# AI vs AI
# The Demise of 'Human' Intervention

**Marius Baczynski**

**Director – Cloud Security Services (EMEA)**

**MSSP Program Lead (EMEA)**

# About Radware

*"Dedicated to Protecting Your Critical Applications"*

## 1000+ Cloud Customers

Morgan Stanley, ING, CATERPILLAR, NYC HEALTH+HOSPITALS, ebay, verizon, Bloomberg, SAS, HSBC, salesforce, fiserv., SAP, AT&T, T-Mobile, Geisinger, bandwidth, Telefónica, SAMSUNG, Deloitte.

## Analysts

IDC Analyze the Future

DDoS MarketScape
**Leader**

Gartner

API & High Security
**Leader**







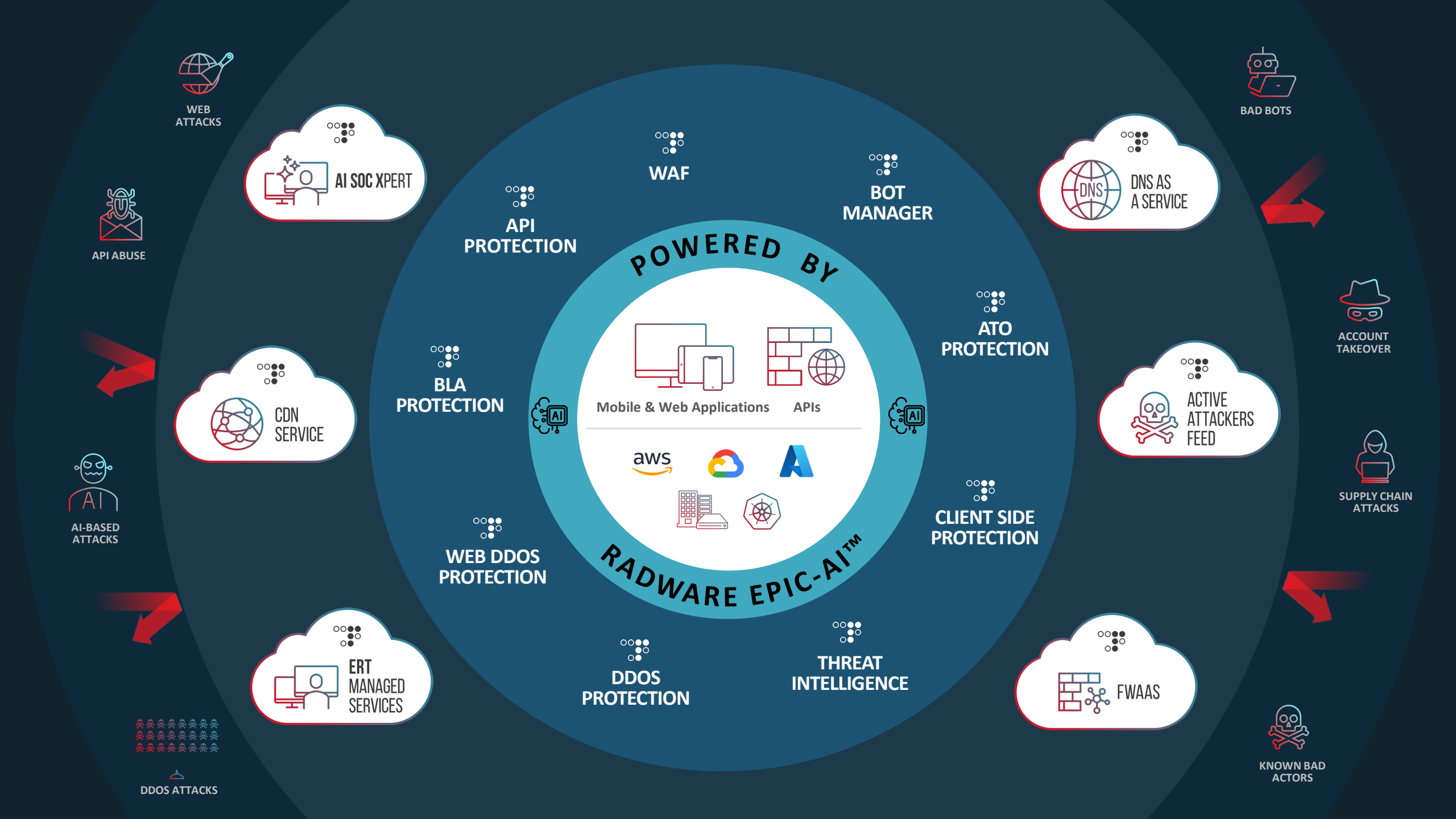

## OEM Partners

CISCO

CHECK POINT

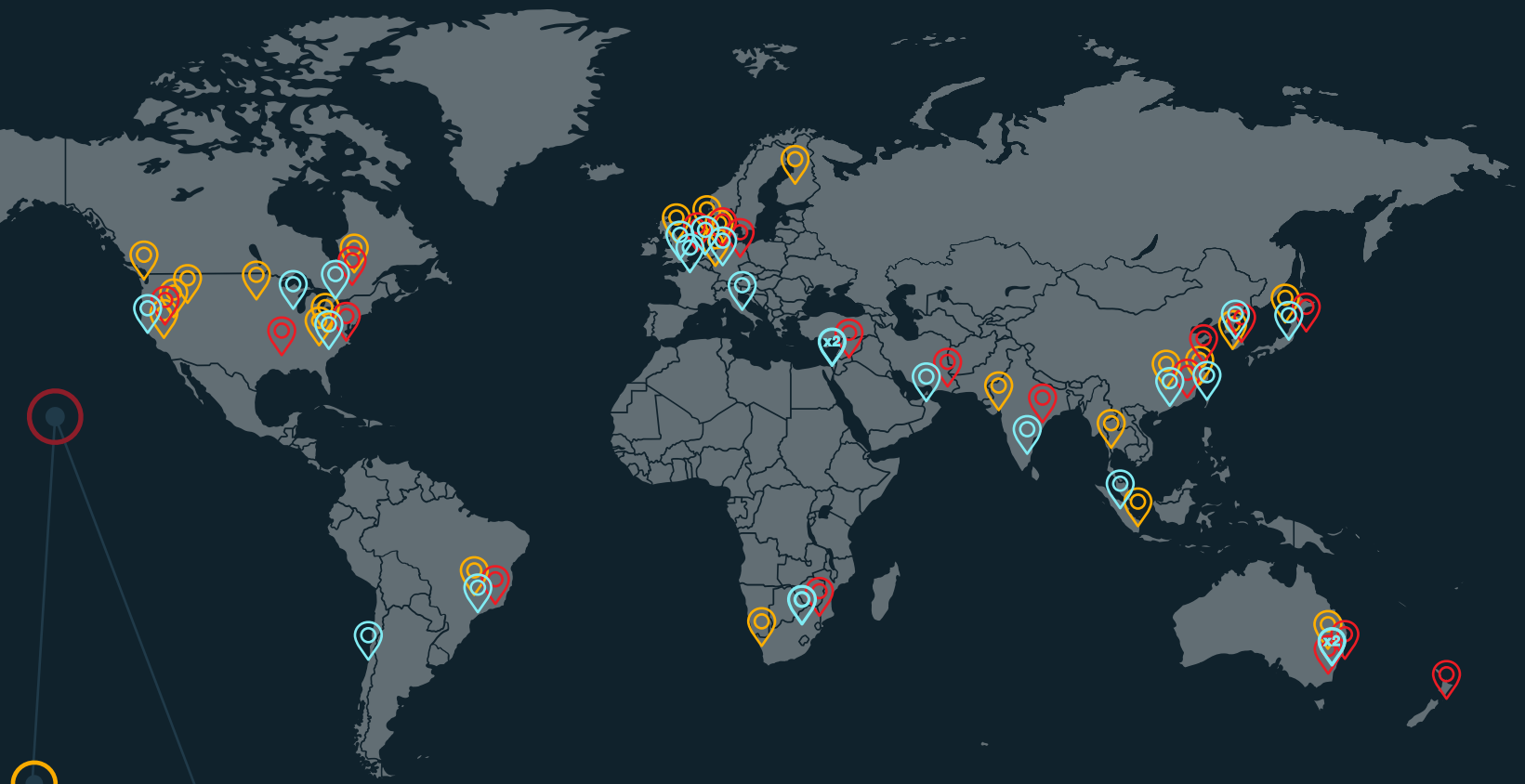
aws

Microsoft Azure


WEB ATTACKS
AI SOC XPERT
API ABUSE
API PROTECTION
WAF
BOT MANAGER
BAD BOTS
DNS AS A SERVICE
ACCOUNT TAKEOVER
ATO PROTECTION
CDN SERVICE
BLA PROTECTION
POWERED BY
Mobile & Web Applications
APIs
aws
ACTIVE ATTACKERS FEED
AI-BASED ATTACKS
SUPPLY CHAIN ATTACKS
CLIENT SIDE PROTECTION
WEB DDOS PROTECTION
RADWARE EPIC-AI™
ERT MANAGED SERVICES
DDOS PROTECTION
THREAT INTELLIGENCE
FWAAS
DDOS ATTACKS
KNOWN BAD ACTORS

# Global Cloud Services Network

Delivered as a Fully Managed Service 24/7



**21** Scrubbing centers **Worldwide**

**15 Tbps** of global mitigation capacity

**50+** **AppSec PoPs** With Global Coverage

**1200** **CDN POPs** Low latency & fast response

# Unmatched Compliance to the Strictest Standards

| | |
|---|---|
| **BSI qualified** | **DDoS Protection Vendor Listing** |
| **ISO 22301** | Business Continuity Management System |
| **ISO 27001** | Information Security Management Systems |
| **ISO 27017** | **Information Security for Cloud Services** |
| **ISO 27018** | **Information Security Protection of PII in public clouds** |
| **ISO 27701** | **Privacy Information Management for PII controllers and processors** |
| **ISO 27032** | Security Techniques -- Guidelines for Cybersecurity |
| **ISO 28000** | Specification for Security Management Systems for the Supply Chain |
| **EU GDPR** | **EU General Data Protection Regulation** |
| **PCI-DSSv4** | Payment Card Industry Data Security Standard |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **US SSAE16** | SOC-1 Type II, SOC-2 Type II |
| **DORA** | **Digital Operational Resilience Act** |
| **NIS2** | **Network and Information Systems Directive 2022/0383** |

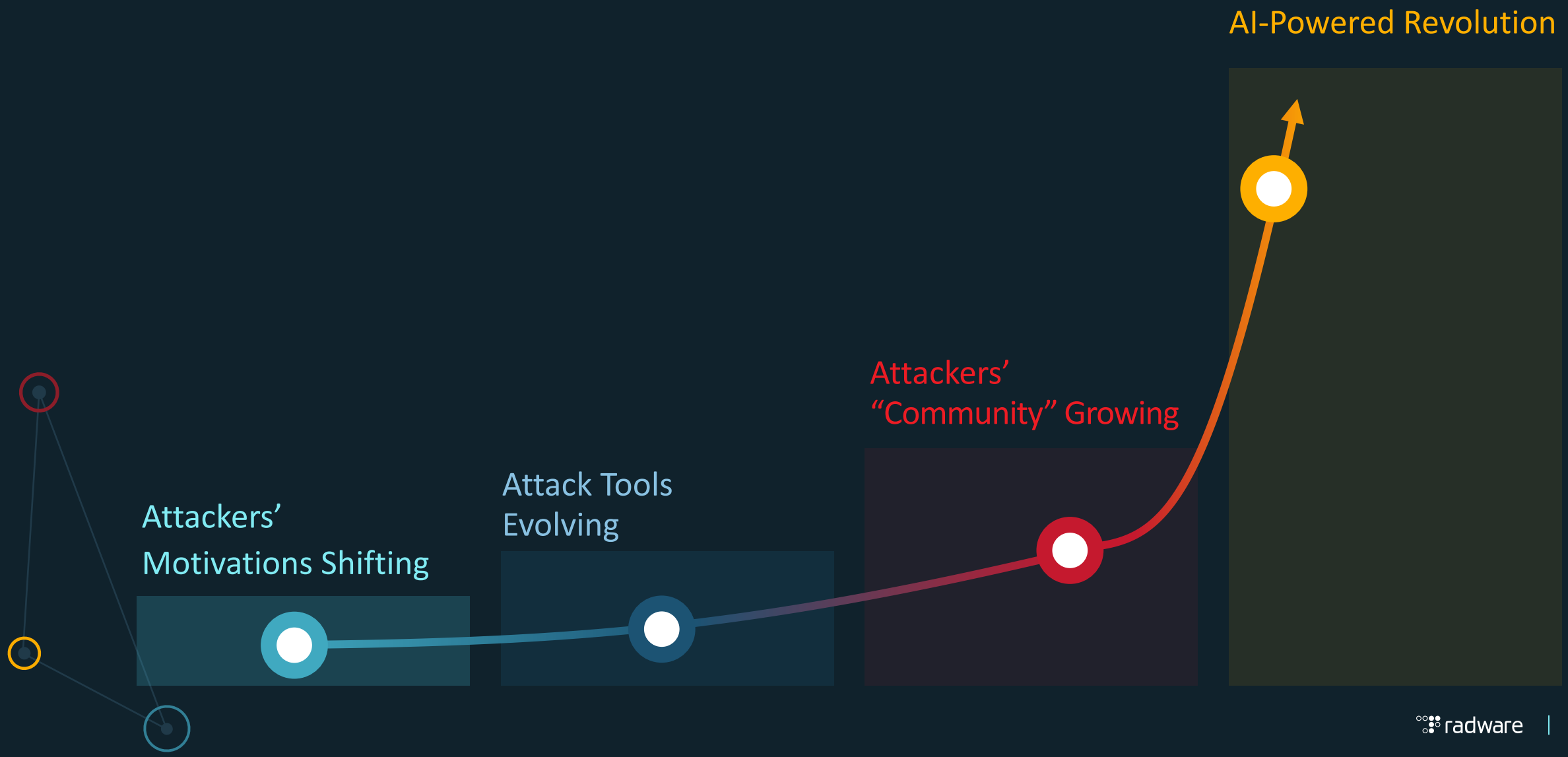




radware

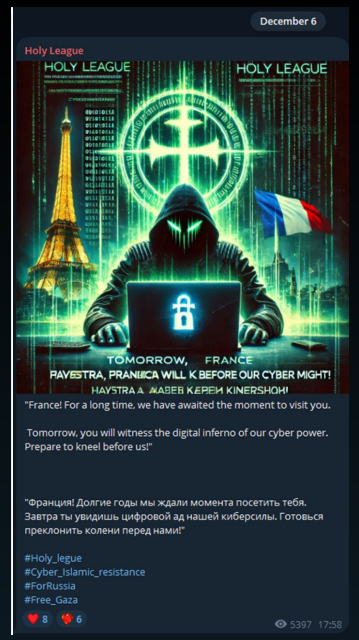
# What's the Problem?

# The Modern Threat Landscape is Shifting Exponentially

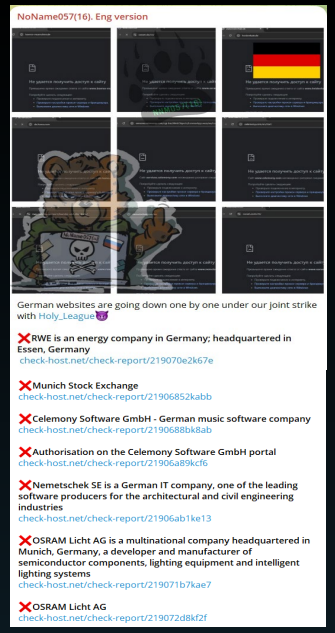


# Shifting Attack Motivations of Hacktivist Groups

## Politically Motivated



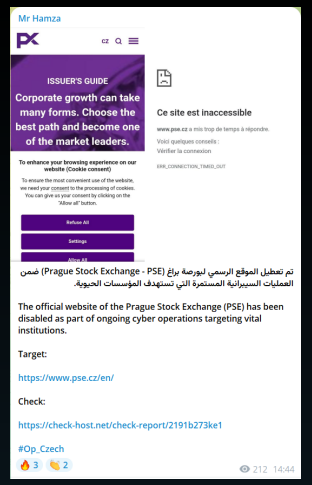

French Gov & AXA Insurance
**(DEC 24)**




Holy League attacks German industries and Munich SE
**(DEC 24)**

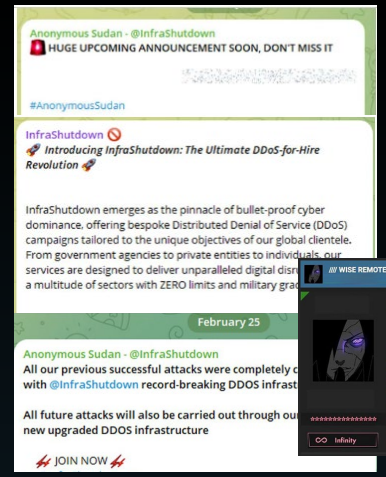
## Religiously Motivated


RipperSec Attack on French Banks
**(DEC 24)**

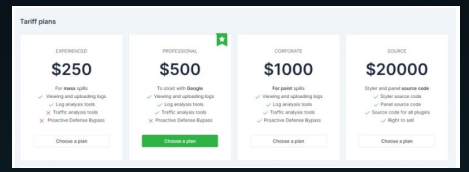



Czech Gov & Prague Stock Exchange
**(DEC 24)**

## Financially Motivated




DDoS & Botnet for hire


Attackers Offering Full Marketplace

# All-in-One Automated Attack Tools on Github


Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

**DDoS attack vectors**

**Bot attack vectors**

**Web application exploits**

**Built-in bypass again common defenses**

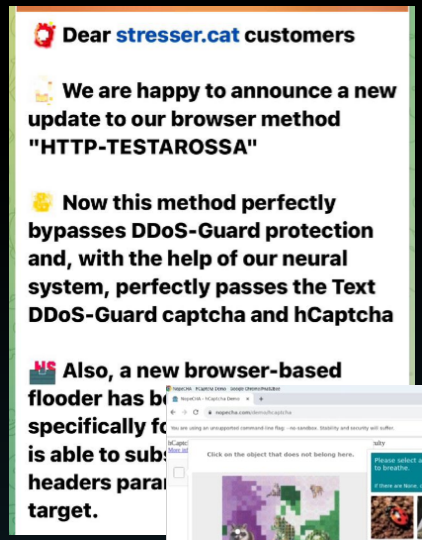
- Attackers don't distinguish between WAF, DDoS, Bot, API attack vectors
- Need an **integrated platform** to **overcome all-in-one attack tools**

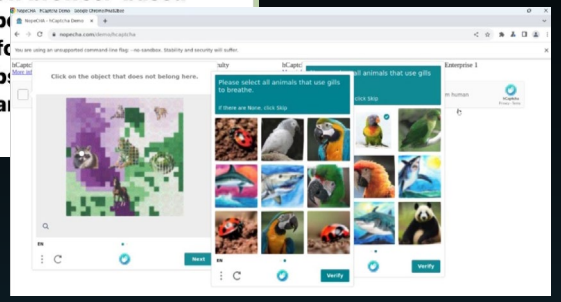
# Attackers Use AI to Automate Attacks





GenAI tools used by attackers



New AI-based CAPTCHA solving tool

| Vulnerability | GPT-4 success rate |
|---|---|
| LFI | 60% |
| CSRF | 100% |
| XSS | 80% |
| SQL Injection | 100% |
| Brute Force | 80% |
| SQL Union | 80% |
| SSTI | 40% |
| Webhook XSS | 20% |
| File upload | 40% |

Research shows how LLM Agents can autonomously exploit one-day vulnerabilities*

* [2404.08144] LLM Agents can Autonomously Exploit One-day Vulnerabilities (arxiv.org)

**Fight AI with AI: Need AI-Powered Intelligent Security**

# AI Introduces ‘Unprecedented Unpredictability’ to Threats

- Signficantly lower barriers to launch sophisticated, unpredictable attacks
- AI-driven attacks can evolve rapidly and create new, unforeseen vulnerabilities
- Even cognitive SOARs struggle with dynamic nature of AI-driven attacks
- Application security must develop AI models that can understand normal behavior, identify anomalies and adapt in real-time

radware

# ‘No AI’ is NOT an option.

## What’s Needed to Stay Ahead?

# Cloud Security Platform Powered by Radware EPIC-AI™

LOWER MTTR

## SOC Management Core

- AI-powered SOC tools & managed services
- SecOps enablement
- Compliance, analytics & integrations

## Cross-Platform Fabric

- Threat intelligence insights & preemptive protection feeds
- Cross-module AI-based correlation
- Continuous AI-powered policy tuning & recommendations

## RT Cloud Protection Engines

DDOS PROTECTION | WEB DDOS PROTECTION | WAF | API & BLA PROTECTION | BOT MANAGER | ATO PROTECTION | CLIENT SIDE PROTECTION

## Enforcement Points

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

# Real World EPIC-AI Protection Where It Matters Most


Accelerate SOC ops & reduce MTTR by upto 20X

Quickly identify root cause & resolve incidents with Radware's AI SOC Xpert


Block malicious sources across the platform

Preemptive protection with AI-driven 'Source Blocking' algorithms


Surgically block Web DDoS Tsunami Attacks

AI-powered Web DDoS Protection with 'surgical' real-time signature creation

> *Radware is the **only vendor** in this analysis **to earn a top score** on the **AI enhanced vulnerability detection** criterion*
>
> GIGAOM

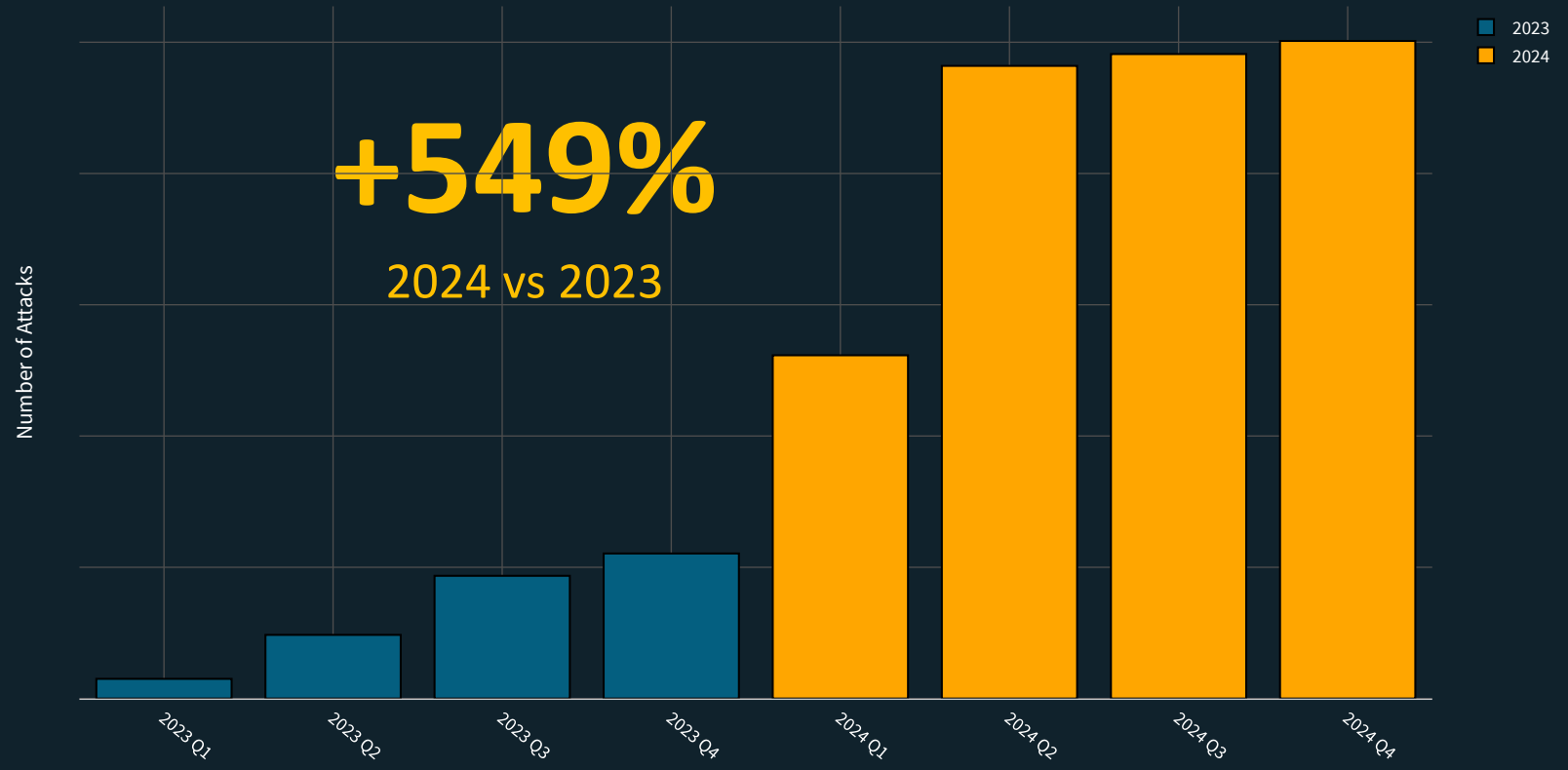
> *Gartner clients **value the automated learning approach** that Radware takes*
>
> Gartner

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

# Web DDoS
# The preferred Weapon of Cyber Crime

Hard to detect,
Difficult to mitigate

Web DDoS Attack per Quarter 2023-2024



# Deadly Web DDoS Tsunami Attacks

**AI-powered** approach essential for **accurate** detection & mitigation

Basic techniques (Rate limiting, Geo-blocking, CAPTCHA, JS Challenge) impact legitimate traffic and/or user experience

- Low traffic volume – Ultra high RPS
- Encrypted floods
- Appear to be legitimate requests
- Multiple, sophisticated evasion techniques (randomized headers, IP spoofing, etc)

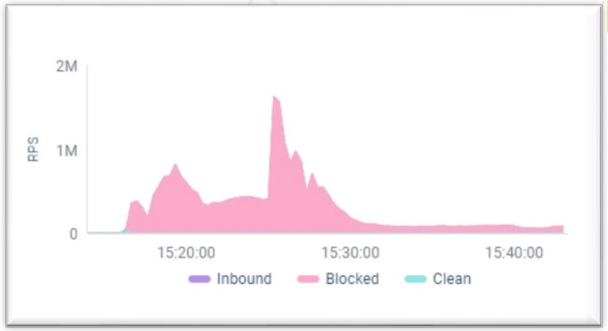
# Significant WebDDoS attack on large European Airline

Mitigation

Total Requests
Received 7,323,560,508
Dropped 7,322,893,004

Average Values
Requests per Second 839,857 RPS

Maximum Values
Requests per Second 1,892,054 RPS



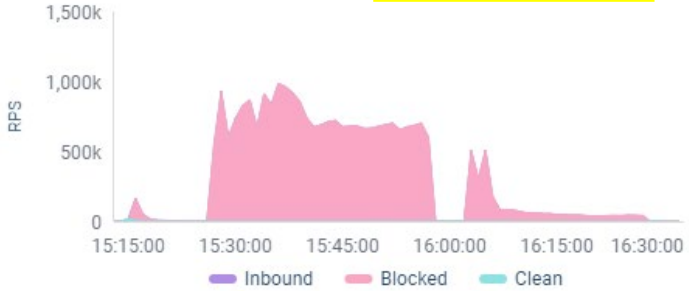

Mitigation

Total Requests
Received 1,546,214,661
Dropped 1,544,249,607

Average Values
Requests per Second 333,235 RPS

Maximum Values
Requests per Second 1,289,856 RPS

Requests Rate
Detection Manual
Attack Start Value 92,937 RPS




Mitigation

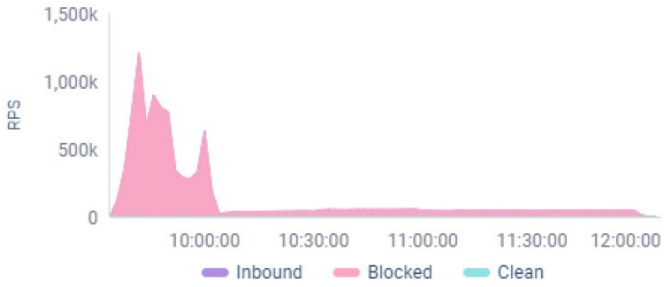
Total Requests
Received 1,240,818,185
Dropped 1,240,530,161

Average Values
Requests per Second 138,022 RPS

Maximum Values
Requests per Second 1,776,723 RPS

Detection

Requests Rate
Detection Manual
Attack Start Value 4,140 RPS



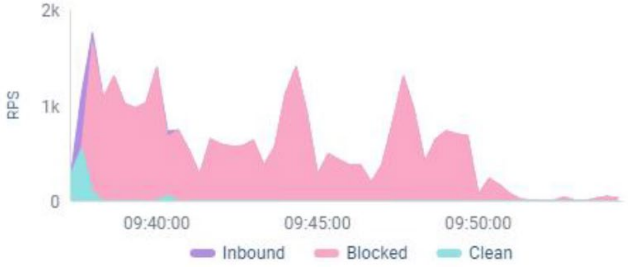

Mitigation

Total Requests
Received 575,899
Dropped 561,448

Average Values
Requests per Second 559 RPS

Maximum Values
Requests per Second 2,031 RPS

Requests Rate
Detection Manual
Attack Start Value 755 RPS



# Radware Protects EMEA Bank from Web DDoS Tsunami Attacks


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

***Radware Customer, Tech Services***

PeerSpot

## Attack Peaks

Up to

**14.6M**

**RPS**

## Attack Length

Several days w/ multiple waves lasting

**10-20**

**HOURS**

## Attack Signature

Signature created in real-time includes

**27**

**PARAMETERS**

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

# Radware UNIQUE Value Proposition

- Market-leading, consolidated security platform across all layers of OSI stack
- Sophisticated, AI-enabled, automated, behavioral threat response capabilities
- 'Single pane of glass' security and visibility across entire application environment
- Futureproof architectural flexibility compatible with any type of application environment
- Fully integrated with one of the largest and fastest CDNs on the planet (AWS)
- Delivered as a Fully Managed Service 24/7 supported by 200+ top cybersecurity experts

# Announcing MSSP Application Security by Netnordic!



BEST OF BREED:

- Best in class technology by Radware
- Best in class technological competence and service quality by Netnordic
- Local language, local timezone, local touch

**Let Netnordic experts take care of all your Application Security needs!**

# Thank you!