radware

Infographic

5 Reasons It's Time for Better Bot Management

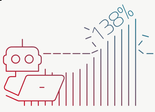
#1 AI Has Arrived

How hackers are using generative AI tools:

- Seeking out vulnerabilities
- Creating scripts for zero-day attacks
- De-bugging and relaunching bots (in minutes rather than weeks)

#2 Bad Bots Are Rising Fast

138% - Growth in bad bots detected and mitigated in the last 24 months



#3 They're More Disruptive than Before

More sophisticated
Rotating IPs, morphing, closely mimicking human behavior

More persistent
Faster fixing bugs and returning to attack

More aggressive
Attacking at a higher volume

#4 Standard Responses Aren't the Answer

Why responsive protection like pre-set signatures, CAPTCHAs and rate limiting can't do it alone:

Not Enough to Ensure Protection
Outsmarted by bots that morph and mimic human behavior

Work Against Real Users
Block legit users and provide a poor customer experience

#5 Bad Bots Come With a Cost

Bad bots drain resources, hurt conversion rates, cause customer churn and impact revenues.

- Bandwidth Consumption
- Computing Power
- Cost of Conversion
- CDN Cost
- Traffic Decryption
- Cost of Fraud
- Denial of Inventory
- Scraping
- Scalping

Bad Bots at a Glance

25–30%
Share of web traffic made up of bad bots

82.6%
Businesses experiencing bot attacks at least monthly

10%
Share of attacks focused on native iOS and Android mobile apps

The Best Ways To Stop a Bot

Fight AI with AI
Utilize AI to discover anomalies and correlate threat data.

Get There Early
Automatically block unwanted IPs and identities before they do damage.

Use Multiple Protection Layers
Stay secure with preemptive protection, behavioral-analysis detection and advanced mitigation.

Learn how you can stop the new generation of bad bots at Radware.com.

Stop the Bots

RWI - 230 | 04.10.2024

radware