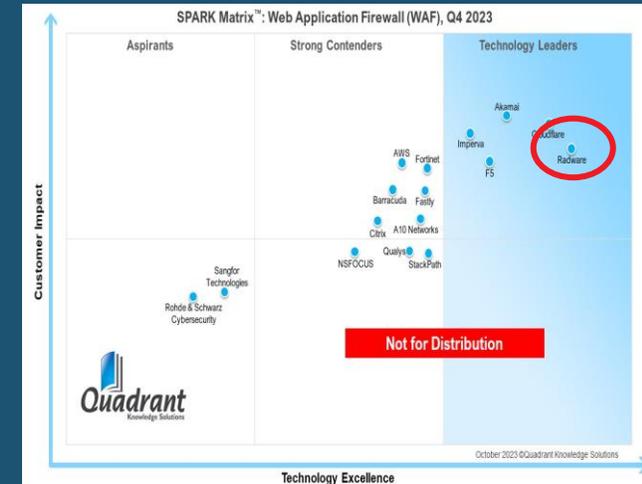
Web Application Firewall 2023
TECH LEADER

Market Leaders in Customer Recognition

Gartner peer insights™

Akamai Prolexic
by Akamai
10 ratings

Overall Rating — 70% willing to recommend
4.3/5
- 5 Star — 60%
- 4 Star — 20%
- 3 Star — 20%
- 2 Star — 0%
- 1 Star — 0%
(10 Reviews)

Cloudflare DDoS Protection
by Cloudflare
225 ratings

Overall Rating — 94% willing to recommend
4.6/5
- 5 Star — 63%
- 4 Star — 34%
- 3 Star — 3%
- 2 Star — 0%
- 1 Star — 0%
(225 Reviews)

Radware Cloud DDoS Protection Service
by Radware
23 ratings

Overall Rating — 95% willing to recommend
4.7/5
- 5 Star — 74%
- 4 Star — 26%
- 3 Star — 0%
- 2 Star — 0%
- 1 Star — 0%
(23 Reviews)

Radware Cloud WAF Service Reviews
by Radware in Cloud Web Application and API Protection
4.7 ★★★★★ 149 Ratings

Radware Bot Manager Reviews
by Radware in Online Fraud Detection
4.6 ★★★★★ 26 Ratings

Radware DefensePro Reviews
by Radware in DDoS Mitigation Solutions
4.6 ★★★★★ 51 Ratings

"Truly exceptional protection for web apps & APIs"
Telecommunication industry, company size $1B–3B

"ML & AI technology for threat detection & mitigation"
Manufacturing industry, company size $3B–10B

"Fortifying our online presence against the rising threat of DDoS attacks"
Healthcare and Biotech industry, company size $250M–500M

radware | 25

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
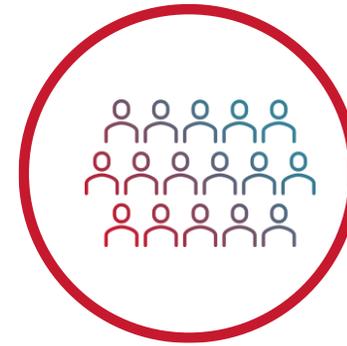
radware |

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

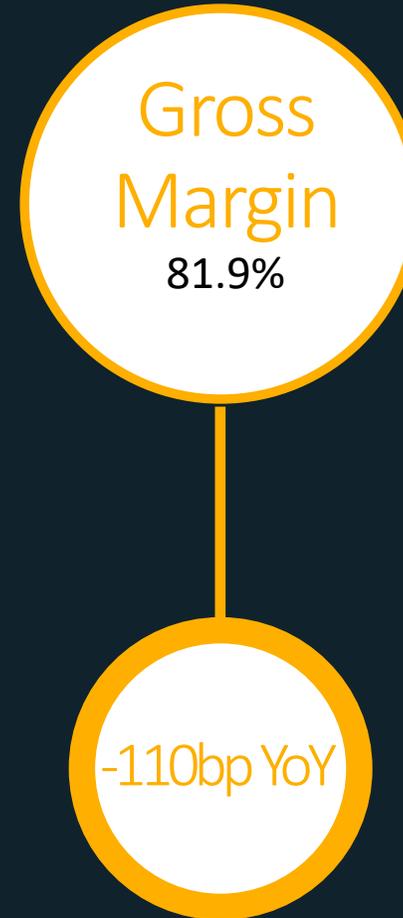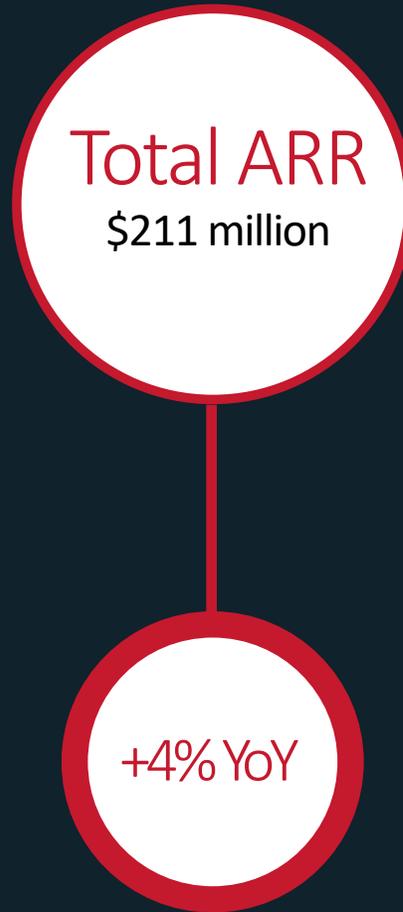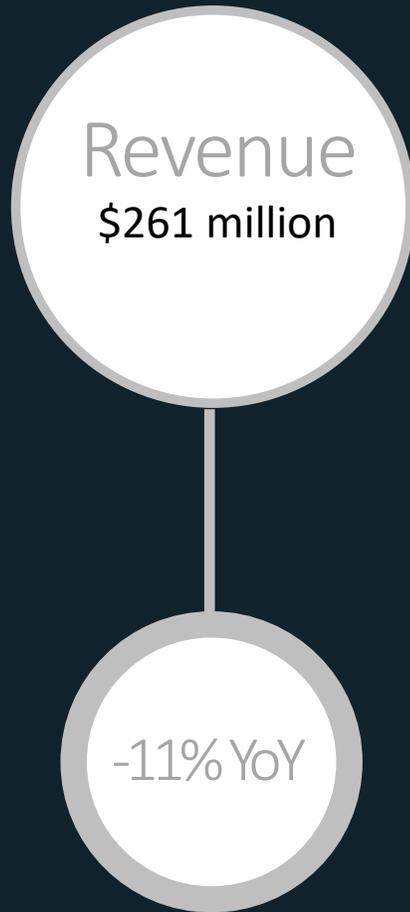- Promoting inclusion of underrepresented communities

Financial Overview

Q4 2023 Highlights
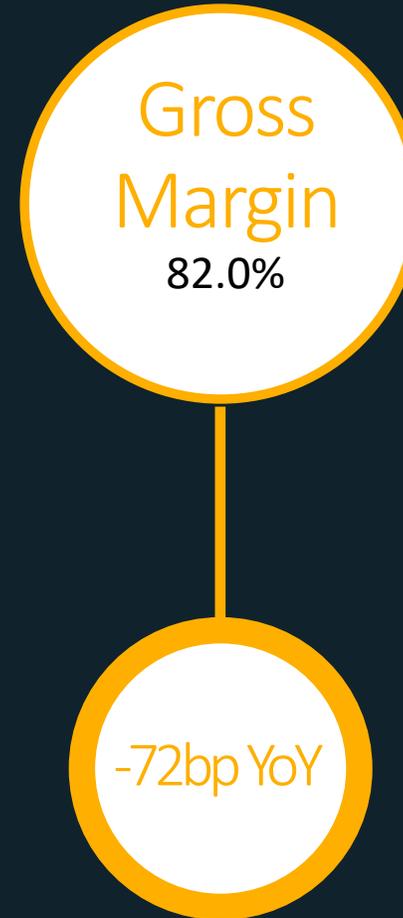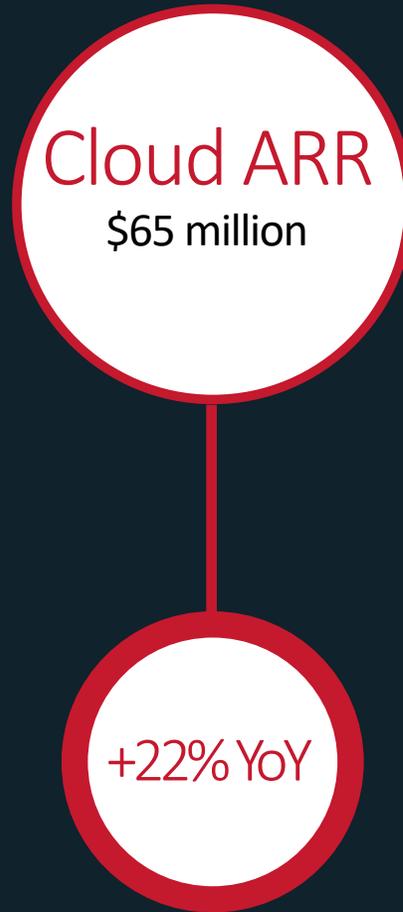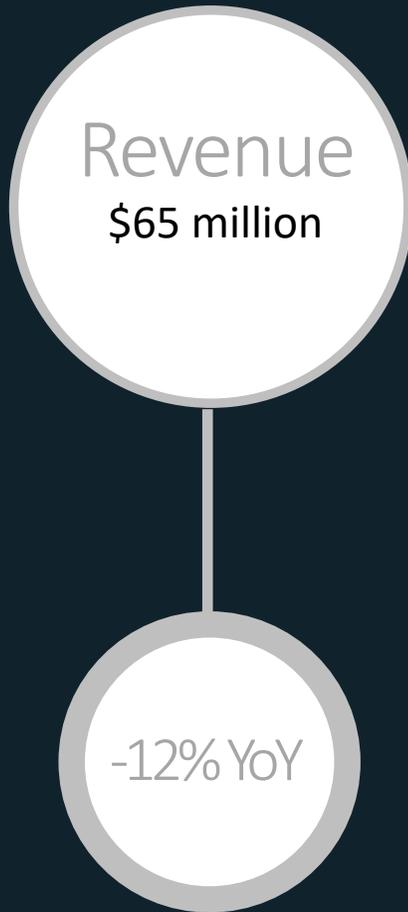
Revenue
$65 million

Cloud ARR
$65 million

Gross Margin
82.0%
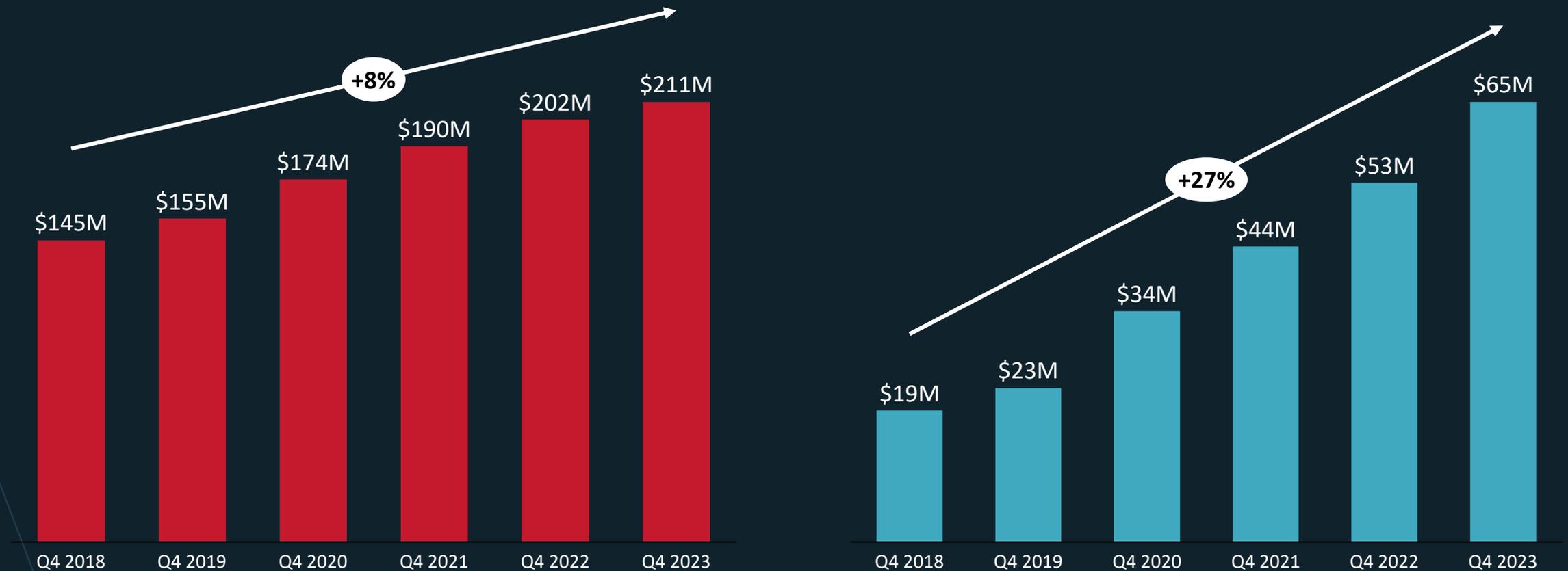
EPS
$0.13

-12% YoY

+22% YoY

-72bp YoY

-24% YoY

* 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

radware | 29

2023 Highlights

Revenue
$261 million

-11% YoY

Total ARR
$211 million

+4% YoY

Gross Margin
81.9%

-110bp YoY

EPS
$0.43

-37% YoY

* 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
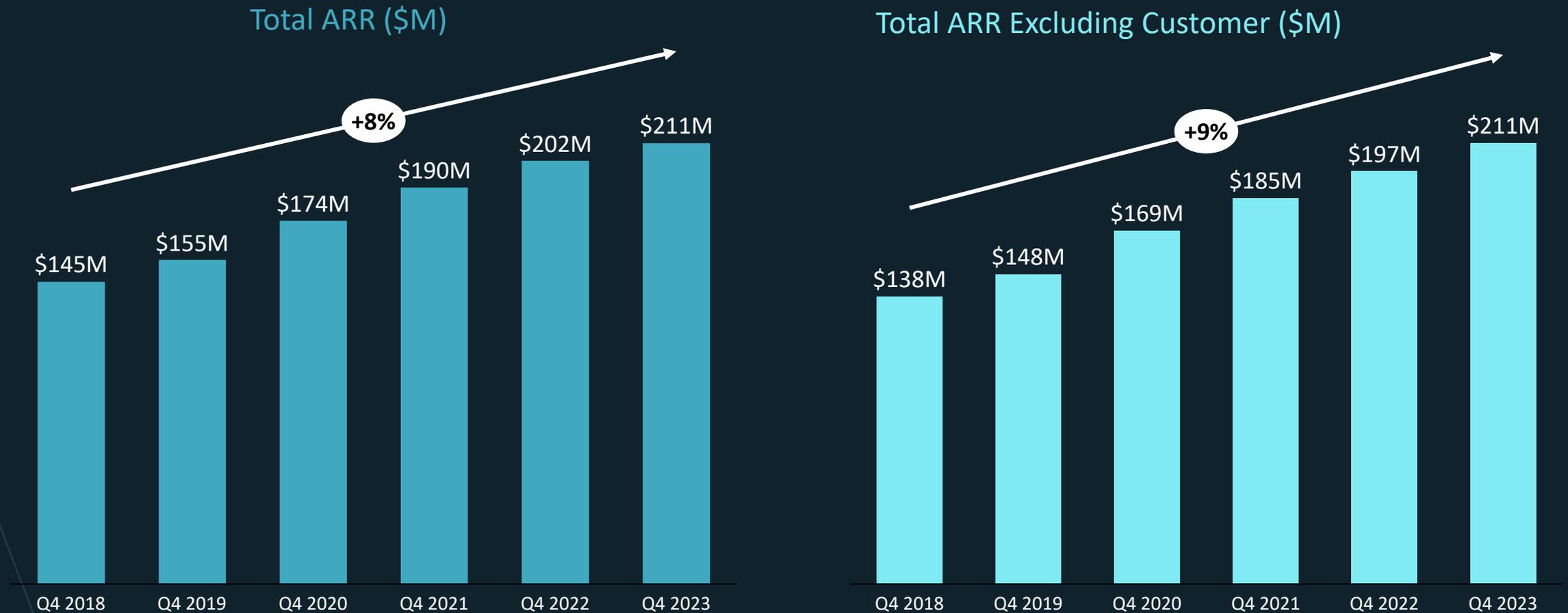
Total ARR Driven by Cloud ARR

+8%

Q4 2018	Q4 2019	Q4 2020	Q4 2021	Q4 2022	Q4 2023
$145M	$155M	$174M	$190M	$202M	$211M

+27%

Q4 2018	Q4 2019	Q4 2020	Q4 2021	Q4 2022	Q4 2023
$19M	$23M	$34M	$44M	$53M	$65M

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
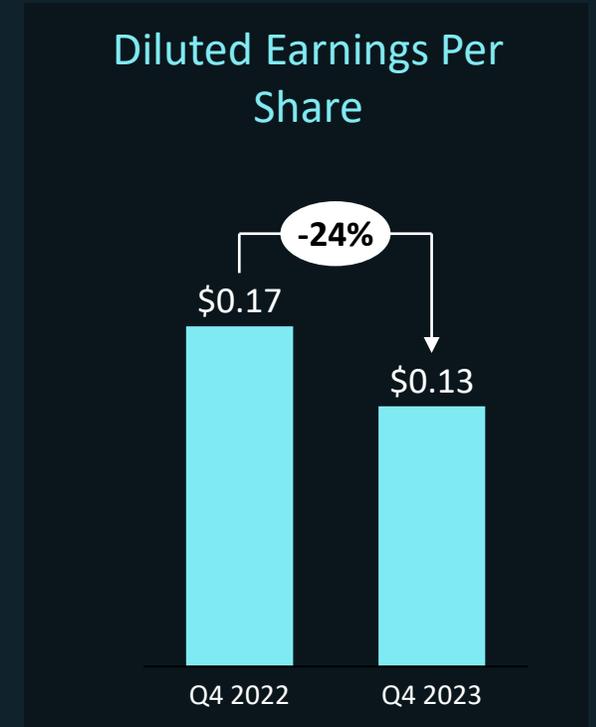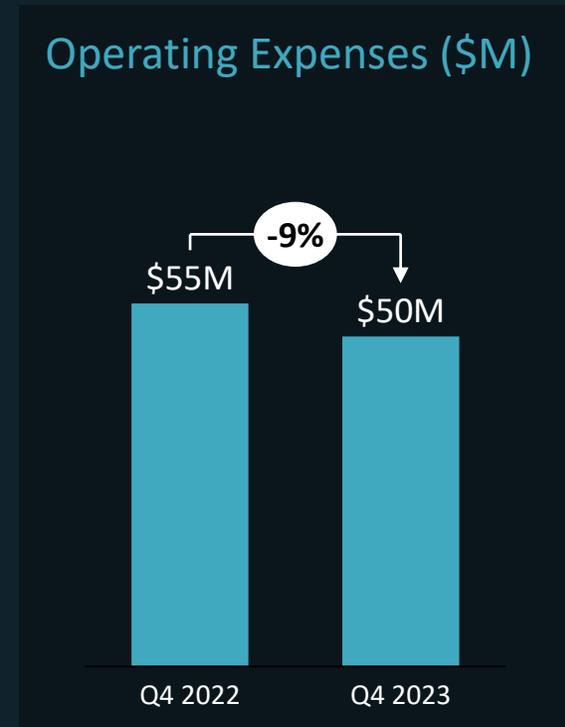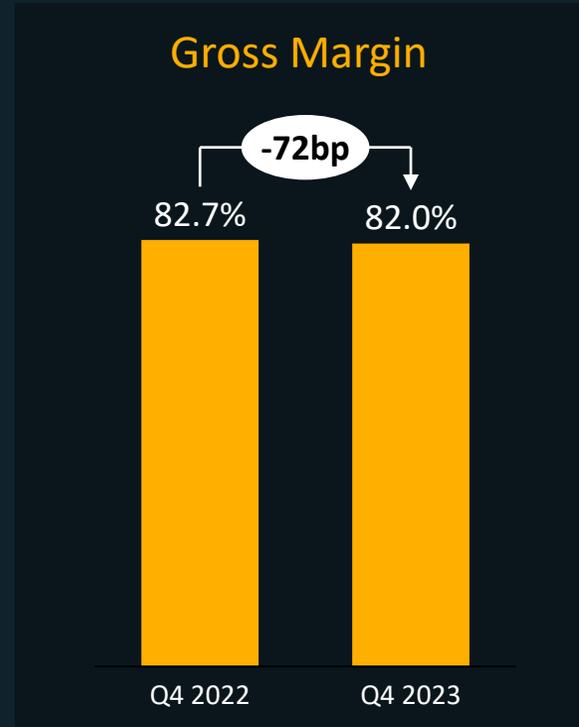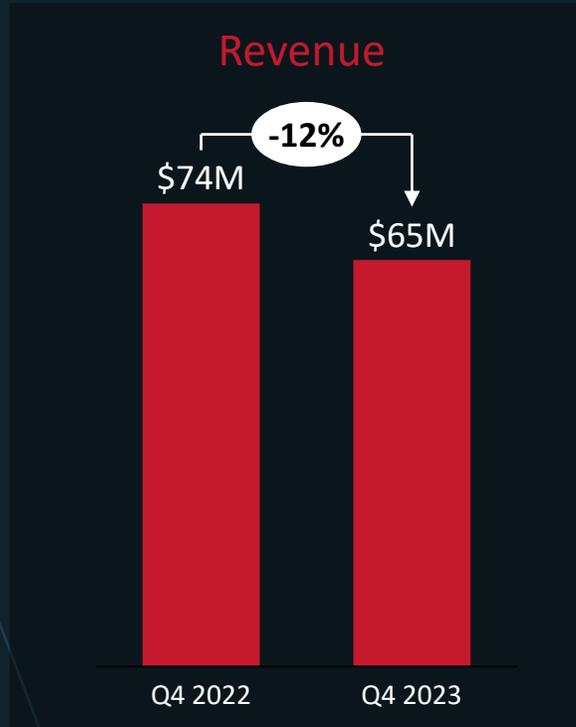
Numbers are rounded

Total ARR Excluding Customer Termination Agreement

Total ARR ($M)

Total ARR Excluding Customer ($M)

Total ARR ($M):
- Q4 2018: $145M
- Q4 2019: $155M
- Q4 2020: $174M
- Q4 2021: $190M
- Q4 2022: $202M
- Q4 2023: $211M
- +8%

Total ARR Excluding Customer ($M):
- Q4 2018: $138M
- Q4 2019: $148M
- Q4 2020: $169M
- Q4 2021: $185M
- Q4 2022: $197M
- Q4 2023: $211M
- +9%

* 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
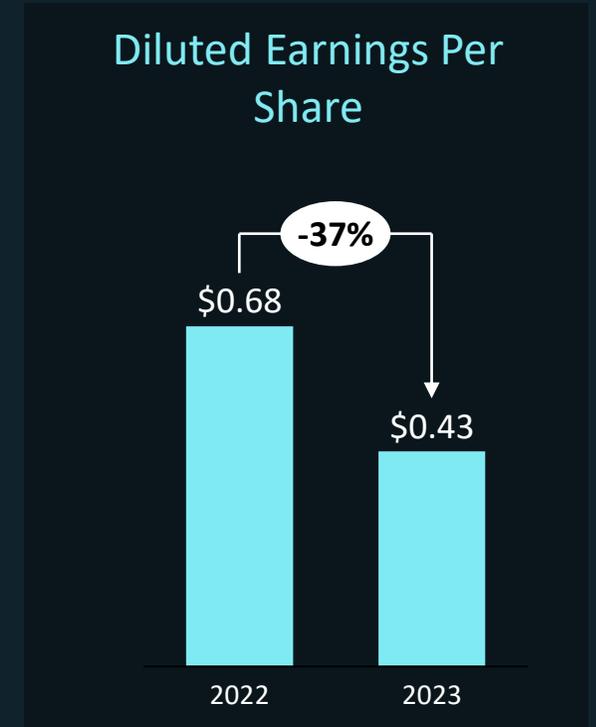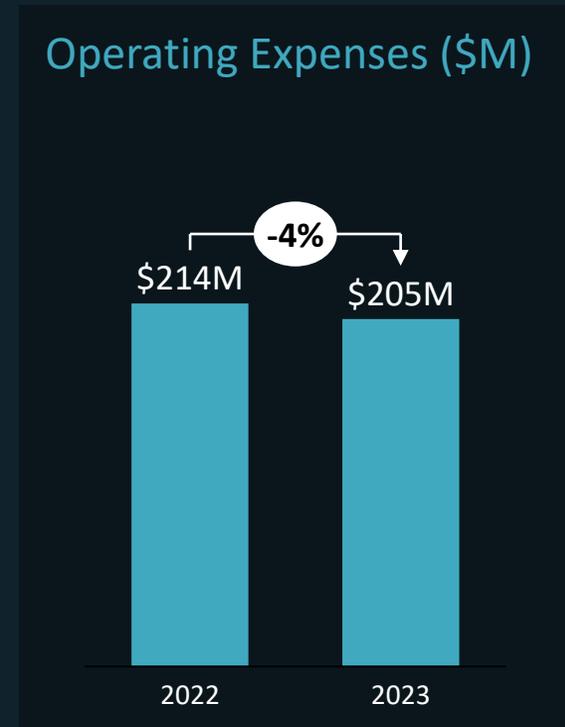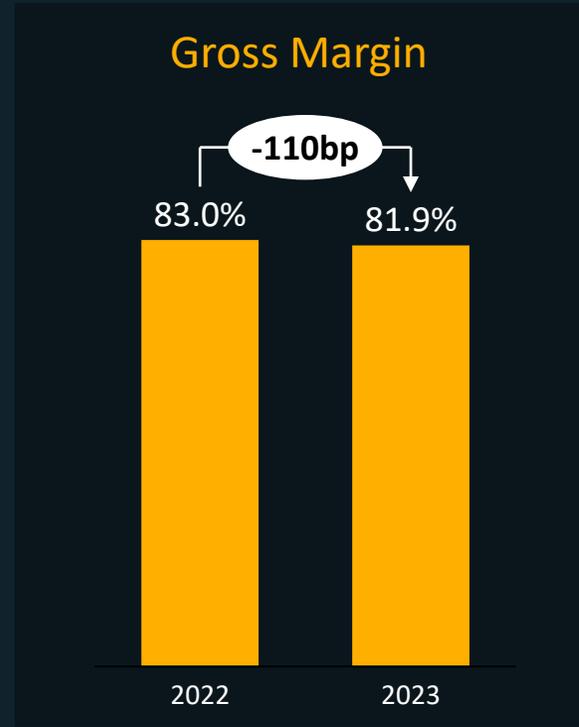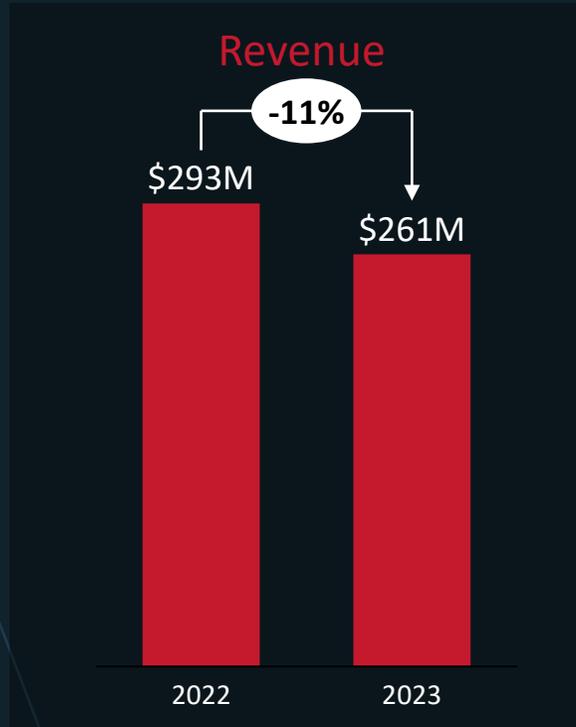
* Numbers are rounded

Q4 2023 Financial Data

Revenue

-12%

$74M

$65M

Q4 2022   Q4 2023

Gross Margin

-72bp

82.7%

82.0%

Q4 2022   Q4 2023

Operating Expenses ($M)

-9%

$55M

$50M

Q4 2022   Q4 2023

Diluted Earnings Per Share

-24%

$0.17

$0.13

Q4 2022   Q4 2023

* All numbers are non-GAAP

radware | 33

2023 Financial Data

Revenue

-11%

$293M

$261M

2022   2023

Gross Margin

-110bp

83.0%   81.9%

2022   2023

Operating Expenses ($M)

-4%

$214M $205M

2022   2023

Diluted Earnings Per Share

-37%

$0.68

$0.43

2022   2023

* All numbers are non-GAAP

Geography Breakdown ($M)

Q4 2023

APAC
$15.5M, -13% YoY
24%

AMERICAS
$24.6M, -23% YoY
38%

EMEA
$24.9M, +2% YoY
38%

2023

APAC
$61.4M, -6% YoY
23%

AMERICAS
$103.4M, -17% YoY
40%

EMEA
$96.5M, -7% YoY
37%

Cash Generation

Legend: OCF (red), FCF (light blue), CapEx (dark blue), Buyback (yellow)

2020
- OCF: $64M
- FCF: $55M
- CapEx: -$9M
- Buyback: -$45M

2021
- OCF: $72M
- FCF: $66M
- CapEx: -$6M
- Buyback: -$52M

2022
- OCF: $32M
- FCF: $23M
- CapEx: -$9M
- Buyback: -$59M

2023
- OCF: -$4M
- FCF: -$9M
- CapEx: -$5M
- Buyback: -$63M

$364 Million
- Cash & Equivalents: $70.6M
- Marketable Securities: $119.5M
- Deposits: $173.7M

* Numbers are rounded

radware | 36

Thank you!

radware