radware

VEM DRIVING DIGITAL

TECH TALKS

LA SICUREZZA NELL'ECOSISTEMA AI-DRIVEN: dalle API agli agenti autonomi

ALBERTO PERETTI

Presales Manager Italy & Spain, Radware



40 YEARS ANNIVERSARY

VALORI
ESPERIENZE
MERAVIGLIE



La Sicurezza nell'ecosistema AI driven: dalle API agli agenti autonomi

Alberto Peretti, Sales Engineer Team Leader Italy&Spain

VEM Annyversary – Forlì, 9 Ottobre 2026

Radware, leader in DDoS and WAF

INDUSTRY WIDE RECOGNITION

Quadrant Knowledge Solutions	IDC Analyze the Future	Gartner	FORRESTER
Bot Management Leader WAF Leader DDoS Protection Leader	DDoS MarketScape #1 Leader	#2 API Security ADC MQ Leader WAF MQ Visionary	DDoS Wave Leader

OEM

PARTNERS

CISCO

CHECK POINT

CERTIFICATIONS

Cloud Marketplace
AGENZIA PER LA CYBERSICUREZZA NAZIONALE

HIPAA COMPLIANCE
Health Insurance Portability and Accountability Act

PCI DSS COMPLIANT

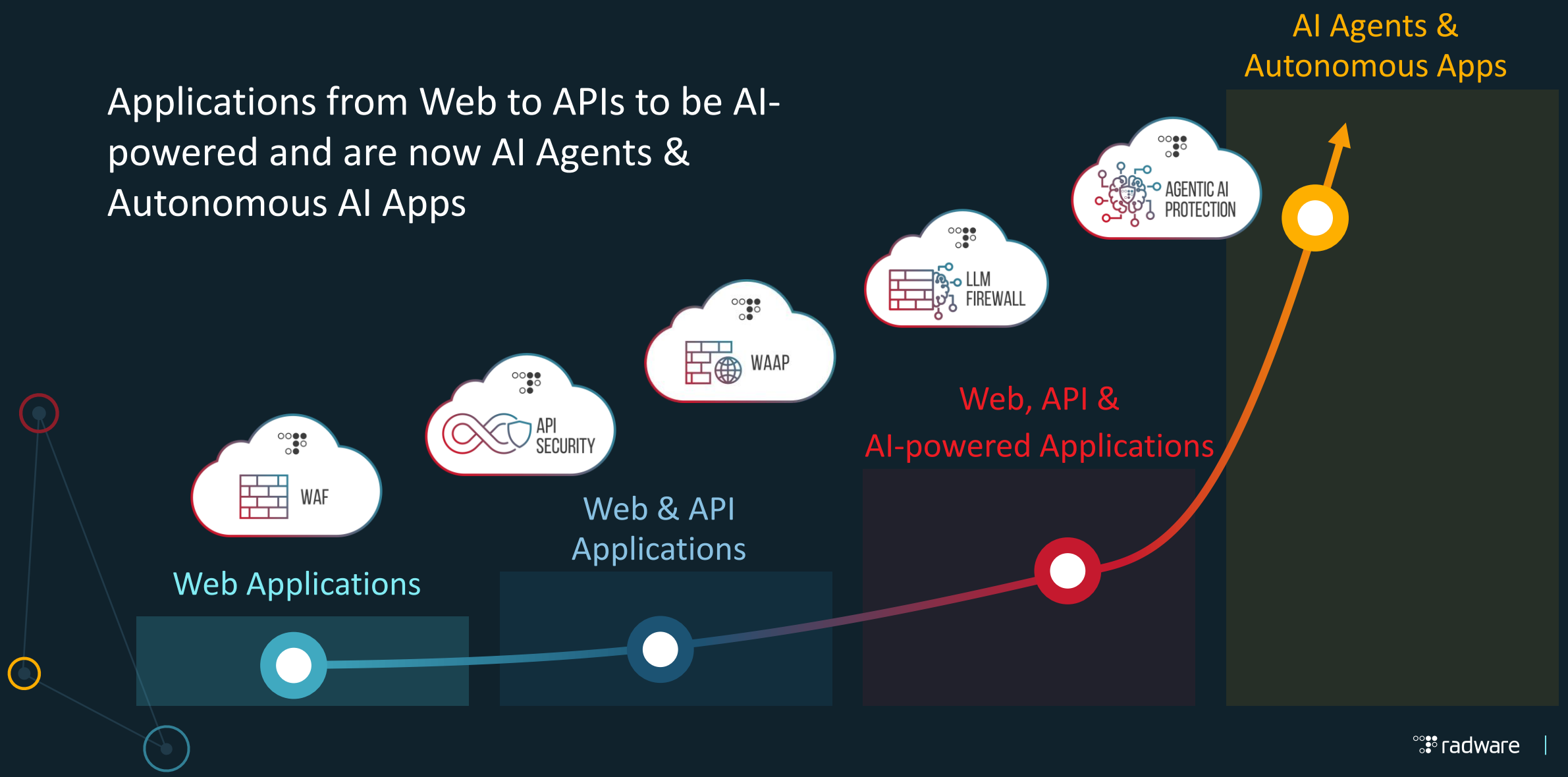
GDPR

SSAE 16

ISO

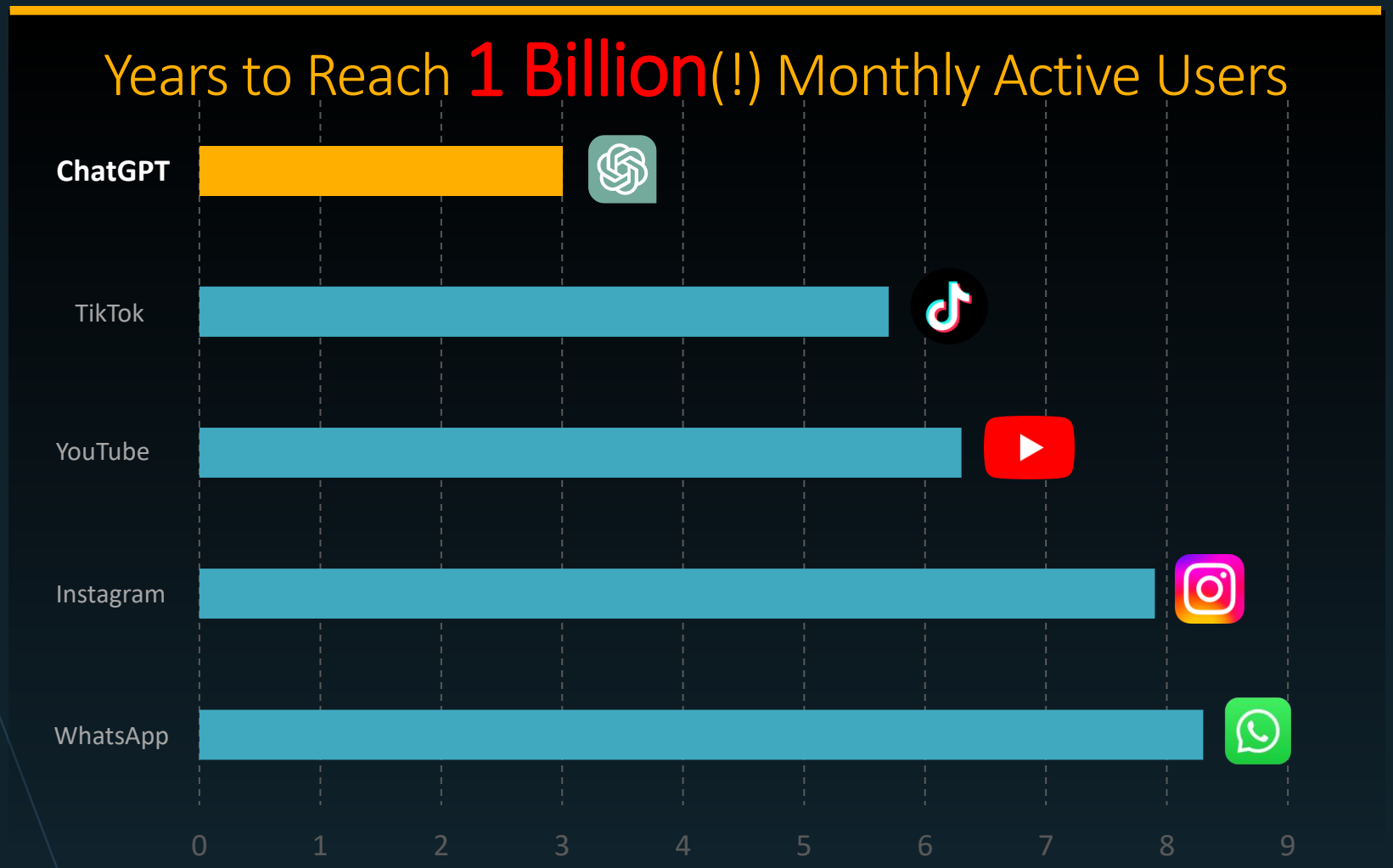
Applications on the Way to Becoming Fully Autonomous

Applications from Web to APIs to be AI-powered and are now AI Agents & Autonomous AI Apps




“By 2028, AI agent machine customers will replace 20% of the interactions at human-readable digital storefronts.”
Gartner

AI Adoption is Accelerating at Record Pace



ChatGPT Reaches **1 Billion** Monthly Active Users in **3 Years**!

640%

Y-o-Y growth in Claude AI's monthly active user base *(Jun'26)*

*Mobile App Users (iOS and Google Play)

AI Drine Fraud: il caso Fideuram

Cosa è successo

- Fideuram è stata vittima di una sofisticata frode basata su social engineering.
- Gli attaccanti hanno simulato comunicazioni provenienti da figure di alto livello dell'azienda.
- Sono stati utilizzati messaggi, telefonate e documentazione apparentemente credibili per richiedere trasferimenti urgenti di denaro.
- L'operazione ha portato all'autorizzazione di bonifici per decine di milioni di euro (si stimano circa 95 milioni di euro).

Come è stata utilizzata l'AI

- L'intelligenza artificiale è stata impiegata per clonare la voce di persone conosciute e fidate.
- Le tecniche di deepfake vocale hanno aumentato la credibilità delle comunicazioni fraudolente.
- L'AI ha reso più efficace l'attacco di impersonificazione e social engineering.

Qual è stata l'incidenza dell'AI

- L'AI non ha compromesso infrastrutture o sistemi bancari.
- L'elemento chiave è stato il social engineering supportato dall'AI.
- L'AI ha agito come fattore moltiplicatore della credibilità dell'attacco, consentendo ai criminali di superare controlli basati sul riconoscimento della voce e sull'identità percepita.

"L'aumento di deepfake e AI-driven social engineering evidenzia la necessità di estendere i principi di cybersecurity agli AI Agent, assicurandone visibilità, governance, autorizzazioni e monitoraggio."

The Agentic Eco-System is Extremely Complicated



Discovery

Visibility

Control & Governance

Attackers Already Have the Upper Hand





> *13% of organizations already reported breaches involving AI models in 2024.*
> ***By 2027, nearly 1/5 of cyberattacks will involve AI,***
> *which is pushing companies to invest in AI-focused security controls.*
>
> Gartner

Mythos: The Future of AI-Driven Cyber Attacks?

What is Claude Mythos?

- A **restricted AI model** publicly disclosed by Anthropic
- Demonstrates how AI can **automatically find vulnerabilities**
- Can **generate & chain exploits** with little human effort

What is the Risk?

- **Time-to-exploit is collapsing** (from weeks to hours)
- Advanced attacks **no longer require elite skills**
- **Patch cycles can't keep up** with AI-driven discovery
- Web, API, and cloud attack surfaces are **continuously exposed**

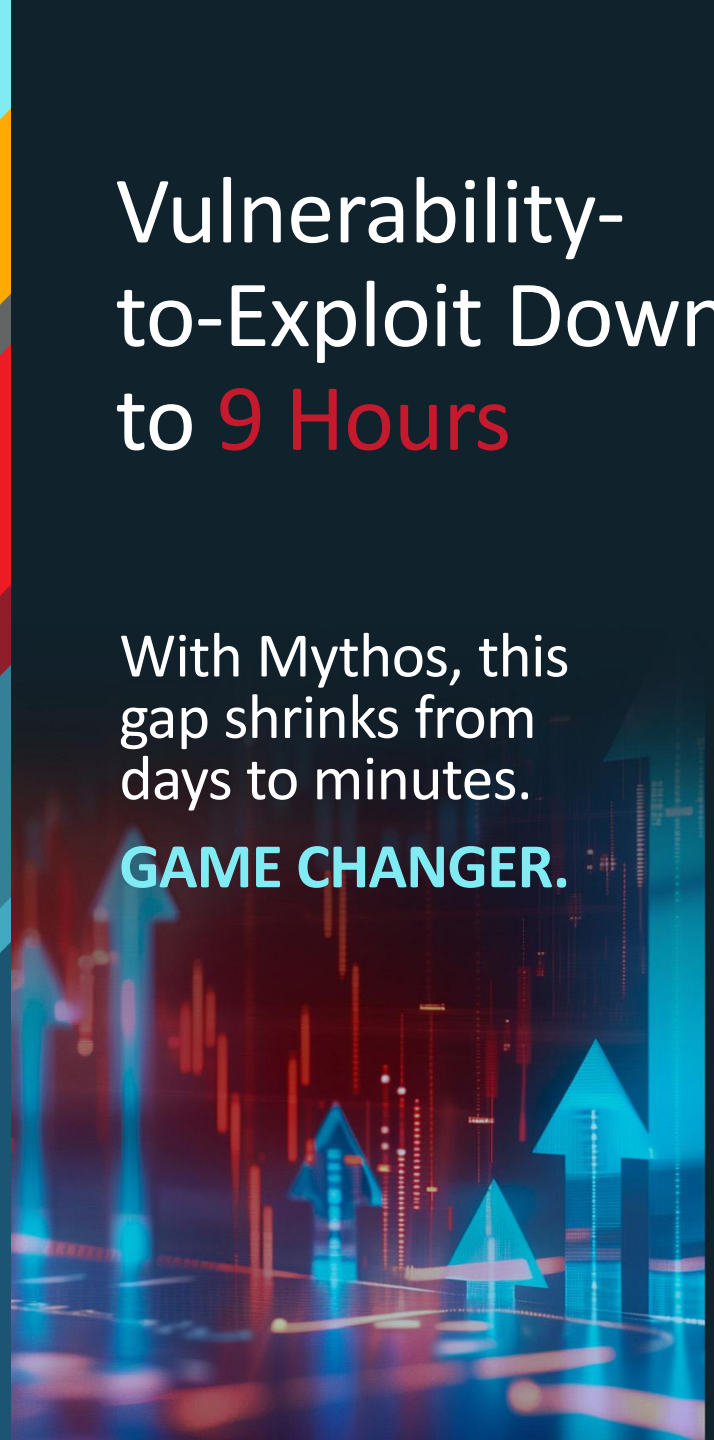


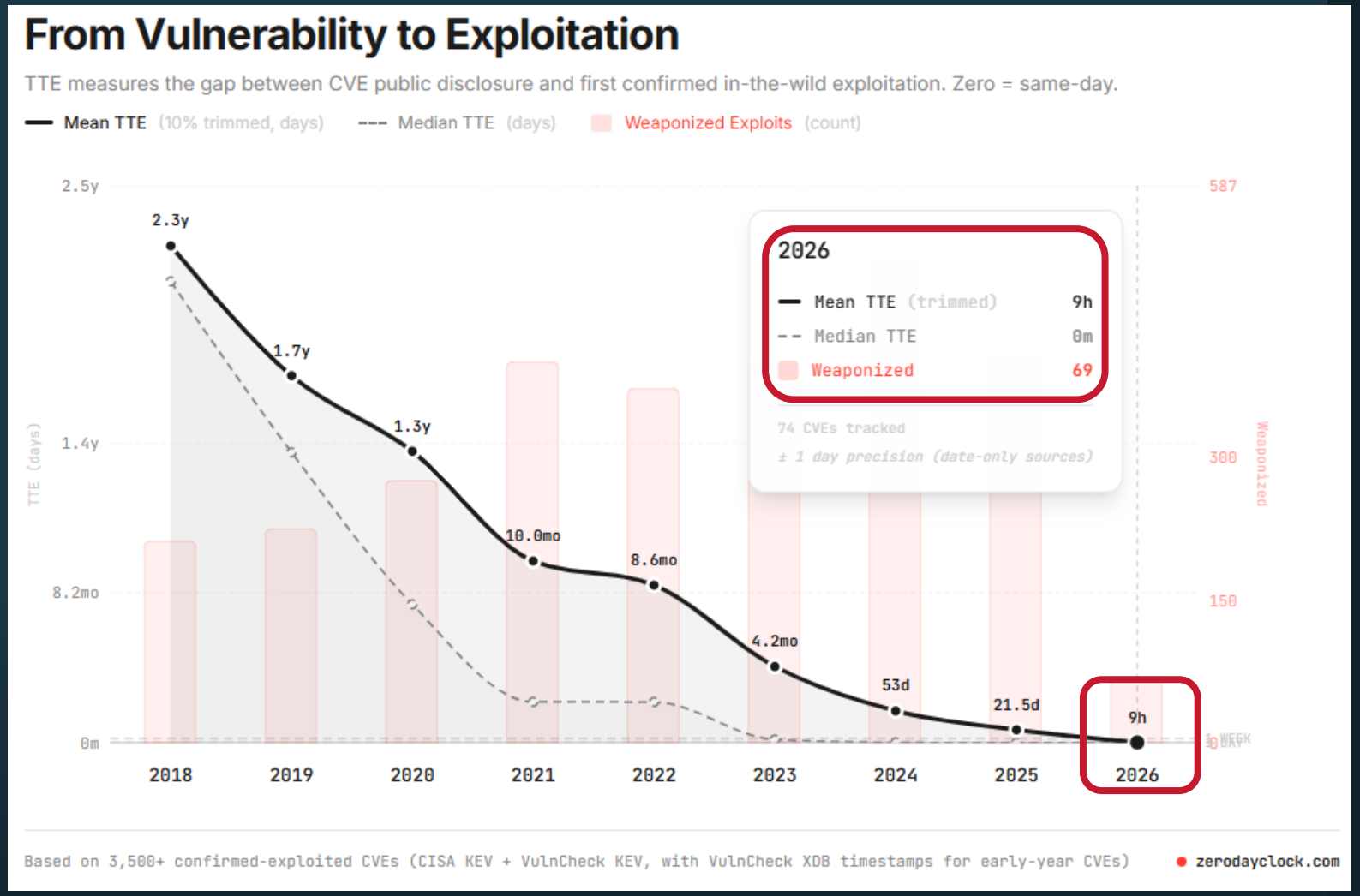
Attackers are evolving. Defenses must as well.

Vulnerability-to-Exploit Down to 9 Hours

With Mythos, this gap shrinks from days to minutes.

GAME CHANGER.





Source: https://zerodayclock.com/, June 2026

The Agent Economy Tradeoff

Organizations **Risk Massive Losses** Without Agent-Ready Cybersecurity

Block All AI Agents

- Missed revenue from legitimate automated transactions
- Lose customers to competitors who support AI agent interactions
- Damaged brand reputation

Allow All AI Agents

- No visibility into agent access and actions
- Cannot respond to malicious agents
- Resource abuse and infrastructure costs

Need a trust-based framework that ensures security and business value

What is Needed to Stay Ahead?

Protect the Web & API Economy

Prepare for the Agent Economy

Powered by AI

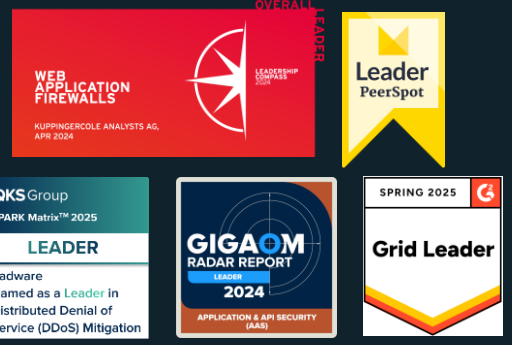
Fight AI with AI-powered defense to stay ahead

Protect the AI

Protect LLMs & AI Agents from misuse and abuse

Serve the AI

Enable secure, legitimate Agent traffic



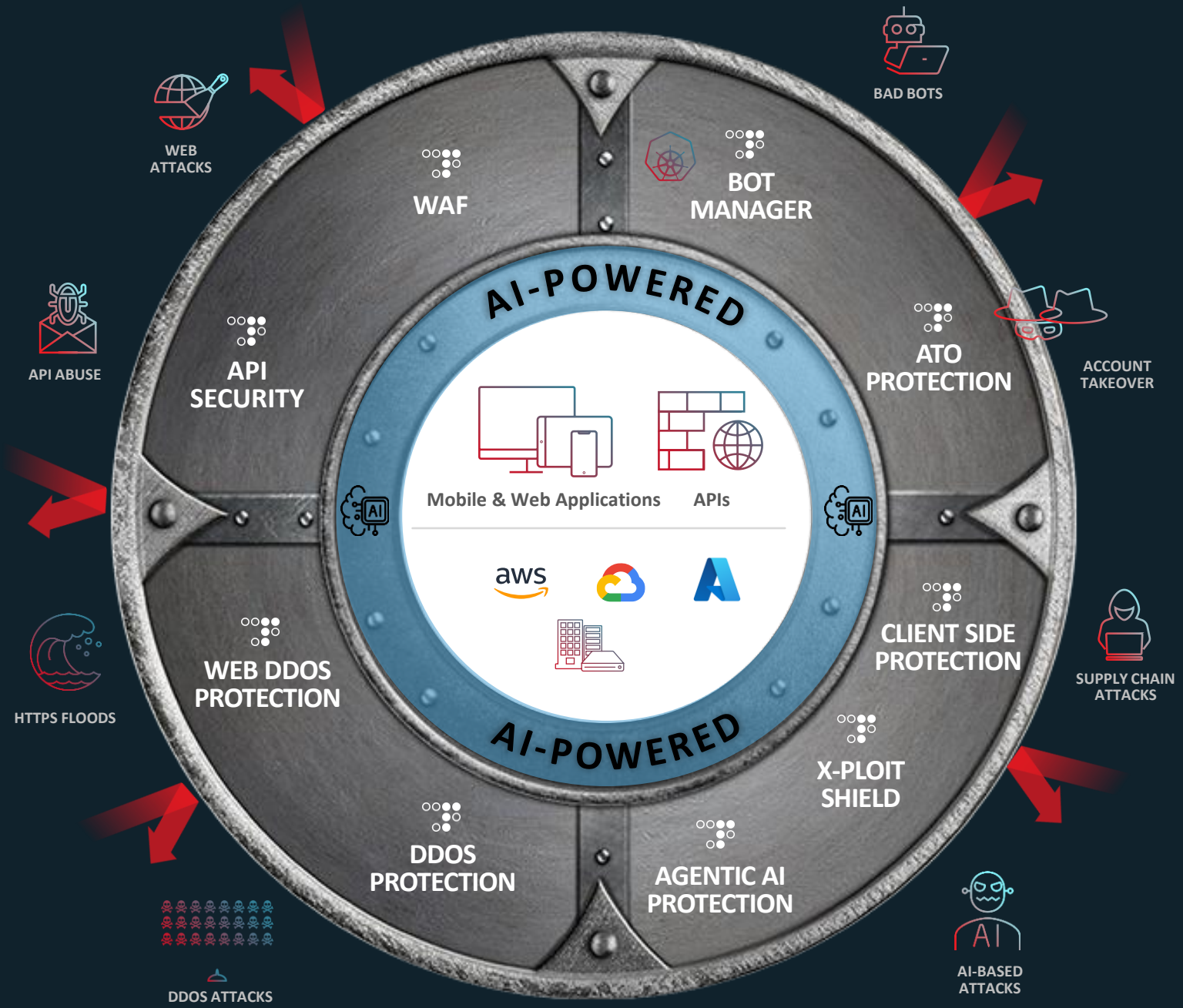
Radware. Your Apps. Your APIs. Your AI. Secured

Complete Protection by Radware's Cloud Security Platform

Gartner Peer Insights™

*Truly **exceptional protection** for web apps & APIs*

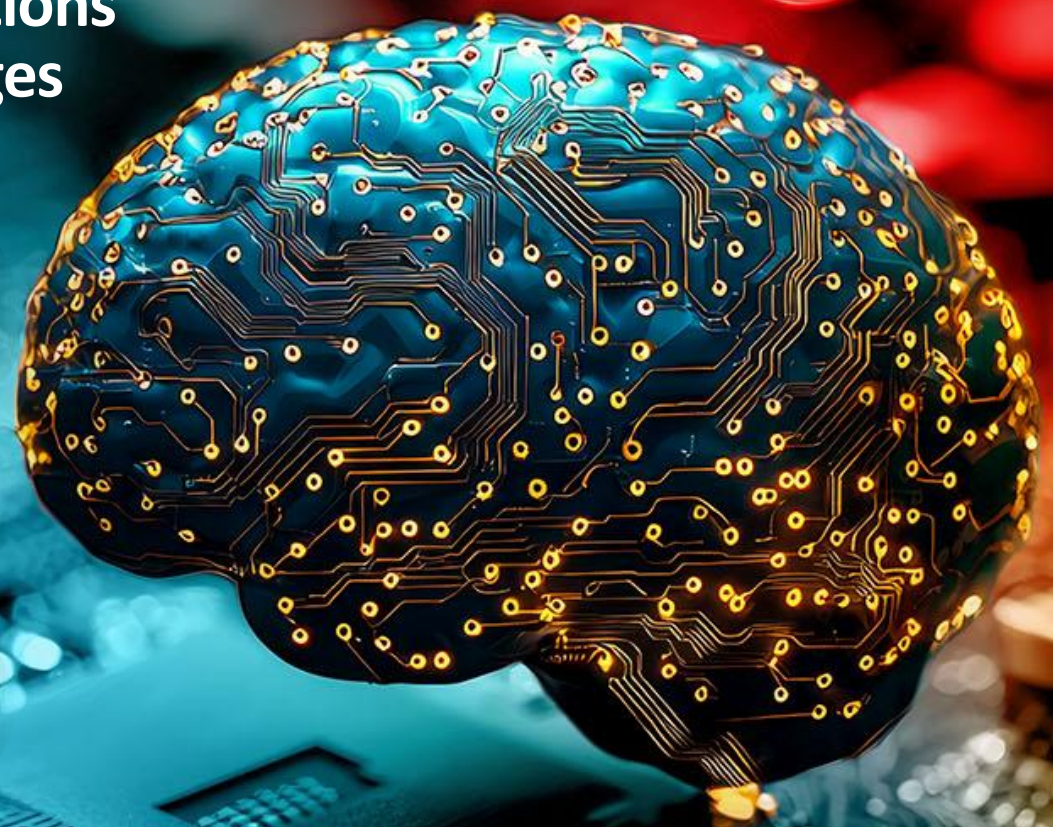
Radware Customer, Telecommunications

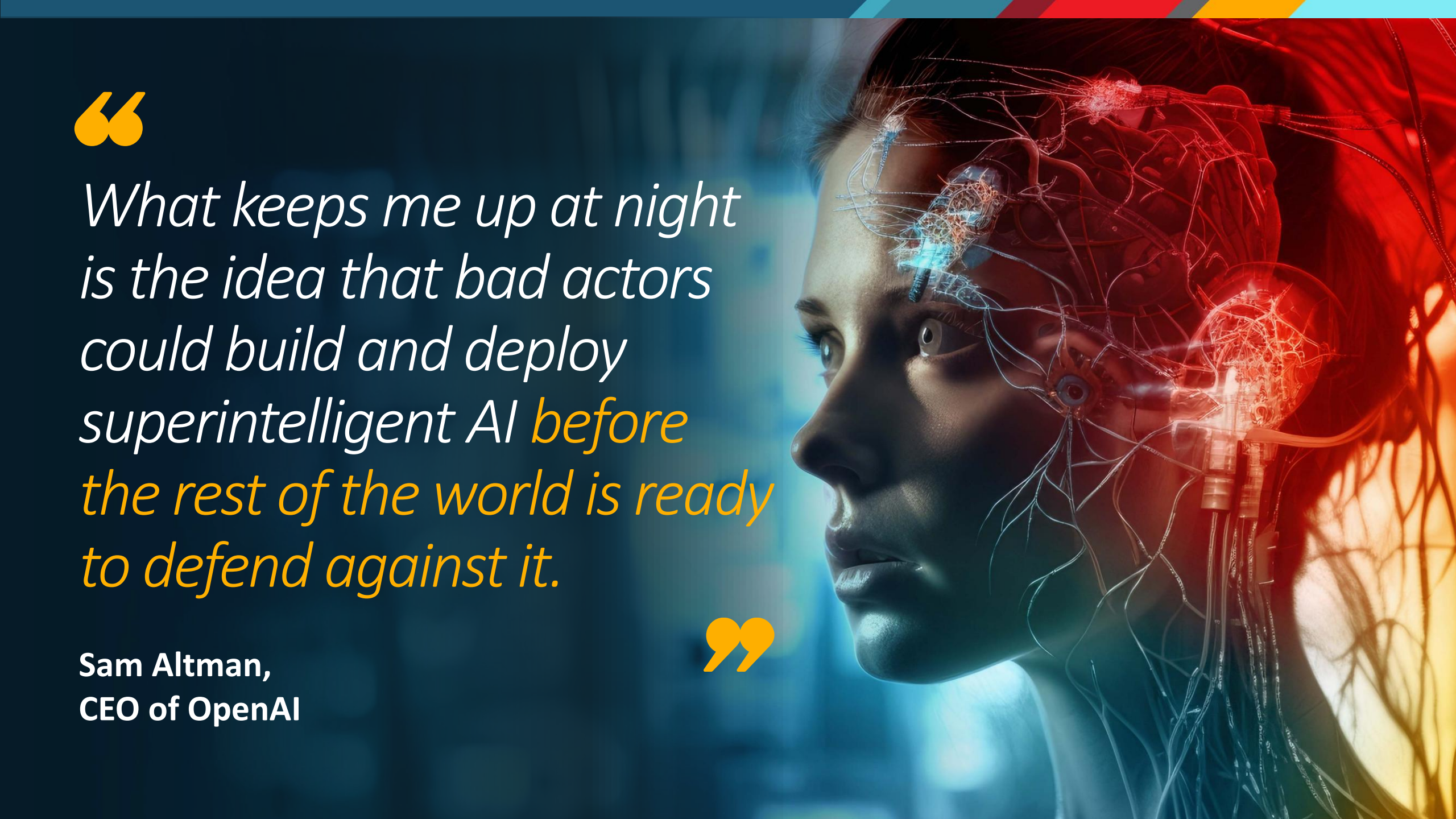


Radware’s Agentic AI Protection

Purposely designed and built to help organizations overcome the new agentic AI security challenges

1. Complete visibility into your agent economy – discover your agent landscape
2. Sophisticated behavioral algorithms to protect against agentic AI security risks
3. Deep integration with organization’s agents and tools
4. Comprehensive analytics and posture managements




“
What keeps me up at night is the idea that bad actors could build and deploy superintelligent AI before the rest of the world is ready to defend against it.
”
Sam Altman,
CEO of OpenAI


THANK YOU!
radware