radware

CYBER RESILIENCE: *LEARNING FROM THE FRONT LINES THROUGH DIGITAL ATTACK STORIES*

Eran Danino

Regional Sales Manager – Sales Expert, CEE

APRIL 2026

radware

Agenda

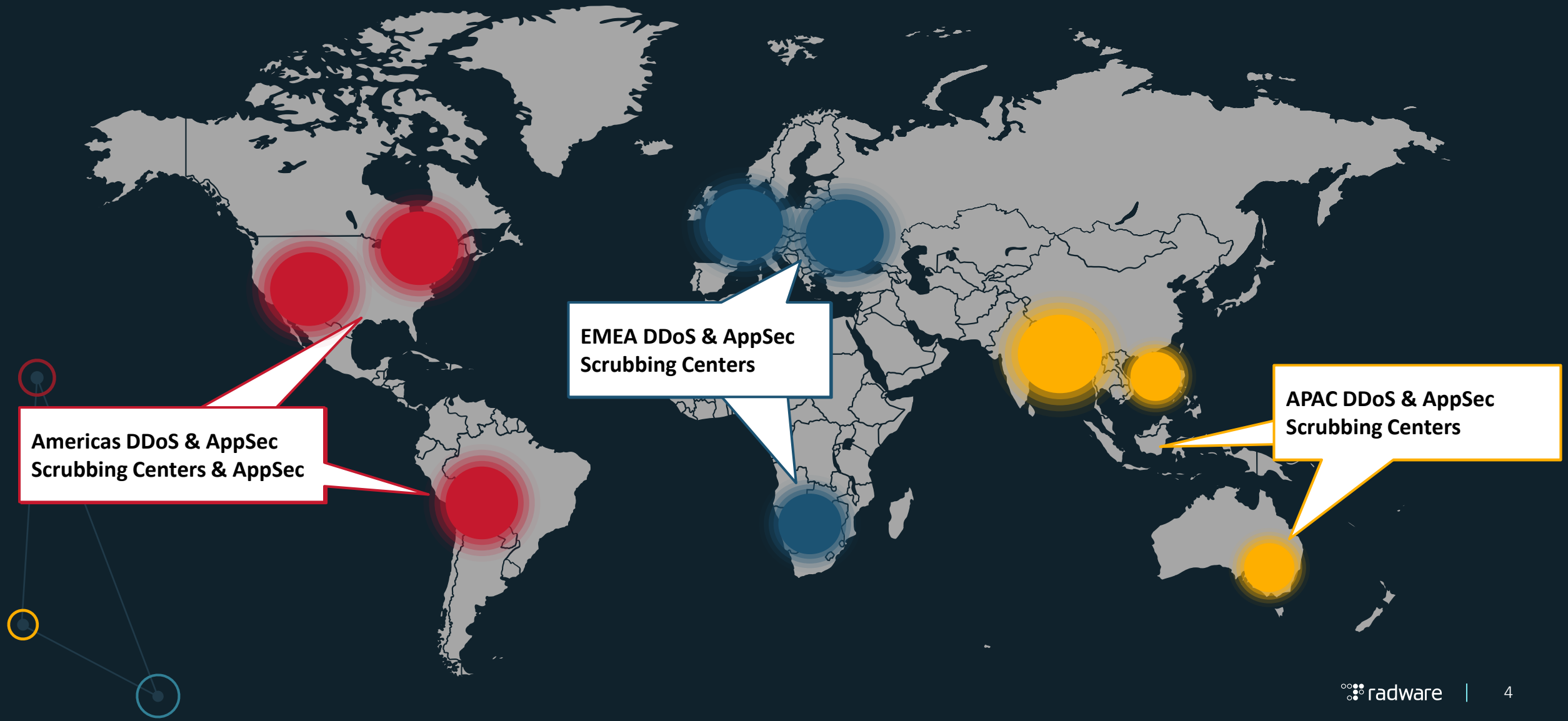
- Top Cyber Attacks
- Top Attacked Verticals
- Top Hacker Groups
- Real Attack Stories

radware

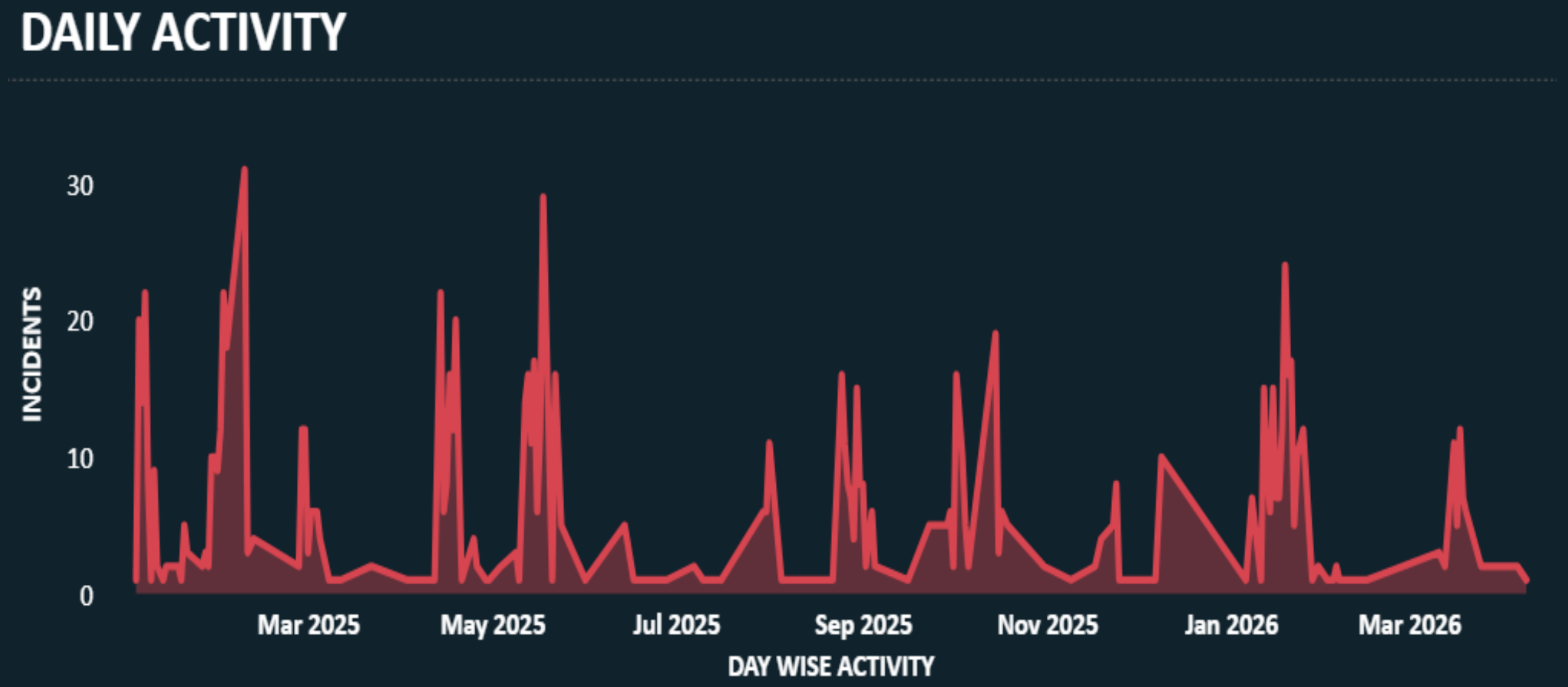
Agenda

- Top Cyber Attacks
- Top Attacked Verticals
- Top Hacker Groups
- Real Attack Stories

POINT OF SOURCES



CEE organizations are under targets of large-scale DDoS attacks



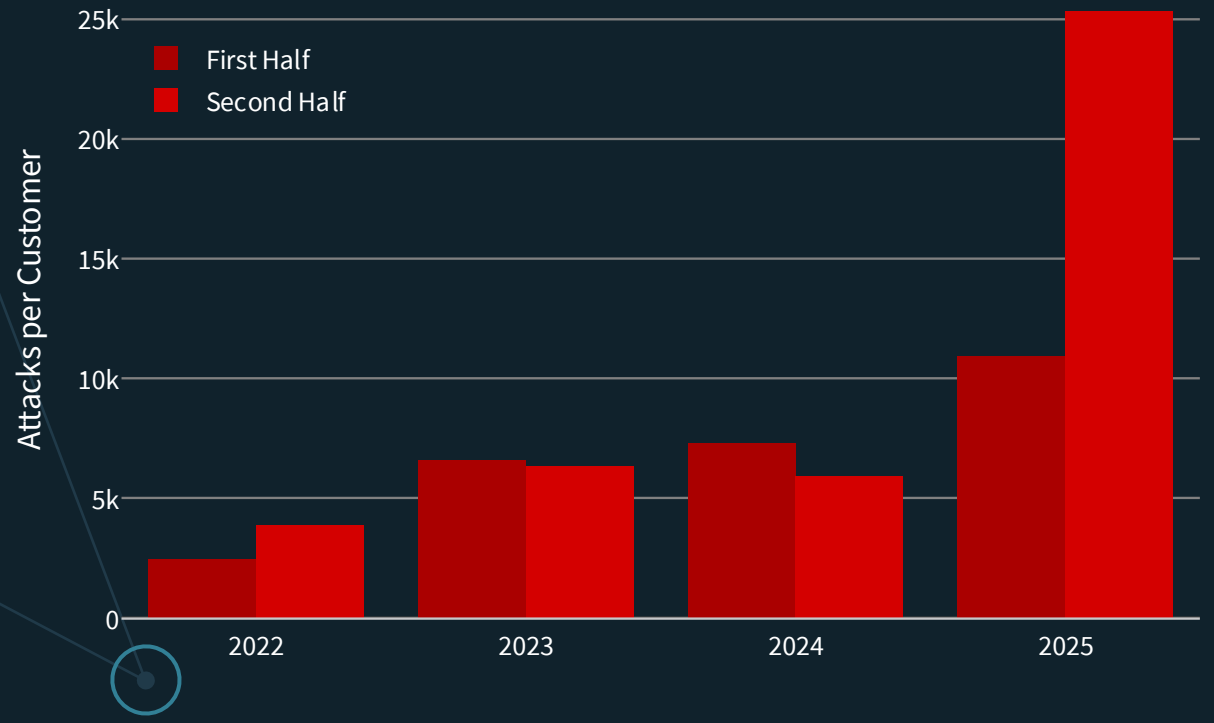
>1,000 large DDoS attacks on CEE organizations in the last year

BRUTE FORCE RESURGENCE

+168.2% 2025/2024

Increase in Network DDoS Attacks

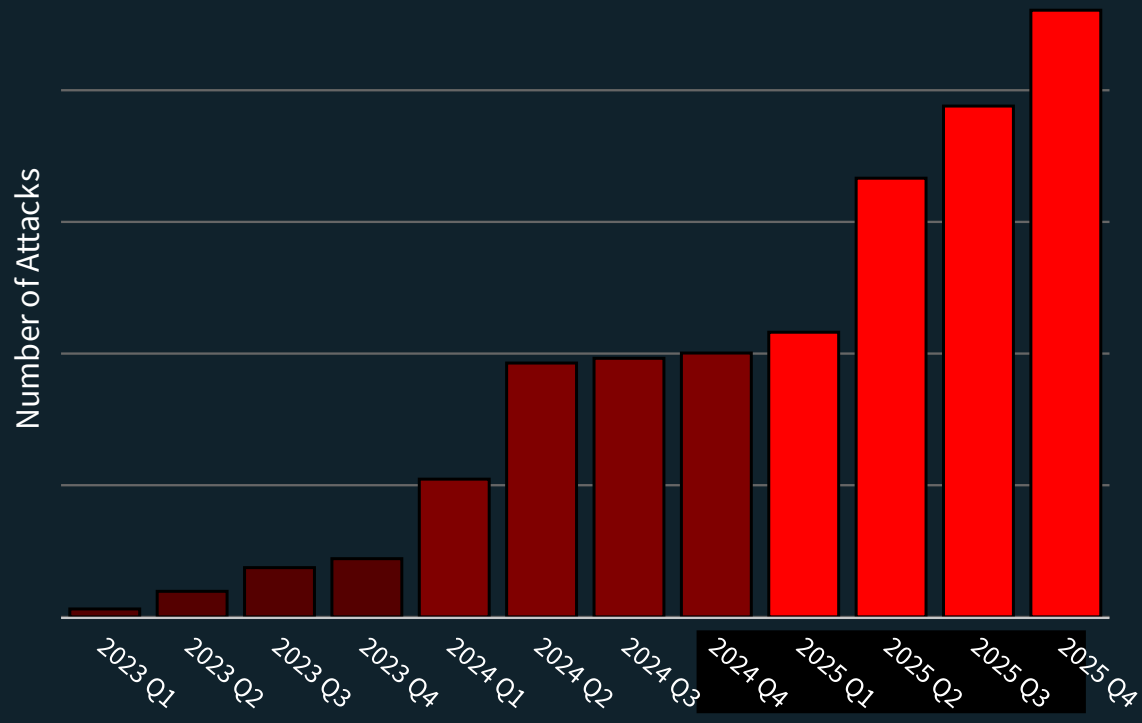
- Global Record: 29.7 Tbps (Aisuru-Kimwolf Botnet)
- Technique: Carpet-bombing & UDP Floods



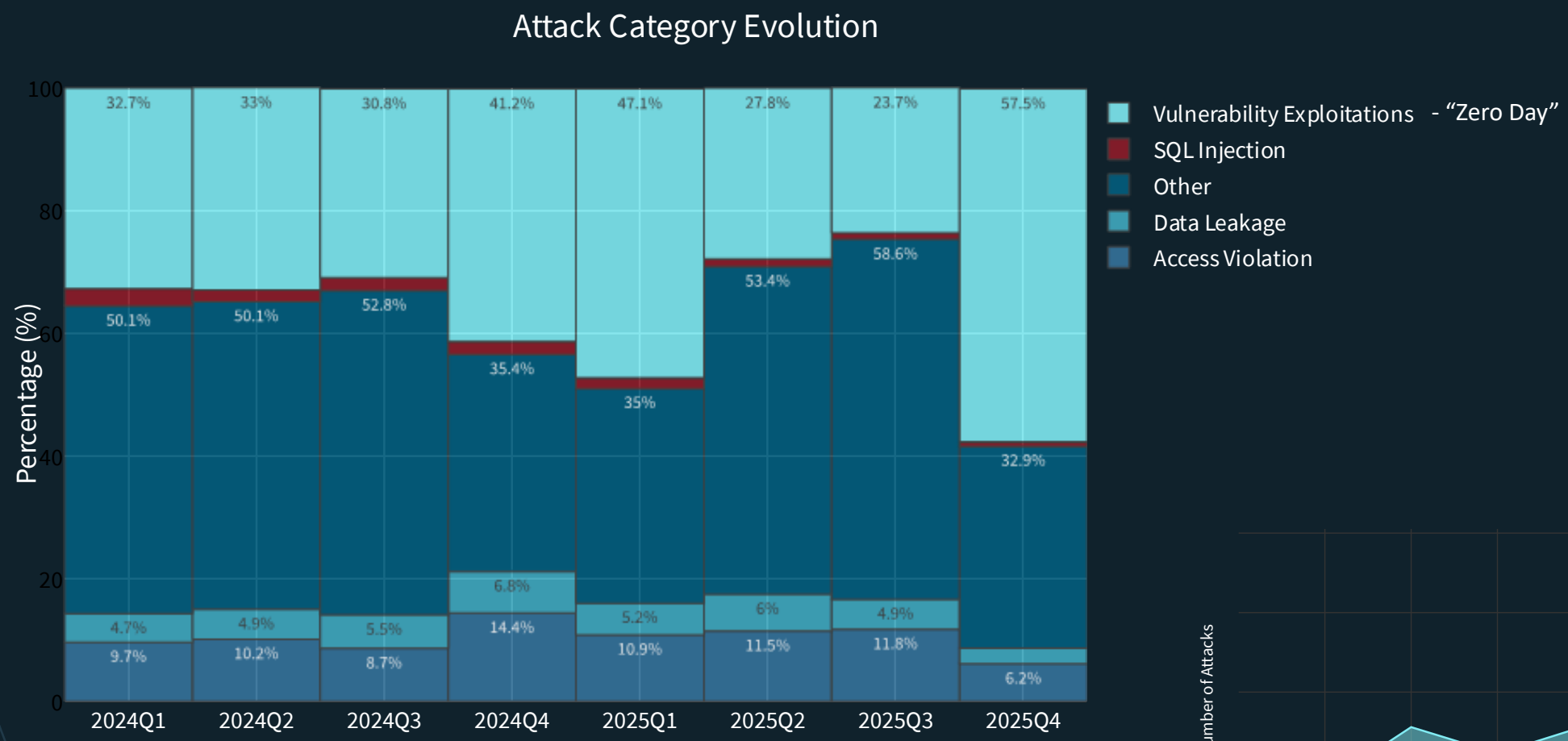
+101.4% 2025/2024

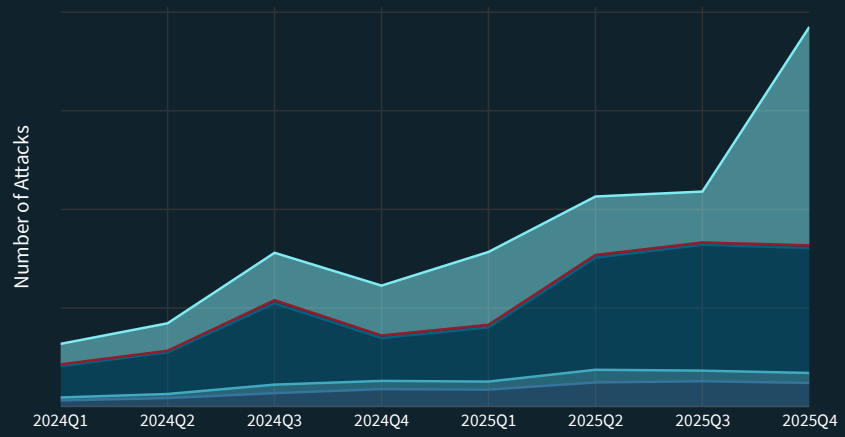
Increase in Web DDoS Attacks

- Global Record: 398M RPS (HTTP/2 Reset)
- Technique: Backend Resources & APIs

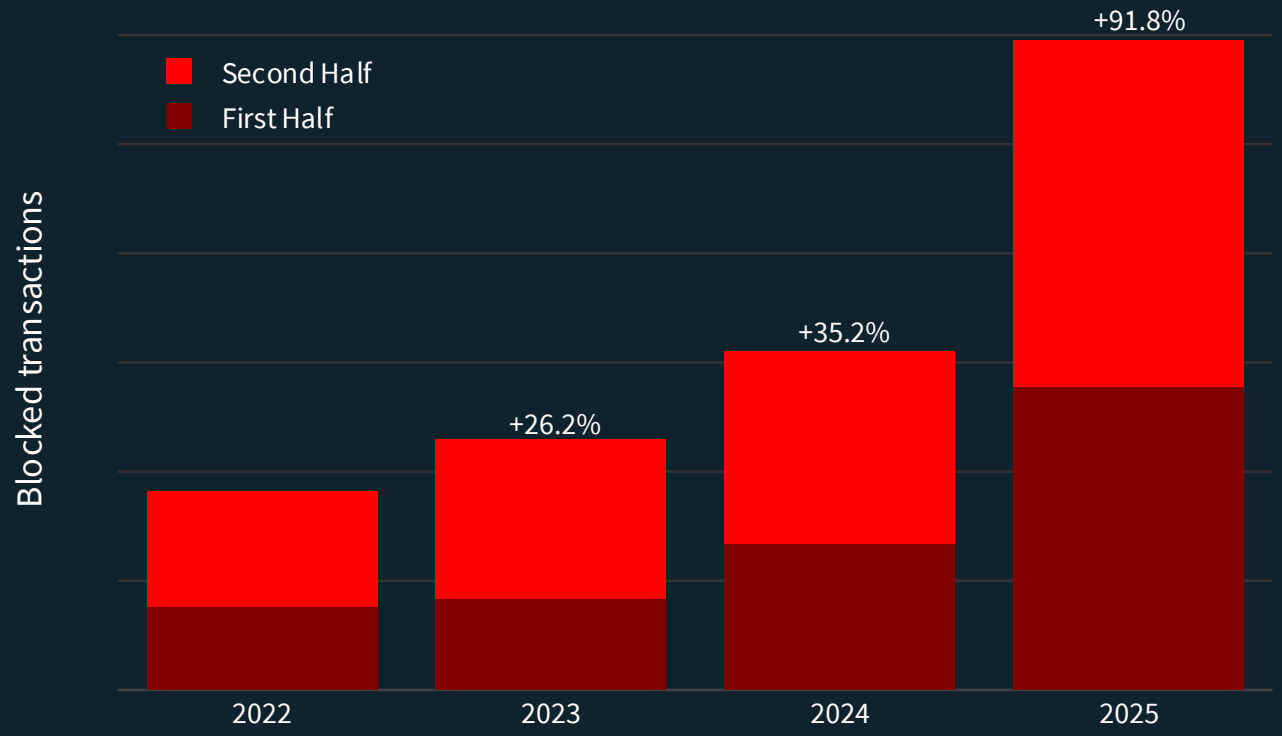


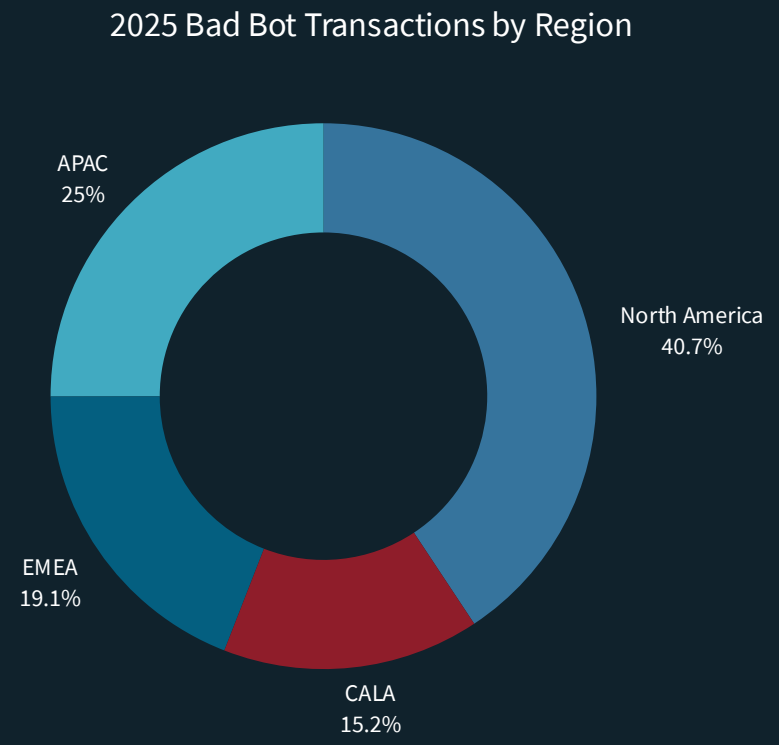
WEB APPLICATION AND API ATTACK CATEGORIES





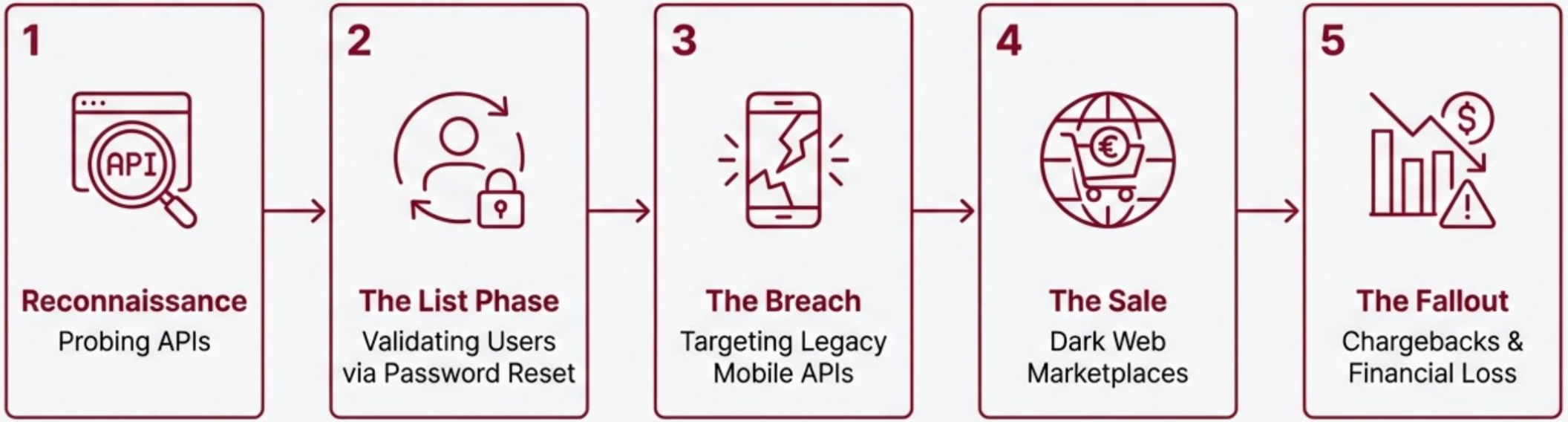
BAD AI BOT TRANSACTIONS





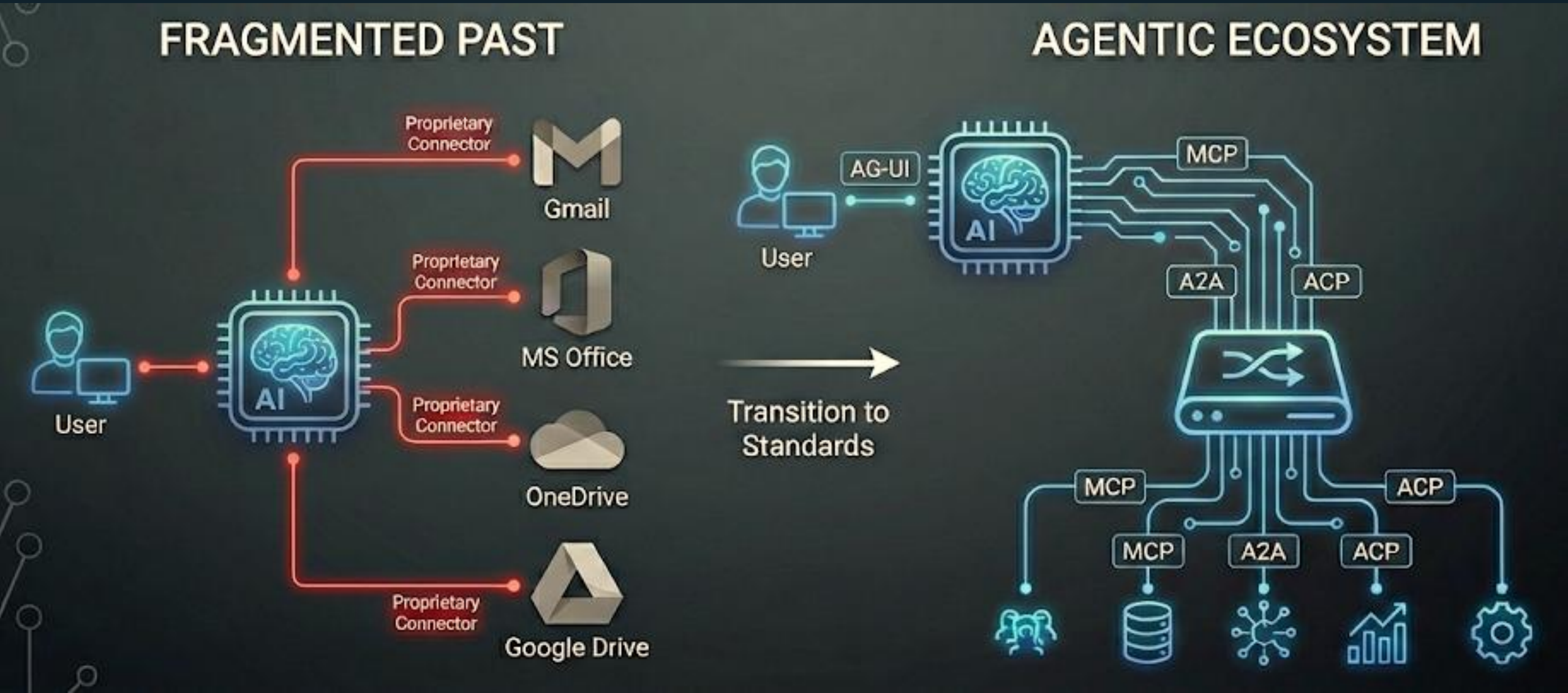
THE CASHOUT ATTACK KILL CHAIN

We are fighting ecosystems, not scripts. (**+91.8%** Growth in Bad Bots)



THE AGENTIC ECOSYSTEM

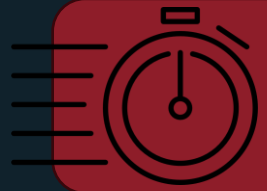
From Fragile Connectors to a Scalable Agentic Ecosystem



HUMAN VS MACHINE

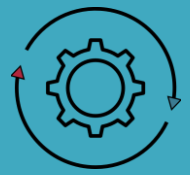
Defenders are Fighting Machines Now, Not Humans

DAYS → MINUTES



Lower Time To Exploit (Newly Disclosed CVEs)

Increased Scale (Global Reach)



Automation & Orchestration (Targeted Attacks)

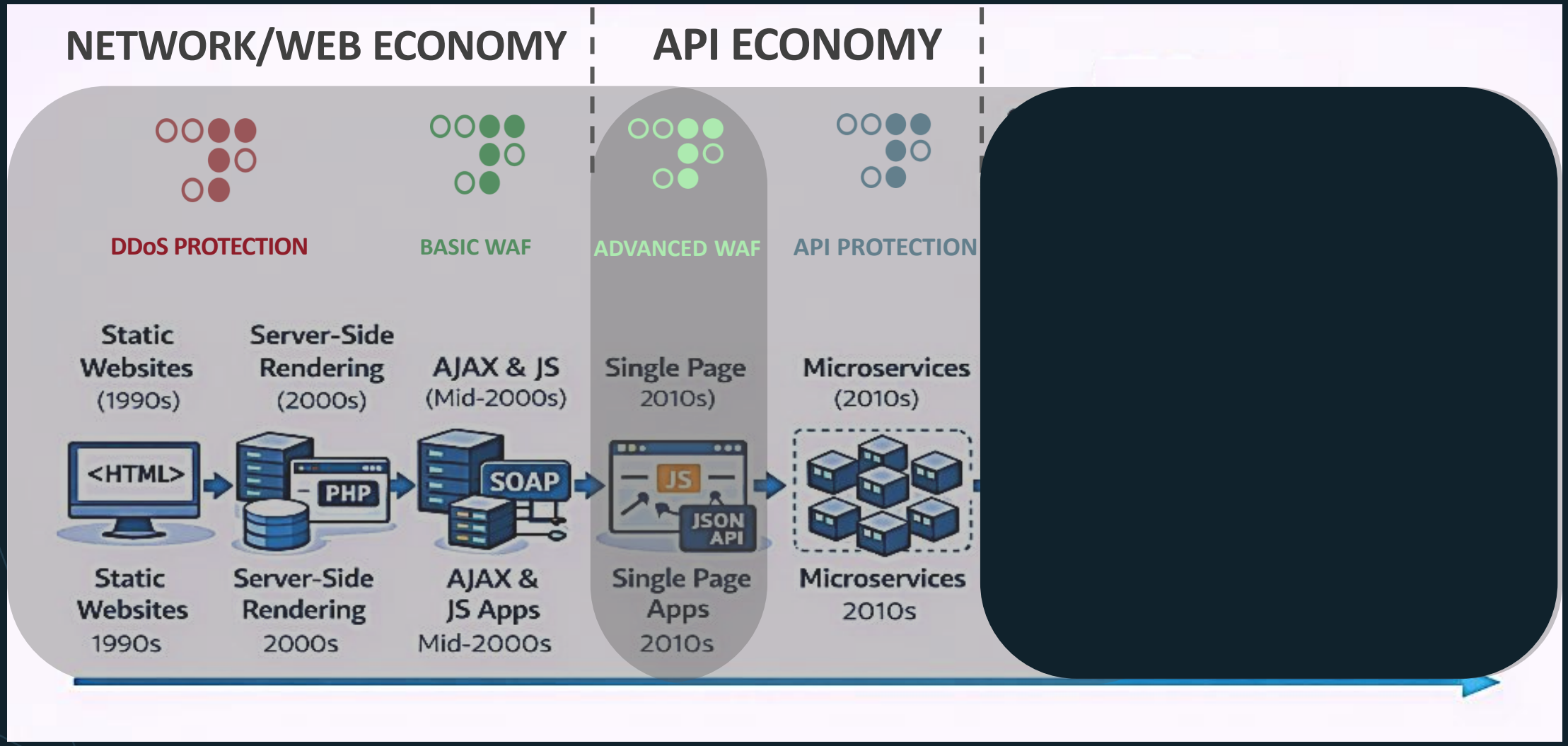
Machines Never Sleep

HOW DID WE GET HERE?

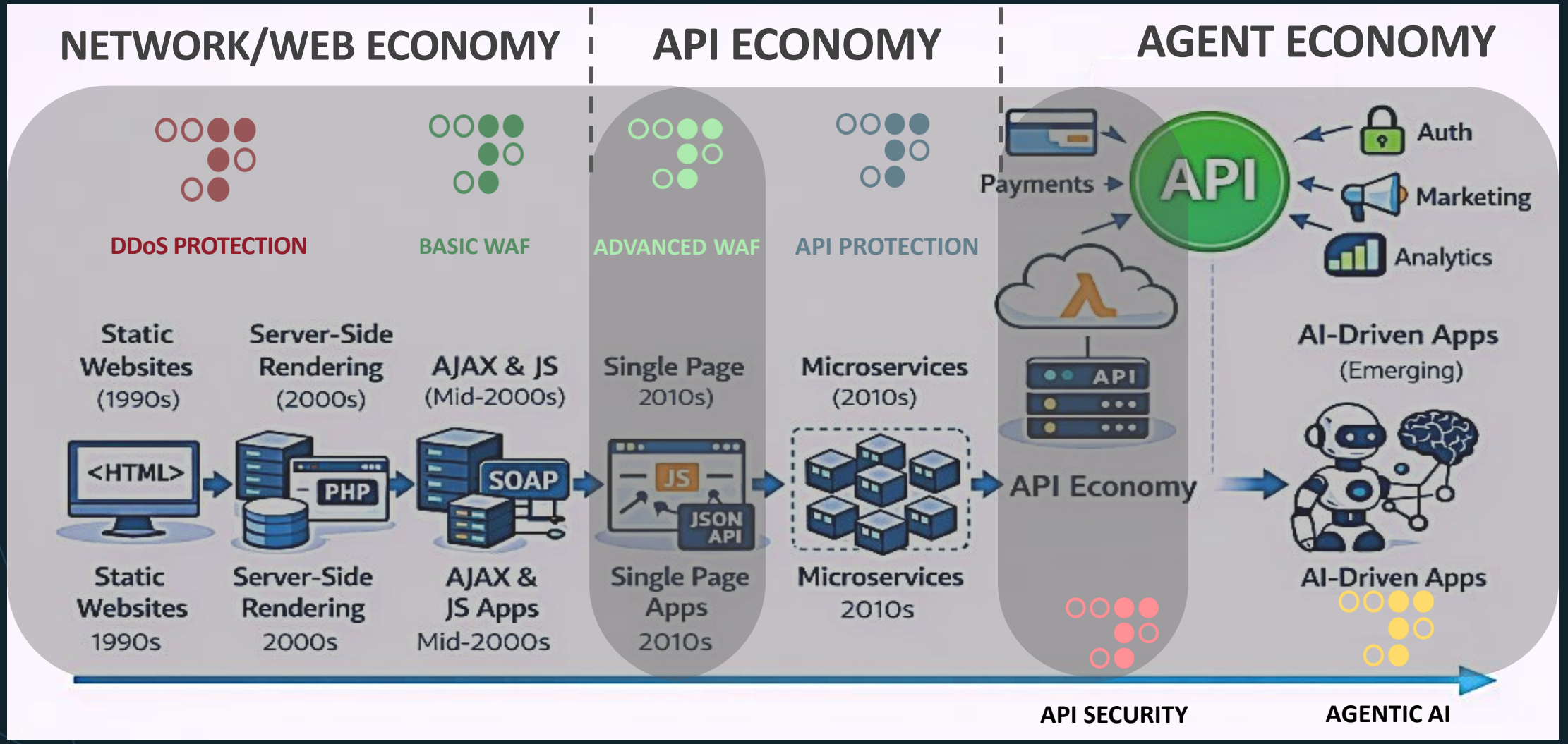
Market Evolution: Solutions Need to Adapt

Evolution of Web Application Architecture

Evolution of Web Application Architecture



Evolution of Web Application Architecture



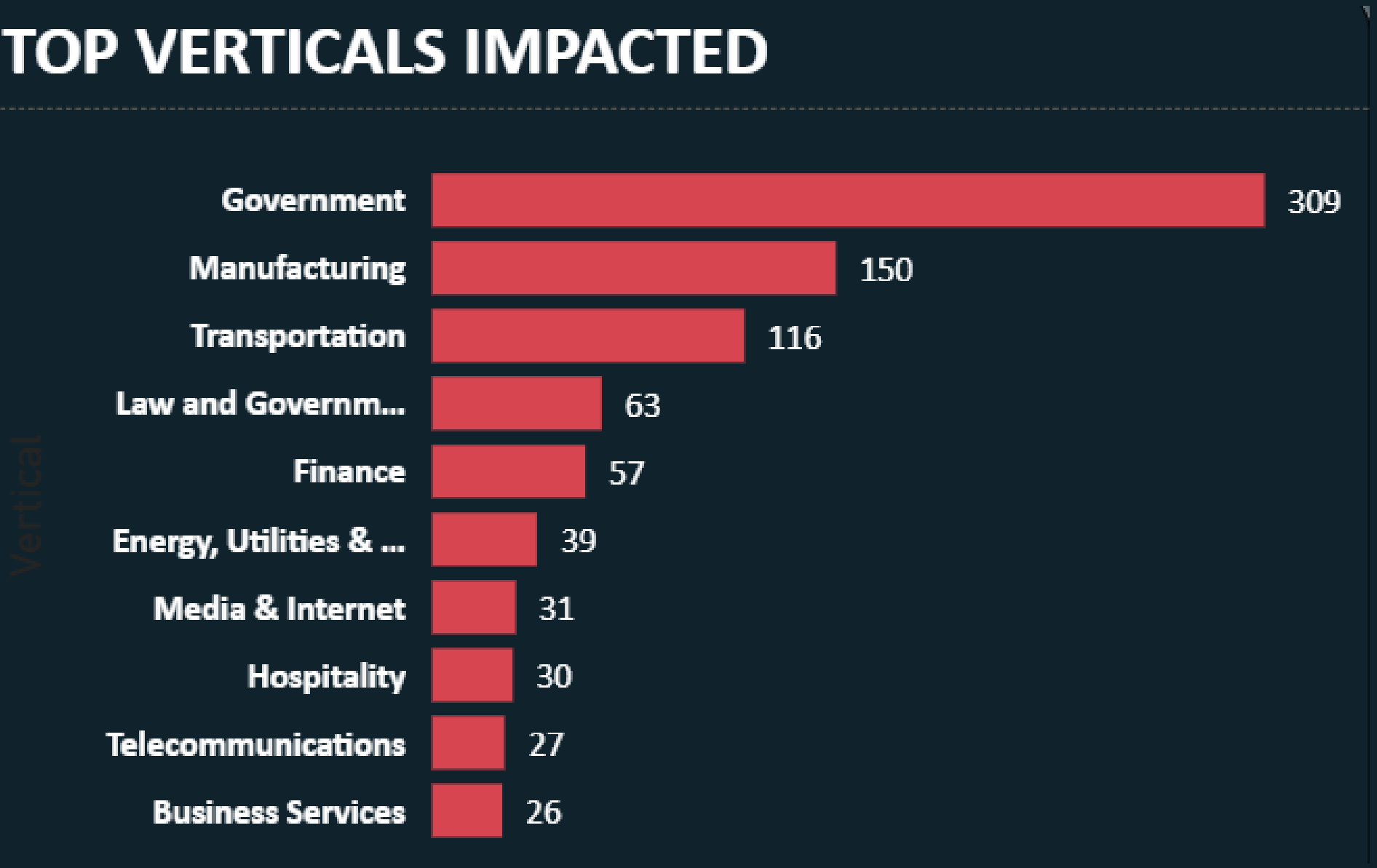
radware

Agenda

- Top Cyber Attacks
- Top Attacked Verticals
- Top Hacker Groups
- Real Attack Stories

Who is Attacked?

TOP VERTICALS IMPACTED



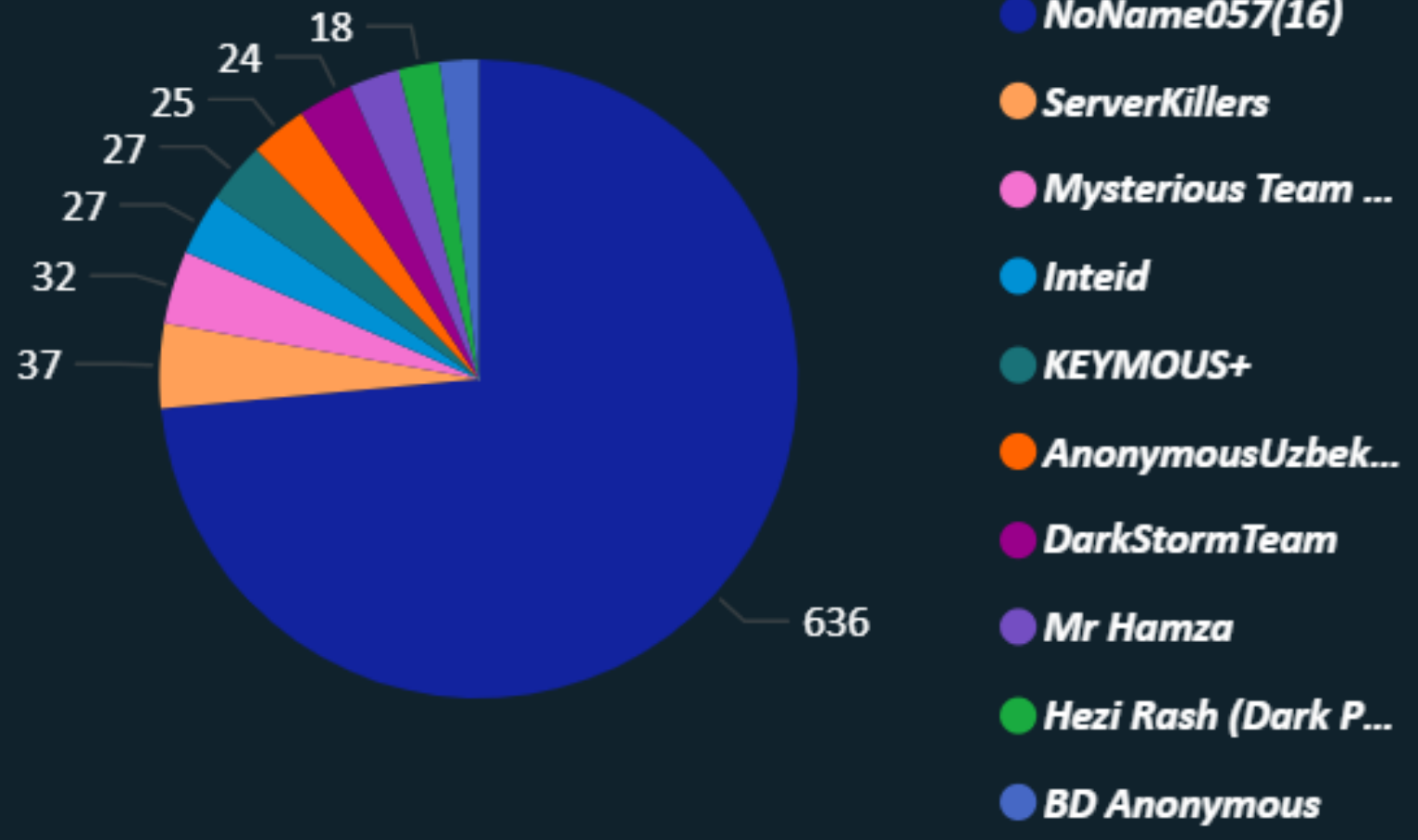
radware

Agenda

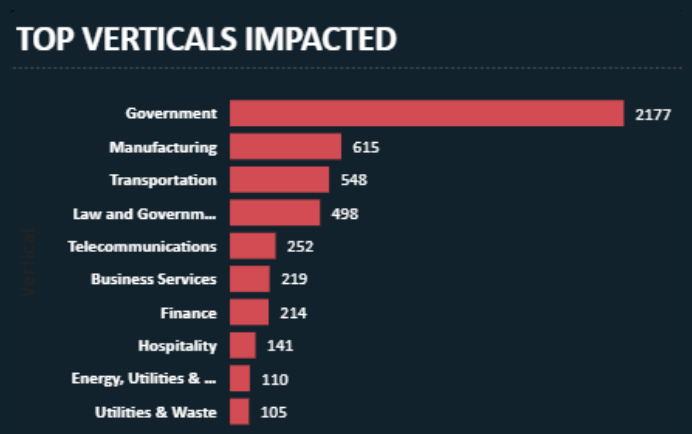
- Top Cyber Attacks
- Top Attacked Verticals
- Top Hacker Groups
- Real Attack Stories

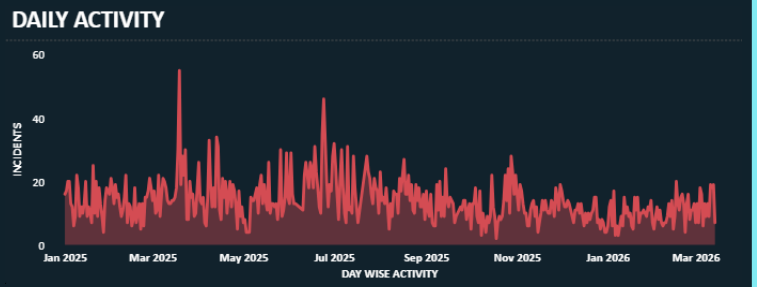
Who is Attacking?

TOP HACKER GROUP



NoName057(16)





- State-sanctioned Russian hacktivist group
- Attacks motivated by perceived actions against Russian interests
- Attack Tool: Project DDoSia attack toolkit, includes cryptocurrency wallet to receive financial rewards
- Attack vector: **Application-layer large scale HTTPs floods**

radware

Agenda

- Top Cyber Attacks
- Top Attacked Verticals
- Top Hacker Groups
- Real Attack Stories

Why Web DDoS Attacks are Difficult to Detect & Mitigate?

Flood of encrypted HTTPs requests are identical to legitimate requests

The traditional mitigation toolset is ineffective

- **Rate Limiting** → Ineffective, as it impacts legitimate traffic
- **IP Blacklisting** → Ineffective, as floods are generated from large botnets
- **Geo Blocking** → Ineffective, as attackers use local proxies
- **Manual Filters** → Ineffective, as attacks automatically mutate HTTPs methods and parameters
- **CAPTCHA** → Ineffective, as it impacts user experience, and cannot mitigate HTTPs on APIs

30-min-long 1 million RPS Attack on a Major Public Financial Service in Europe

Distributes allowances and financial aid to over 30 million beneficiaries

Action	Attack ID	Time	Application Name	Host	Account Name	Source	Attack Vector	Severity	Status
Blocked	76b9f677-906e-433d-9...	13 Apr 2026 05:05:05				Multiple	HTTPS Attack	Critical	Terminated

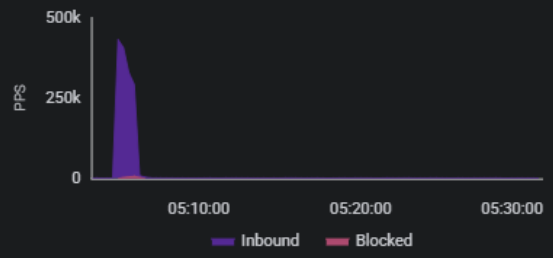
Summary

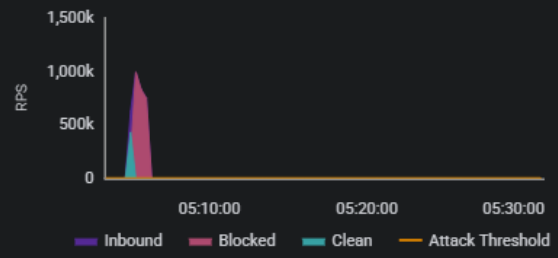
Attack ID: 76b9f677-906e-433d-9...
Application: [redacted]
Account: [redacted]
Security Module: Web DDoS Protection
Attack Vector: HTTPS Attack
Start Time: 13 Apr 2026 05:05:05 AM
End Time: 13 Apr 2026 05:31:10 AM
Protection Duration: 26 minutes 5 seconds
Protection Status: Terminated
Source: Multiple
Action: Blocked

Detection

Attack throughput was over 500 times larger than the legit traffic!

Requests Rate
Attack Threshold: 1,763 RPS
Attack Start Value: 341,007 RPS





Application Behavior
Attack Threshold: 6
Attack Start Value: 9

Mitigation

Total Requests
Received: 49,014,435
Dropped: 42,375,403

RPS Values
Average: 31,219 RPS
Maximum: 987,818 RPS

Total Packets
Received: 23,538,862
Dropped: 286,225

Total Blocked RPS Rate Limit
Total Dropped RPS: 3,696,367 RPS

L7 Signature | Block Geo | Block IP

Latest Real Time Signature

A narrow signature was created in real time with to automatically block only the attack traffic

Number of Path Elements = 2 AND
HTTP Method = GET AND
Number of Query Arguments = 3 AND
Number of Cookies = 0 AND
Number of Standard Headers = 5 AND
Number of Non-Standard Headers = 0 AND
Header 'authorization' does not exist AND
Header 'cache*' does not exist AND
Header 'content*' does not exist AND

The result: No impact on the service!

1.5 Hour-long ~2.5 million RPS Attack on a Major Hospital in Europe

Distributes allowances and financial aid to over 30 million beneficiaries

The result: No impact on the hospital's on-line services

1 Hour-long 5 Million RPS Attack on a Major European University

The result: No impact on the university's services

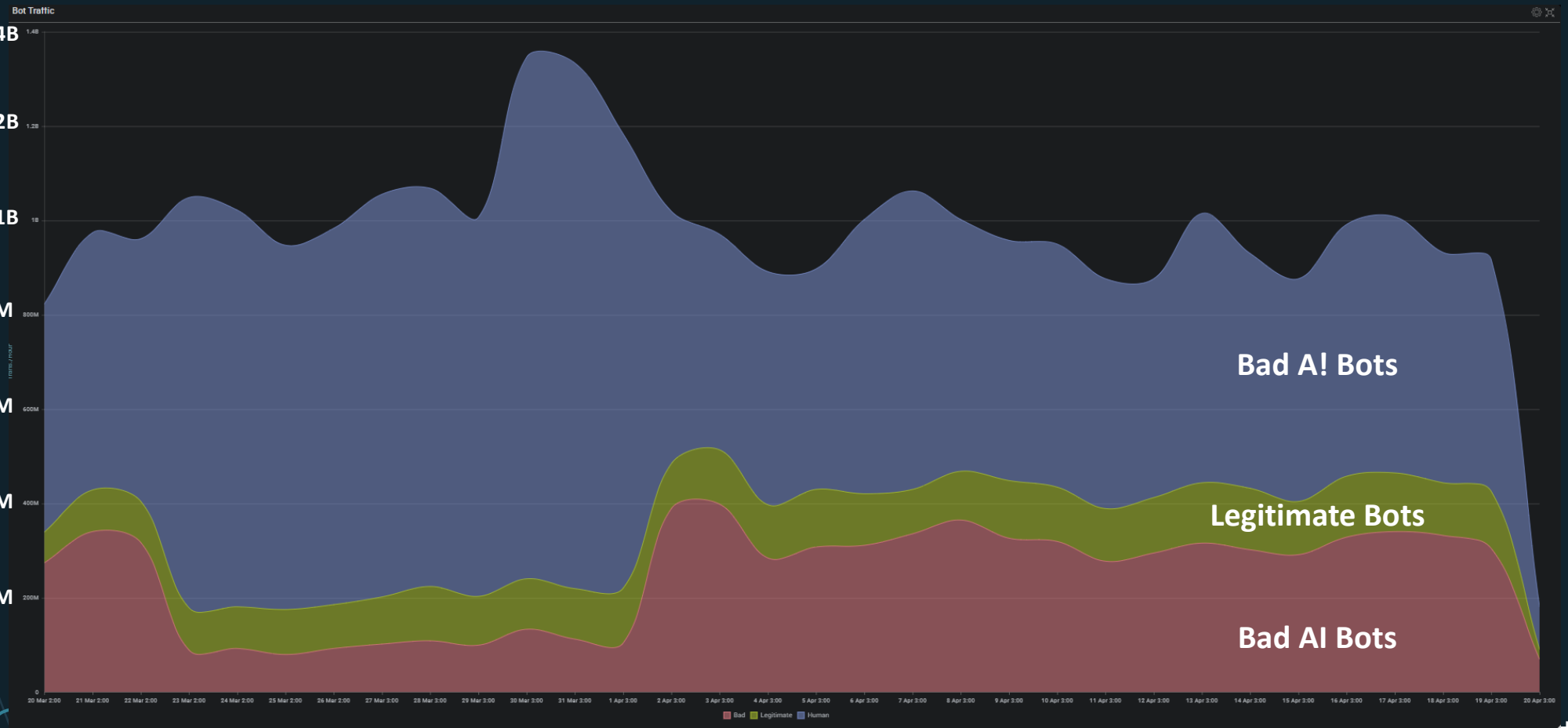
1 Hour-long 10 Million RPS Attack on a National Payment Card Infrastructure

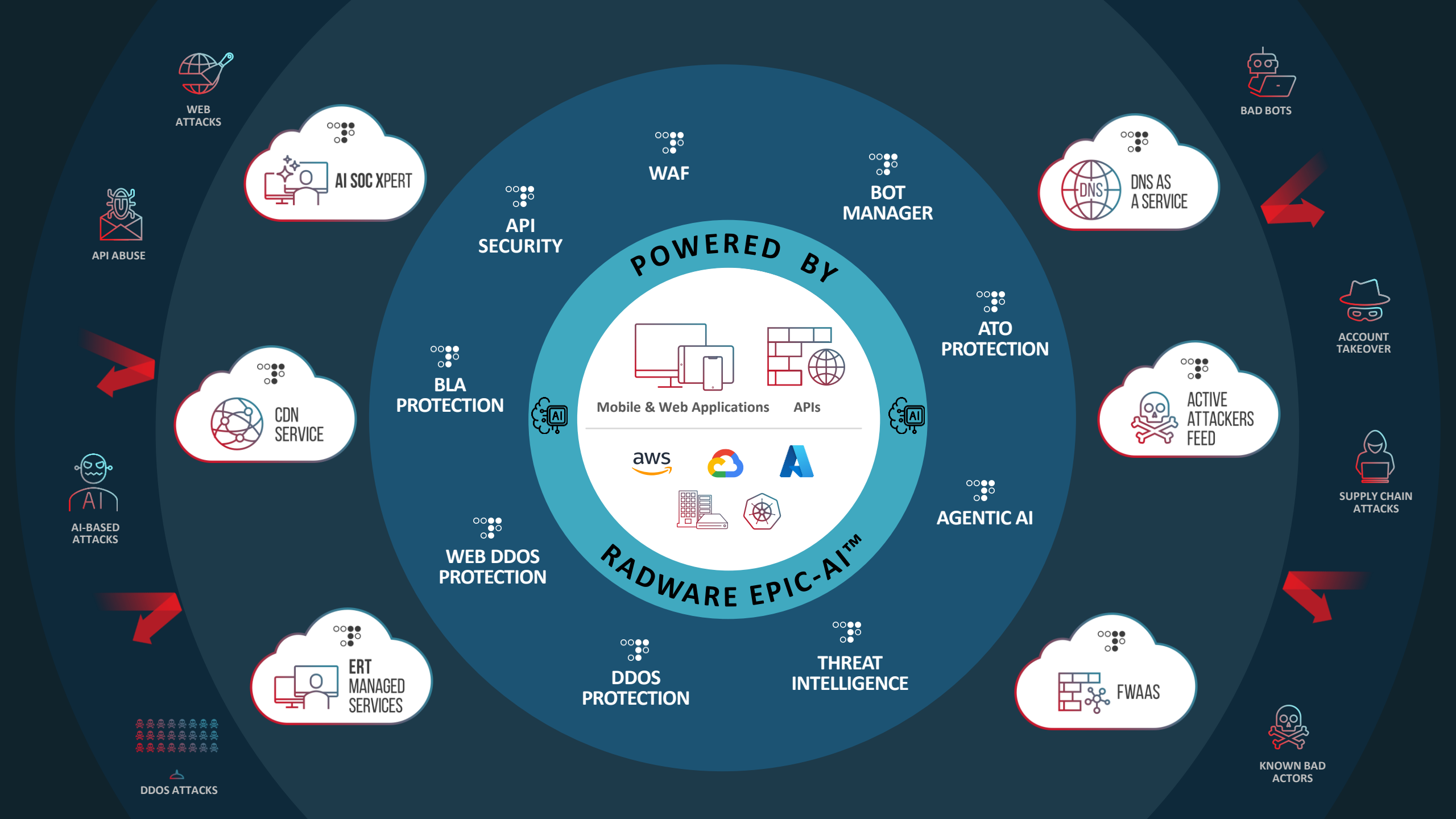
The result: No impact on the National Payment Card Infrastructure

2 Hour-long 12 Million RPS Attack on a European Public Government Services

The result: No impact on the Government services

Protecting Online Business from Malicious AI Bots (20/3/26 - 20/4/26)




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


“
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!