Bot Detection

Identify and mitigate automated attacks in real time

Fraudulent sign-ups are killing your ROI. Bots are to blame.

Bots now make up nearly half of all internet traffic.[1]

Some are harmless. Many are not. And these automated attacks extend beyond account takeovers. Fake sign-ups are on the rise, driven by bots that exploit promotions, bonuses, and loyalty programs.

According to the Auth0 Customer Identity Trends Report[2]:

- During sustained attacks, fraudulent signups can outnumber real users by a factor of 120
- 44.5% of registration attempts on the Auth0 platform met the criteria of "a sign up attack"
- 65-70% Retail and Financial Services are top targets of fraudulent signup attempts in 2024

Bots are more than just a security issue. They're a business problem. The financial impact of automated threats is undeniable. Malicious bots hurt your bottom line, draining resources and eroding customer trust.

76% of organizations experienced a bot attack in the past year[3]

$2.9M is the average cost of a significant bot attack[4]

Not all bot detection is created equal.
Many bot protection solutions fight fraud by adding friction often at the expense of legitimate users. Because many legacy detection systems struggle to distinguish between advanced bots and real humans, they end up treating everyone as suspicious.

The result: your defenses are slowing down the very people you're trying to protect. Every extra CAPTCHA, timeout, and login loop pushes real users away.

40% of real users have abandoned purchases due to CAPTCHA frustration.[5]

When defenses create friction for legitimate users, security stops being protection and starts becoming a barrier to business.

And it's not just user experience that suffers:

- **Marketing:** Conversions fall and ROI takes a hit as real users abandon.
- **Engineering:** False positives mislabel real users, wasting time and resources on endless triage.
- **Product:** Growth slows as frustrated customers churn before engaging.

In addition, the actual challenges themselves aren't all equal. Some AI-powered bots are now capable of solving traditional picture based CAPTCHAs. Not only are challenges frustrating, but they also do not always stop bots. You need to be able to use the appropriate bot challenges for the risk - ones that are user-friendly but tough on bots.

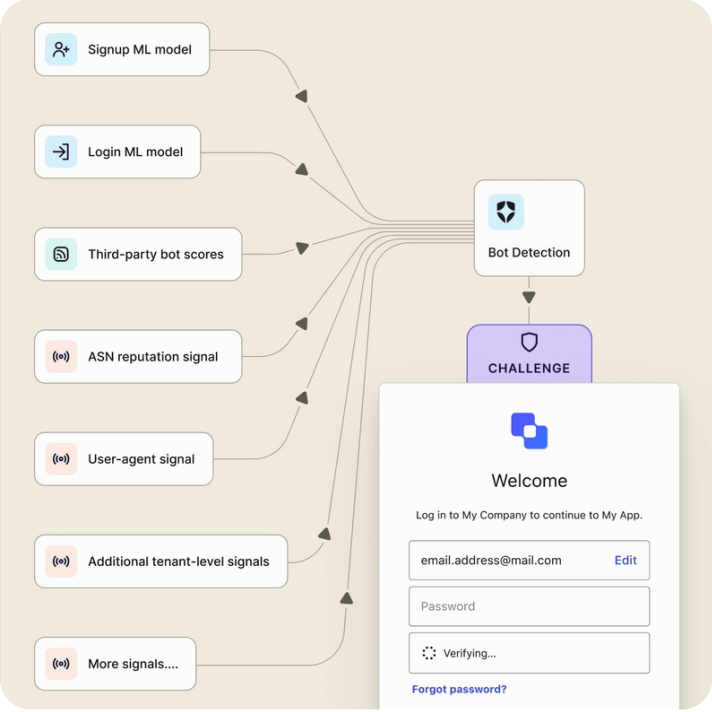
Protect your platform and your bottom line
At Auth0, we layer defenses across multiple dimensions. The goal is simple: stop bad traffic before it ever reaches your authentication system.

[1] Bad Bot Report, Imperva, 2024
[2] Customer Identity Trends Report, Auth0, 2025
[3] How Bad Bots are Hurting Businesses Survey, Fastly, 2024
[4] How Bad Bots are Hurting Businesses Survey, Fastly, 2024
[5] CAPTCHA Conundrum Article, Peakhour, 2025
[6] Cinepolis Customer Use Case, Auth0, 2024

Bot Detection — your first line of defense against identity based attacks

It's not about challenging everyone, it's about challenging the right ones. Auth0 uses machine learning models, tailored to login and signup to increase bot detection accuracy. By analysing **over 60 real time signals, less than 5% of legitimate users were shown a challenge** (based on average Auth0 traffic).

When bot challenges are needed, select from an array of native and pre-integrated third party options to suit your risk level and user experience needs. Auth0's native Auth Challenge offers a CAPTCHA free user experience and uses risk signals like browser characteristics, device information, IP address reputation, and behavioral patterns to verify the user.



Tenant Access Control List (ACL)

With self-service controls, you can proactively allow, block or redirect known suspicious or unwanted traffic — like certain IP ranges, ASNs, or even entire geographies— before it reaches your login box. Think of it as putting guardrails at the edge of your tenant. This allows you to protect your tenant from known threats, and even help conserve rate limits.

JA3 / JA4 Fingerprinting

When assessing traffic, go beyond traditional IP-based filtering with TLS fingerprinting to detect even more suspicious clients and evasive bots. These signals identify client software and correlate related malicious activity across changing IPs and sessions.

Monitor Mode

With Auth0, you can observe how identity security features would affect real application traffic without actually impacting it, which allows you to fine-tune policies like bot detection or Tenant Access Control Lists in a risk-free environment. You can evaluate their impact, optimize configurations, and roll out protections with confidence, without disrupting the user experience.

With Auth0, Cinépolis achieved a **16% reduction in fraudulent transactions** that stemmed from both fake accounts and unauthorized use of rewards from legitimate accounts.[6]

With Auth0's bot defenses, create less friction for real users to drive greater long-term value, while targeted friction for bots reduces fraud and safeguards your bottom line.

Ready to level up your security posture?

Get the tools you need to secure users.
https://auth0.com/platform/login-security