Barracuda Advanced Bot Protection

Keep bad bots at bay.

Bot-spotting is getting harder.

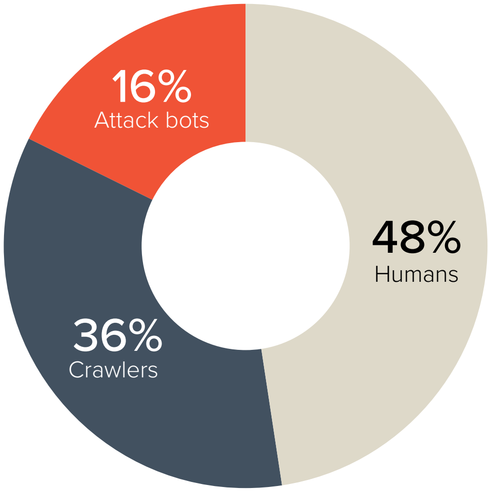
Incredible as it may seem, bots generate more than half of today's internet traffic—including a lot of the malicious traffic that seeks to penetrate your web applications in order to attack your network and your data.

Not all bot traffic is malicious, however. Allowing traffic from legitimate crawlers is critical to accessing markets and getting your information in front of consumers. And, of course, you want to be sure not to block legitimate human traffic.

The most advanced malicious bots in use today are increasingly good at mimicking human online behavior—and many bot-detection solutions just can't keep up with today's sophisticated bots.

Malicious bot behavior

As online-commerce apps have proliferated, bad actors have developed many techniques to use bots in ways that result in high costs for organizations like yours. While simple bots have long been used to launch DDoS attacks that can freeze your operations, today's more sophisticated bots might buy up all the tickets to an event or an airline flight—typically using stolen credit-card numbers—in order to re-sell them at inflated prices on a scalping site. The potential impact to your business can be severe, in terms of both revenue and reputation.



52% bot traffic
is a major concern for businesses.

Figure 1 - Humans, crawlers, and attack bots

A multi-layered approach to bot-blocking

As bots evolve and simulate human behavior more and more closely, bot detection and mitigation strategies must evolve as well. Today's "low-and-slow" bots, which request data slowly and rotate IP addresses often, require special fingerprinting techniques to detect.

Barracuda Advanced Bot Protection is a cloud-delivered service that combines Barracuda's vast, real-time Global Threat Intelligence Infrastructure with advanced machine-learning technology. It scans incoming application traffic in real time, using AI traffic analysis and behavioral classification to identify even the most sophisticated, human-seeming bots—while minimizing false-positives that could block legitimate traffic and harm your business.

Each e-commerce application offers unique opportunities for bots. A generic bot detection methodology cannot address the specific bots written to target a specific application. Our state-of-the-art machine-learning layer provides automatic profiling of each individual application to provide application-specific bot detection and mitigation capabilities to help ensure the highest possible level of protection.

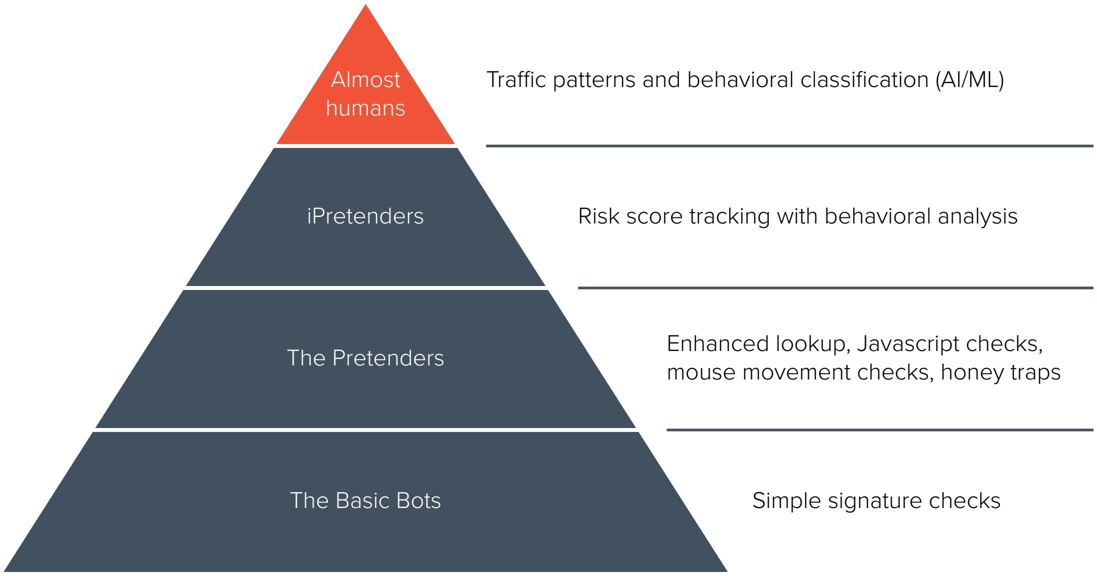

Almost humans
Traffic patterns and behavioral classification (AI/ML)
iPretenders
Risk score tracking with behavioral analysis
The Pretenders
Enhanced lookup, Javascript checks, mouse movement checks, honey traps
The Basic Bots
Simple signature checks

Figure 2 - Defending against bots

Features and capabilities

Complete protection from Advanced Bots

- Detect all bot-related activity and attacks:
  - Scraping of inventory/prices
  - Content scraping
  - Account takeover/credential-stuffing
  - Scalping, carding etc.
  - OWASP automated Top 21 protection included
- Detect basic and advanced bots, including “almost-human” bots

Multiple deployment options, all backed by a battle-tested machine-learning layer, to protect your applications anywhere

- With Barracuda Web Application Firewall (HW/Vx)
- With Barracuda CloudGen WAF (AWS, Azure, GCP)
- With Barracuda WAF-as-a-Service
- As a Server Module

Much more than just bot mitigation when deployed with a Barracuda WAF solution

- OWASP Top 10 protection and more
- Protect any web, API, or mobile application against all application attacks
- Complete DDoS mitigation, including Volumetric DDoS (BADP) and Application DDoS

Barracuda®
Your journey, secured.

SOLUTION BRIEF • US 1.1 • Copyright 2019 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com