VEM LIVE 2023

gruppo VEM

IMPACT

CATALIZZATORI DIGITALI DI EFFICIENZA, EVOLUZIONE E CRESCITA

6 OTTOBRE 2023
GRAND HOTEL RIMINI

VEM LIVE 2023

Cyber Impact

APPLICATION SECURITY: STRATEGIE PER LA PROTEZIONE DELLE APPLICAZIONI IN CLOUD

THOMAS GALLETTI
TECHNICAL SOLUTION ADVISOR SECURITY, VEM SISTEMI

MARCO ZAMBONI
PRESALES ENGINEER, RADWARE

radware

VEM LIVE 2023

gruppo VEM

APPLICATION SECURITY: STRATEGIE PER LA PROTEZIONE DELLE APPLICAZIONI IN CLOUD

Thomas Galletti – Technical Solution Advisor Security, VEM Sistemi

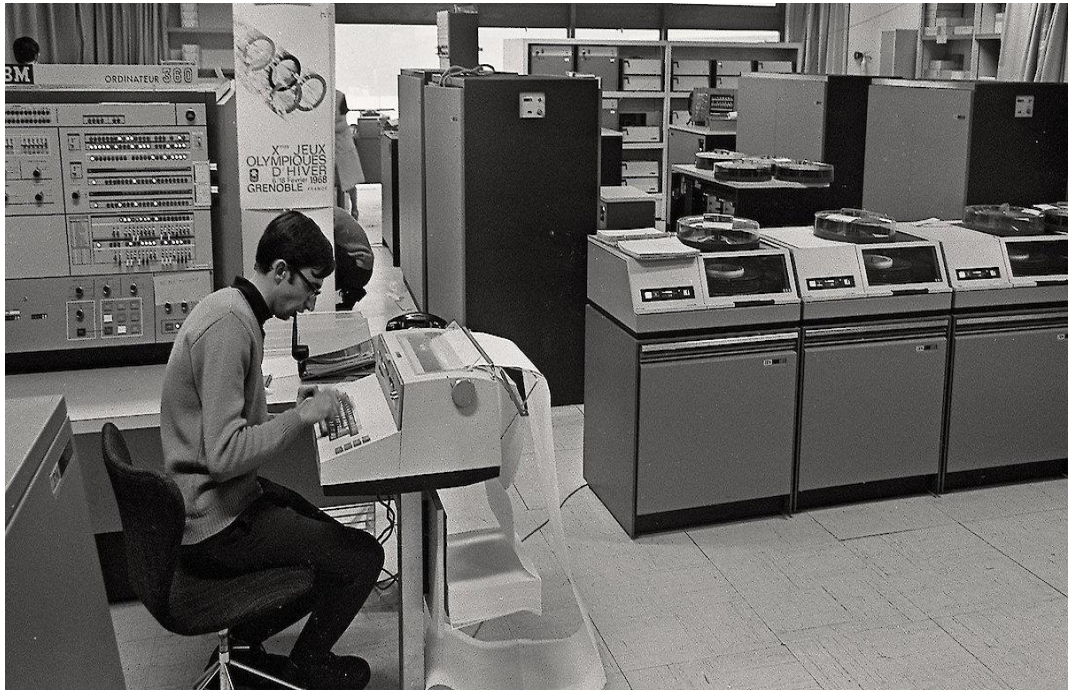
MEANING (in Information Technology)

An application (app)
an application program
or application software

is a computer program designed to help people perform an activity.

(Source: Wikipedia)

EVOLUTION



Legacy
(inside a room)

2007

Breakthrough
(over the internet)

FEATURES

User perspective:

User Friendly

Responsive interface

Multi Device

Business perspective:

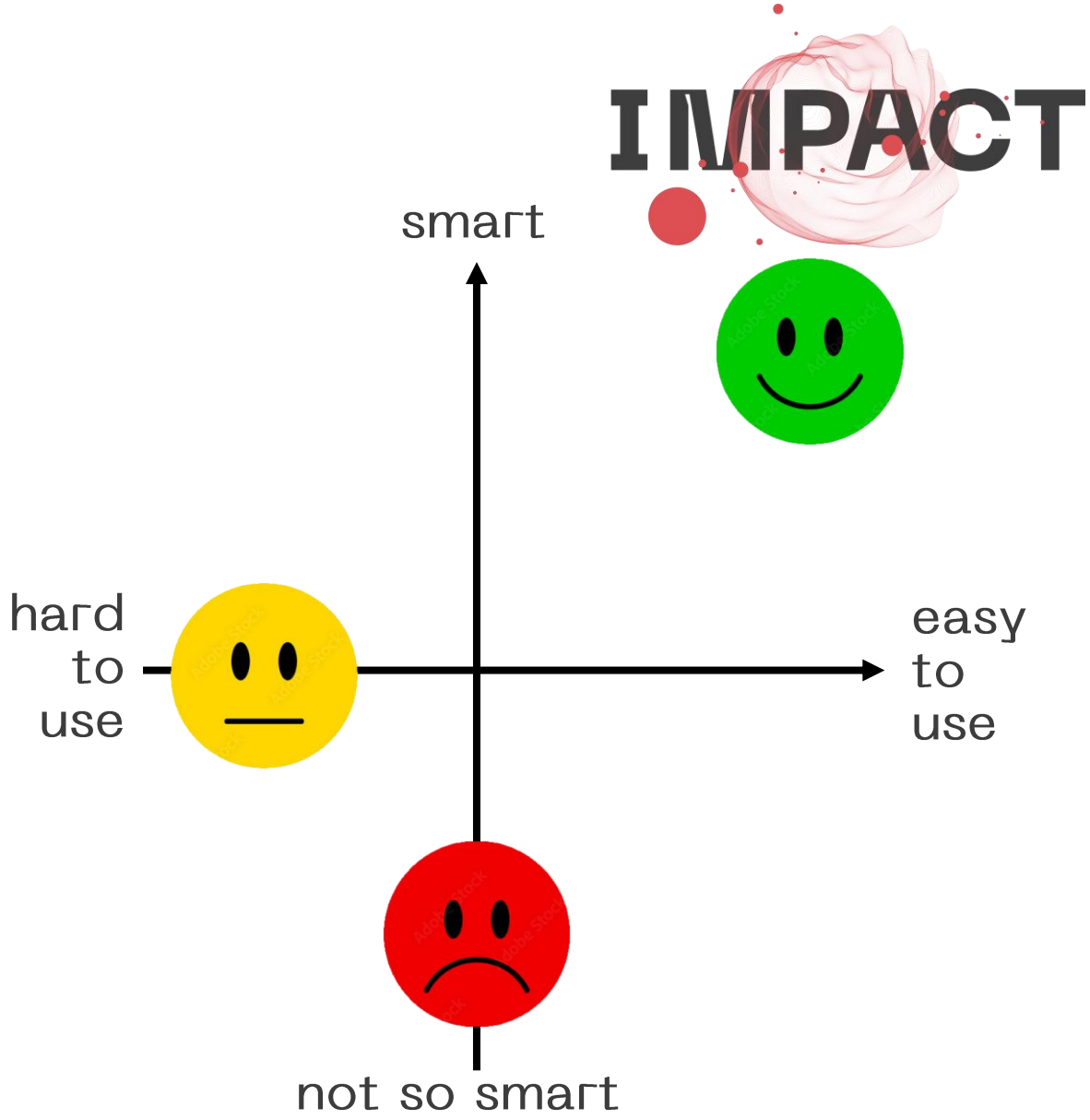
Integrable, Measurable

Available

Security perspective:

Not always considered (often forced)

Secure by Design (sometimes a joke)



TRANSITIONING (to Cloud-Native)

User perspective:

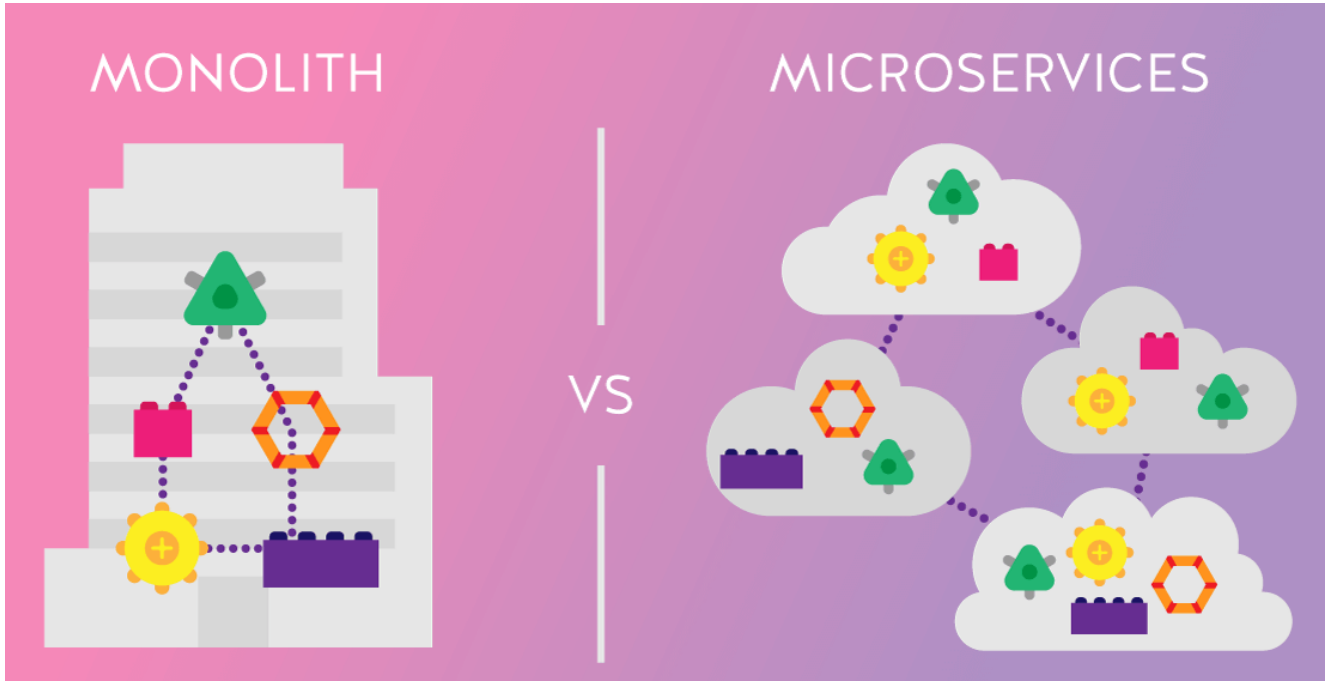
Usable
Responsive interface
Efficient
Multi Device

Business perspective:

Integrated
Available
Automated/Frictionless

Security perspective:

Resilient
Secure by Design (no more jokes)



WHAT'S AHEAD

Increasingly exposed applications on the Internet

Need for more Visibility & Governance

Mandatory Automation

Role of AI

Security Challenge

Extended (Attack/Defence) Surface

New patterns of interactions

Advanced attack techniques

Application Security: Strategie per la protezione delle applicazioni in Cloud

Marco Zamboni
Radware Presales Engineer

Rimini, 06 ottobre 2023

About Radware

Secure Your Apps. Regain Control. Enable Your Business.

Over 12,500 Customers

Bank of America, E*TRADE, ING, Wells Fargo, ebay, Staples, Samsung SDS, Carlsberg Group, salesforce, twitter, SAP, AT&T, Caterpillar, verizon, Tech Mahindra

Analysts Praise Us

IDC Analyze the Future — DDoS MarketScape **#1 Leader**

Gartner — #2 API & High Security

Forrester — DDoS Wave Leader

Quadrant Knowledge Solutions — Bot Management Leader, WAF Leader, DDoS Protection Leader

Our Partners

Cisco, Check Point, Nokia, aws, Microsoft Azure

Growing Number of Risks: No One is Immune

Vulnerability Exploitations

Capital One

100M Records

SERVER-SIDE REQUEST FORGERY

*$80M PENALTY

3.3M Records

DATA BREACH

Bot Attacks

DUNKIN' DONUTS

10M Records

CREDENTIAL STUFFING

533M Records

SCRAPING BOTS

API Abuse

venmo

200M Transactions

API EXPOSURE

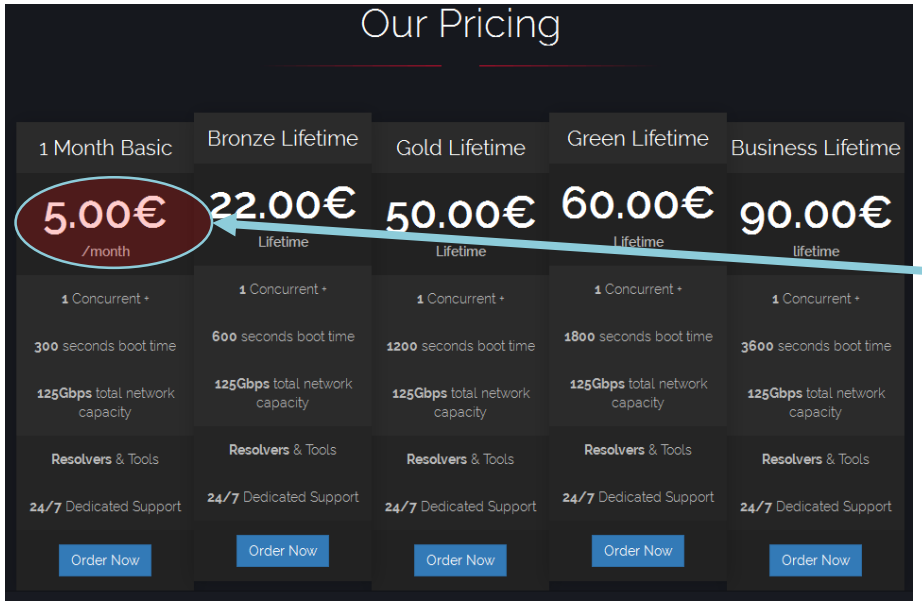
solarwinds

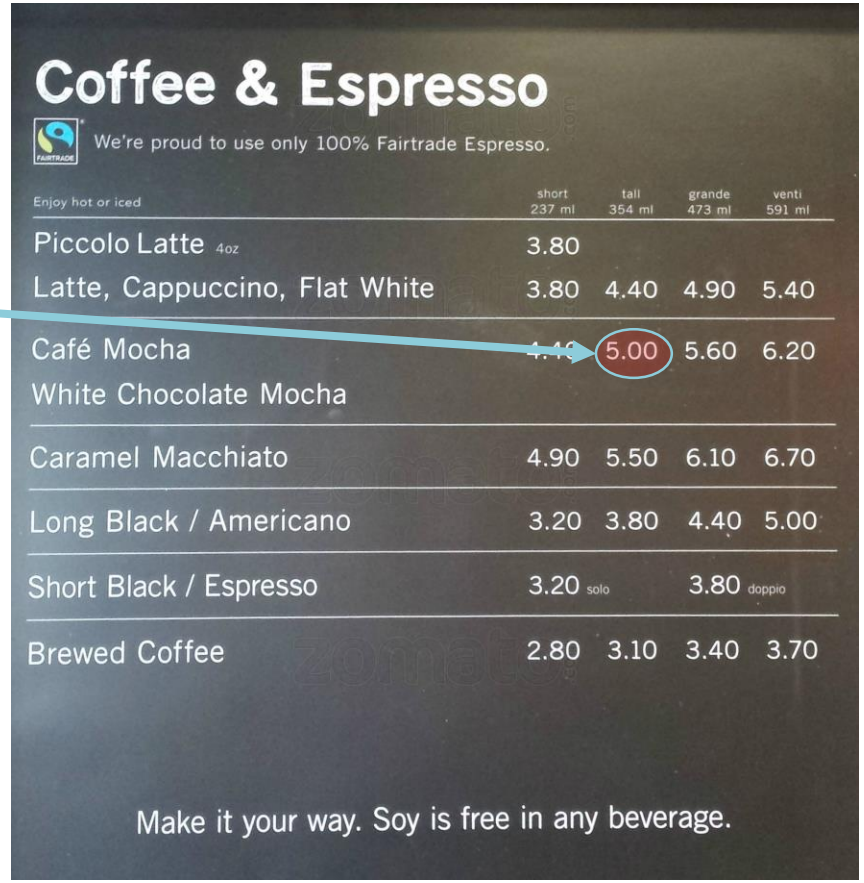
18K Companies

UP TO $100B IN DAMAGES

Maximizing security requires covering all possible threats

The Cybercriminal PriceList





Challenges to Maintaining Application Security

1. Growing Threat Landscape
2. Cloud Transition Introduces Uncertainties
3. Evolution of Modern Applications
4. Shortage in Security Experts & Skills

Growing Threat Landscape

1

DDoS Attacks Reaching New Heights

Application Attacks Continue to Grow

New Attack Vectors Challenging Defenses

Need for **state-of-the-art security** to safeguard against emerging attack campaigns

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 →

Evolution of Modern Applications

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

3

1

Application Code is Distributed Across Microservices (K8S)

2

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

3

Content Integrated With 3rd/4th Party Plug-ins **Browser Heavily Used** to Compose the Content

Modern app design creates **multiple** entry points which must be secured

Traditional WAF / WAF Appliances No Longer Enough


radware
Recent Web DDoS Attack Campaigns & Complexity of Bot vectors

New Disruptive Web DDoS Tsunami Attacks

Higher in volume and throughput

Sophisticated methodologies to bypass traditional app protections (randomized headers, IP spoofing, etc)

Appear to be legitimate requests

Require decryption + deep inspection into L7 headers for accurate detection & mitigation

Why Standard DDoS Protection is Not Effective

Standard DDoS is **Network**-Based (L3-4)

Attacks are detected & blocked based on L3-4 parameters

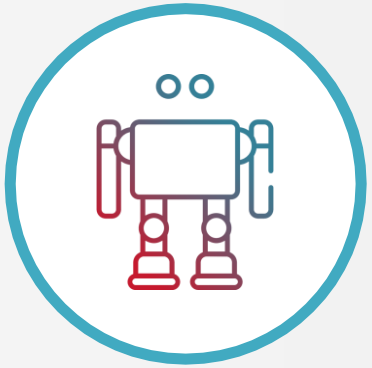
Attacks are **Application**-Based (L7)

Require decryption of attack traffic & deeper inspection into L7 headers

→ Web DDoS attacks go undetected by network-based DDoS protection solutions

Evolution of the Bots
Increased complexity and human like interaction

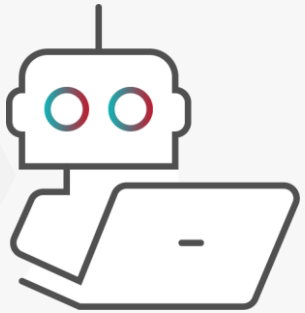
Bot

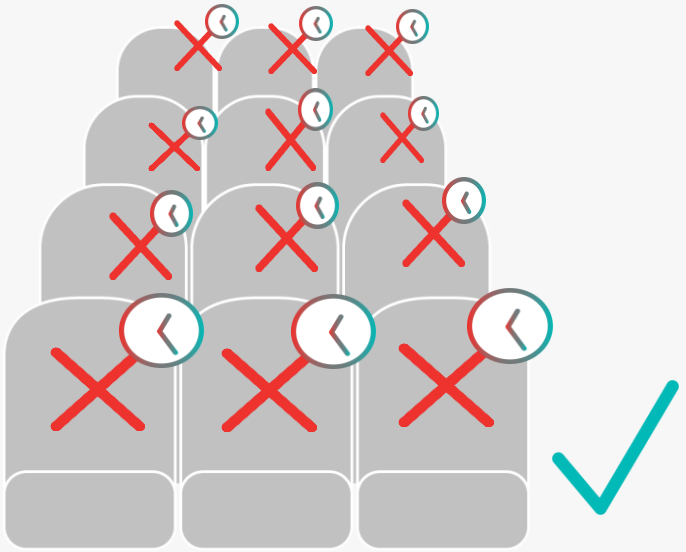
	1st Gen	2nd Gen	3rd Gen	4th Gen
Bots				
	Scripts	Headless Browsers	Human-like interaction	Distributed attacks with advanced evasion
Technology	**Blacklists** IP, User Agent	**Device/Browser** Fingerprinting, JS, iFrame	**Interaction (shallow)** Behavioral Anomalies	**Intent (deep)** Correlation of Indicators based on big-data

BOT – I rischi : Denial of Inventory

Impegnare beni o servizi stock senza mai completare l'acquisto o effettuare la transazione

Come lavora?





45%

Ha sofferto di esaurimento delle scorte

32%

Ha sofferto di impegno dell'inventario

Perdita di utenti

Danni di immagine

Perdita di ricavi

How Radware protects you

radware

How to Drive Down the Total Cost of Ownership

Fully Managed Services

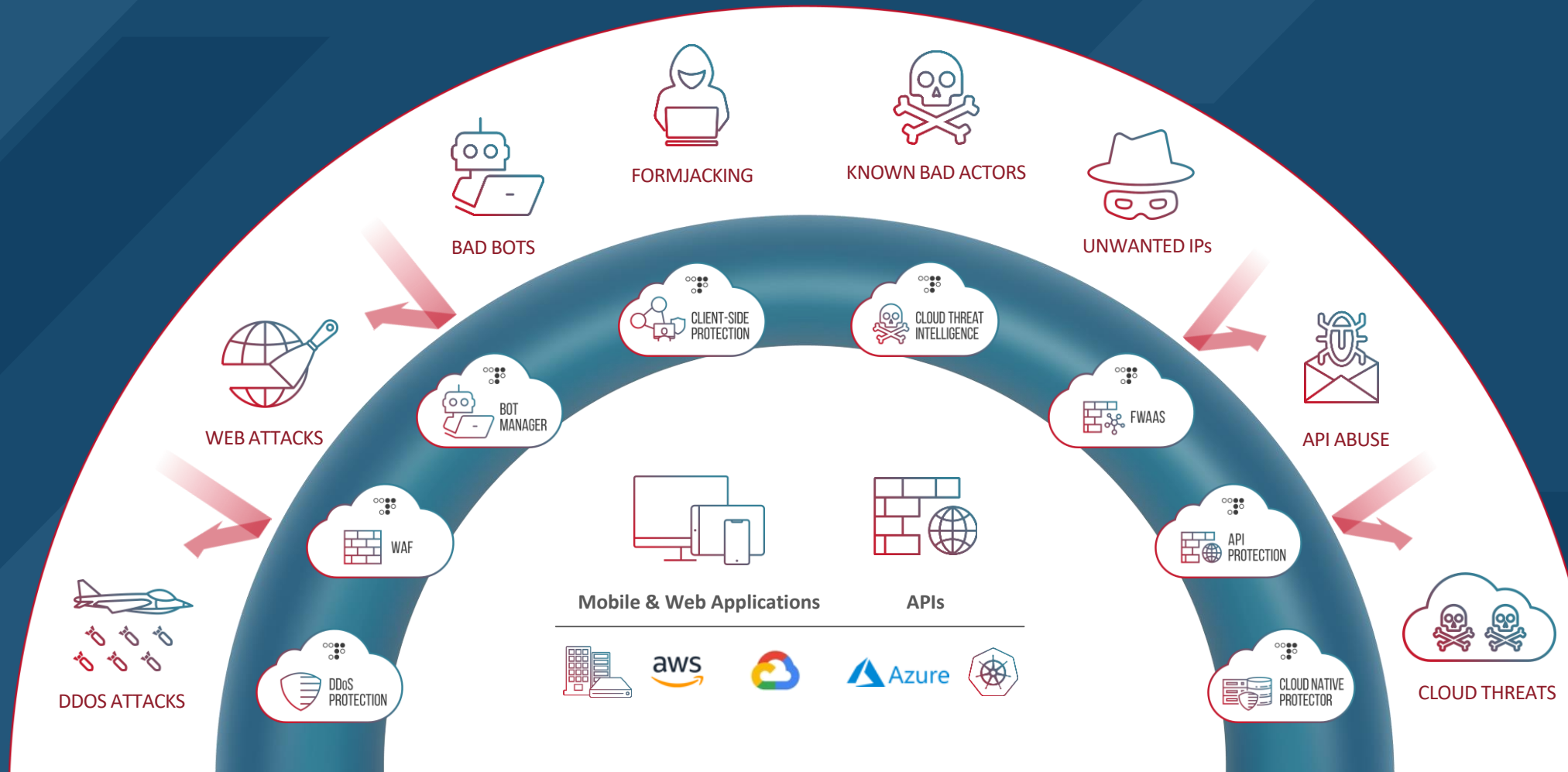
Best-of-Suite: Consolidation of Solutions

Automation of Resource-Heavy Processes

Integrated, Centralized Management & Visibility

Radware 360 Application Protection

Secure Your Apps. Regain Control. Enable Your Business.



Adaptive, Automated

No Human Intervention Required

Network, Application DDoS Protection

Behavioral-based detection w/ real-time signature creation

Advanced protections for L7 DDoS, Burst and Encrypted attacks

Next-Gen Web App Protection

Advanced ML to detect 0-day & emerging attacks

Crypto-challenge bot mitigation

Client-side attack protection

Best User Experience – CAPTCHA-less Bot Mitigation

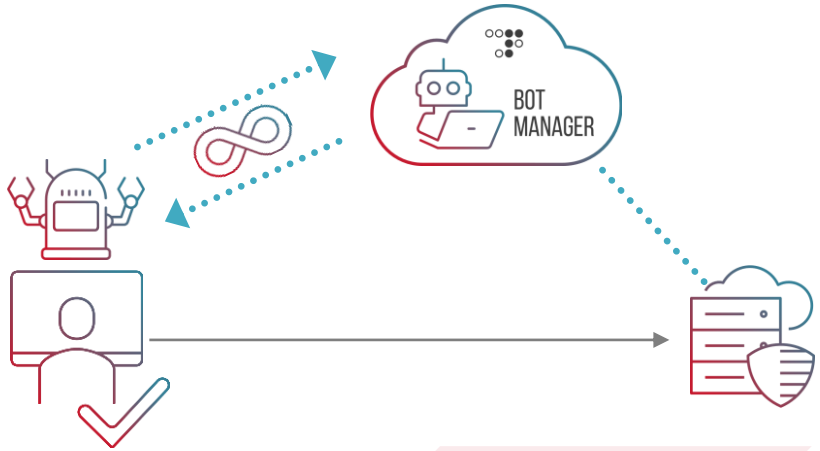
Blockchain Crypto Challenge

An Alternative to CAPTCHA – Why?

- Interactive challenge
- Binary determination
- Impact on UX
- CAPTCHA solving bots and CAPTCHA farms (e.g. 2captcha.com)

The Value of Blockchain

- No Impact on UX
- Continuous challenge, better protection
- Less frustration, less churn
- Keeps bots busy, makes them pay



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

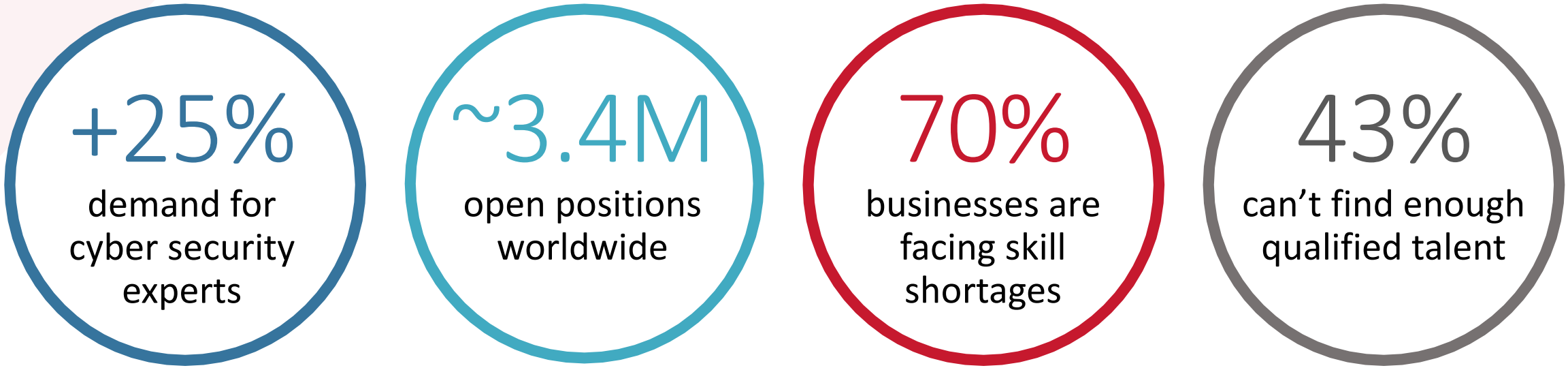
Adaptive, Automated

NO HUMAN INTERVENTION REQUIRED

Fully Managed Services

SUPERIOR SLA, 24/7 EXPERT SERVICE

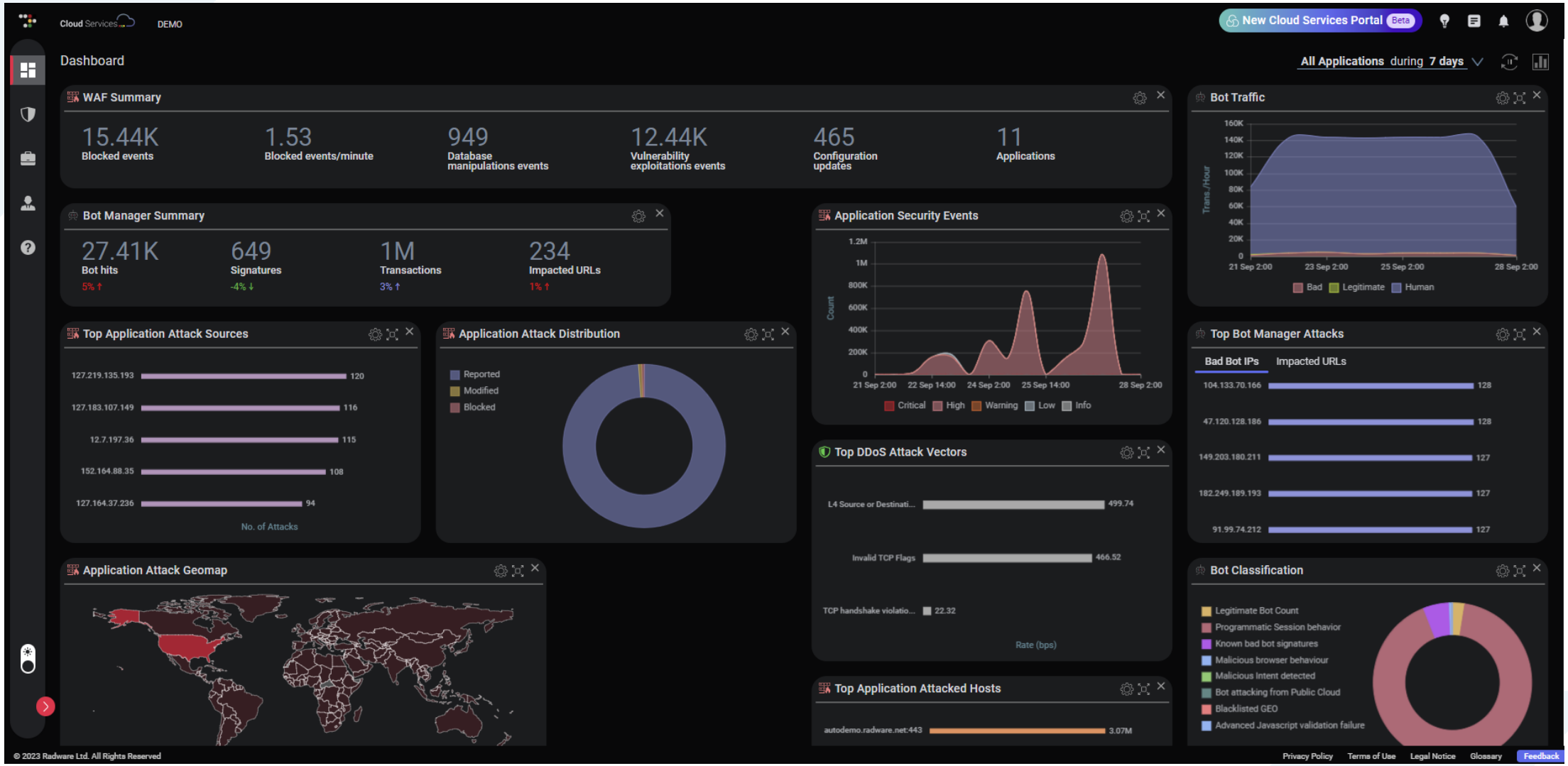
Shortage in Security Experts & Skills



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

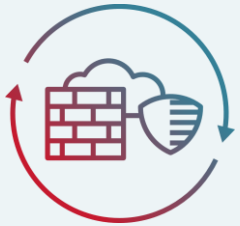
** Sources: 2022 (ISC)² Cybersecurity Workforce Study & Survey by Gaper ISSA/ESG*

Complete Visibility



The Radware Advantage

Fully-Managed Cloud Web Application & API Protection Services



Complete Coverage

WAF, Bot Manager, API Protection & DDoS Mitigation

Faster Deployment

Automatic policy generation and optimization engine for continuous security

Reduced Overhead

Customer Success Management by application security experts

Greater Visibility

Advanced analytics & self-service capabilities

The CISO Challenge

STATE OF THE ART

Protection from the most advanced threats

+

FRICTIONLESS

Security that enables business agility & lowers TCO

→ Organizations Shouldn’t Have to Choose

Thank You!

Q&A

radware