radware

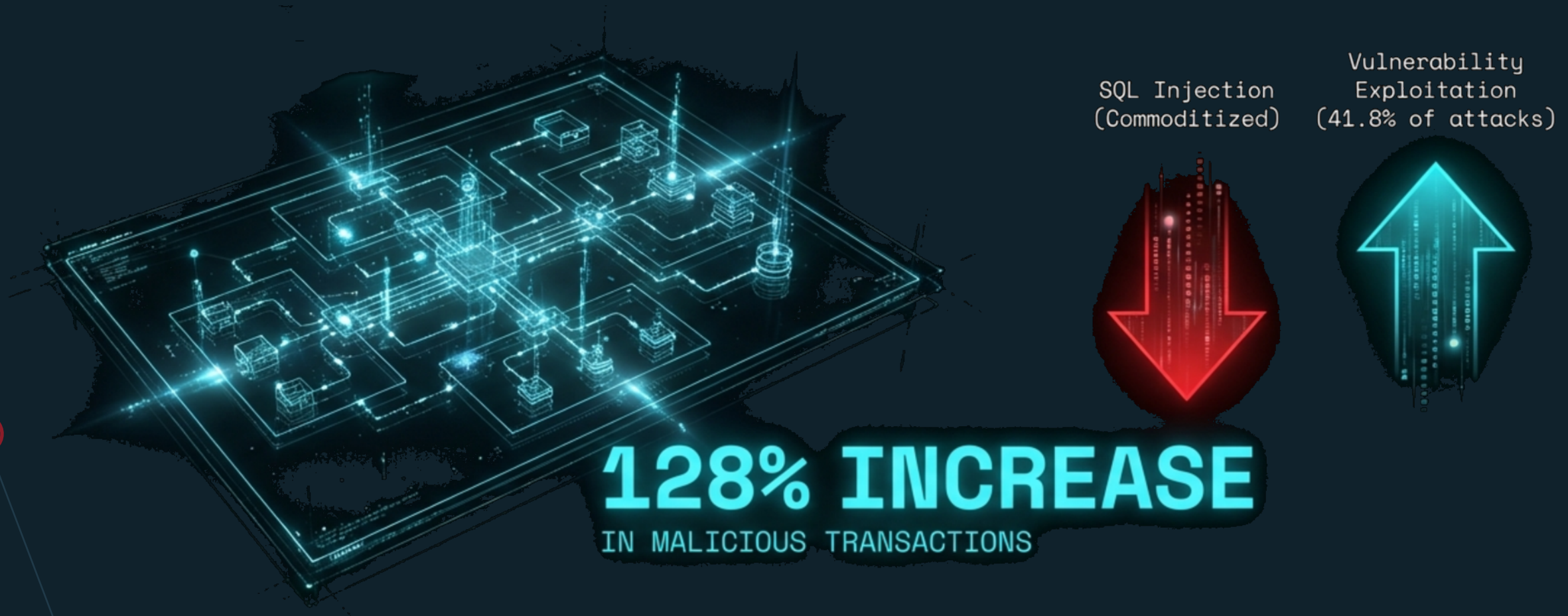
HOW NEW MODERN (AI-BASED) ATTACKS ARE MITIGATED TODAY

Marco Baban

Sales Engineer CEE

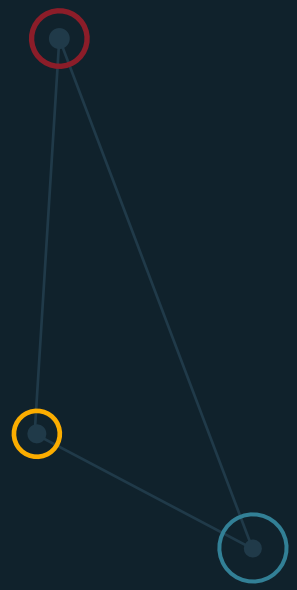
Market Evolution: Solutions Need to Adapt

THE APPLICATION LAYER: THE NEW CENTER OF GRAVITY



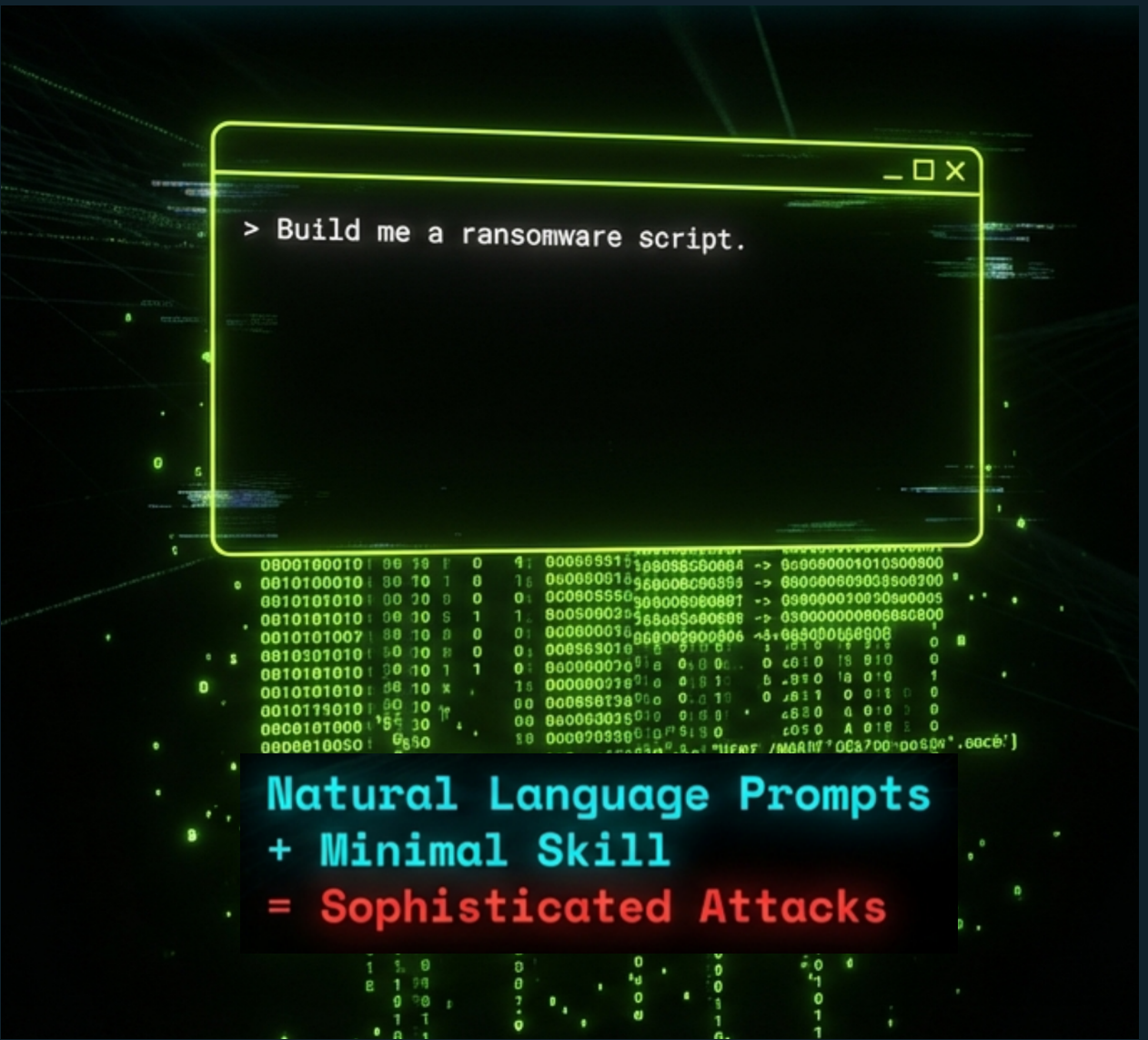
Attackers are abandoning easy vectors for sophisticated strikes targeting business logic and APIs

WEB APPLICATION AND API ATTACK CATEGORIES

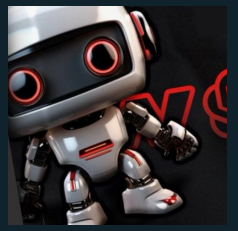


DEMOCRATIZATION OF ATTACK TOOLS

VIBE HACKING



- Closed Models
  - OpenAI GPT, Claude Opus, Google Gemini
  - Using jailbreaks
- Open Models
  - Llama, Mistral, DeepSeek
  - Custom Training Underground Datasets
  - Uncensored, free of guardrails
  - Privacy, unlike online models



WormGPT
(GPT-J 6B)

FraudGPT

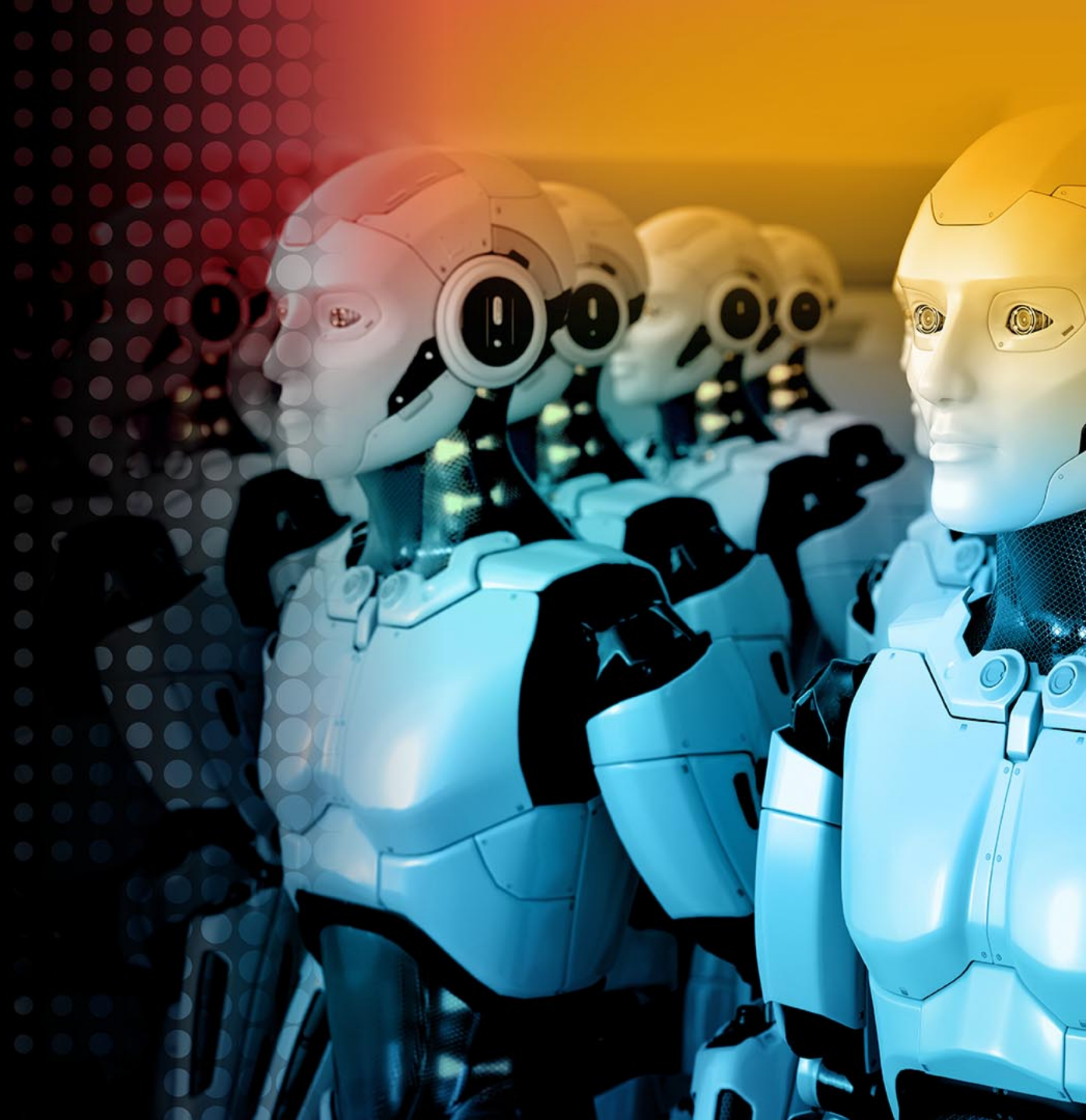
ATTACK AUTOMATION & ORCHESTRATION

XANTHOROX AI: UNCENSORED, PRIVATE & AGENTIC ATTACK SUITE AS A SERVICE

- Privacy: self-hosted GPU servers, no data shared with OpenAI, Google, ...
- Uncensored: no restrictions or guardrails
- Different models for different use cases: coding, vision, web search (CVE, exploits)
- XenCode: coding agent for VS Code
- HEXENCORE: MCP server integration with 200+ offensive security and OSINT tools

radware

Radware's End-to-End API Security



Threat Landscape

Web & API Hybrid Apps

80% *of Applications*

API Attacks

1

Embedded Attacks

- SQL Injections
- Authentication bypass
- Exploiting outdated libraries
- Exploiting insecure endpoints

2

Business Logic Attacks

- API Call Manipulations to alter pricing
- Bypassing rate limits to scrape data
- Exploiting order workflows for fraud

3

API DDoS Attacks

- HTTP floods of API-based apps, Mobile Apps and Web-API hybrid apps

McDonalds / Paradox.AI API Attack

1

Admin Account Access

- UName/PWD 123456:123456
- Admin Access to Test Account
- No MFA – Admin Level Foothold
- McHire Hiring System Exploited

2

Broken Object Level AUTH API Attack

- API Call Manipulations like GET /api/v1/candidate/<userID>
- API did NOT check/ enforce user AUTH or access control
- Sensitive Applicant data exposed

3

Reputation Damage

- 64 Million Applicant's Data Exposed
- No 3rd Party Vendor Testing & Validation
- Underscores need for Runtime Posture Mgm't & Runtime BLA Protection

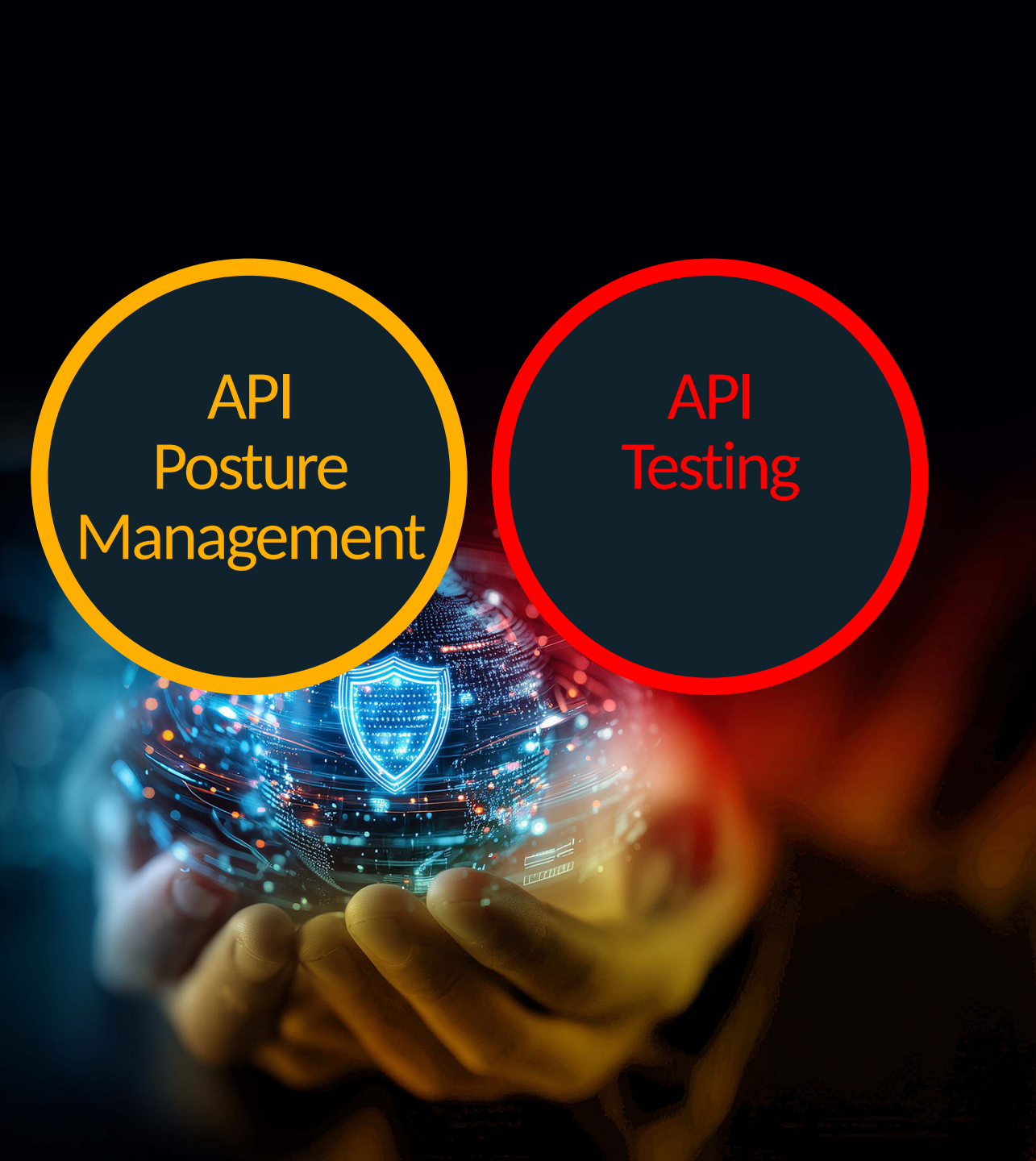
Radware API Security Service

API Discovery & Management

API Runtime Protection

API Posture Management

API Testing



API Management & Analytics

Comprehensive view of API Security, helping teams quickly identify trends, anomalies, and application issues.

- Automated API Discovery (incl. auto schema file generation)
- API catalog metrics
- Business Logic Sequence Explorer
- Performance metrics
- Usage metrics

API Runtime Protection

AUTHENTICATION

- Token Authz Control
- Client Certificate

API ABUSE MITIGATION

- Quota Limit (REST)
- Query Limit (GraphQL)
- Global Rate Limit

NEGATIVE SECURITY

- Malicious Payload Protection
- Data Leakage Prevention
- API Bot Protection

POSITIVE SECURITY

- GraphQL & REST
- **Full** Schema Enforcement
  Documented & Undocumented
- **Business Logic Protection**

VOLUMETRIC ATTACK

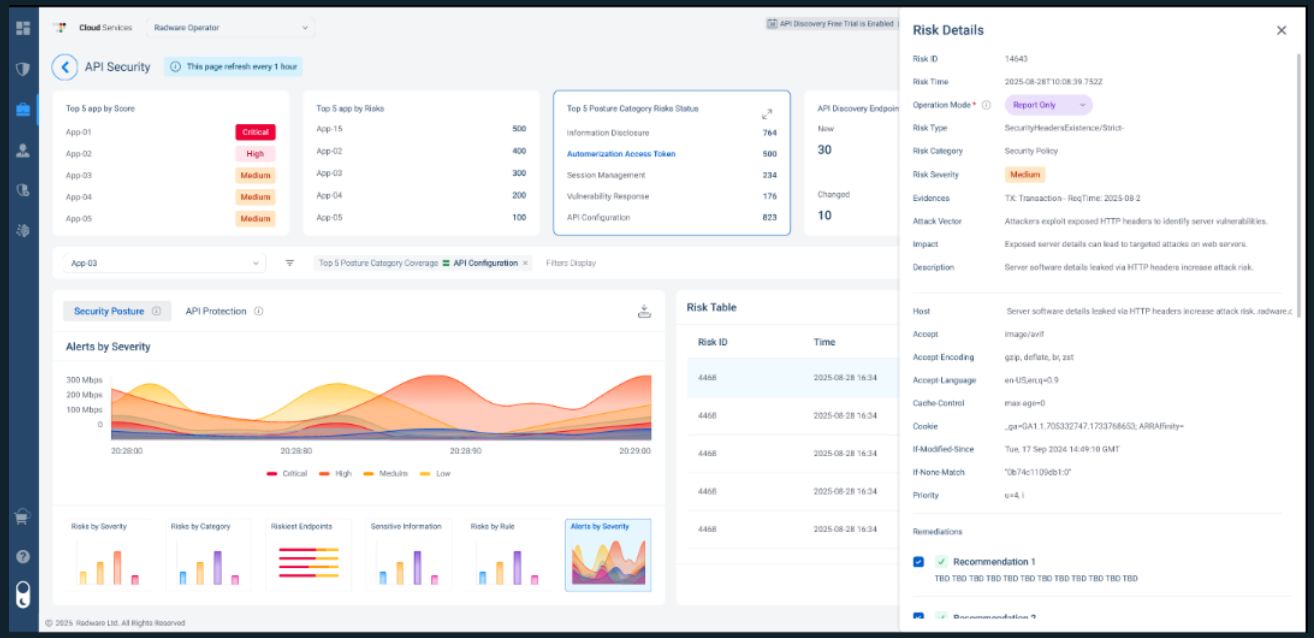
- API L7 DDoS Protection

SECURITY ADD-ONS

- LLM Firewall
- EAAF
- Threat Intelligence

Runtime Posture Management

- **Continuous Risk** assessment
- **Detect** vulnerabilities, misconfigurations and security policy inconsistencies
- **Monitor Production** traffic of real users to uncover security holes missed earlier in the pipeline
- **Prioritize & Remediate** - Dynamic prioritization based on real-time threats and attackers' intent



OWASP API Security Top 10

Business Logic Protection

API1:2023

Broken Object Level Authorization

Improper access controls allowing users to view or modify other users' data through API endpoints.

Example: Changing user ID in API request to access another user's profile information.

Business Logic Protection

API3:2023

Broken Object Property Level Authorization

Exposure of sensitive object properties through API responses without proper authorization checks.

Example: User role field exposed in API response allowing unauthorized modification.

Business Logic Protection

API5:2023

Broken Function Level Authorization

Users able to access API functions beyond their authorized permission level.

Example: Regular user accessing admin-only API endpoints.

Token Authz Control

ATO Protection

API2:2023

Broken Authentication

Flaws in authentication mechanisms that allow unauthorized access to API endpoints.

Example: Weak token validation allowing expired tokens to remain valid.

Quota Limit

Strong Schema Enforcmt.

API4:2023

Unrestricted Resource Consumption

Lack of proper rate limiting or resource quotas leading to potential DoS attacks.

Example: Unlimited API requests causing server overload.

OWASP API Security Top 10

Token Authz Control

Business Logic Protection

API6:2023

Unrestricted Access to Sensitive Business Flows

Critical business processes exposed without proper controls or rate limiting.

Example: Automated bulk purchases bypassing inventory controls.

Strong Schema Enforcmt.

Signature based Protection

API7:2023

Server Side Request Forgery

API endpoints vulnerable to malicious requests targeting internal systems.

Example: API fetching data from user-provided URLs without validation.

Strong Schema Enforcmt.

Signature based Protection

API8:2023

Security Misconfiguration

Improper security settings in API infrastructure, frameworks, or dependencies.

Example: Exposed error messages revealing sensitive system information.

API Discovery

Business Logic Protection

API9:2023

Improper Inventory Management

Lack of proper documentation and monitoring of API endpoints and versions.

Example: Deprecated API versions remaining active with known vulnerabilities.

Strong Schema Enforcmt.

Signature based Protection

API10:2023

Unsafe Consumption of APIs

Insufficient validation of data received from external APIs leading to security issues.

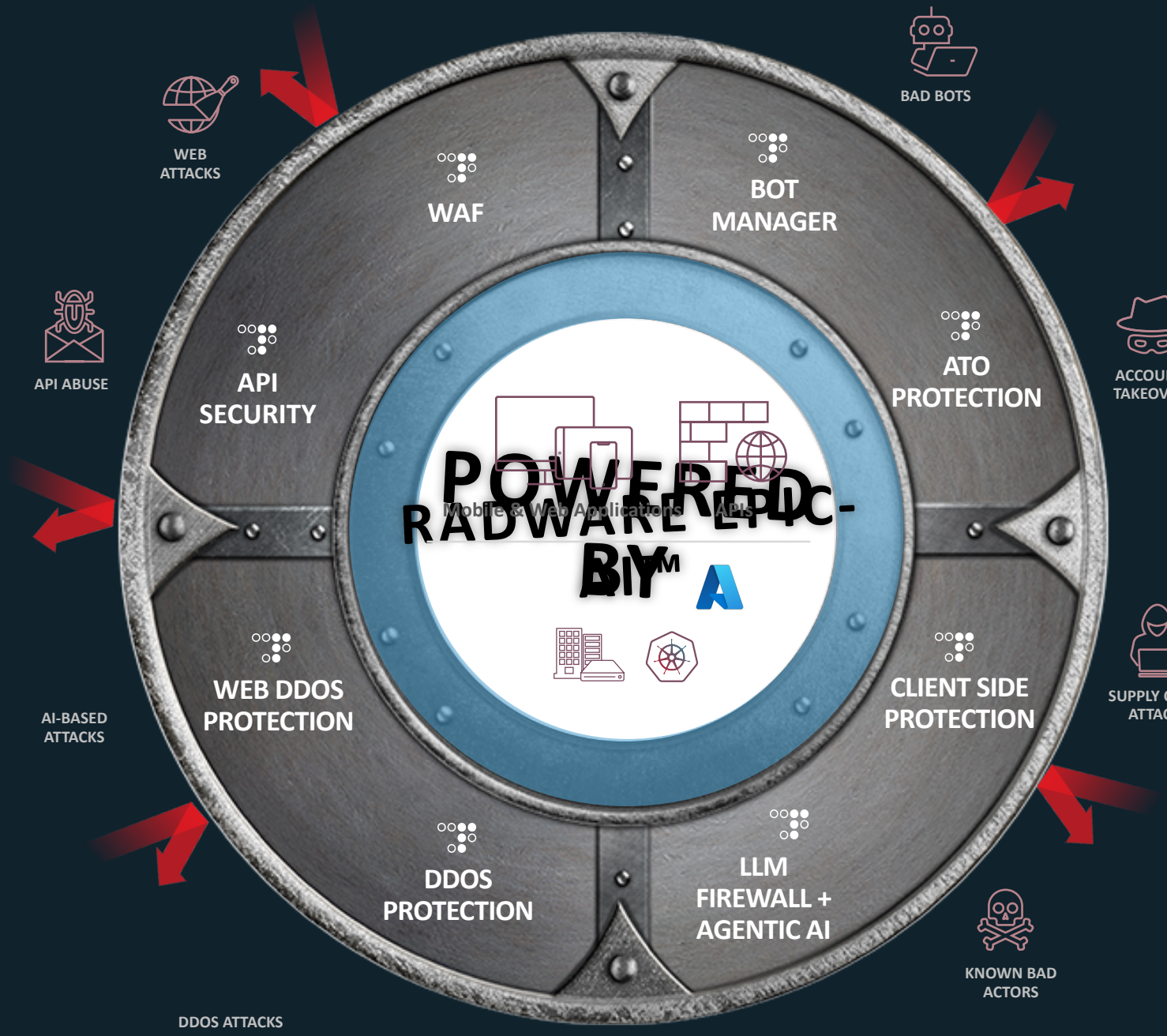
Example: Blindly trusting and processing data from third-party APIs.

Complete Protection by Radware's Security Platform

Gartner Peer Insights™

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

Radware Customer, Telecommunications

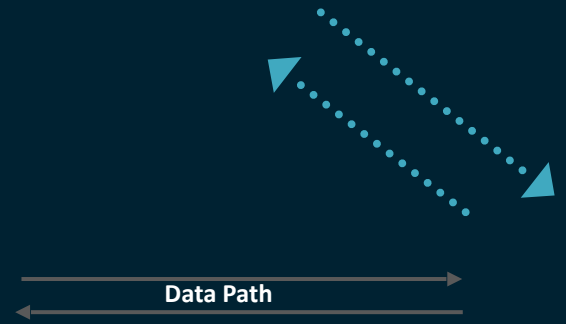


Consistent Application Protection for Multi-Clouds

In-line

END USER

API-based Out-of-Path



END USER

Thank you!

radware