radware

Infographic

2026 Threat Report Cheat Sheet

Top stats and insights from Radware's Global Threat Analysis Report

Defining Trends of 2026

01 DUAL THREAT
Defenders face attacks with unprecedented scale and autonomous sophistication

DDOS TIME COMPRESSION 02
Duration for most record-level attacks is under 5 minutes—some are less than 60 seconds

03 AI IDENTITY CRISIS
Attackers spoof legitimate AI agents to bypass current protection

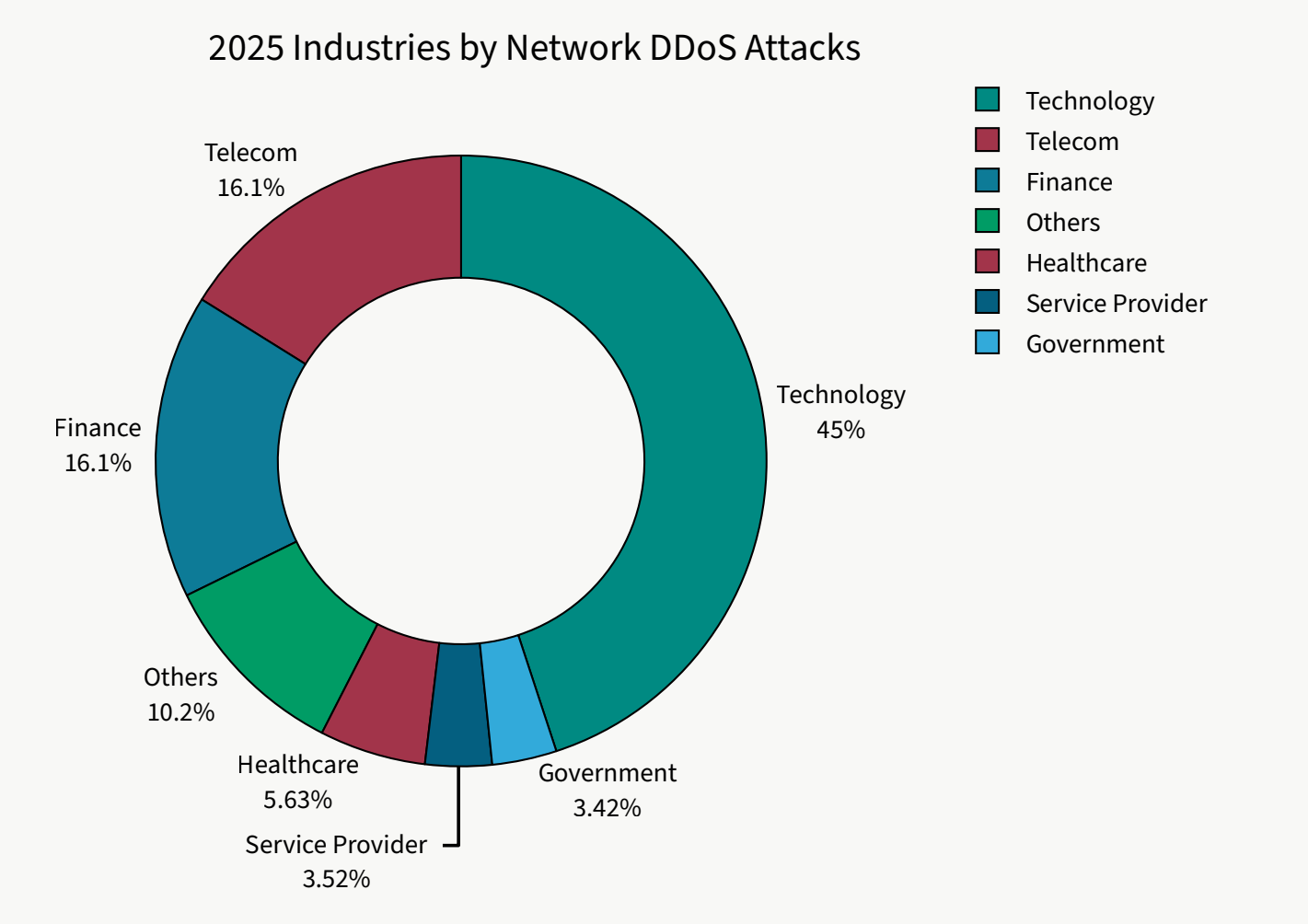
INVISIBLE IPI VULNERABILITIES 04
Zero-click attacks turn trusted AI agents into silent insider threats

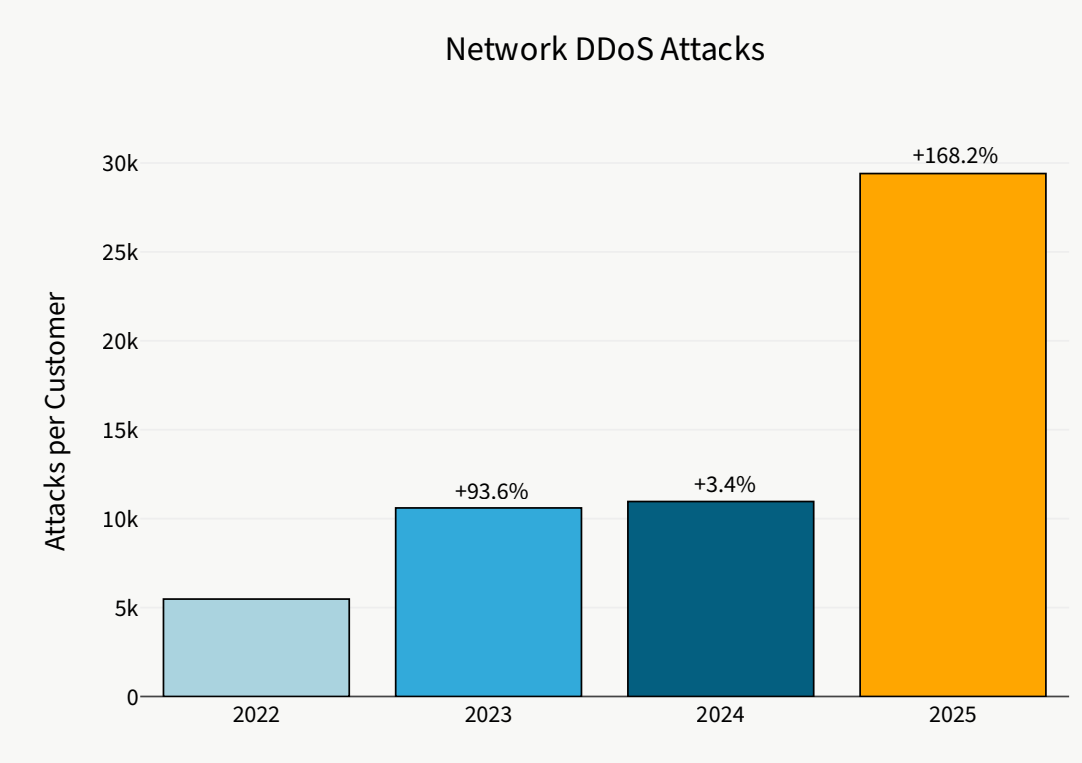
5 Key Intel Insights

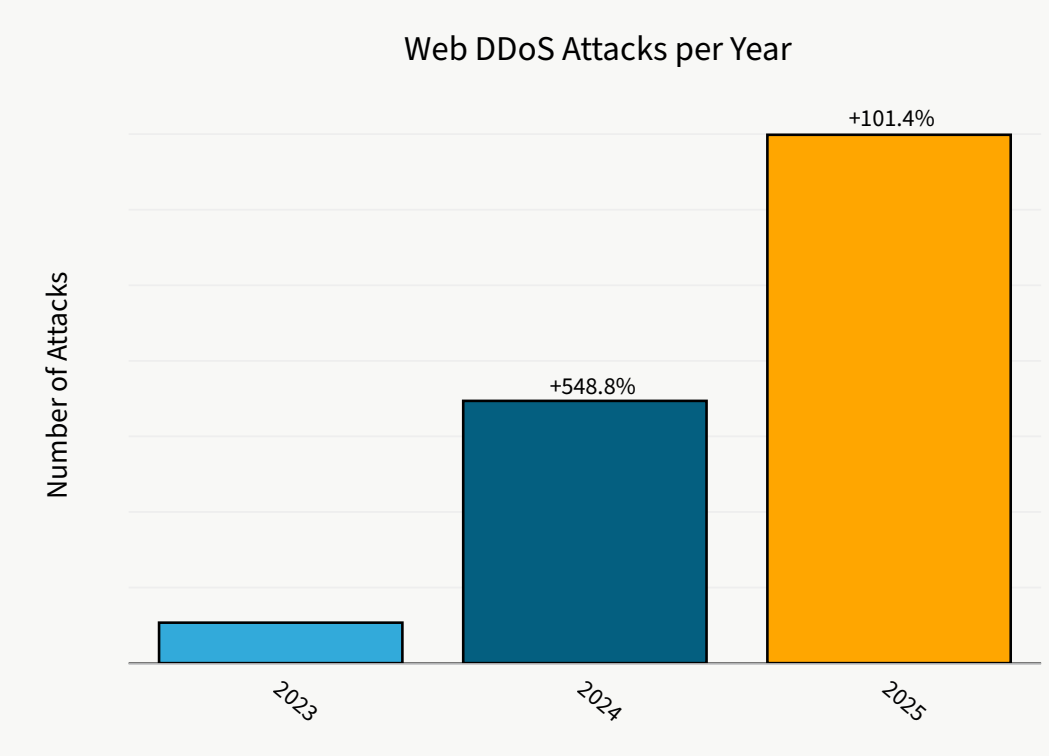
01 DDoS

The brute-force revival has arrived

168.2%
increase in network DDoS attacks



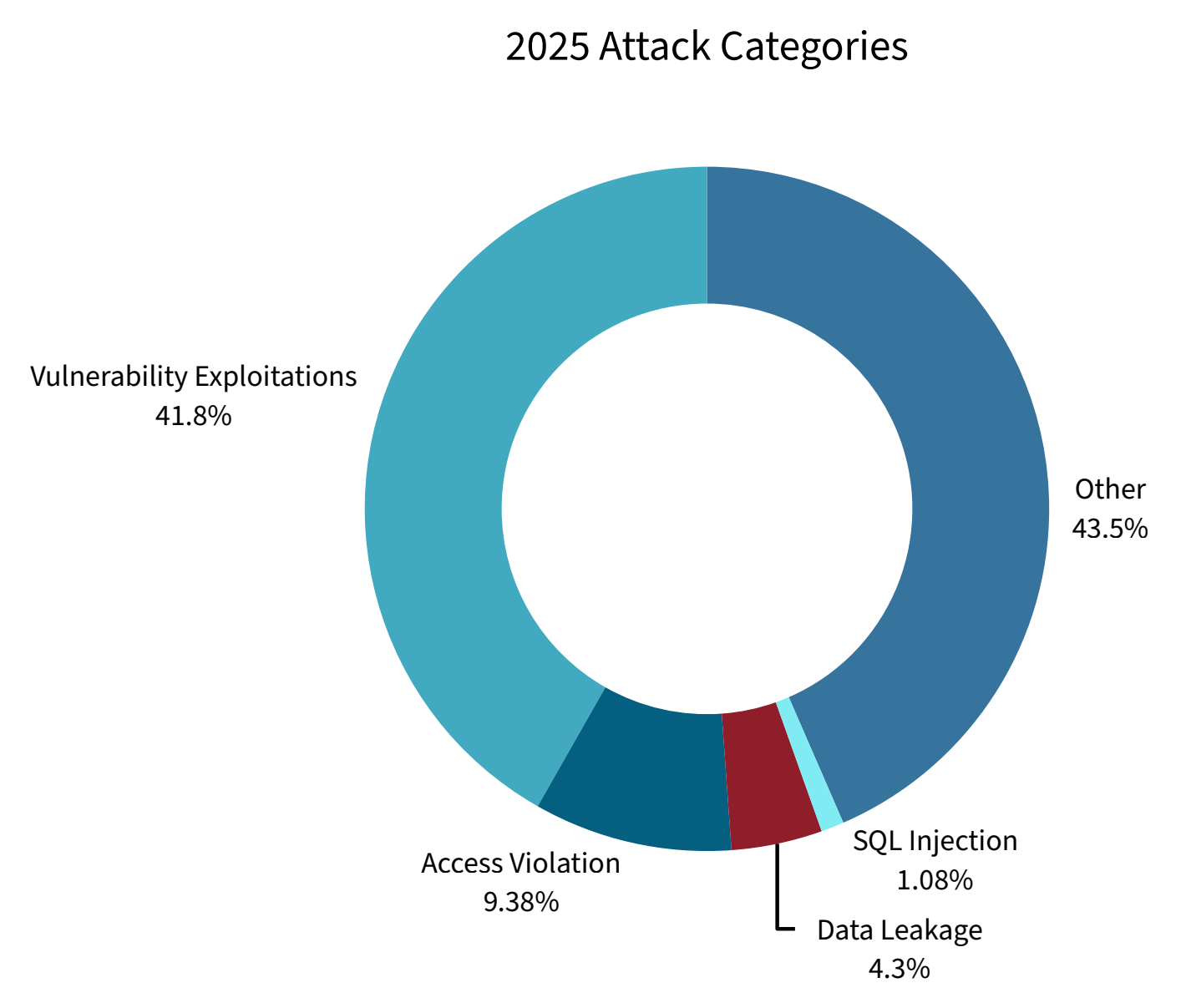


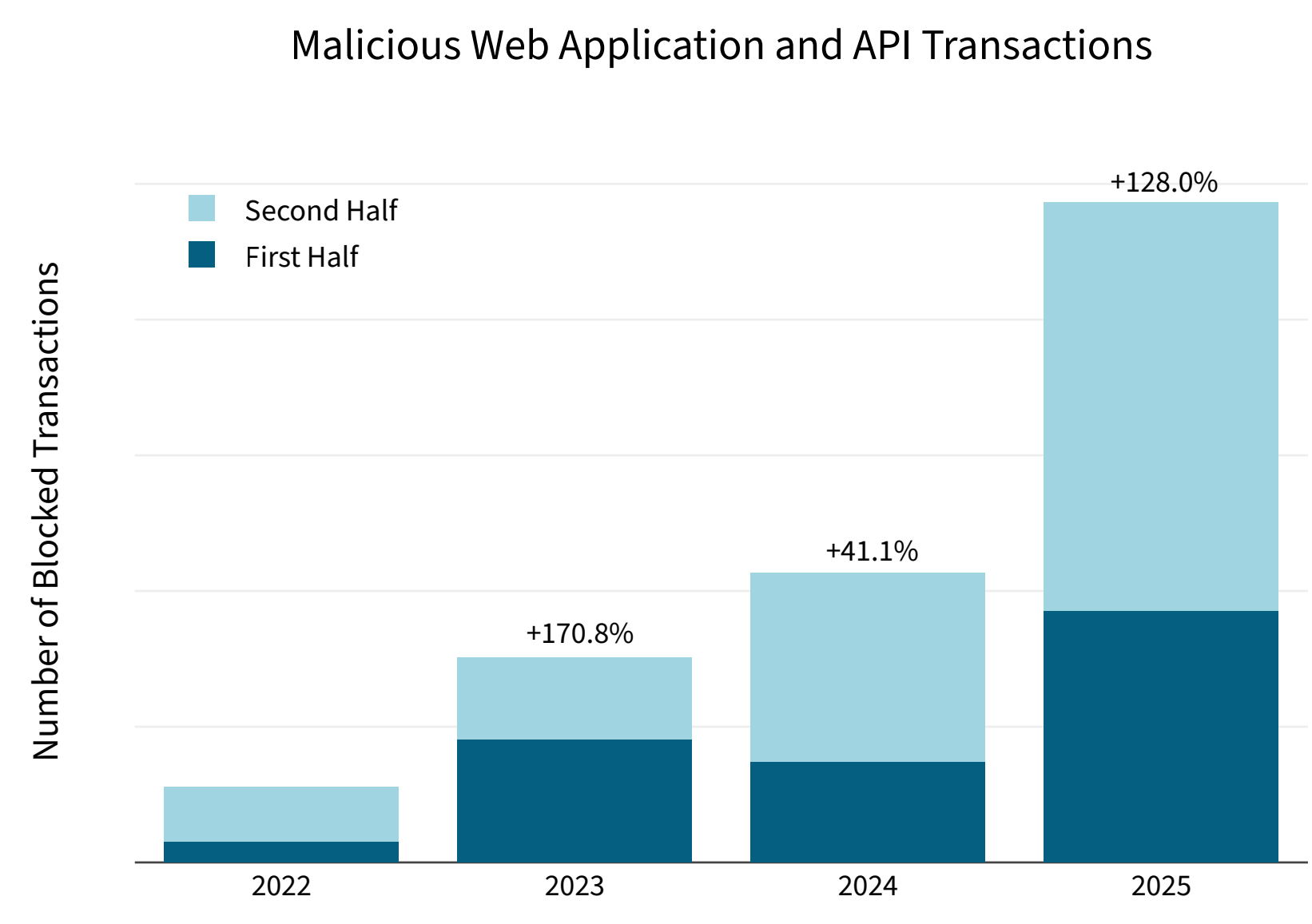


02 Application Layer

AI fuels surgical strikes on business logic and APIs

128%
increase in malicious transactions

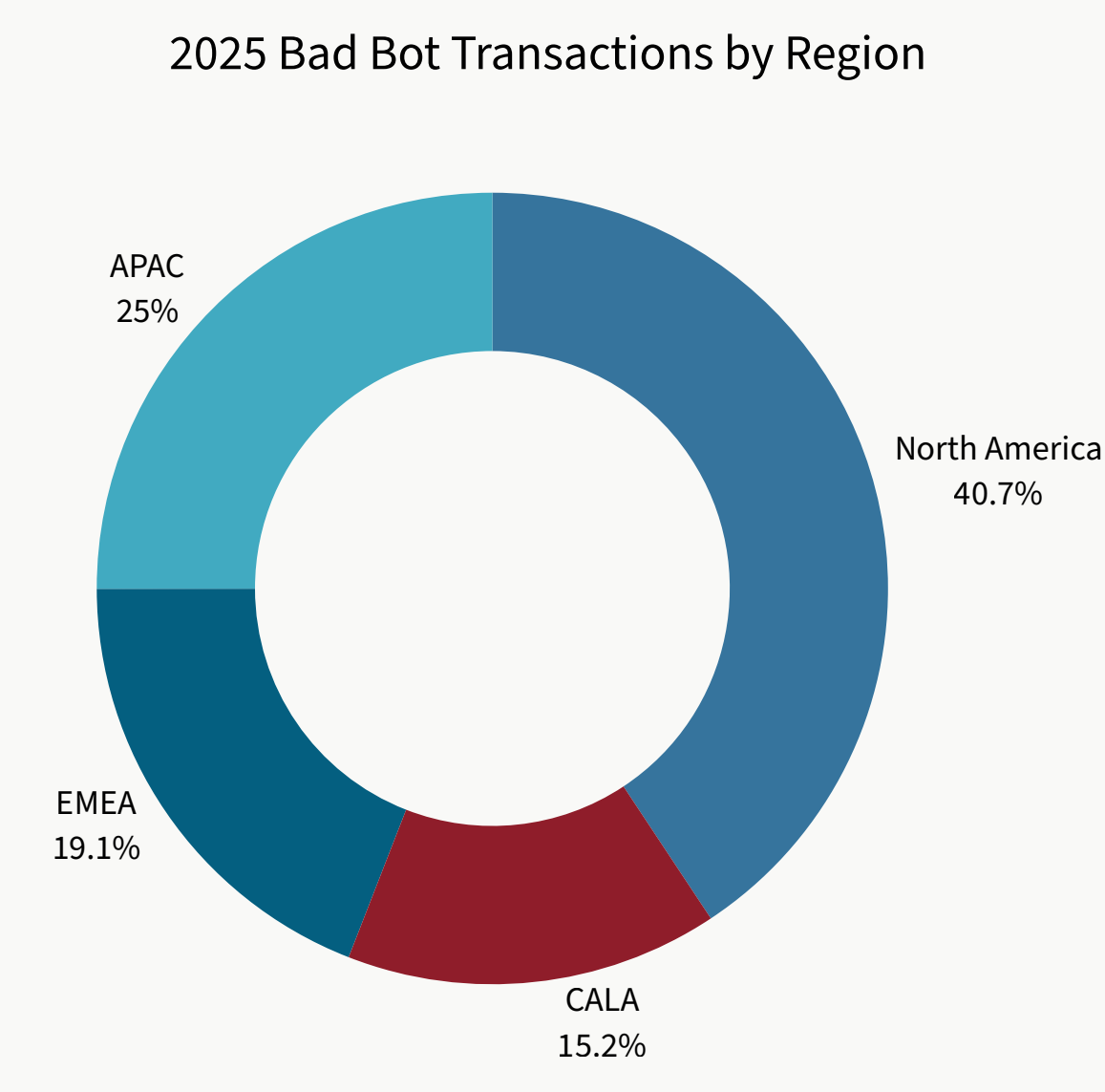


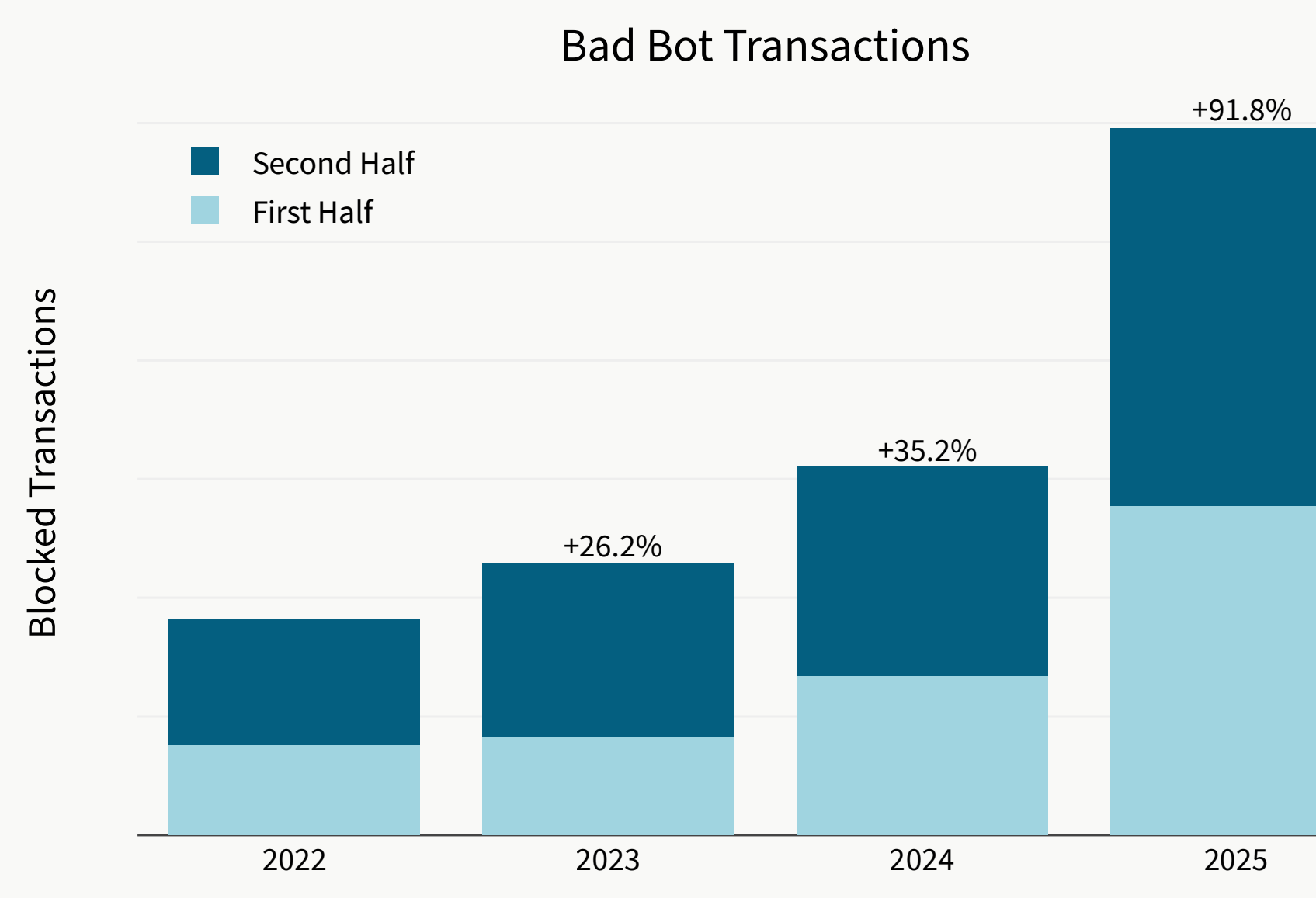


03 Bots

Bad bots thrive in automated and coordinated ecosystems

91.8%
increase in bad bot activity

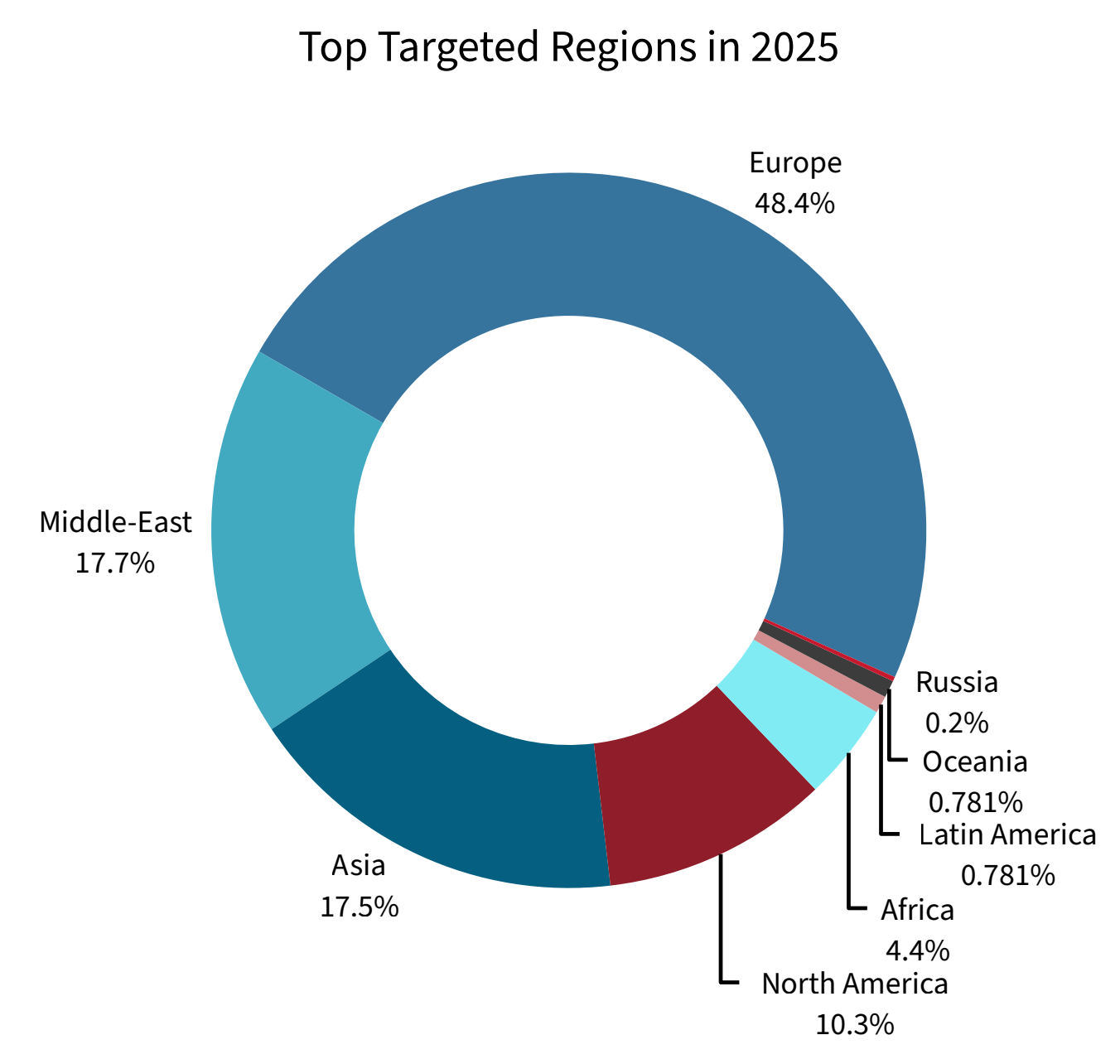


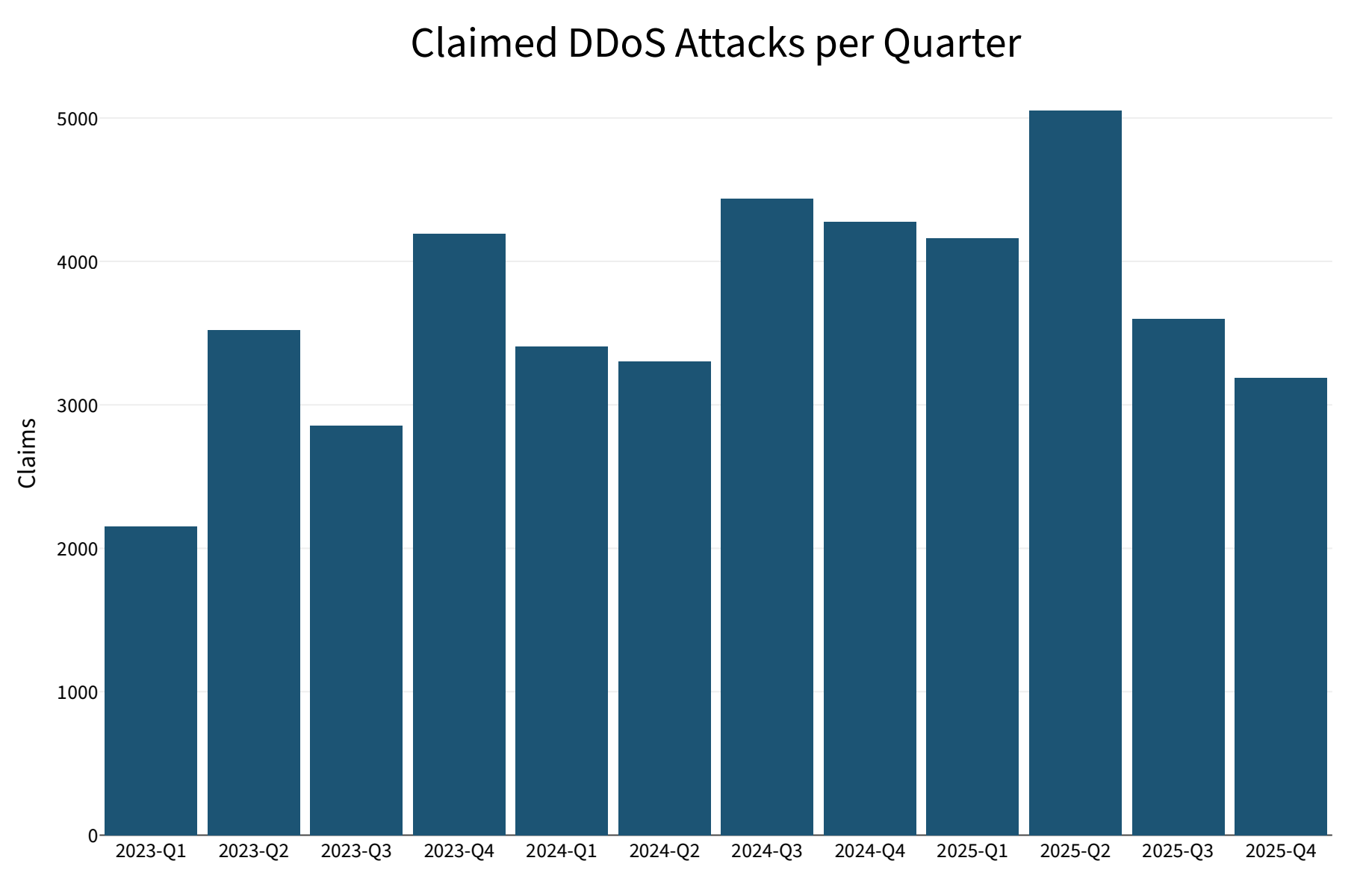


04 Hacktivism

Hacktivism is now a persistent, high-volume threat

16,000
unique attack claims were made on Telegram in 2025





Top 6 Most Active Hacktivist Groups

01 NoName057(16) 4,692 Claimed Attacks

02 Keymous+

03 Hezi Rash (Dark Power)

04 Mr Hamza

05 Anonymous NLBN

06 RipperSec

05 Artificial Intelligence

AI is both a tool and a target of attacks

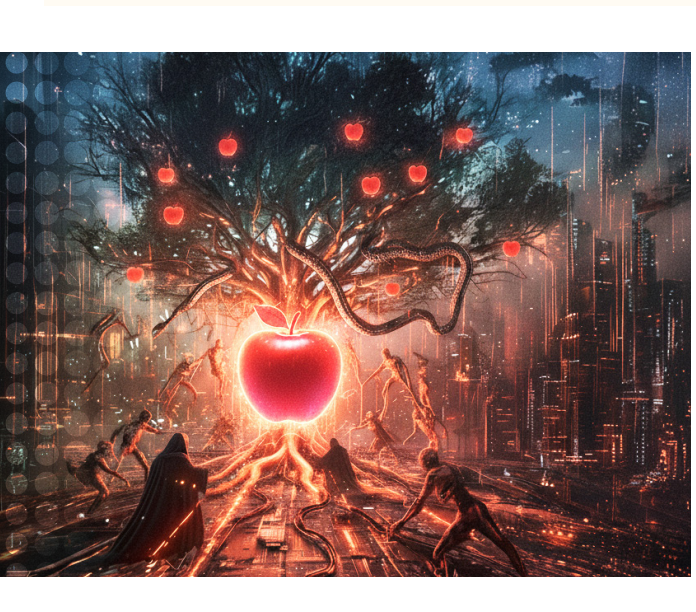
- Bad Actors Attack by Spoofing AI Agents
- AI Simplifies Cybercrime for Amateurs
- Vibe Hacking Shortens Dev Timelines
- Attacks Happen 24/7 (Machines Never Sleep)
- AI Makes Decisions in Milliseconds (Humans Take Minutes)

Your 2026 Security Strategy

Automation
Defend at machine speed to counter rapid attack cycles

Massive Scale
Mitigation infrastructure must absorb Tbps-class floods

Integrated Intelligence
Behavioral & intent-based analysis needed to tell real from spoofed AI agents



radware

RWI6283 | 02.18.2026