

# Investor and Analyst Day

February 2023



# AGENDA

## **Radware's Journey and Strategy**

Roy Zisapel: President and CEO

## **Scaling Go-To-Market**

Yoav Gazelle: Chief Business Officer

## **Good Enough Security is NOT Good Enough**

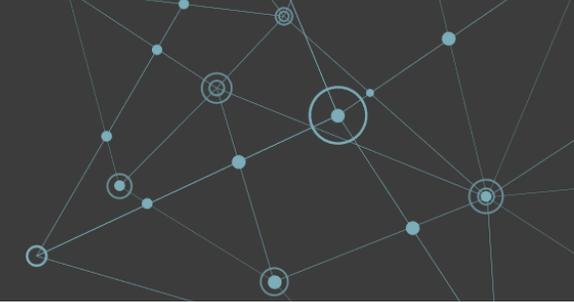
David Aviv: Chief Technology Officer

## **Driving Profitable Growth**

Guy Avidan: Chief Financial Officer

## **Q&A**

# 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; 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](http://www.sec.gov) or may be obtained on Radware’s website at [www.radware.com](http://www.radware.com).*

# Radware's Journey and Strategy

**Roy Zisapel**

President and CEO

# Why Radware?



Leading Critical Cyber Security Vendor



Large Growing TAM and SAM



Leading Differentiated Technology



Large Enterprise and Carriers Customer Base

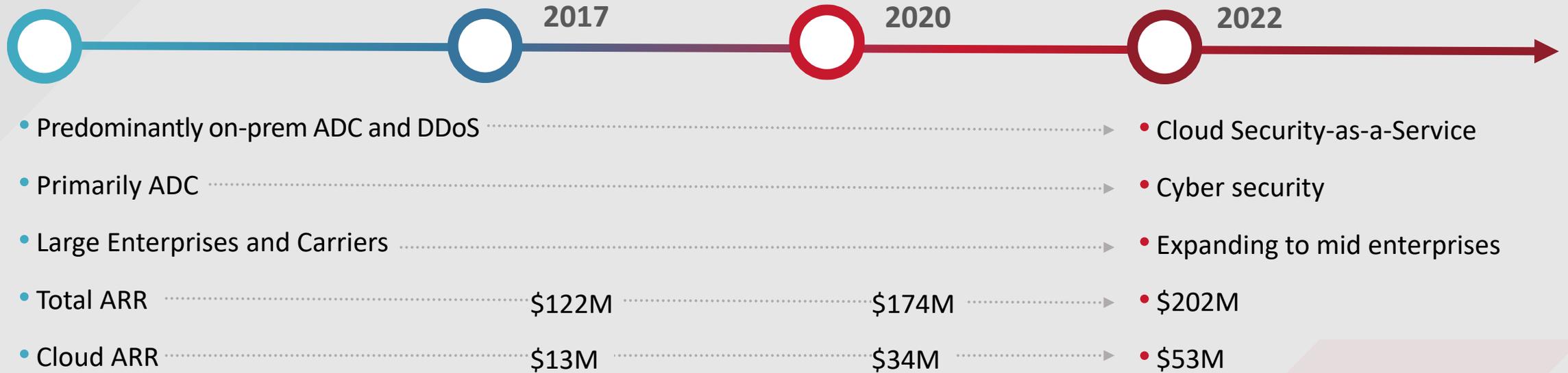
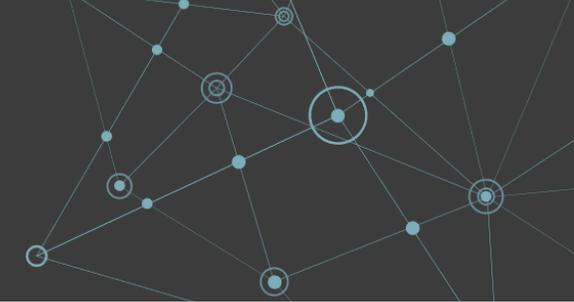


Fast Growing Cloud Security Business



Sustainable Growth and Profitability

# Radware Journey



# 2022 Highlights\*

>\$200  
Million

Total ARR

+21%

Cloud ARR  
Growth

+22%

Cloud total  
customers

8

Cloud centers  
were opened  
in 2022

Core  
Radware

Spin off  
Hawks and  
focus on  
AppSec

\* Compared to full year 2021

# Radware Complete Mitigation Suite

## Radware's Core Business

### Application Availability

Application delivery



### Application and Data Center Security

Mitigation of denial-of-service and application attacks



### Cloud Security As-a-Service

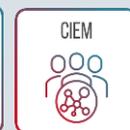
Mitigation of data centers, web applications, API and automated attacks



## The Hawks Business

### SkyHawk

Protection of application hosted in the public cloud

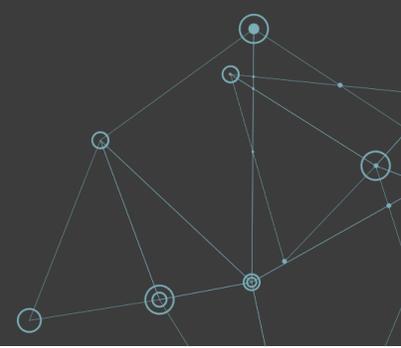


### EdgeHawk

Protection of carriers' Edge

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

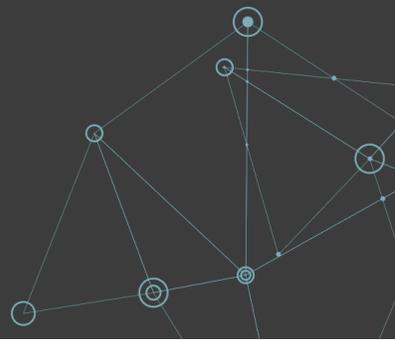
Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Growing Threat Landscape



DDoS  
Attacks  
Reaching  
New Heights

DDoS attacks  
+228%\*

Application  
Attacks  
Continue  
to Grow

Web attacks +128%\*  
Bad bots +105%\*

New Attack  
Vectors  
Challenging  
Defenses

# Attack Campaign on Airports October 2022



## US airports' sites taken down in DDoS attacks by pro-Russian hackers

By Bill Toulas

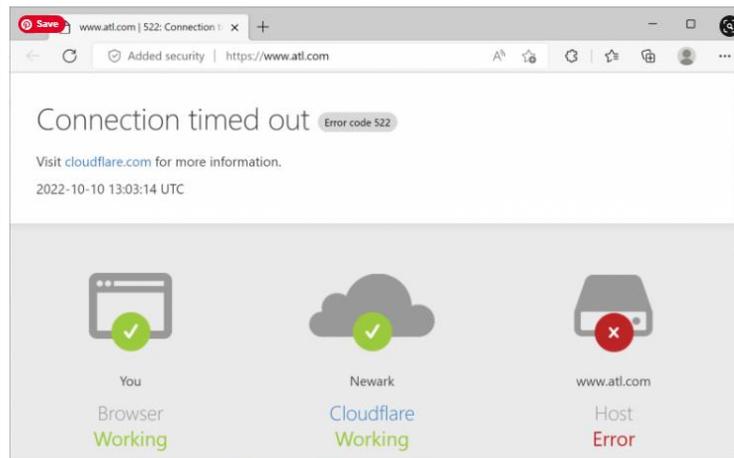
October 10, 2022 10:15 AM 3



Update: Title of story modified to indicate it was the sites taken down.

The pro-Russian hacktivist group 'KillNet' is claiming large-scale distributed denial-of-service (DDoS) attacks against websites of several major airports in the U.S., making them inaccessible.

Notable examples of airport websites that are currently unavailable include the Hartsfield-Jackson Atlanta International Airport (ATL), one of the country's larger air traffic hubs, and the Los Angeles International Airport (LAX), which is intermittently offline or very slow to respond.



WE ARE KILLNET  
Ваш выход хакеры  
Список ниже для Вас

Аэропорты:

- Атланта - <https://www.atl.com>
- Алабама - <https://www.flybirmingham.com>  
<http://www.gadsdenairport.com>  
<https://flymgm.com>
- Аризона - <https://deervalleyairport.com>  
<https://www.gatewayairport.com>  
<https://www.skyharbor.com>
- Арканзас - <https://www.flyxna.com>  
<https://flyeld.com>
- Калифорния - <https://www.flylax.com/>  
<https://www.flyontario.com>  
<https://www.longbeach.gov/lgb/>
- Колорадо - <https://www.flydenver.com>  
<https://coloradosprings.gov/flycos>  
<https://www.flydurango.com>
- Коннектикут - <https://bradleyairport.com>
- Делавэр - <http://www.newcastleairportilg.com>  
<https://delawarecoastalairport.com>
- Флорида - <https://www.mlhair.com>  
<https://flylcpa.com>  
<https://orlandoairports.net>
- Джорджия - <https://www.atl.com>  
<http://www.cityofdouglas.com/index.aspx?NID=95>
- Гавайи - <https://airports.hawaii.gov/hnl/>
- Айдахо - <https://www.flyboise.com> <https://iflysun.com>  
<https://www.idahofallsidaho.gov/181/Airport>
- Иллинойс - <https://cira.com>  
<https://www.flychicago.com/ohare/home/pages/default.aspx>  
<https://flycu.com>
- Индиана - <https://www.indianapolisairport.com>
- Айова - <http://www.dsmaairport.com>  
<https://flycid.com> <http://www.flyalo.com>
- Канзас - <https://www.flykci.com>
- Кентукки - <http://cca.ky.gov> <https://www.flylouisville.com>  
<https://www.cvgairport.com>
- Луизиана - <https://flymsy.com>  
<https://www.flyaex.org>
- Мэриленд - <https://www.bwairport.com>
- Массачусетс - <https://aeromanagementllc.com>
- Мичиган - <https://westmichiganregionalairport.com>
- Миннесота - <https://www.msairport.com>
- Миссисипи - <https://jmaa.com>  
<http://www.flygpt.com>  
<https://www.meridianairport.com>
- Миссури - <https://www.flystl.com>  
<https://nwregionalair.com>

1179 453 150 28 17 12 7  
7 5 4 2

25.1K 1:50 PM

163 comments

# Attach Campaign On Health Care February 2023

**SC MEDIA** TOPICS INDUSTRY EVENTS PODCASTS RESEARCH RECOGNITION

Threat intelligence, Application security, Vulnerability management

f t e in

## Killnet DDoS attacks inflicting damage on healthcare: 'This is war'

Jessica Davis February 13, 2023



Recent alerts to the health sector warn that the Russia-Ukraine war have spurred hacktivists to leverage more destructive tactics. (iStock via Getty Images)

The Killnet hacktivist group's DDoS attacks against healthcare and the mass data exfiltration in January was reportedly just the first round of targeting. Industry leaders have grown increasingly concerned over the impact of nation-state actors and the

<https://www.scmagazine.com/news/threat-intelligence/killnet-ddos-attacks-inflicting-damage-on-healthcare-this-is-war>

**Malwarebytes LABS** Personal Business Pricing Partners

Search Labs



CYBERCRIME | NEWS

## KillNet hits healthcare sector with DDoS attacks

Posted: February 10, 2023 by Pieter Arntz

At the end of January, the Health Sector Cybersecurity Coordination Center warned that the KillNet group is actively targeting the US healthcare sector with distributed denial-of-service (DDoS) attacks.

The Cybersecurity and Infrastructure Security Agency (CISA) says it helped dozens of hospitals

<https://www.malwarebytes.com/blog/news/2023/02/killnet-group-targets-us-and-european-hospitals-with-ddos-attacks>

← **Automatic Translation**  
Russian → English

**ATTENTION TO TEAMS THAT JOIN OUR MISSION!**

👉 Everyone hit L7 on 50 hospital targets - 50 states of America!

**Alaska**  
<https://www.providence.org>  
<https://check-host.net/check-report/e77f515k82d>

**Arizona**  
<https://www.abrazohealth.com>  
<https://check-host.net/check-report/e77f5a2kcbce>

**Arkansas**  
<https://arksurgicalhospital.com>  
<https://check-host.net/check-report/e779e33kf96>

**California**  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

**Colorado**  
<https://www.sclhealth.org>  
<https://check-host.net/check-report/e7821b1kf6>

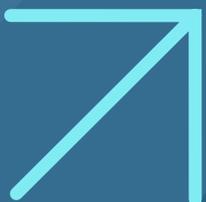
**Connecticut**  
<https://gfp.griffinhealth.org>  
<https://check-host.net/check-report/e781374kbab>

**Delaware**  
<https://christianacare.org>  
<https://check-host.net/check-report/e77a063kb3e>

**Florida**  
<https://www.leehealth.org>  
<https://check-host.net/check-report/e77fbeck78c>

**Georgia**  
<https://www.northside.com>  
<https://check-host.net/check-report>

# 2022 New Norm: 400Gbps – 1.1Tbps DDoS Attacks



## Cyber Attacks on US Infrastructure

Series of DDoS attacks by pro-Russian hacker groups, targeting US civilian infrastructure, such as websites of major airports



## 1.1Tbps Attack on Service Provider

US service provider under attack for over 36 hours



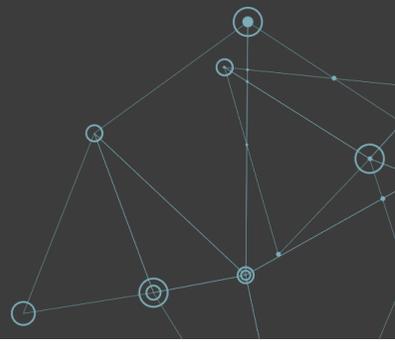
## Ukraine Gov't Under Attack

Nation-State attacks peaking at 235Gbps & over 400Gbps



# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Cloud Transition Introduces Uncertainties

Pace & Final Deployment Unknown

## Multi-Cloud Creates New Security Risks



**99%** Deploy Applications in at Least One Public Cloud

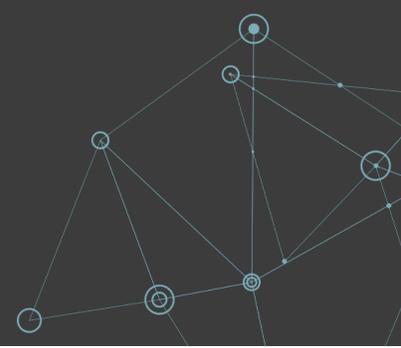
**69%** Experienced Data Exposure Due to Inconsistencies Between Platforms

**70%** Aren't Confident in Level of Security by Their Public Cloud Vendor

Need for **consistent security** across all clouds

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

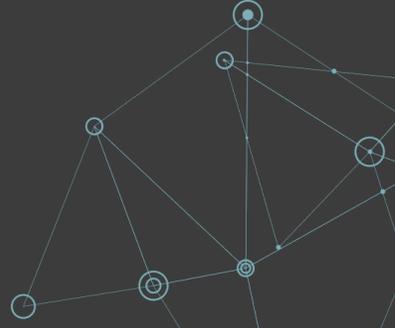
Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Shortage  
in Security  
Experts &  
Skills

# Accelerated Digital Transformation



Multiple End-Users & Partners



Distributed Workforce



Increased Use of APIs



Online Consumption of Goods



Applications  
at Center  
of Business

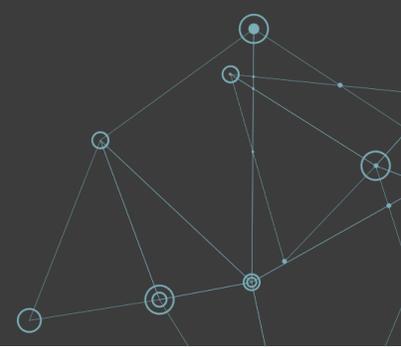


**Time to market** and **agility**  
are critical to staying  
competitive

Need **frictionless security** that does not hold you back

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

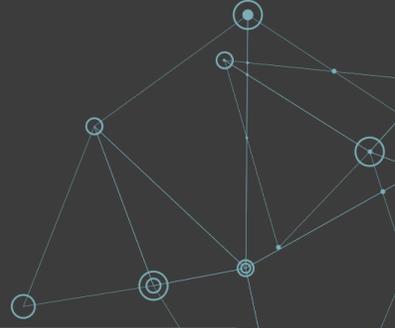
Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

# Shortage in Security Experts & Skills

+25%

demand for  
cyber security  
experts

~3.4M

open positions  
worldwide

70%

businesses are  
facing skill  
shortages

43%

can't find enough  
qualified talent

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

# Industry Trends

Leading Critical Cyber Security Vendor



Growing  
Threat  
Landscape

Critical, Need  
State-of-the-Art  
Security

Cloud  
Transition

Consistent  
Security  
Across Clouds

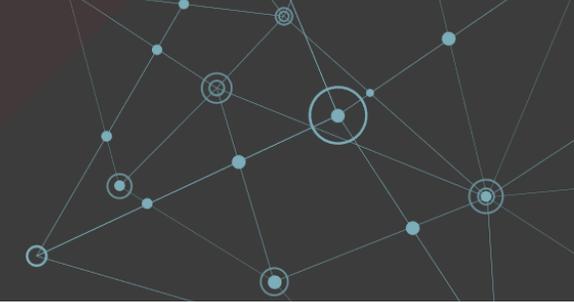
Accelerated  
Digital  
Transformation

Frictionless  
Security

Shortage  
in Security  
Experts &  
Skills

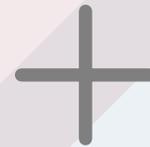
Automation  
Fully Managed

# The CISO Challenge



## STATE OF THE ART

Protection from the most advanced threats



## FRictionLESS

Security operations that enables business agility

➔ Organizations Shouldn't Have to Choose

# The Radware Difference

Combining State-of-the-Art & Frictionless Security

## State-of-the-Art Protection

From the Most Advanced Threats



### Widest Coverage

ALL APP SURFACES, ALL VECTORS



### Highest Accuracy

FUZZY LOGIC, BLOCKCHAIN & MACHINE LEARNING ALGORITHMS



### Real-Time Protection

ZERO-DAY ATTACK PROTECTION, AUTO CONTINUOUS LEARNING, CRYPTO CHALLENGE

## Frictionless Security

Enables business agility & lowers TCO



### Agnostic, Consistent

ACROSS ALL CLOUDS, FULLY INTEGRATED



### Adaptive, Automated

NO HUMAN INTERVENTION REQUIRED



### Fully Managed Services

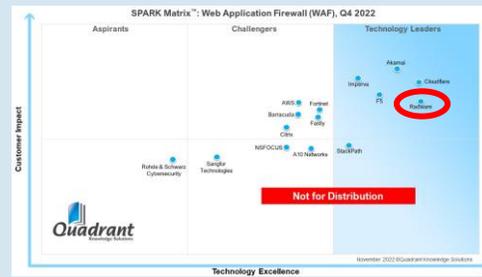
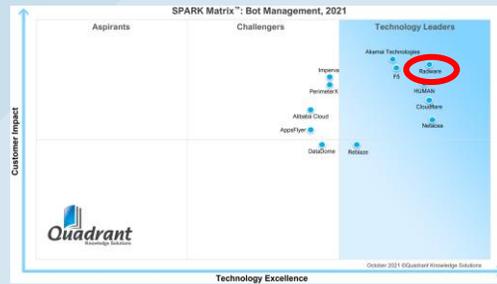
SUPERIOR SLA, 24/7 EXPERT SERVICE

# Winning Industry Recognition

**BOT MANAGEMENT 2022  
LEADER**



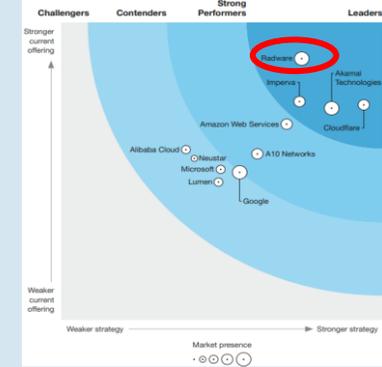
**WAF 2022  
LEADER**



**GIGAOM  
APP & API PROTECTION 2022  
LEADER & OUTPERFORMER**



**FORRESTER®  
DDoS MITIGATION WAVE 2021  
LEADER**

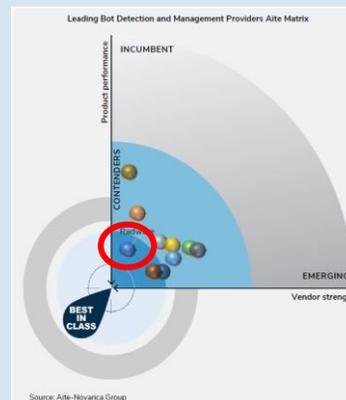


**AiteNovarica**

**BOT DETECTION MATRIX, 2022  
BEST IN CLASS**



*“The largest global financial institutions, brokerage firms, and financial services companies use Radware’s Bot Manager.”*



**kuppingercoie  
ANALYSTS**

**WAF LEADERSHIP  
COMPASS 2022  
OVERALL LEADER  
Product, Innovation  
& Market Leader**



# State-of-the-Art Protection: Winning Industry Recognition in 2022

Gartner.  
Peer Insights™

94%

WOULD RECOMMEND  
Radware Cloud WAF  
Service

94%

WOULD RECOMMEND  
Radware Cloud DDoS  
Protection Service

## Radware Cloud DDoS Protection Service Reviews

by Radware in DDoS Mitigation Services  
4.8 ★★★★★ 19 Ratings

## Radware DefensePro Reviews

by Radware in DDoS Mitigation Services  
4.9 ★★★★★ 25 Ratings

## Radware Cloud WAF service Reviews

by Radware in Cloud Web Application and API Protection  
4.7 ★★★★★ 124 Ratings

\* Gartner Peer Insight as of Feb. 20<sup>th</sup> 2023

Gartner

CRITICAL CAPABILITIES FOR CLOUD WEB APPLICATION  
AND API PROTECTION (WAAP), 2022

#2 IN HIGH SECURITY & API USE CASES



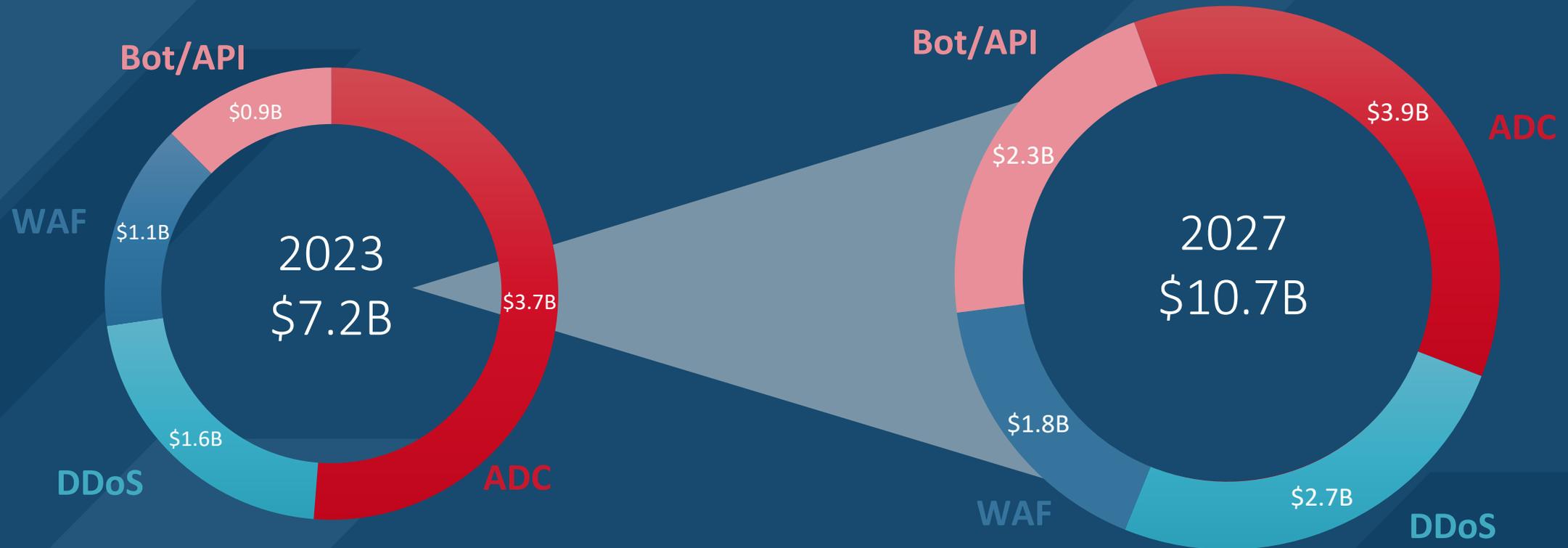
*“Radware Cloud WAF  
Service is a **good**  
candidate, especially for  
the high-security use case”*



*“Radware offers one of the  
stronger API security  
offerings on the WAAP  
market”*

# Growth Strategy: Profitable Growth Powered by Cloud Security

# The Markets We Operate In



Source: IDC: Worldwide Application Protection and Availability Forecast, 2022–2026: Security Powers the Digital Experience, November 2022

# Solid and Balanced Business Model

On-Prem Business  
~\$240M

- Large enterprises and carriers
- Loyal customer base and new logos
- Robust and highly profitable business

# Large Enterprise and Service Providers

Blue Chip Customers



6 OF TOP 10

WORLD'S  
BANKS



7 OF TOP 10

WORLD TELECOM  
COMPANIES



6 OF TOP 12

WORLD'S STOCK  
EXCHANGES



4 OF TOP 10

WORLD'S  
ECOMMERCE  
COMPANIES



4 OF TOP 10

MOST WIDELY  
USED SAAS  
APPLICATIONS

# Solid and Balanced Business Model

Cloud Security  
~\$50M

- Large enterprises and mid-size enterprises
- New logos
- Growing and scaling
- Cloud ARR grew 21% YoY to \$53M in 2022

On-Prem Business  
~\$240M

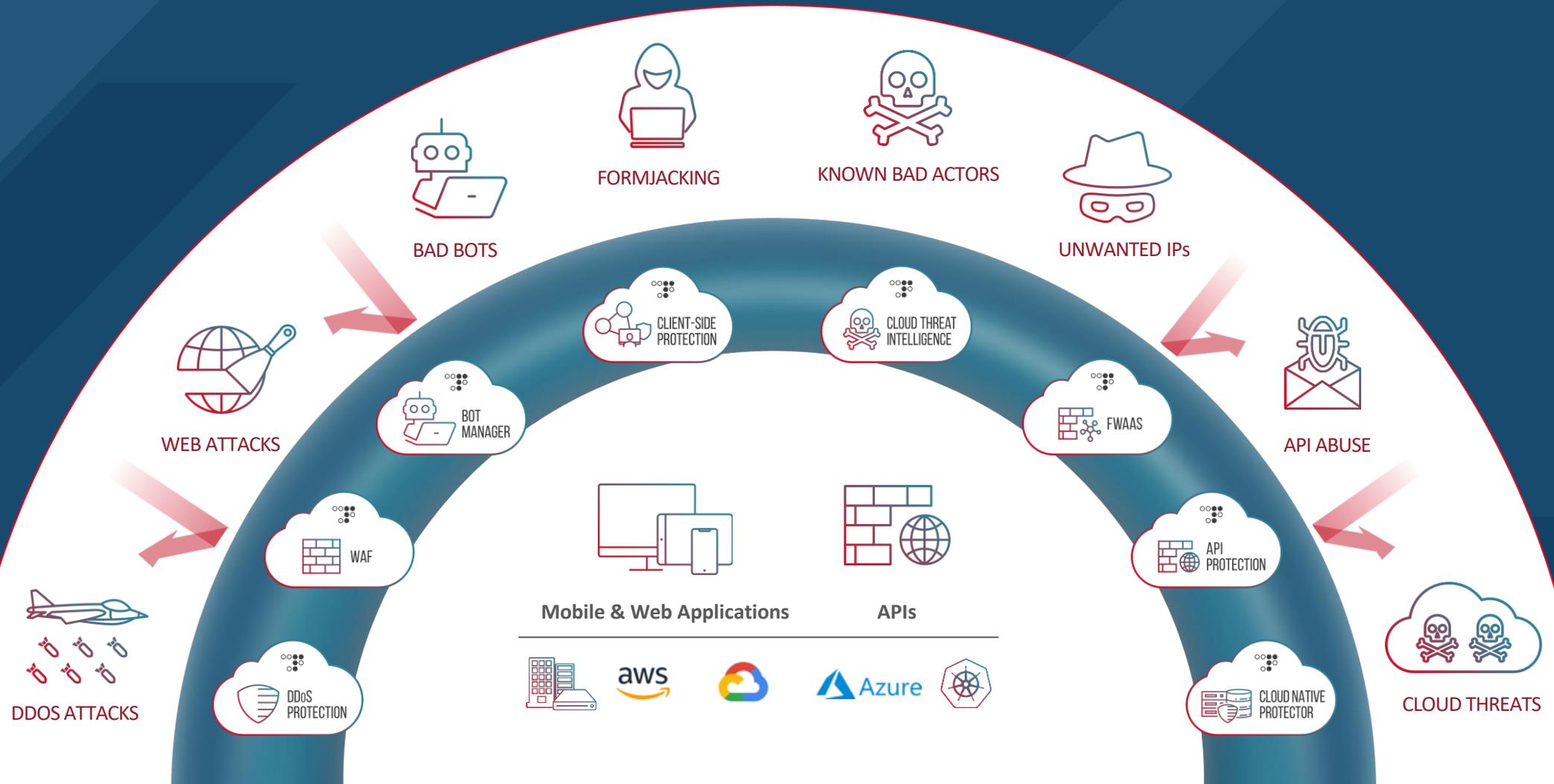
- Large enterprises and carriers
- Loyal customer base and new logos
- Robust and highly profitable business

# Scaling Cloud Security

25% 5-year CAGR in  
Cloud ARR

# Radware 360 Application Protection

Secure Your Apps. Regain Control. Enable Your Business.



# Best of Suite: Selling Packages



## Standard

Industry benchmark protection level with some extra unique features & capabilities



## Advanced

Advanced protection against more sophisticated & unknown attacks



## Complete

Security blanket for the entire application environment. Client-side, server-side & everything in between.

# Best of Suite Service Plans: Add-ons



Service Plans:  
Add-ons



Premium  
Support



CDN



Unlimited  
DDoS  
Protection

# Cloud Security Strategy



1

**Best of Breed: Technology Leadership**  
Maintain and expand technology lead

2

**Best of Suite**  
Selling packages, ARR growth

3

**Mid-Sized Enterprise**  
Expanding SAM, same solution, ease of use

4

**Channels and partnerships**  
Expanding our channel network to reach more customers

5

**Continue to Expand Global Footprint**  
Continue to open more location to cater additional new customers

# Radware Strategy Summary



- 1** On-Prem Business  
TAM is growing, best of breed required
- 2** Critical Areas  
Large, strong and profitable
- 3** Accelerating Cloud Security Business  
Strong growth, expanding SAM, SaaS business model
- 4** Leverage in the Model  
Driving profitable growth with OpEx leverage

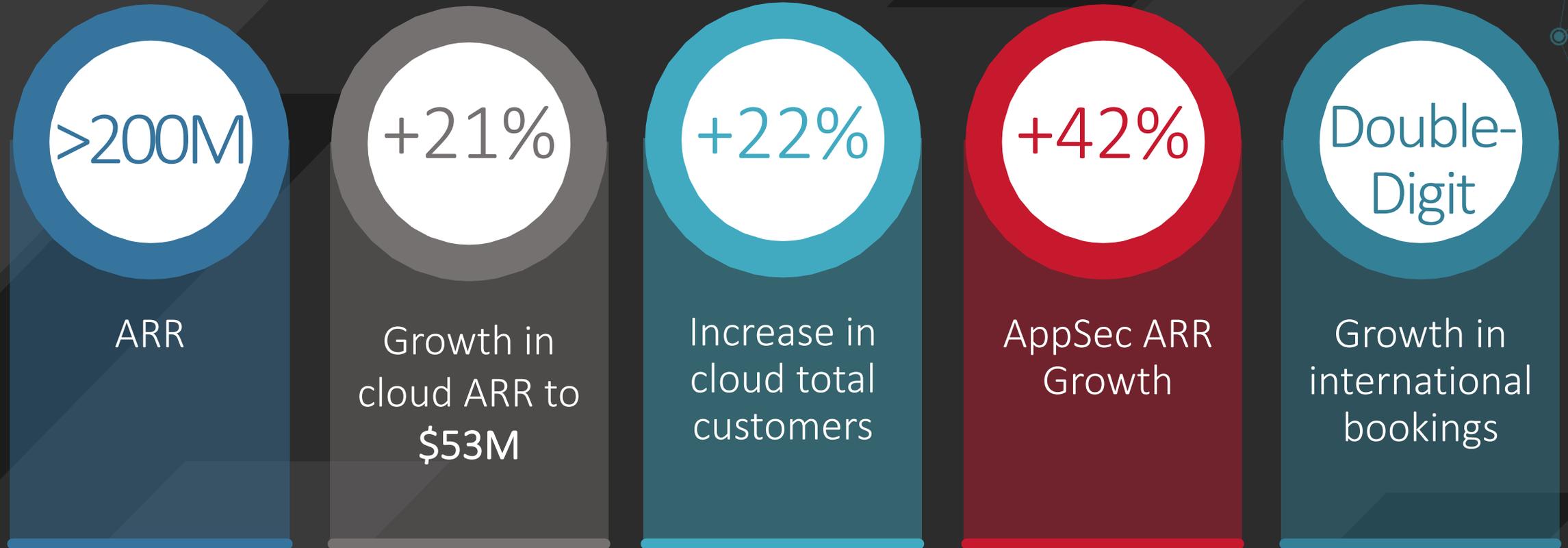
# Sales Strategy & Plan

**Yoav Gazelle**

Chief Business Officer

February 2023

# 2022 Highlights\*



\* Compared to full year 2021

# Large Enterprise and Service Providers

Blue Chip Customers



6 OF TOP 10

WORLD'S  
BANKS



7 OF TOP 10

WORLD TELECOM  
COMPANIES



6 OF TOP 10

WORLD'S STOCK  
EXCHANGES



4 OF TOP 10

WORLD'S  
ECOMMERCE  
COMPANIES



4 OF TOP 10

MOST WIDELY  
USED SAAS  
APPLICATIONS

# 2023 Strategy and Plan

# Focus Areas



## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

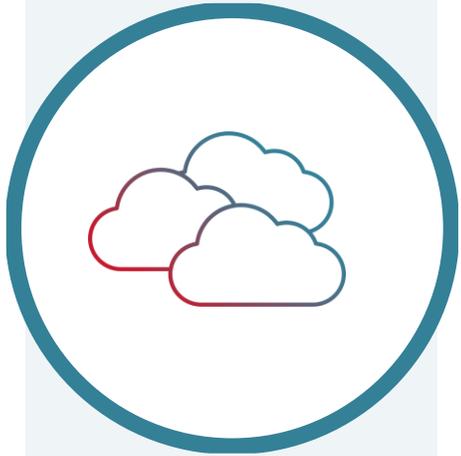
Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Focus Areas



## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



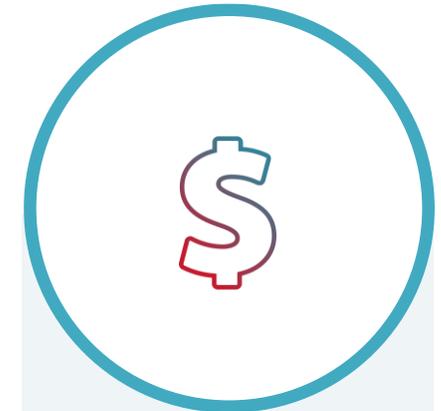
## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Accelerating Cloud Security Growth



## Sale Resources

Adding Cloud Quota Carrying Sellers



## Incentives

New Compensation Plan based on ACV/ARR bookings



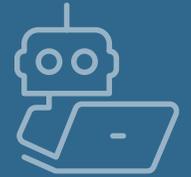
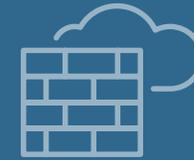
## Best of Suite

New service packages, New portal for cross sales



# Global Cloud Security Network

Enables Cloud Expansion



40+ AppSec PoPs

WITH GLOBAL COVERAGE

12 Tbps OF GLOBAL MITIGATION CAPACITY

19 SCRUBBING CENTERS Worldwide



DDoS MITIGATION SCRUBBING CENTER



CLOUD WAF PoP



BOT MANAGER SERVICE CENTER

# Focus Areas



## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



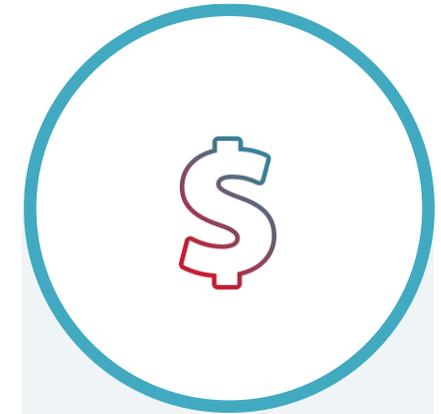
## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Expanding our Partnership With



**CHECK POINT™**



Tighter Partnership



Pipeline Growth



New Logo Wins

# Expanding our Partnership With



Project Turbo



Cisco Enterprise Agreement



Strong Alignment with Security BU

# Focus Areas



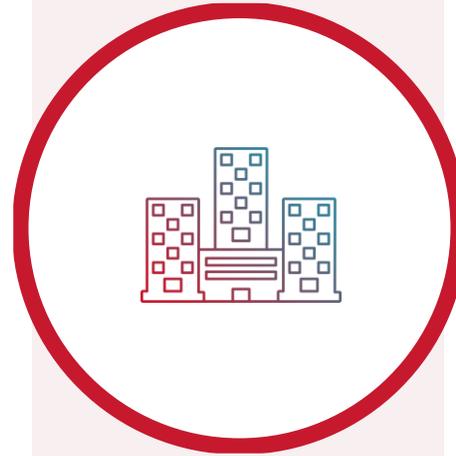
## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



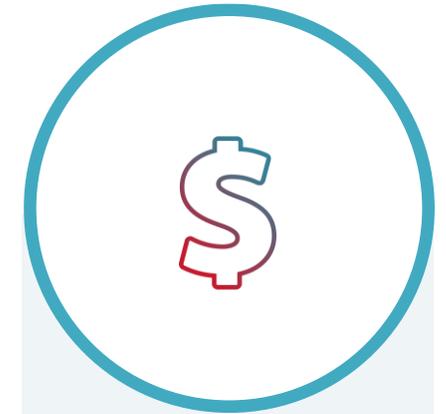
## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

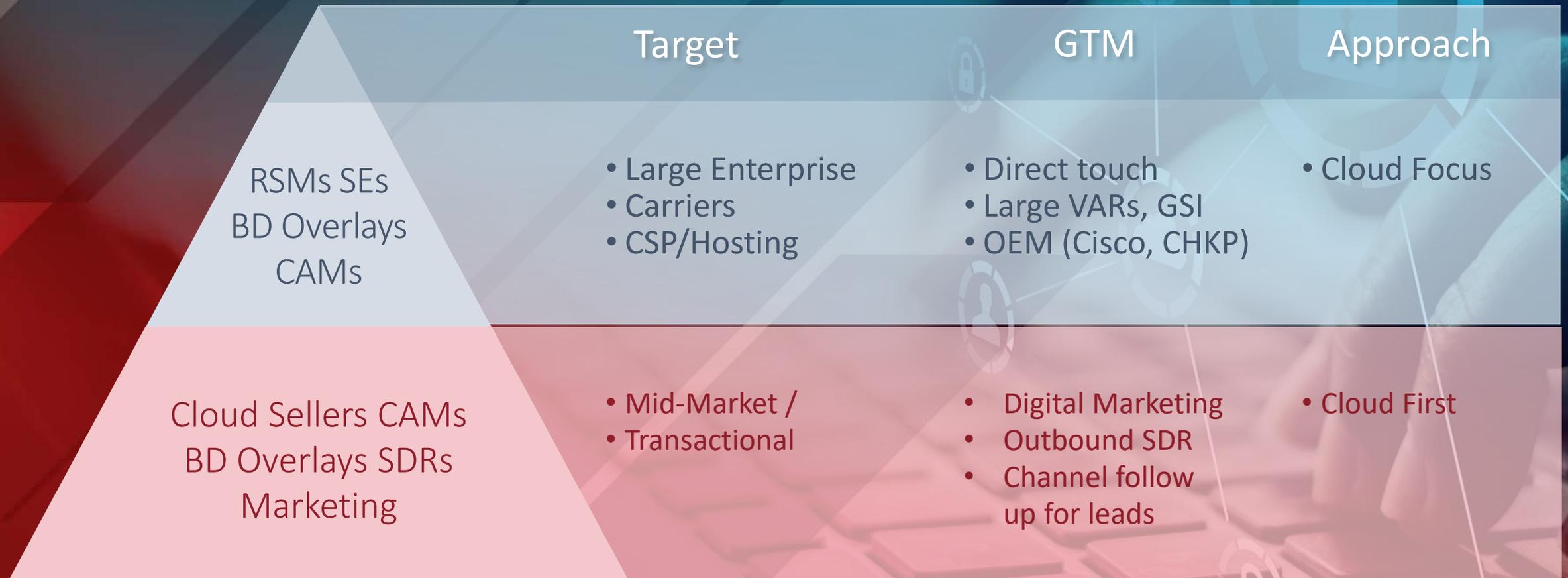
Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Penetrating the Mid-Market Enterprise



# Our Partners for Mid to Large Enterprises



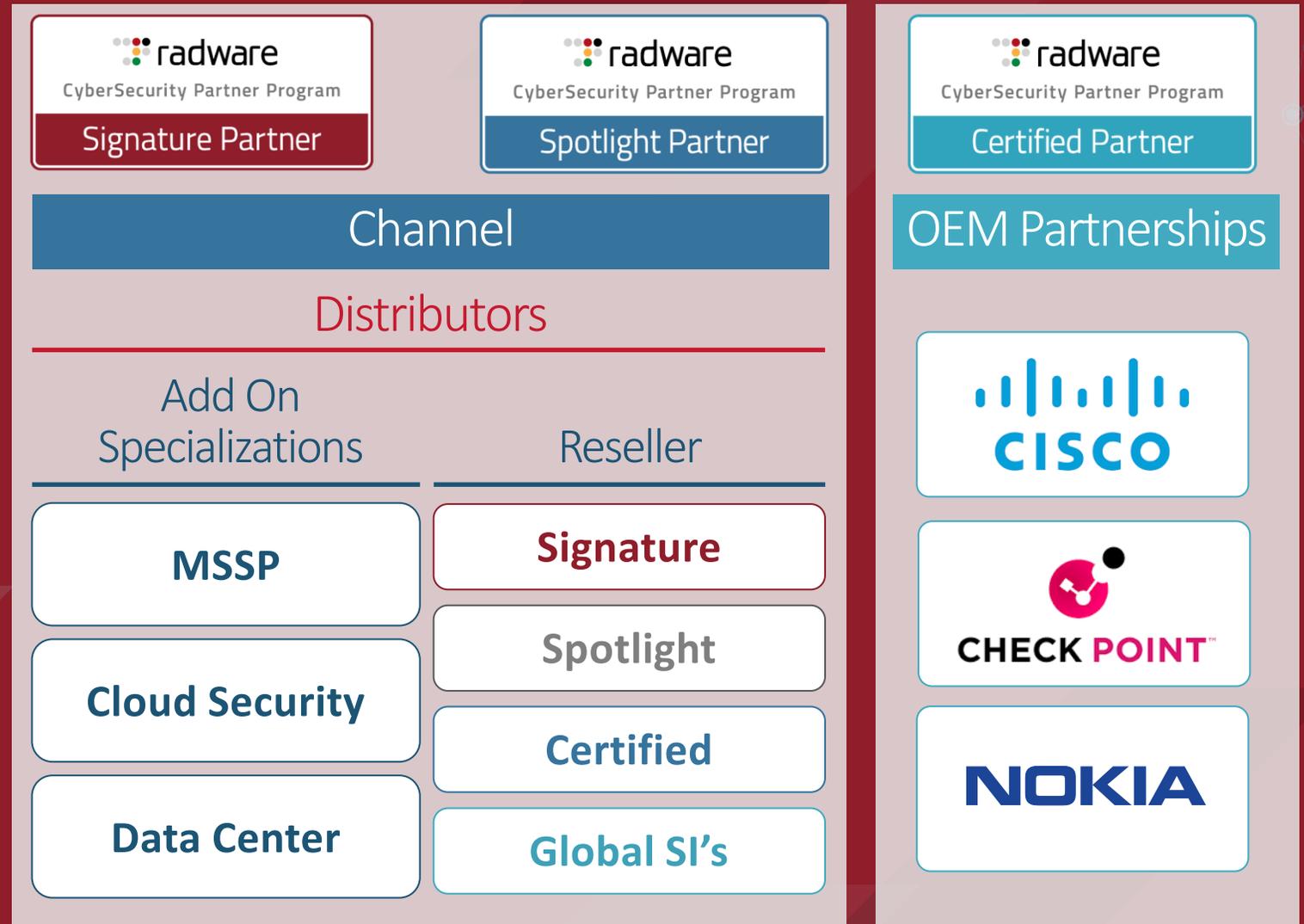
<p>USA</p> <p><b>PRESIDIO</b></p> <p> </p> <p> </p> <p></p>	<p>CALA</p> <p></p> <p></p> <p></p> <p></p>	<p>UKI</p> <p><b>GlobalDots</b></p> <p></p> <p></p>	<p>India</p> <p></p> <p></p>	<p>China</p> <p></p> <p></p>	<p>Korea</p> <p></p> <p></p>
<p>Canada</p> <p></p> <p> </p> <p></p>	<p>South Africa</p> <p></p> <p></p>	<p>DACH</p> <p></p> <p></p> <p></p>	<p>ASEAN</p> <p></p> <p></p> <p><b>CLOUDSEC ASIA</b></p>	<p>Taiwan</p> <p></p> <p></p> <p></p>	<p>ANZ</p> <p></p> <p></p> <p></p> <p></p>

# New Partner Program



Designed for  
Cloud Mid-market

## New Reseller Tiers:



# Focus Areas



## Cloud Security

Accelerating cloud growth and scale cloud business



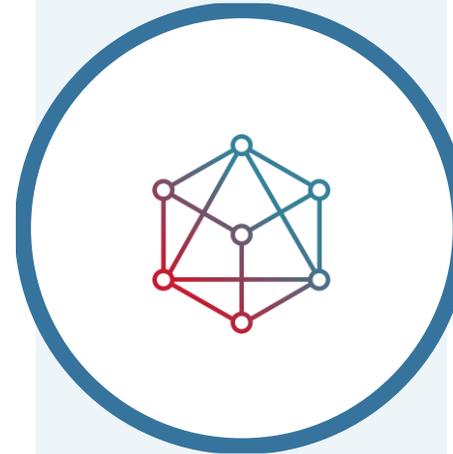
## OEM Partners

Expanding our partnership with OEMs



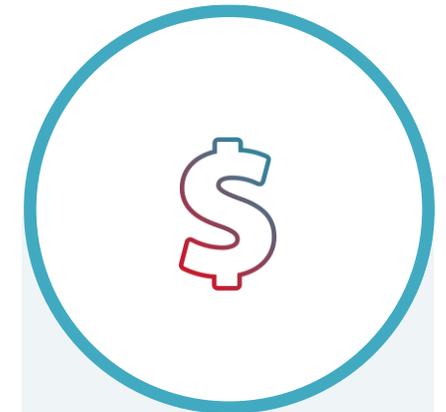
## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Carrier Business



## Sell To

- Growing and critical needs
- Large opportunity
- Limited competition
- Significant technology leadership
- New & advanced offering

## Sell Through

- New cloud network protection offering for SMEs
- Applications protection MSSP offering / resell

# Focus Area



## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# North America Sales



1

New Head of  
Sales for North  
America

2

Set  
Organization  
for Growth

Large Enterprise –  
Carriers – Mid-  
Market - Channels

3

Strengthening  
our Indirect  
GTM

OEMs - Channel  
Partners - GSIs

# Summary: Focus Areas



## Cloud Security

Accelerating cloud growth and scale cloud business



## OEM Partners

Expanding our partnership with OEMs



## Mid-Size Enterprise

Penetrate mid-sized enterprise market with cloud-first approach



## Carrier Business

Capitalize on the sell-to opportunity and develop the sell-through GTM



## N. America Sales

Boosting North America sales to accelerate growth

# Why Radware?

- Leading Critical Cyber Security
- Fast Growing Cloud Security Business
- Leading Differentiated Technology
- Large Enterprise and Carriers Customer Base
- Large Growing TAM and SAM
- Sustainable Growth and Profitability
- Penetrating Mid-Sized Enterprise Market
- Enhancing OEMs Partnerships

# Good Enough Security is NOT Good Enough

**David Aviv**

CTO

# The Perfect Storm Is Here



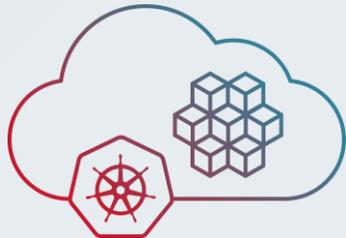
 radware

# Evolution of Modern Applications

Modern Applications are Distributed, With Many **Entry Points**

1

**Application Code is Distributed** Across Microservices (K8s)



2

Hosted in **Multiple Environments** (Public & Private Clouds)



3

**Content Integrated** with 3<sup>rd</sup>/4<sup>th</sup> Party Plug-ins **Browser Heavily Used** to Compose the Content



Modern app design creates multiple **blind spots**, open new leakage opportunities

**Traditional WAF / WAF Appliances No Longer Enough**

# Sophisticated, Targeted Attacks Are on-the Rise



Dark Reading

Vulnerabilities Threats | 5 min read

## Phishing Surges Ahead, as ChatGPT & AI Loom

AI and phishing as a service (PhaaS) are making it easier for threat actors to create malicious email campaigns, which continue to target high-volume applications using popular brand names.

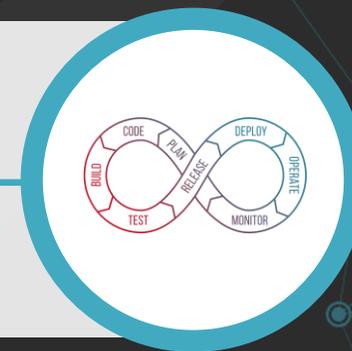
**Elizabeth Montalbano**  
Contributor, Dark Reading

February 09, 2023

Good Enough  
Security is NOT  
Good Enough

## Open Doors for Blind Spots

Supply chain, Application delivery cadence



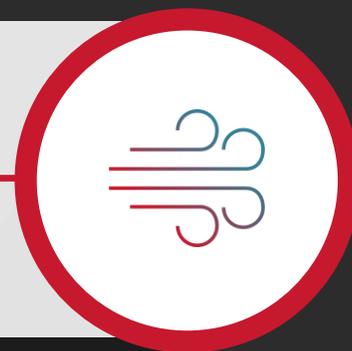
## Aggressive, Targeted App DDoS

Choke critical application resources



## Weaponizing AI: Disruption Today

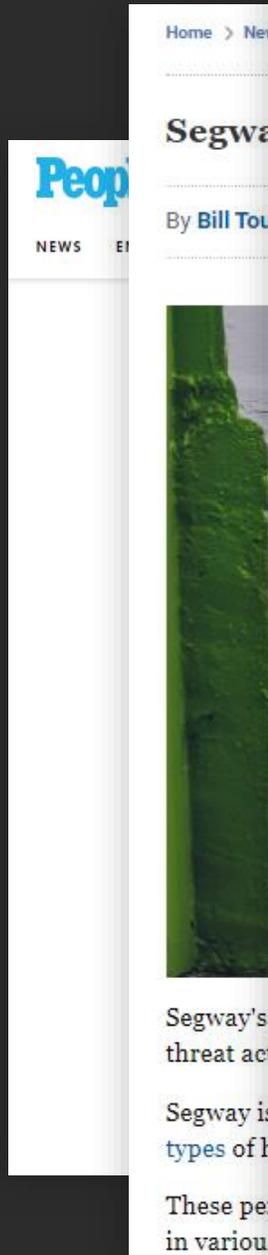
Lower entry barrier, Attack code generation



# Notable Recent Application AppSec Campaigns



Good Enough  
Security is NOT  
Good Enough



**T\_HQ**

Home > News

Segway

By Bill Tou

NEWS

Peop

TWITTER

## Twitter API vulnerability leaves millions exposed

The data breach has resulted in millions of account details being dumped on hacker forums.

6 January 2023

Twitter LinkedIn Facebook



Segway's threat act

Segway is types of h

These per in variou

The APIs that Twitter uses to collect non-public data from its users' accounts may well be leaving that data vulnerable. In fairness, this is hardly news – a

# Technology Leadership

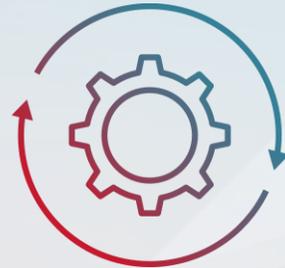


# Radware Innovation Philosophy for Differentiation



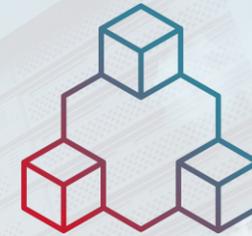
## AI & Adaptive Algorithms

AppSec-AI  
Real-time protection



## Automation for Consistency & SLA

Attack life cycle  
Security follows App's cadence



## Performance Scale, Ops Cost

Cloud-scale security  
New platform lineup

# Sustainable Application Protection Leadership

Protecting the Modern Application Across All Blind Spots

1

Distributed Application Code  
in Microservices (K8s)



Protecting N/S and E/W  
Traffic



2

Hosted in Multiple  
Environments



Architecture for Consistent  
Protection Across Clouds



3

Content Integrated with  
3rd/Nth Party Plug-in



Protecting 3rd Party's  
Java Scripts



# Sustainable DDoS Protection Leadership



## Leading Security Engines Performance

Optimized for Security Processing

---

Install base refresh  
Market share gains  
Carrier-grade  
Radware cloud DDoS



## SecOps Automation Analytics Center

From Real-Time Signatures to Attack-Lifecycle Management

---

Shortage of security experts  
Service Providers/MSSP  
Radware cloud DDoS



## Algorithm-First Approach

Behavioral Self-Learning:  
Fast Morphing, Zero Day

---

Years of IP results in  
unfair competitive advantage

# Sustained Technology Leadership



# Deeper & Wider Security



## Best of Suite

### Wider: Combatting Application Floods

Firewall-aaS  
Encrypted Applications Protection



### Deeper: Expose Application's Blind Spots

Client-side Protections  
Security Follows Application's Cadence



### Cross Suite: Identity-based Protections

Anchor for Continuous Detection of  
Abnormal Activities Across The Security Suite



# Best of Suite Technology Differentiation



Block Chain Inspired,  
AI & Deep Learning



## Identity-based Protections

CAPTCHA-less  
Invisible Control Plane



## Zero-day Protection

X-Cloud Security Stack  
Adapted to App's Cadence

New Cross-Suite Security Layers Amplifies  
Best-of-Breed Insights

# Driving Profitable Growth

**Guy Avidan**  
CFO

# Key Topics



1

Radware  
Journey and  
2022 Recap

2

Long  
Term  
Model

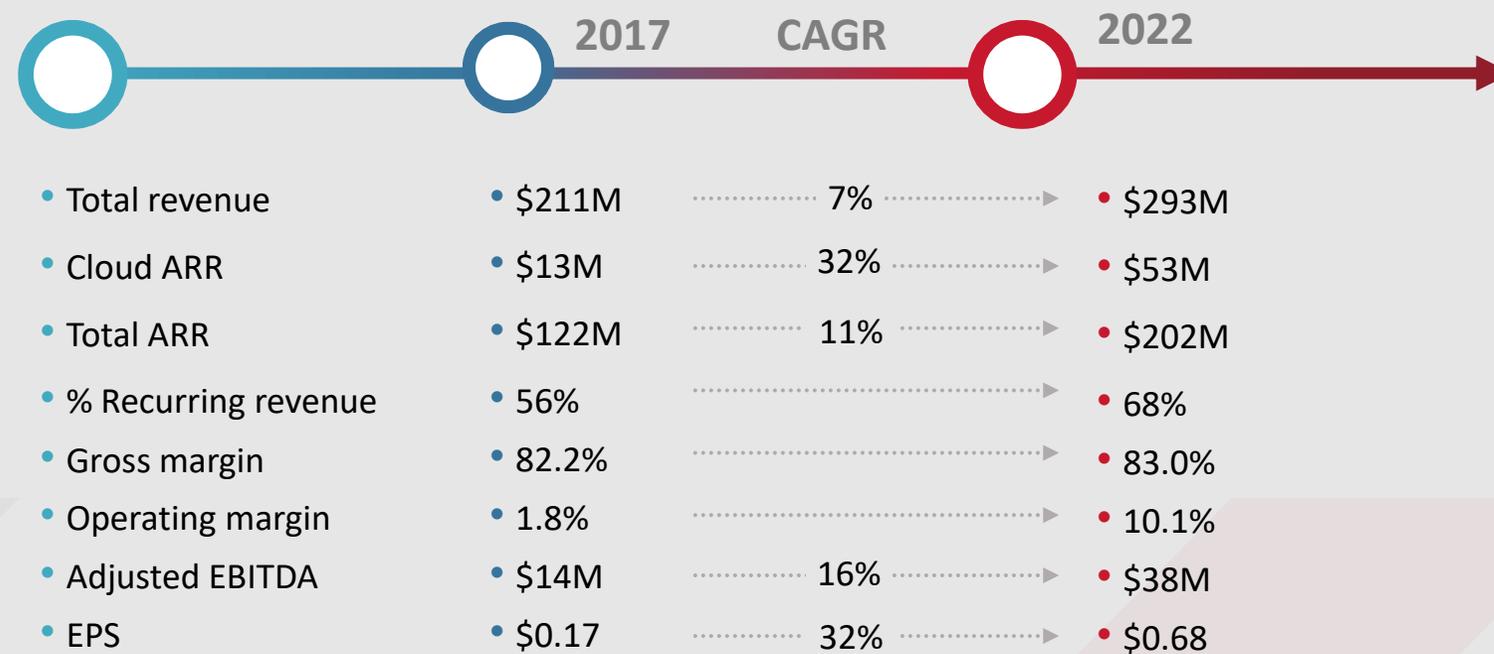
3

Investment  
Highlights and  
New KPI

# Radware Journey



## Six Years Look Back



# Full Year 2022 Highlights

\$293M

**Revenue**  
2% increase  
YoY

68%

**Recurring  
Revenue**  
Compared to  
66% last year

\$202M

**Total ARR**  
7% increase  
YoY

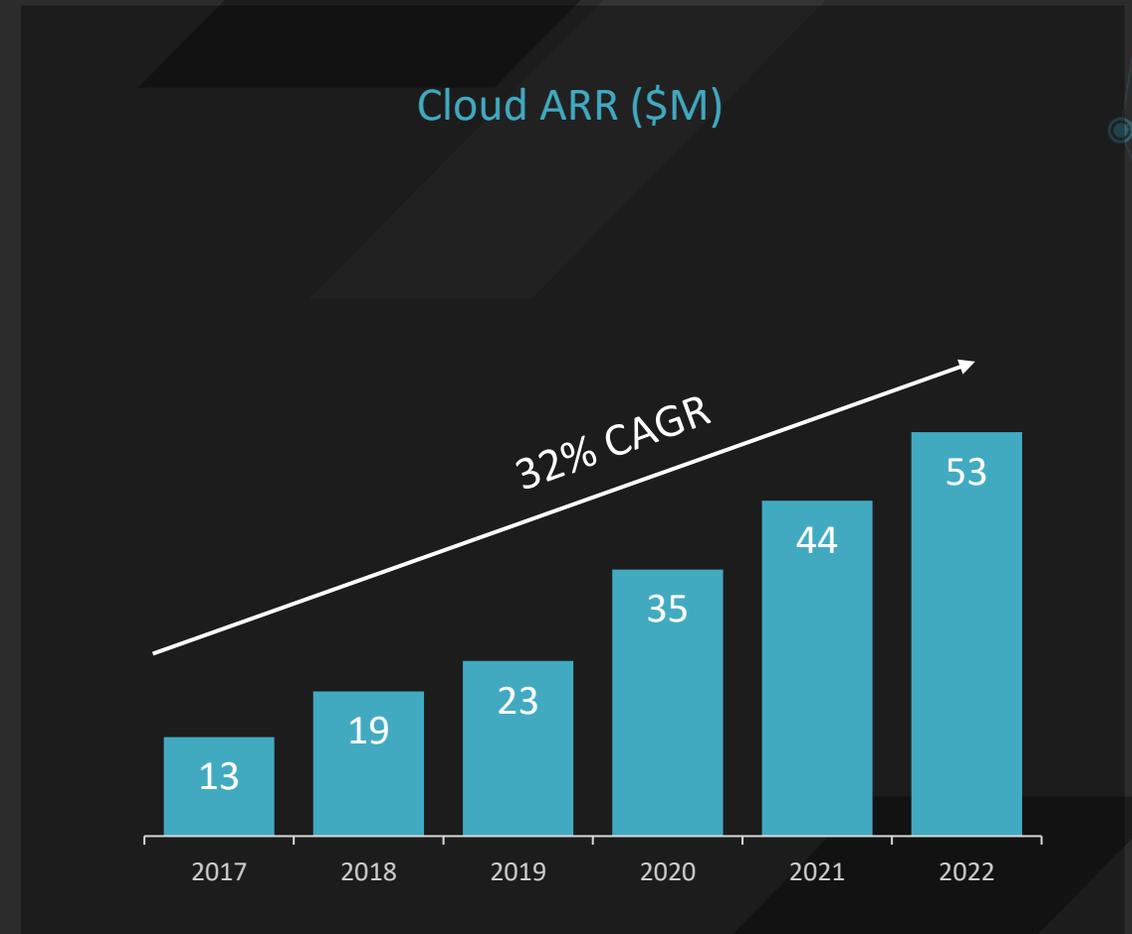
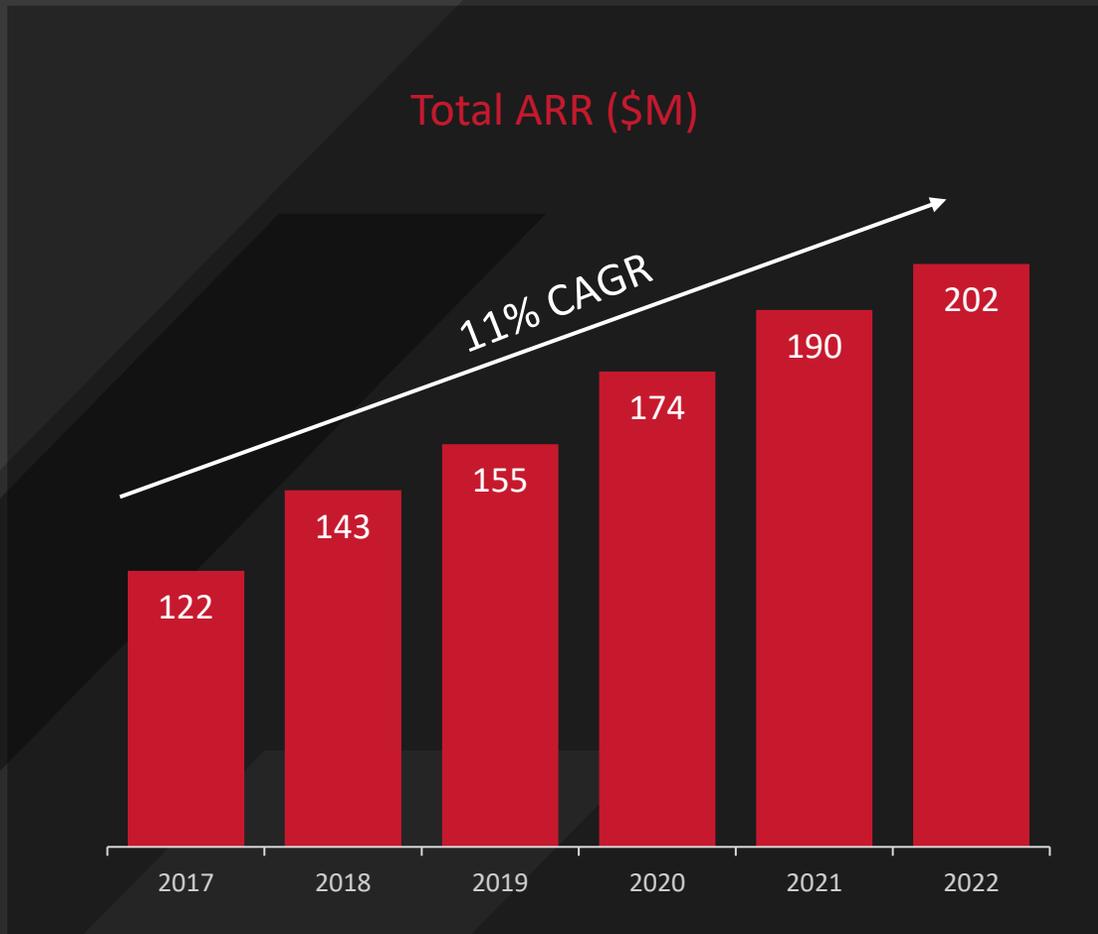
83.0%

**Gross Margin**  
Compared to  
82.4% last  
year

+35%

**Number of  
new large  
deals (>\$1M)**

# ARR Driven by Cloud ARR



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

\* Errors due to rounding

# Long Term Model: 2027



~\$460 Million of Revenue  
24% Adjusted EBITDA  
Margin for Full Year 2027

# Long Term Model Assumptions



1

Accelerating Top Line Growth

Driven by our cloud security business

2

Best of Suite Offering

Improving cross-sell potential

3

Subscription Business Model

Increase recurring revenue and cloud ARR

4

Sustainable Gross Margin

5

OpEx Leverage

# Macroeconomic Environment Impact



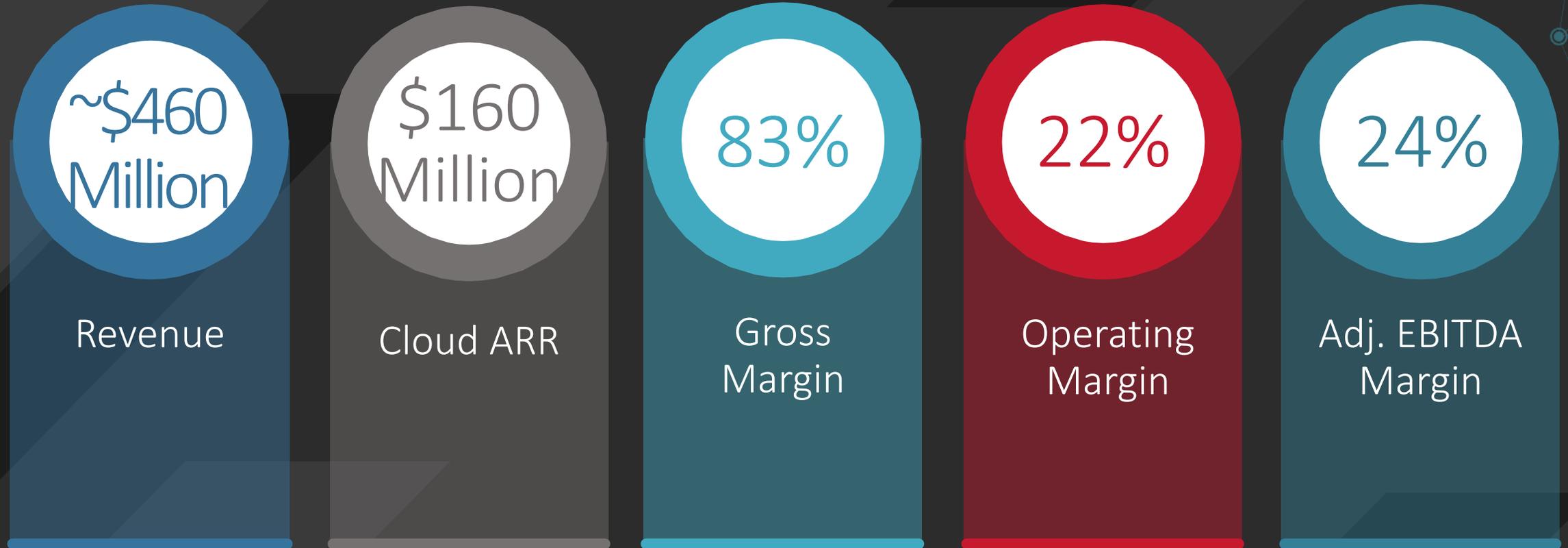
## Short Term

- Elongated sale cycle
- Budget scrutiny
- Multi-phased deployments

## Long Term

- Catch up mission critical products
- Acceleration of the shift to Managed Services

# 2027 Long Term Model



# Catalysts Driving Our Expansion

## Double Digit Revenue Growth in 2027

1

### Cloud Security

Growing our cloud security-as-a-service business

2

### Best of Suite

Scaling our portfolio from best of breed to best of suite

3

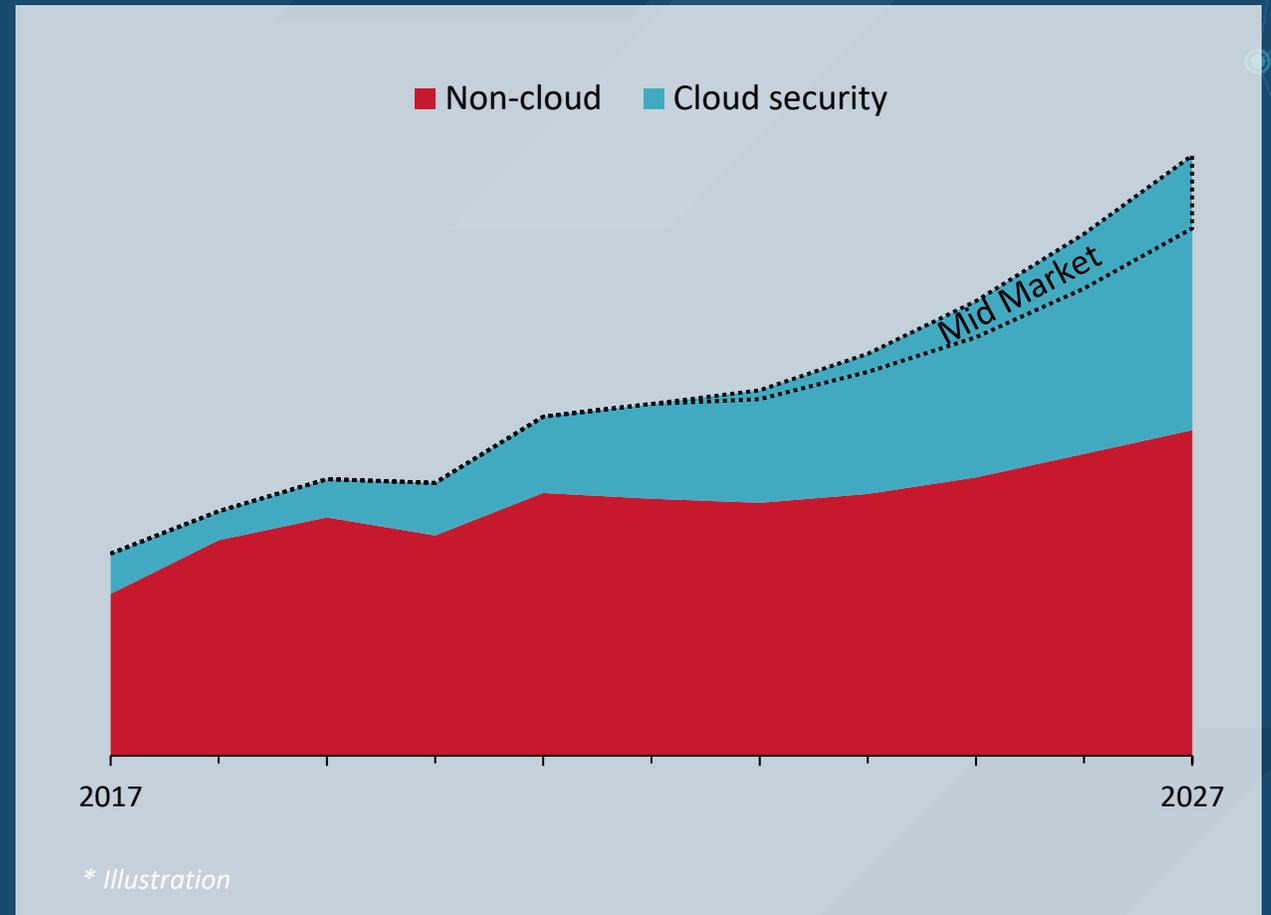
### Go-To-Market

Expanding our GTM to enhance SAM

4

### M&A

Entering key adjacent market



# Sustainable Gross Margin



Sustain 83% Gross  
Margin in 2027

1

## Best of Suite

Scaling our portfolio from best of breed to best of suite

2

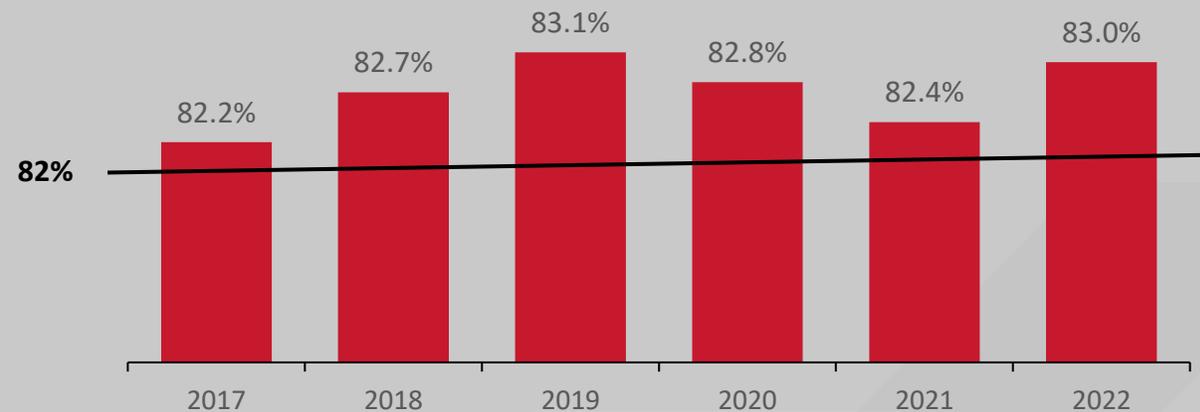
## Cloud Security

Scale and automation

3

## Product Mix

Cloud security business vs. on-prem business



# Operating Leverage



Continue to Invest in Growth While Gaining GTM Efficiencies

## Cloud Business

- Economies of scale
- Stickiness, bundles
- Automation and fully managed

## On-Prem Business

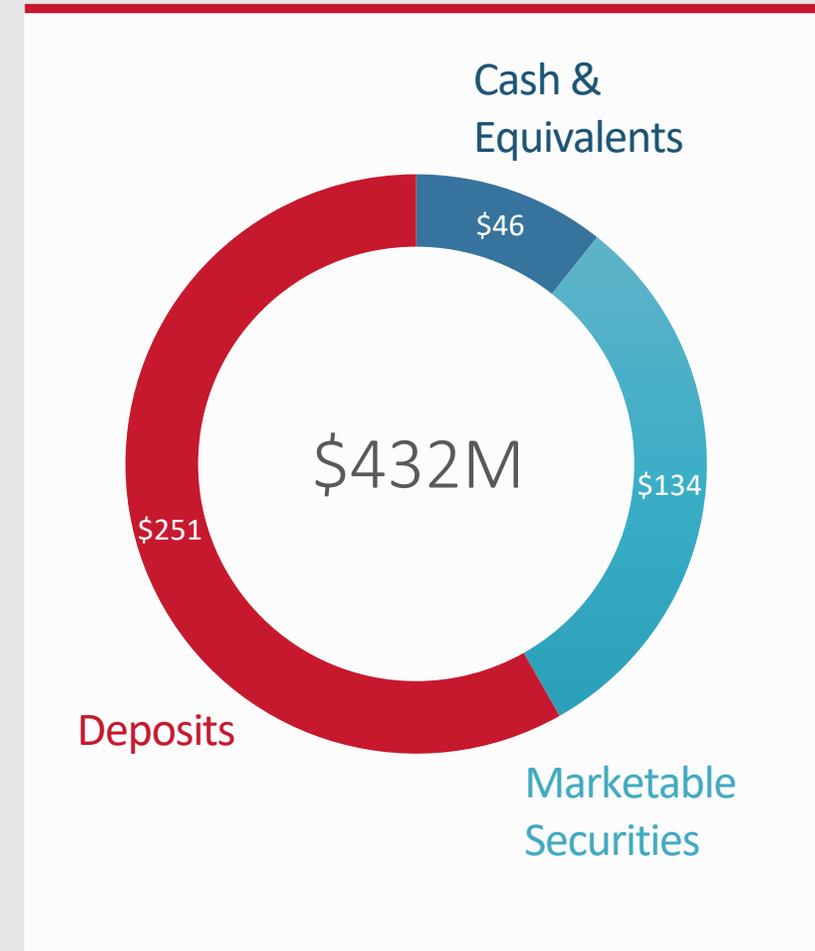
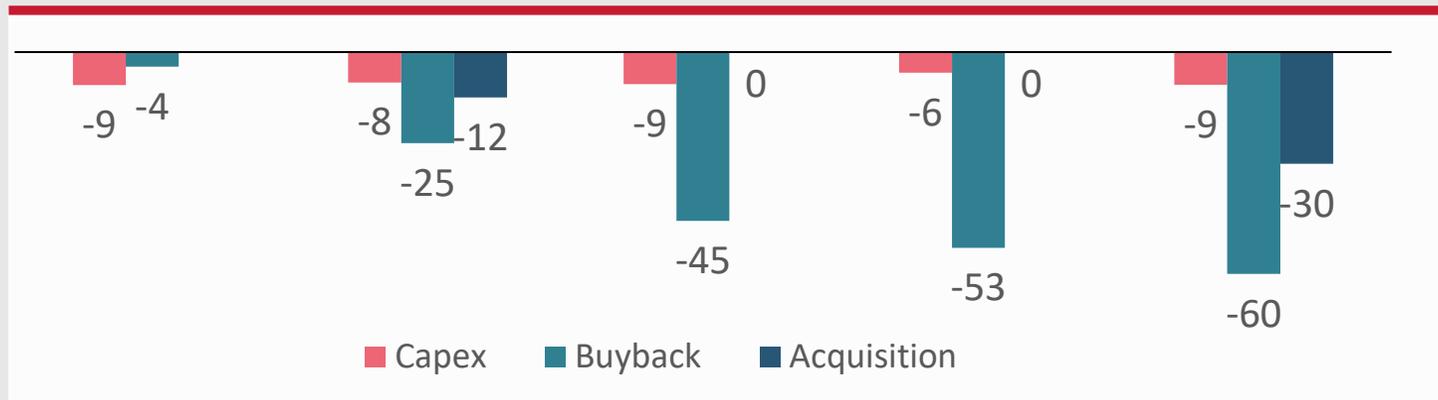
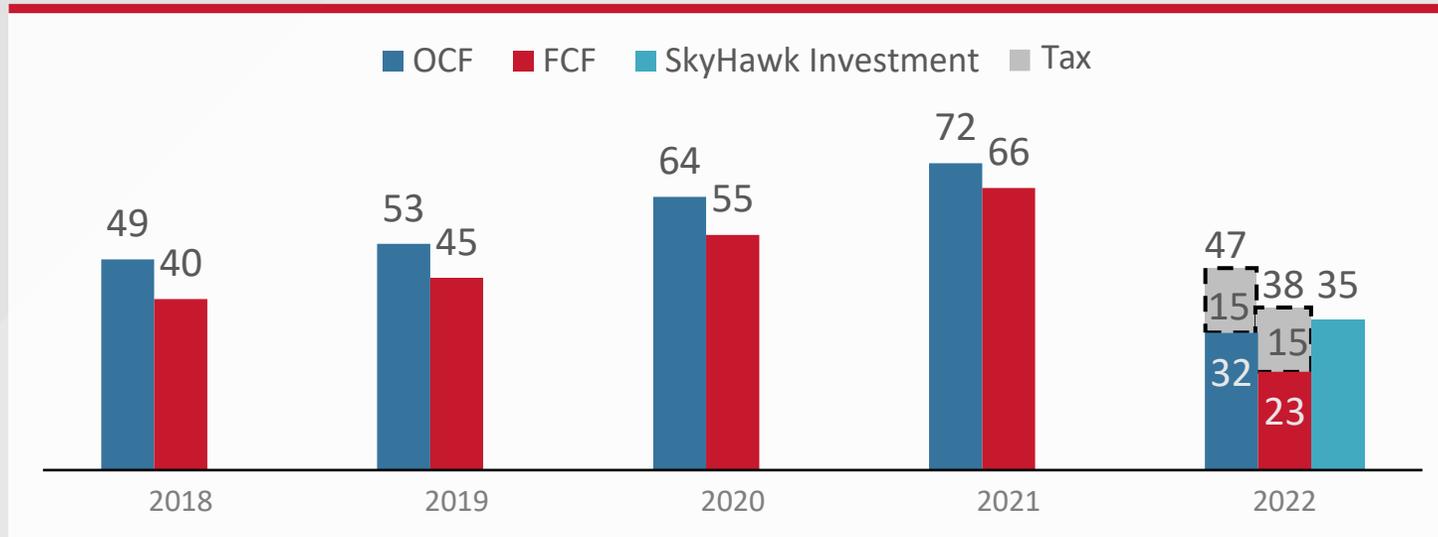
- OEMs
- Channels

# Long Term Model



Non-GAAP	2022	2027 Estimate
<b>Revenue</b>	<b>\$293M</b>	<b>\$460M</b>
Gross Margin	83%	83%
<b>OpEx</b>	<b>\$214M</b>	<b>\$282M</b>
Operating Margin	10%	22%
<b>Adj. EBITDA</b>	<b>\$38M</b>	<b>\$110M</b>
Adj. EBITDA Margin	13%	24%

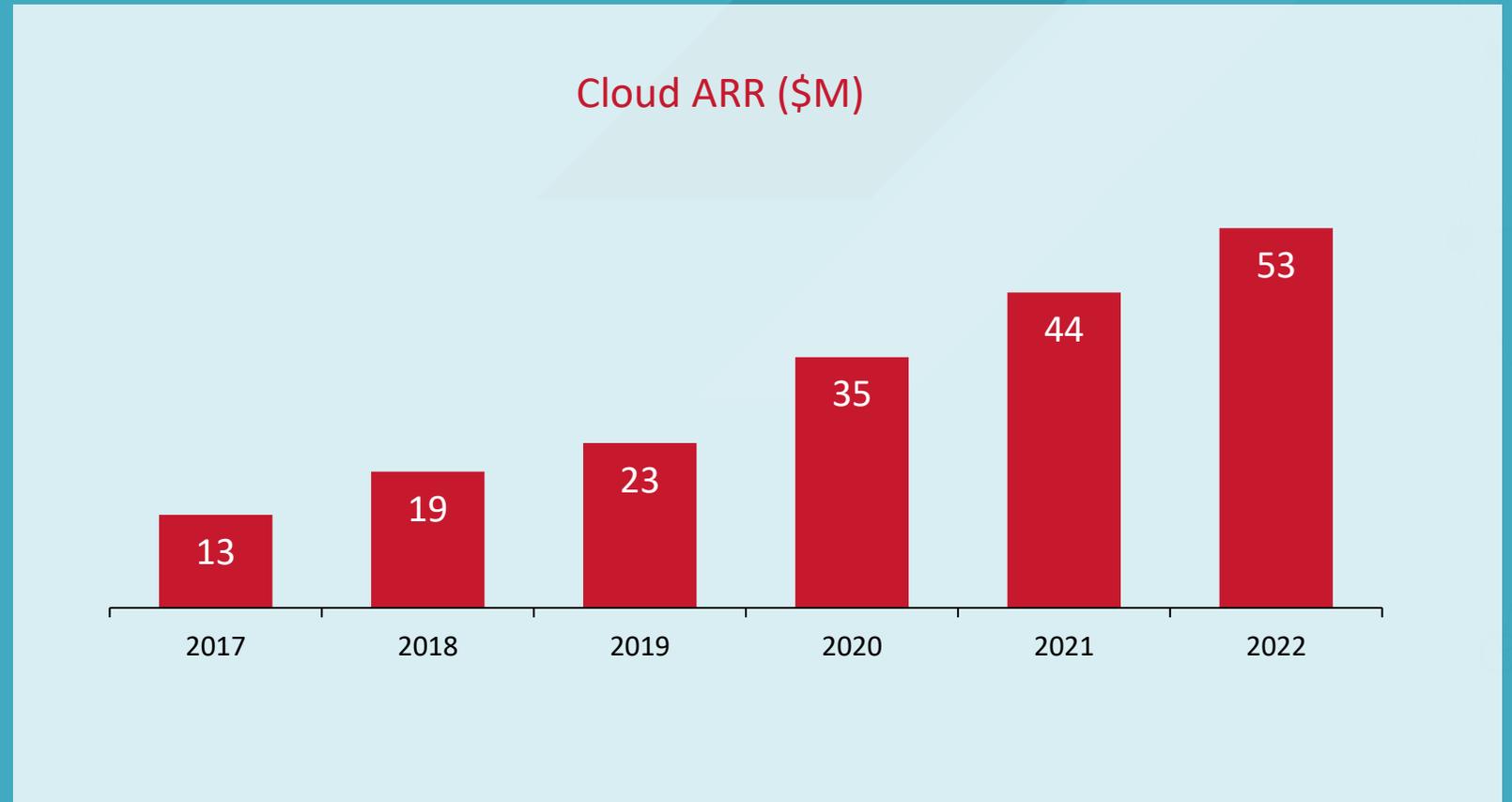
# Cash Generation



# New KPI: Cloud ARR



25% 5-Year CAGR  
in Cloud ARR in  
2027 to \$160M



## CLOUD REVENUE IS INCREMENTAL

Large Opportunities with organizations moving to cloud WAF and API  
Limited cannibalization within our cloud DDoS on-prem customers

# EBITDA Core and Hawks

M\$	2022	2027E
Radware Core	\$46.2	\$110
<b>Core EBITDA Margin</b>	<b>16%</b>	<b>24%</b>
Hawks	(\$8.5)	\$0.0
<b>Total</b>	<b>\$37.7</b>	<b>\$110</b>
<b>Total EBITDA Margin</b>	<b>13%</b>	<b>24%</b>

# Mergers & Acquisitions



## Valuation

May be attractive in 6-18 months



## Target

Increase security ARR, predominantly Cloud ARR

# Why Radware?



Leading Critical Cyber Security Vendor



Large Growing TAM and SAM



Leading Differentiated Technology



Large Enterprise and Carriers Customer Base



Fast Growing Cloud Security Business



Sustainable Growth and Profitability

# Thank You!

