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 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.
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
Why Radware?

- Leading Critical Cyber Security Vendor
- Fast Growing Cloud Security Business
- Large Growing TAM and SAM
- Large Enterprise and Carriers Customer Base
- Leading Differentiated Technology
- Sustainable Growth and Profitability
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
Critical, Need State-of-the-Art Security

Cloud Transition

Accelerated Digital Transformation

Shortage in Security Experts & Skills
Growing Threat Landscape

Shift in Attackers’ Motivation

Shift to Attacks on Application Layer (incl. Web DDoS)

Shift to Automated Tools
Attach Campaign On Health Care February 2023

Threat intelligence, Application security, Vulnerability management

Killnet DDoS attacks inflicting damage on healthcare: ‘This is war’

Jessica Davis  February 13, 2023

The Killnet hacktivist group’s DDoS attacks against healthcare and the mass data exfiltration in January were reportedly just the first round of targeting. Industry leaders have warned that the impact of cyberattacks on the health sector is significant.

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

KillNet hits healthcare sector with DDoS attacks

Published: February 13, 2023 by Peter Arzu

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.

Claimed Attacks on Telegram: Global

Canadian PM (June 2023)

Claimed Attacks on Telegram: Global

Canadian PM (June 2023)

Claimed Attacks on Telegram: Global

UPS (April, June & Sept. 2023)

Claimed Attacks on Telegram: Global

UPS (April, June & Sept. 2023)

Claimed Attacks on Telegram: Global

Wells Fargo (Sept. 2023)

Claimed Attacks on Telegram: Global

Wells Fargo (Sept. 2023)
#OpIsrael 2023: Anonymous Sudan Joins the Islamic Jihad
Launches cyber attacks against Israeli sites (gov’t, utilities, energy, civil defense)

Israel Early Warning App (Red Colour)

Israeli News Portal: Rotter.net
May’23: Attack bypassed Cloudflare; site went down

Sept’23: Attack blocked by 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!
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
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
  Frictionless Security

- 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
  Automated Protection and Fully Managed Services
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

* Sources: 2022 (ISC)² Cybersecurity Workforce Study & Survey by Gaper ISSA/ESG
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
What is Needed to Stay Ahead?

**REAL-TIME**
Immediate, real-time protection from advanced, unknown threats

**INTELLIGENT**
Automated protections based on AI + ML-based algorithms that evolve as the attacks morph

**UNIVERSAL**
360-degree, consistent protection across all environments and entry points
Radware 360 Application Protection
The Radware Difference

REAL-TIME
- Immediate Protection
- Behavioral-based Zero-Day Attack Protection
- Advanced challenges (crypto challenge)

INTELLIGENT
- AI & ML Algorithms
- Adaptive & Continuous Learning
- Auto Detection & Mitigation
- No Human Intervention Required

UNIVERSAL
- Agnostic, Consistent & Integrated
- Across All Environments, K8S, APIs & Browser-side
- Expert & Managed Services
State-of-the-Art Protection: Winning Industry Recognition

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

“Radware is recognized as a WAF 2023 Overall Leader & Outperformer, Product, Innovation & Market Leader.”

“Aite Novarica noted that ‘The largest global financial institutions, brokerage firms, and financial services companies use Radware’s Bot Manager.’”
State-of-the-Art Protection: Winning Industry Recognition

Gartner Peer Insights:

98% WOULD RECOMMEND Radware Cloud WAF Service

94% WOULD RECOMMEND Radware Cloud DDoS Protection Service

* Gartner Peer Insight as of Feb. 20th 2023

“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

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
Global Cloud Services Network

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 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
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 in 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
Q3 2023 Highlights

- **Recurring Revenue**: 79% compared to 71% last year
- **Gross Margin**: 81.1% compared to 82.9% last year
- **Total ARR**: 5% increase YoY*
- **Revenue**: $62M, 13% decrease YoY
- **Cloud ARR**: $63M, 25% increase 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 growth of 8% when excluding ARR churn from previous quarters due to the unique customer relationship.
ARR Driven by Cloud ARR ($M)

Total ARR ($M)

Q3 2018: 137
Q3 2019: 150
Q3 2020: 168
Q3 2021: 185
Q3 2022: 195
Q3 2023: 204

8% CAGR

Cloud ARR ($M)

Q3 2018: 18
Q3 2019: 22
Q3 2020: 31
Q3 2021: 42
Q3 2022: 50
Q3 2023: 63

28% CAGR

* 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
* ARR 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

*ARR numbers are rounded
Recurring Revenue (%) Driven by Cloud ARR ($M)

Q3 2018: 13%
Q3 2019: 15%
Q3 2020: 18%
Q3 2021: 23%
Q3 2022: 26%
Q3 2023: 31%

Cloud ARR as % of Total ARR:
- Q3 2018: 61%
- Q3 2019: 64%
- Q3 2020: 65%
- Q3 2021: 65%
- Q3 2022: 71%
- Q3 2023: 79%
Non-GAAP Financial Data

Total Revenue ($M)
- Q3 2022: $70.5
- Q3 2023: $61.6
- Change: ~13%

Gross Margin
- Q3 2022: 82.9%
- Q3 2023: 81.1%
- Change: ~180bp

Operating Expenses ($M)
- Q3 2022: $53.2
- Q3 2023: $50.4
- Change: ~5%

EPS ($)
- Q3 2022: $0.15
- Q3 2023: $0.07
- Change: ~53%
Q3 2023 Revenue Breakdown by Geographies ($M)

- **AMERICAS**
  - $24.9 Million
  - -24% YoY

- **EMEA**
  - $19.4 Million
  - -13% YoY

- **APAC**
  - $17.3 Million
  - +12% YoY

Total Revenue: $61.6 Million
Cash Generation

<table>
<thead>
<tr>
<th></th>
<th>Q3 2020</th>
<th>Q3 2021</th>
<th>Q3 2022</th>
<th>Q3 2023</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCF</td>
<td>7</td>
<td>18</td>
<td>2</td>
<td>-10</td>
</tr>
<tr>
<td>FCF</td>
<td>5</td>
<td>16</td>
<td>-3</td>
<td>-11</td>
</tr>
<tr>
<td>Capex</td>
<td>-2</td>
<td>0</td>
<td>-6</td>
<td>-1</td>
</tr>
<tr>
<td>Buyback</td>
<td>-16</td>
<td>-1</td>
<td>0</td>
<td>-21</td>
</tr>
</tbody>
</table>

Deposits: $32M
 Marketable Securities: $135M
 OCF: $204M
 FCF: $371.6M

OCF: Operating Cash Flow
FCF: Free Cash Flow
Capex: Capital Expenditure
Buyback: Share Buyback