



Investor Presentation

May 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 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

Challenges to Maintaining Application Security

1

Shifting
Threat
Landscape

2

Adopting
Cloud

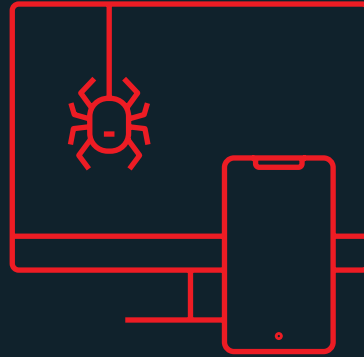
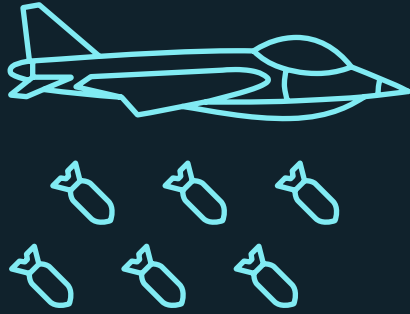
3

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

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)

NoName057(16)



Не удалось получить доступ к сайту

Узнали, что канадский премьер Джастин 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.

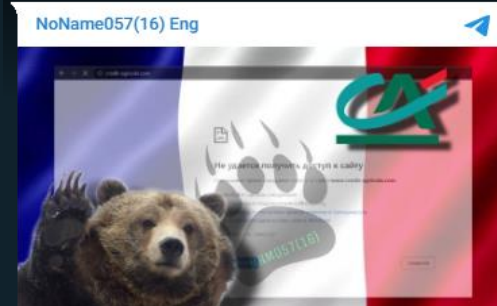
Подписывайтесь на канал NoName057(16)
Вступайте в наш DDoS-проект
Подписывайтесь на резервный канал
Eng version

Победа За нами!

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

Credit Agricole (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>

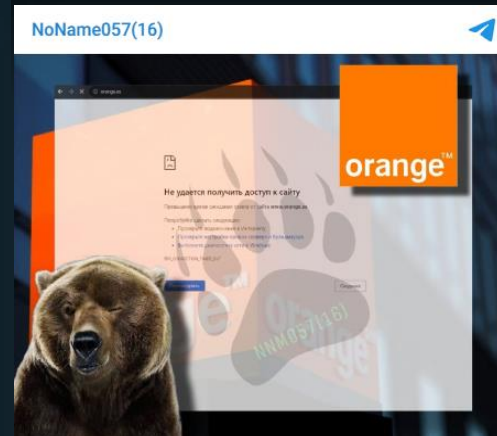
Subscribe to NoName057(16)
Join our DDoS-project
Subscribe to reserve channel

Victory will be ours!

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

Orange Spain (AUG 23)

NoName057(16)



Не удалось получить доступ к сайту

The site administrators of the Spanish operator Orange Espagne, sensing our attack, closed the resource for foreigners:

✗ <https://check-host.net/check-report/10ccb5bek8da>

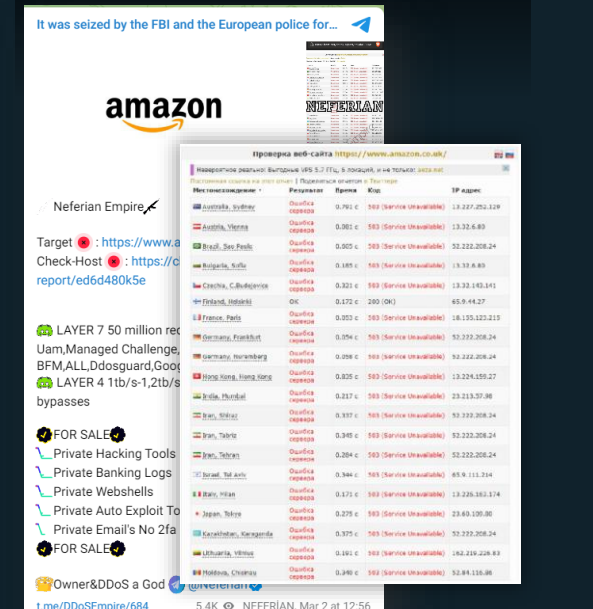
Subscribe to the channel NoName057(16)
Join our DDoS project
Subscribe to the backup channel
Eng version

Victory is behind us!

t.me/noname05716/4330 5.2K Christmas 28 at 13:34

Amazon Global (JUN-SEP 23)

It was seized by the FBI and the European police for...




Neferian Empire

Target: <https://www.amazon.co.uk/>
Check-Host: <https://check-host.net/check-report/ed6d480k5e>

LAYER 7 50 million requests
Uam, Managed Challenge, BFM, ALL Ddosguard, Google, Layer 4 1tb/s-1,2tb/s bypasses

FOR SALE
Private Hacking Tools
Private Banking Logs
Private Webshells
Private Auto Exploit Tool
Private Email's No Zf

Owner & DDoS a God
t.me/DDoSEmpire/684 5.4K NEFERIAN, Mar 2 at 12:56



amazon.co.uk

We're sorry

An error occurred when we tried to process your request. We're working on the problem and expect to resolve it shortly. Please note that if you were trying to place an order, it will not have been processed at this time. Please try again later.

We apologize for the inconvenience.

Click here to return to the Amazon.co.uk home page

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



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

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



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

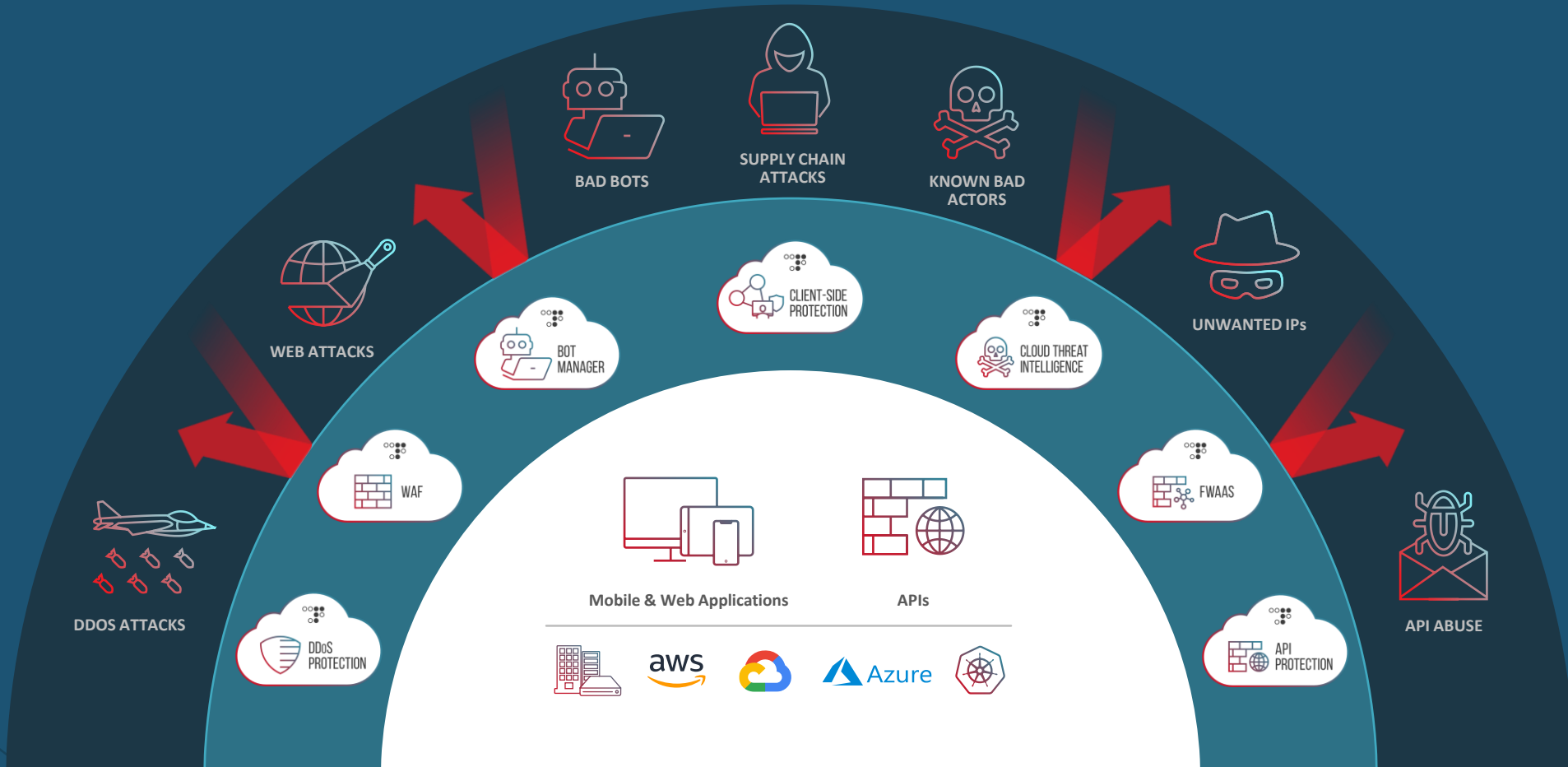


Expert Defense

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

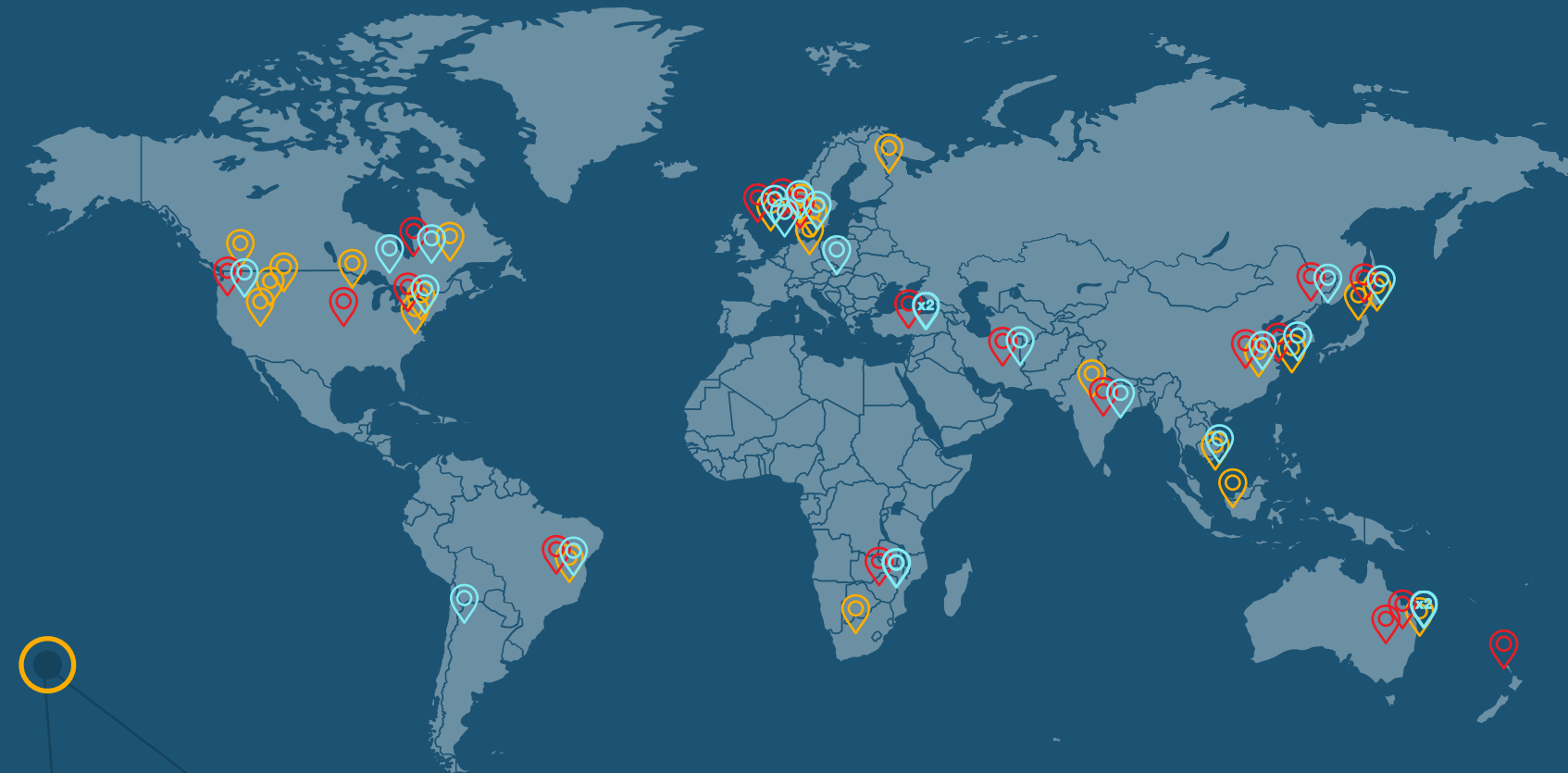


Expert Defense

- 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

Reduce TCO With Fully Managed Services

Take the Burden Off Your Shoulders



Under Attack
Immediate Service
24/7

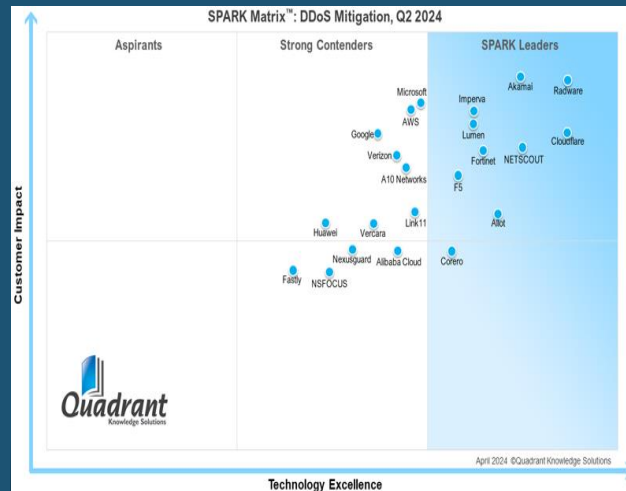


Security Policy
Configuration
& Tuning



Outsource to
Radware's
Security Experts

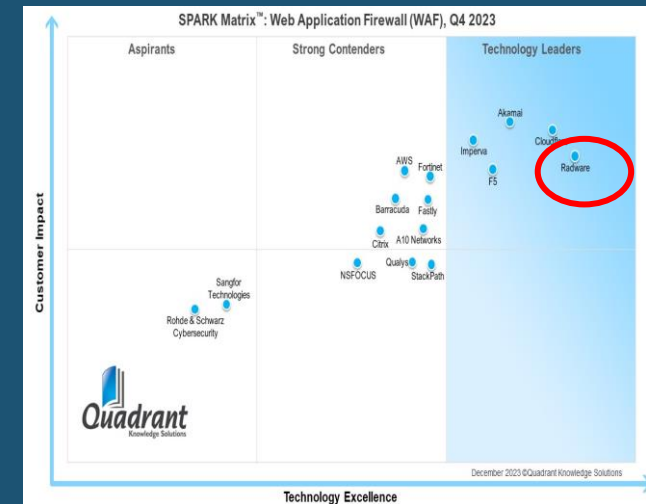
Winning Industry Recognition



DDoS Mitigation 2024
LEADER

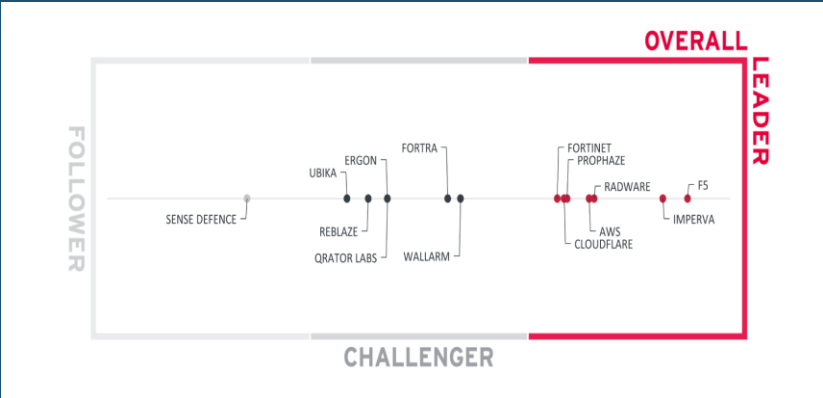


Bot Management 2023
LEADER

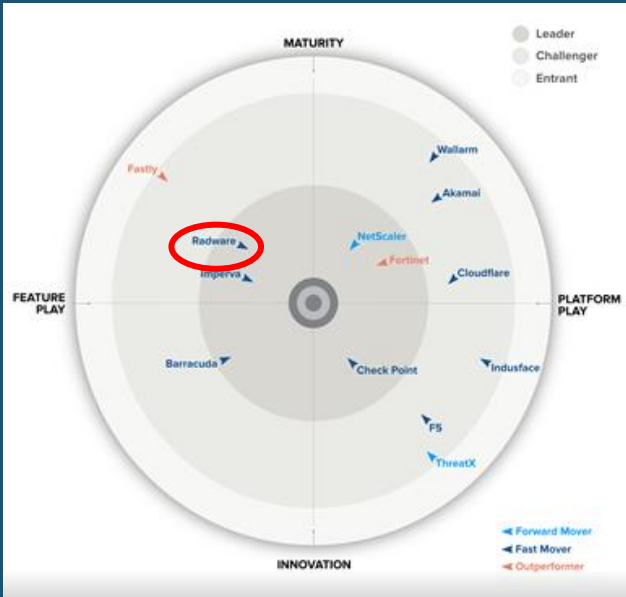


Web Application Firewall 2023
TECH LEADER

Winning Industry Recognition



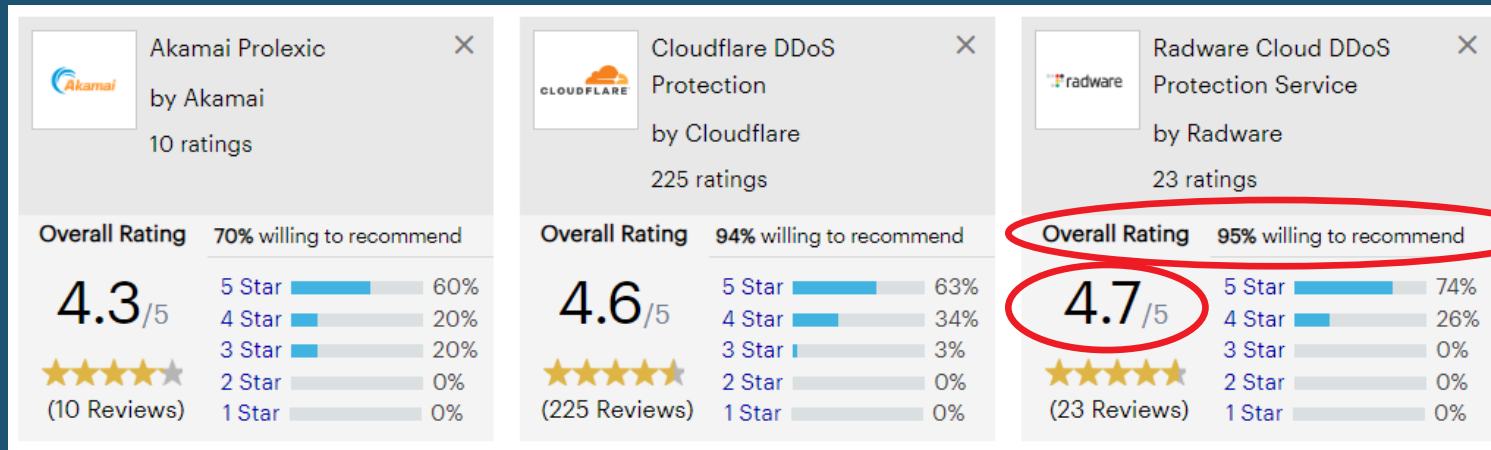
Web Application Firewall Q1 2024
LEADER



Application and API Security 2024
LEADER

| | AVERAGE SCORE | KEY FEATURES |
|----------------|----------------|-------------------------------------|
| | | AI-Enhanced Vulnerability Detection |
| ★★★★ | Exceptional | ↑↓ |
| ★★★★ | Superior | ↑↓ |
| ★★★ | Capable | |
| ★★ | Limited | |
| * | Poor | |
| — | Not Applicable | |
| Akamai | 3.4 | ★★★ |
| Barracuda | 4 | ★★★★ |
| Check Point | 4 | ★★ |
| Cloudflare | 3.1 | ★★ |
| F5 | 3.4 | ★★★ |
| Fastly | 3.1 | ★★★ |
| Fortinet | 3.7 | ★★★★ |
| Imperva | 4.1 | ★★★★ |
| Indusface | 2.6 | * |
| NetScaler | 3.6 | — |
| Radware | 3.9 | ★★★★★ |
| ThreatX | 3.3 | — |
| Wallarm | 3.3 | ★★★ |

Market Leaders in Customer Recognition



“Truly exceptional protection for web apps & APIs”

Telecommunication industry, company size \$1B–3B

“Fortifying our online presence against the rising threat of DDoS attacks”

Healthcare and Biotech industry, company size \$250M–500M

“ML & AI technology for threat detection & mitigation”

Manufacturing industry, company size \$3B–10B

Gartner Peer Insights VoC report for Cloud Web Application and API Protection: “99% of our customers are willing to recommend Radware”.

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

Financial Overview



Q1 2024 Highlights

Revenue
\$65.1 million

-6% YoY

Cloud ARR
\$67 million

+22% YoY

Gross
Margin
82.0%

-30bp YoY

EPS
\$0.16

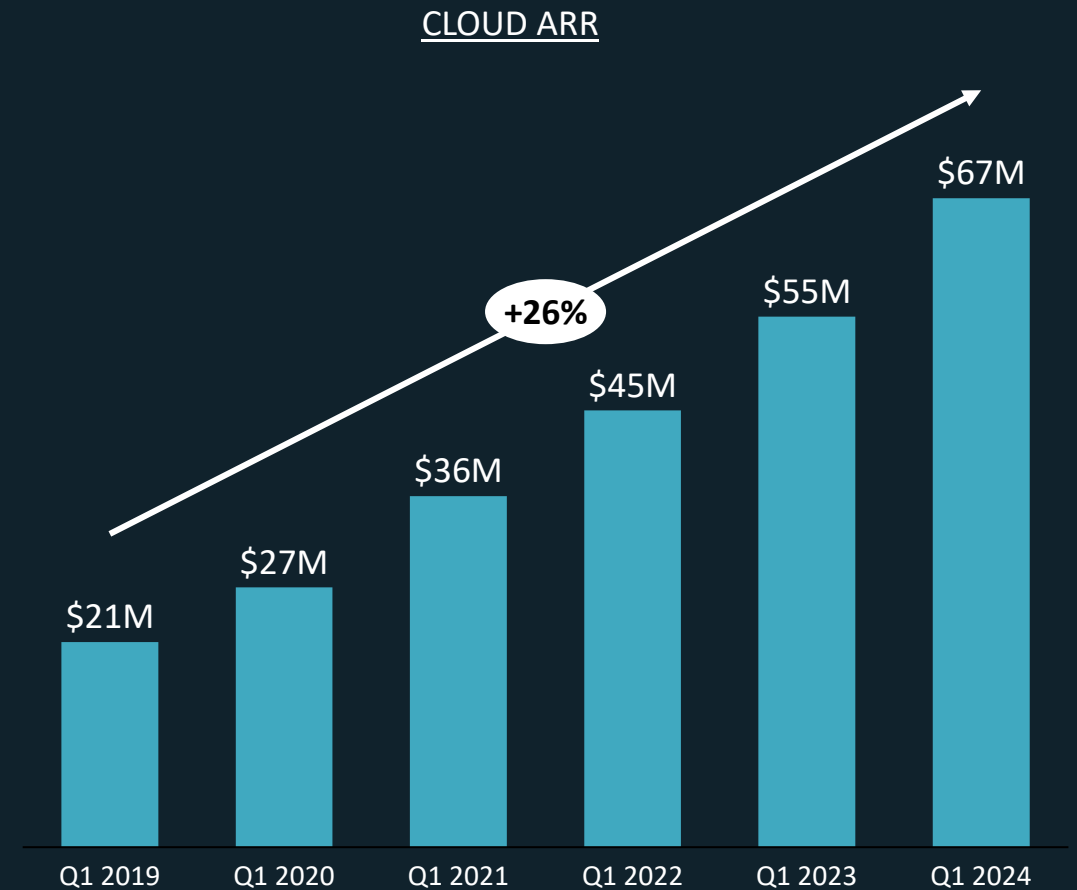
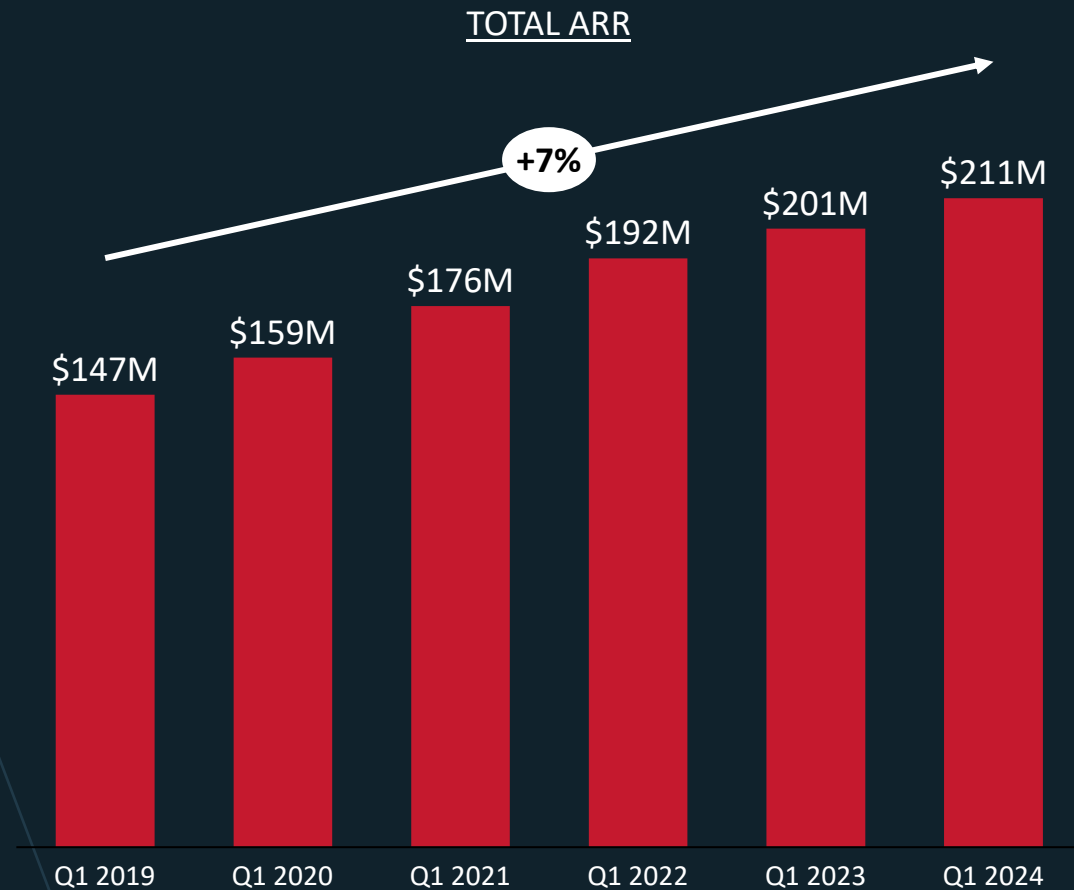
+14% YoY

Operating
CF
\$21.1 million

Compared to
-\$1.2M
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*

Total ARR Driven by Cloud ARR



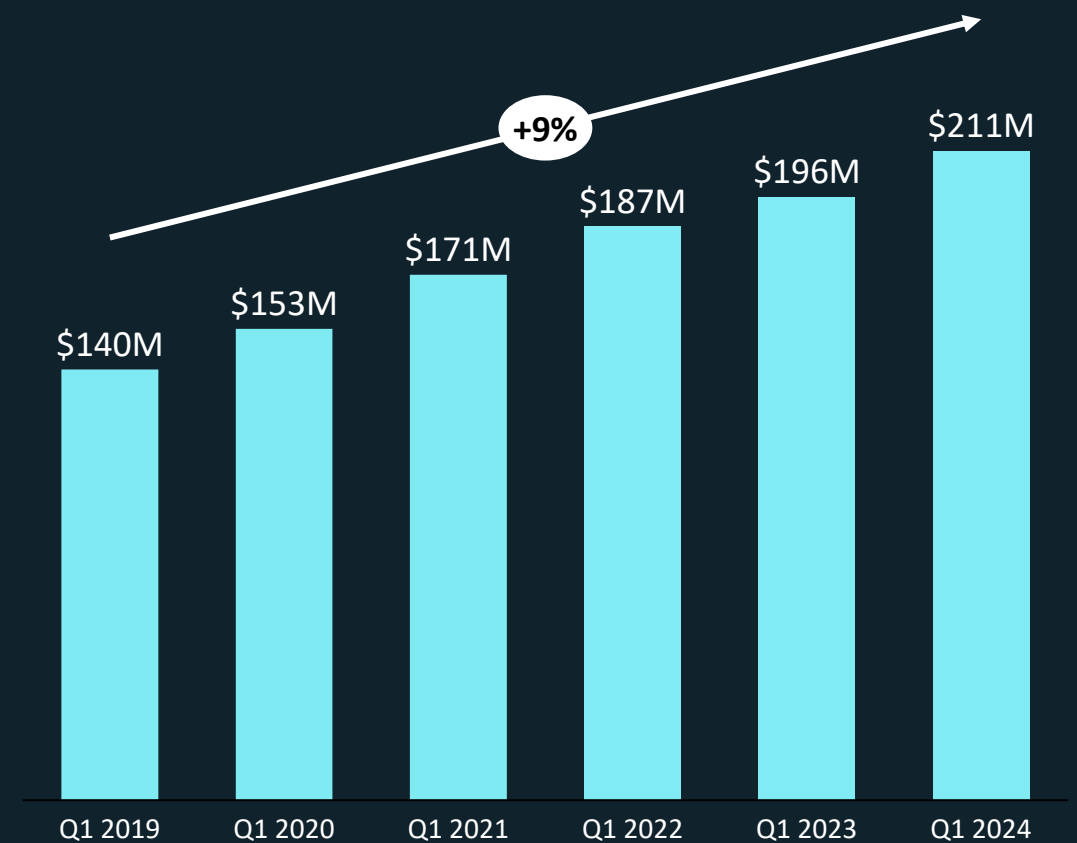
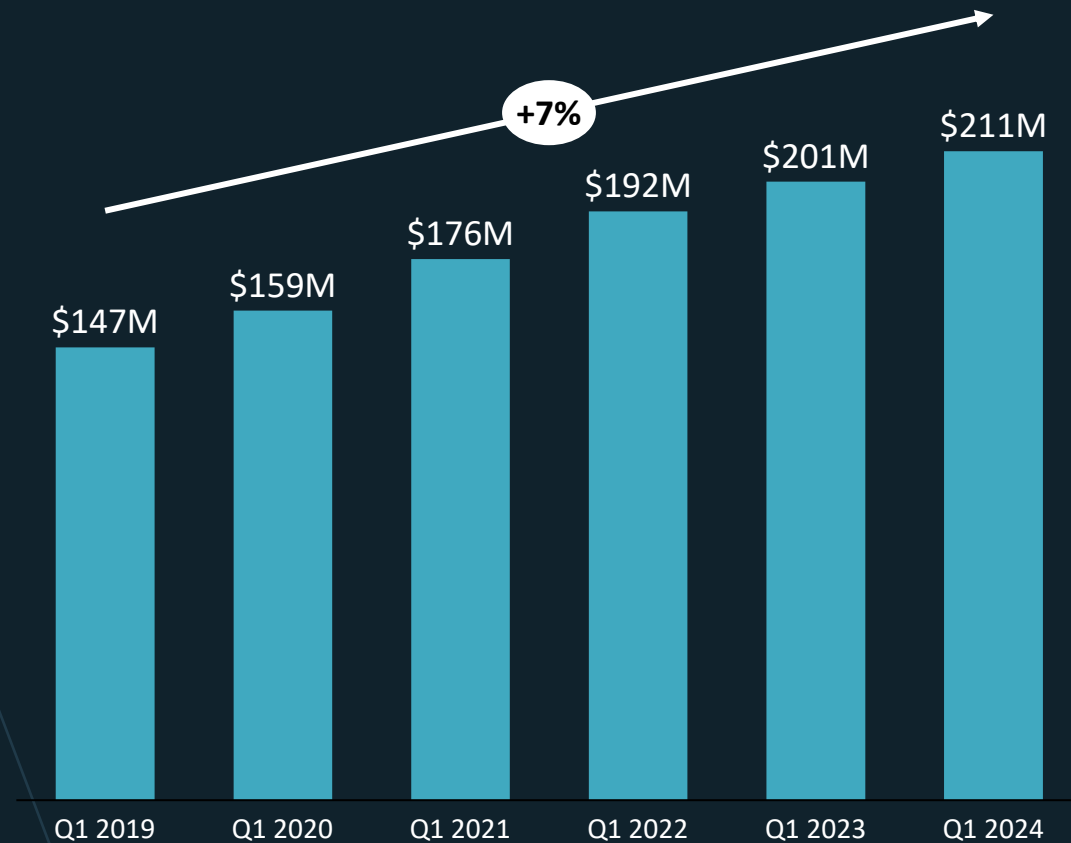
* Total ARR includes the annualized value of booked orders for services, subscription licenses and maintenance contracts that are in effect at the end of a reporting period

* Numbers are rounded

Total ARR Excluding Customer Termination Agreement

Total ARR (\$M)

Total ARR Excluding Customer (\$M)



* 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

Q1 2024 Financial Data

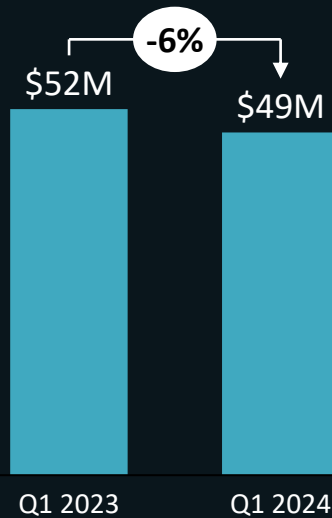
Revenue



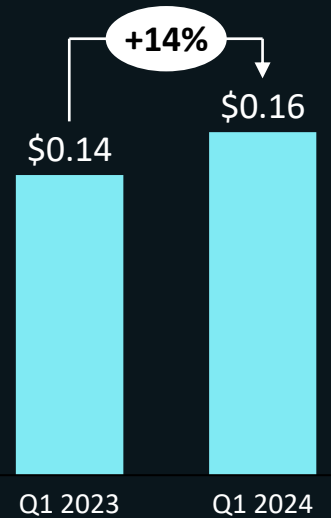
Gross Margin



Operating Expenses (\$M)

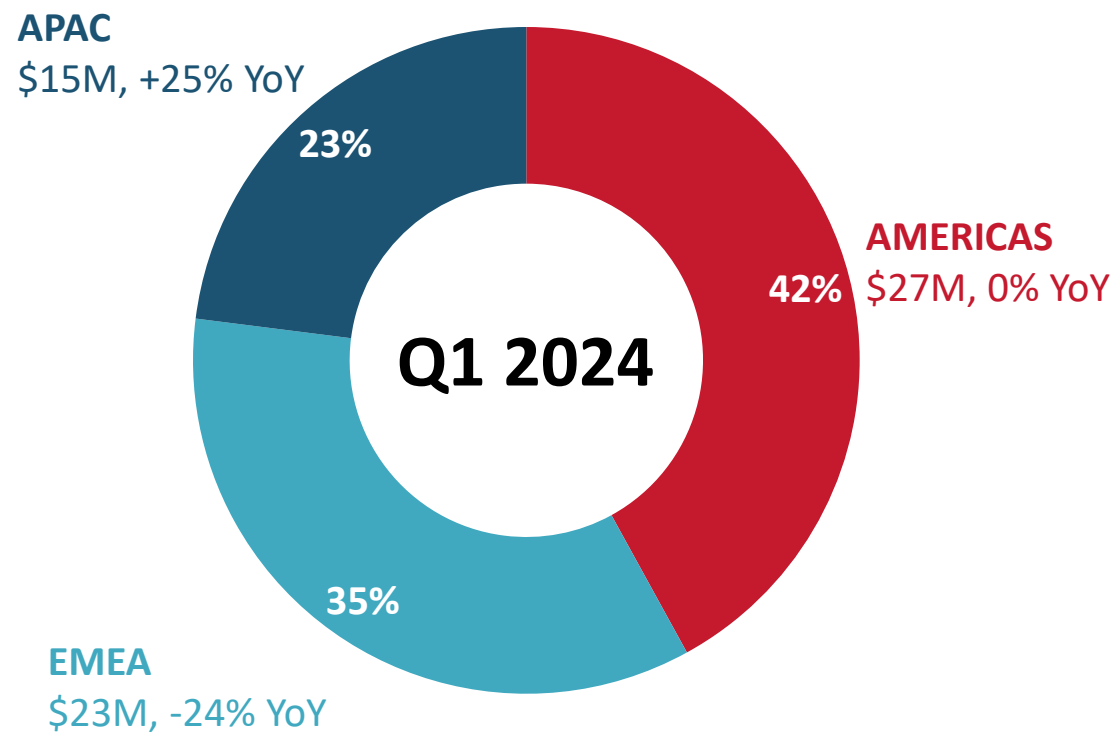


Diluted Earnings Per Share

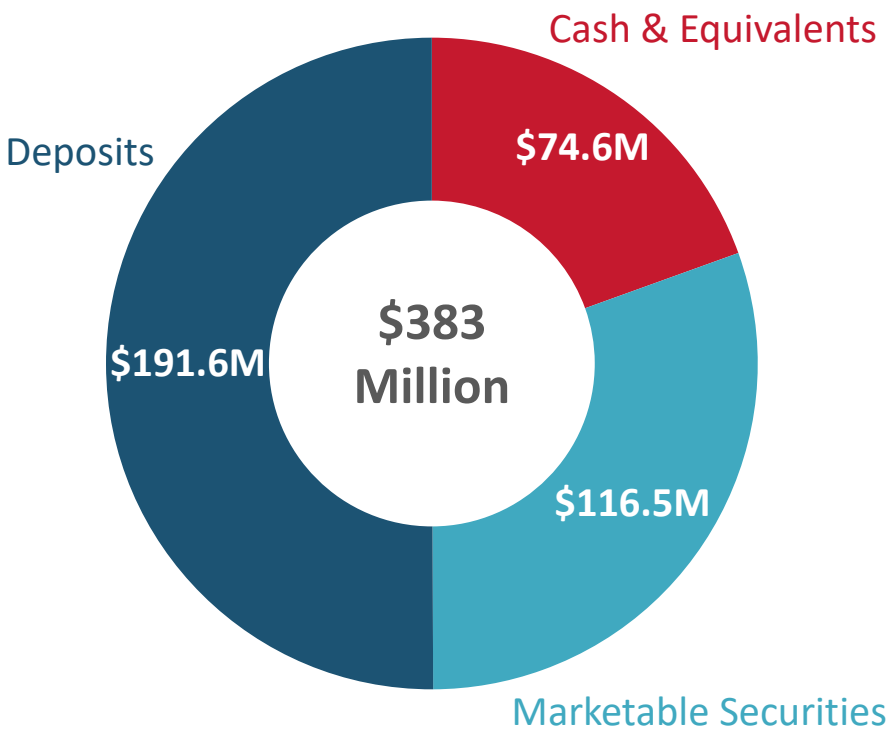
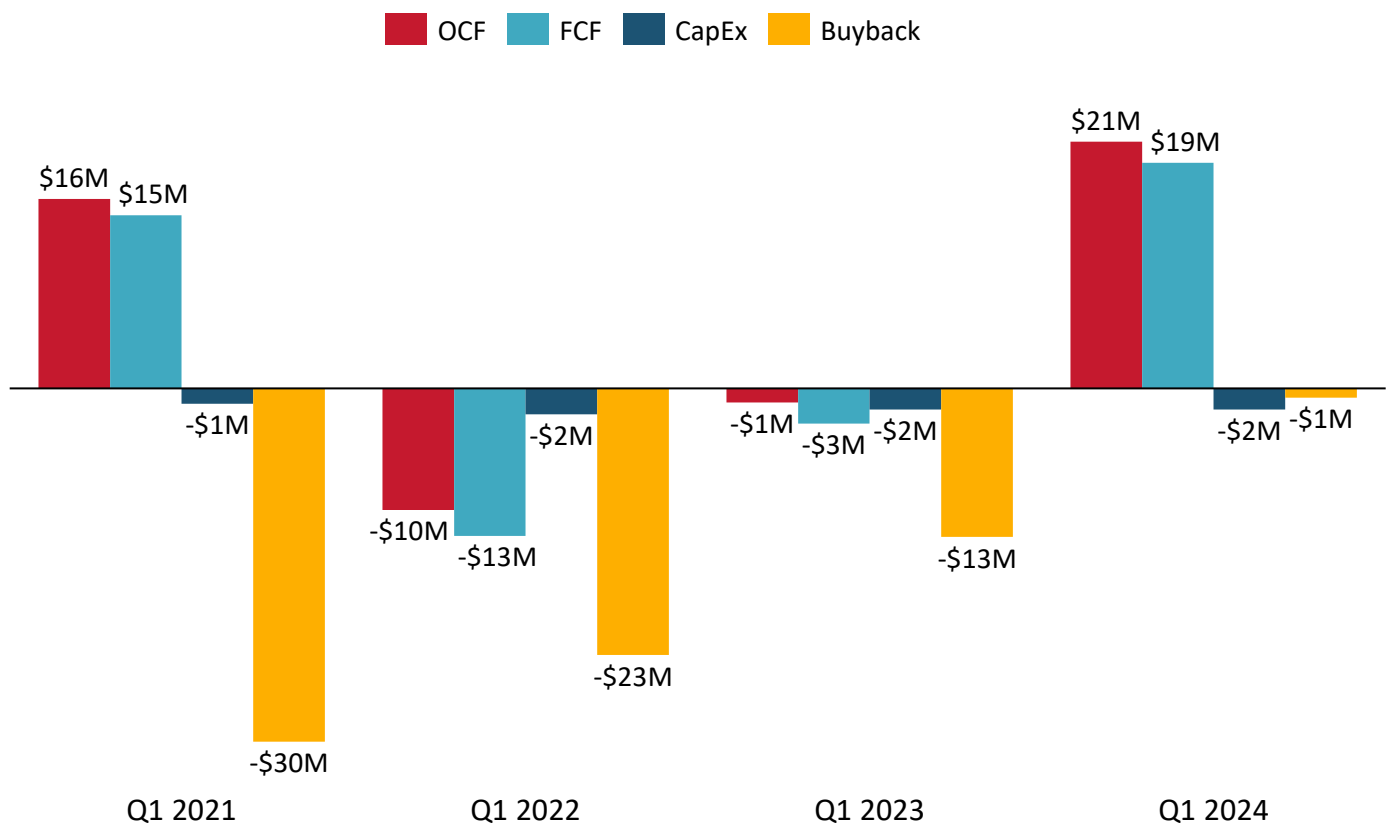


* All numbers are non-GAAP

Revenue Geography Breakdown (\$M)



Cash Generation



* Numbers are rounded



Thank you!

