CHECK POINT™

Leading DDoS Protection

Itay Raviv, Security Product Manager, DDoS

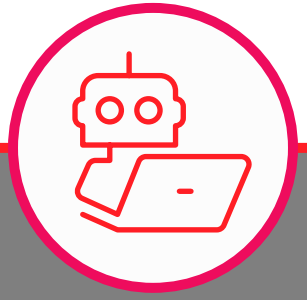
October 2024

YOU DESERVE THE BEST SECURITY

Shifting Threat Landscape

+94%

Increase in number of DDoS attacks, 2023 vs. 2022



82%

Experience a bot attack on a daily, weekly or monthly basis

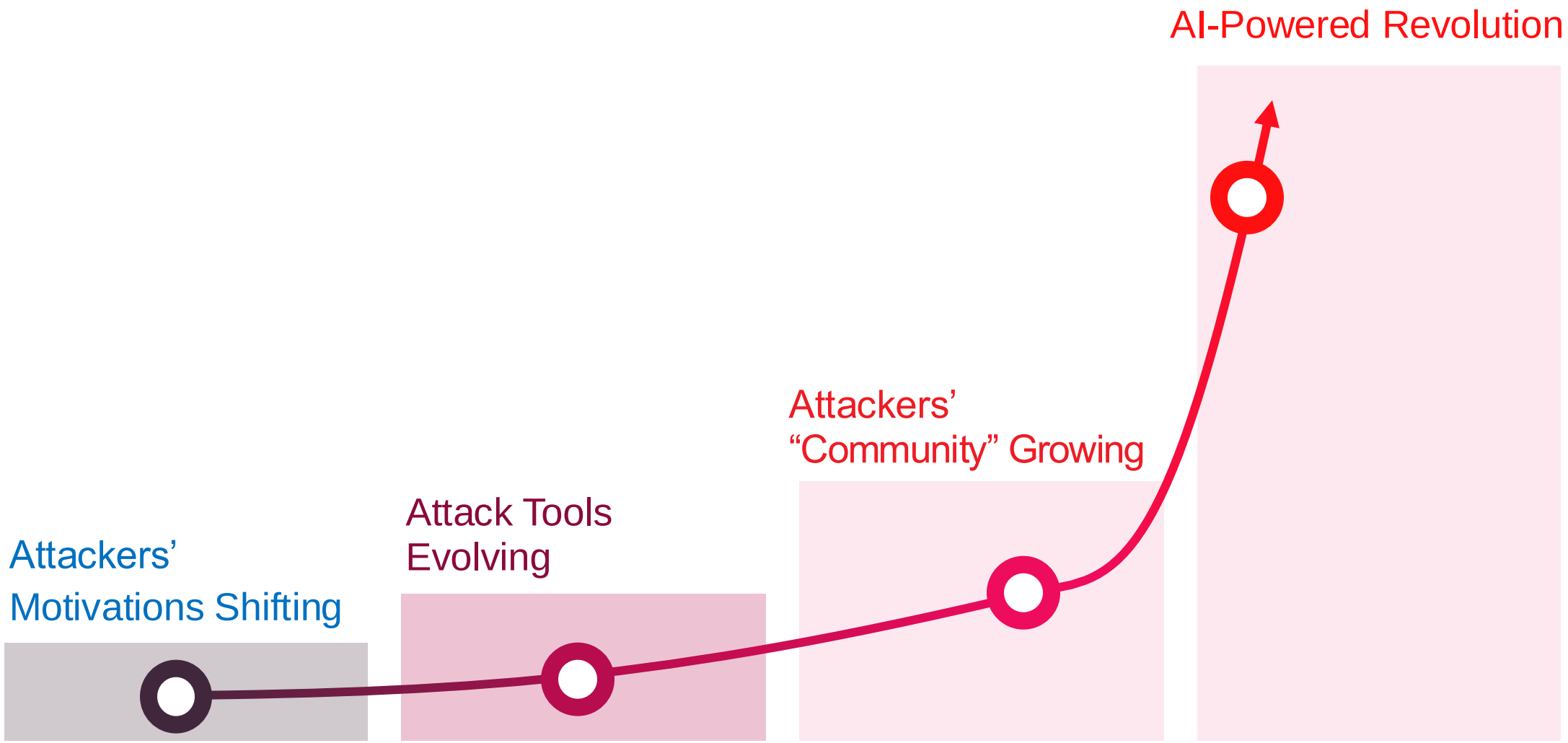
+171%

Increase in malicious web traffic, 2023 vs. 2022

Attacks increase in frequency, size and complexity across all attack vectors

Source: Radware Threat Landscape Report 2024

What is Fueling the Shifting Threat Landscape?



All-in-One Modern Attack Tools on Github

Features And Methods

- Layer7
  - GET | GET Flood
  - POST | POST Flood
  - OVH | Bypass OVH
  - RHEX | Random HEX
  - STOMP | Bypass chk_captcha
  - STRESS | Send HTTP Packet With High Byte
  - DYN | A New Method With Random SubDomain
  - DOWNLOADER | A New Method of Reading data slowly
  - SLOW | Slowloris Old Method of DDoS
  - HEAD | https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/HEAD
  - NULL | Null UserAgent and ...
  - COOKIE | Random Cookie PHP 'if (isset($_COOKIE))'
  - PPS | Only 'GET / HTTP/1.1\r\n\r\n'
  - EVEN | GET Method with more header
  - GSB | Google Project Shield Bypass
  - DGB | DDoS Guard Bypass
  - AVB | Arvan Cloud Bypass
  - BOT | Like Google bot
  - APACHE | Apache Expliot
  - XMLRPC | WP XMLRPC expliot (add /xmlrpc.php)
  - CFB | CloudFlare Bypass
  - CFBUAM | CloudFlare Under Attack Mode Bypass
  - BYPASS | Bypass Normal AntiDDoS
  - BOMB | Bypass with codesenberg/bombardier
  - KILLER | Run many threads to kill a target
  - TOR | Bypass onion website

DDoS attack vectors

Bot attack vectors

Web application exploits

Built-in bypass again common defenses

- Attackers don't distinguish between WAF, DDoS, Bot attack vectors
- Need an **integrated platform** to **overcome all-in-one attack tools**

Growing Community of Attackers

1 Gamers Turning Attackers

4 of 5
attackers involved in ATO & DDoS are Gamers

700M
new players emerged since COVID

30%
cracked account market traffic comes from gaming sites

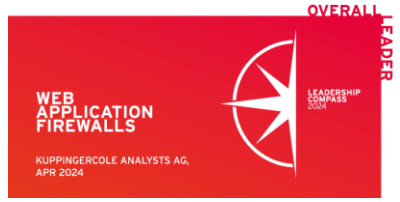
2 Breadth & Depth of Online Networks

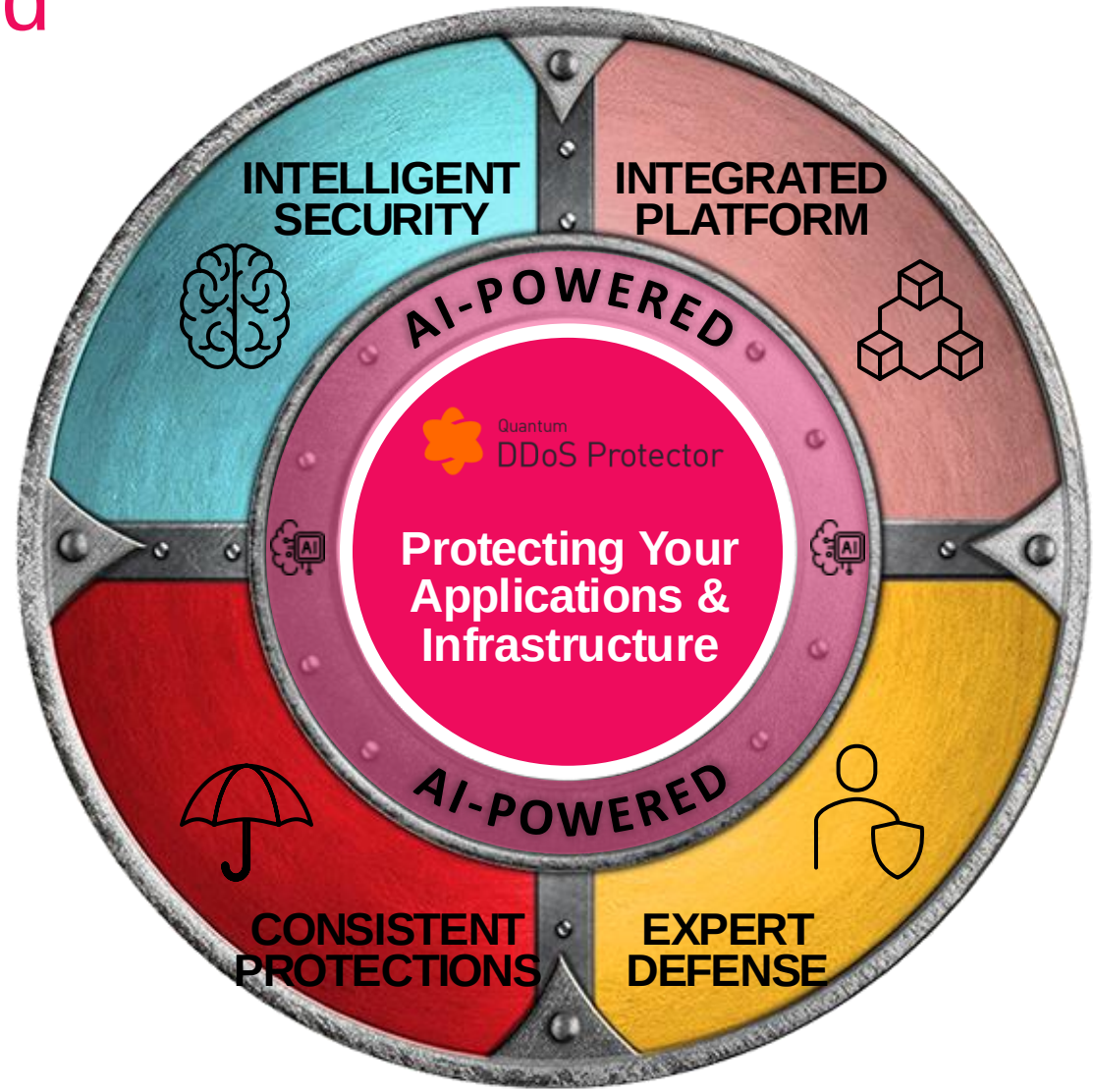
Social networks as billboards

More marketplaces & hacking malls

What is Needed to Stay Ahead

Quantum
DDoS Protector





Flexible Deployment Modes

Cloud Service

Always-On & On-Demand

Hybrid

Integrated Cloud & Appliance

Appliance

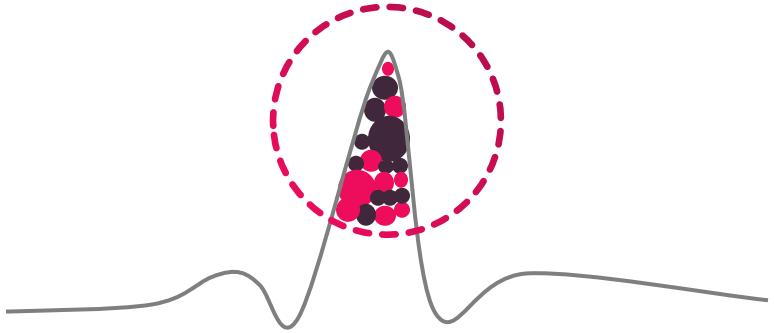
Physical / Virtual

Unique Behavioral-based Detection

Radware uses machine-learning algorithms to automatically distinguish between legitimate user traffic and attack traffic.

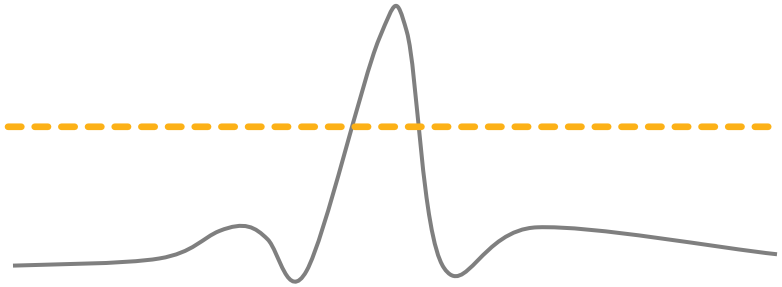
DDoS Protector

BEHAVIORAL-BASED DETECTION



Others

RATE-BASED DETECTION



Superior security with fewer false-positives

Built to Protect From Advanced Attacks

Carpet Bombing Attacks

Amplification & Reflection attacks protection

DNS Attacks

Automated **Behavioral DNS Protection** for authoritative & recursive DNS

Burst Attacks

Behavioral-Based Burst attack protection

Encrypted Threats

Multi-layer **TLS-Flood** protection
Only vendor supporting **TLS 1.3**

IoT Botnets

Real-time intelligence feed **to block active attackers**

Multi-Layered Protection

CHECK POINT™

Transition

YOU DESERVE THE BEST SECURITY