kasada

Bot Mitigation Reimagined for Retail & eCommerce

Retail bot attacks have grown 106%

Where there's a will, there's a way - and cybercriminals have their sights set on copping the latest retail items, stealing loyalty points, swiping payment information, and much more. In the past few years, their efforts have grown in size and complexity, maneuvering around many "leading" bot management solutions on the market and leaving organizations vulnerable.

Most solutions can't keep up

Rule-based, static defenses aren't agile enough to respond to adversarial retooling and reverse engineering. First-generation detection systems rely on IP blocking, device fingerprinting, and rate limiting which have become frustratingly ineffective to detect modern bots. These methods first let requests in to look for suspicious activity but by then it's already too late.

A better approach - simple yet effective

It's time to stop bad bots for good. Protect your customers, revenue, and data from automated attacks in real-time with an easy-to-use solution. Up and running within 30-minutes, Kasada adapts as fast as attackers, frustrating and striking back at them to destroy their profits.

- → Real-time detection
- → Invisible defenses
- → Long-term efficacy
- → Actionable insights

Protection from login to checkout

1 Login
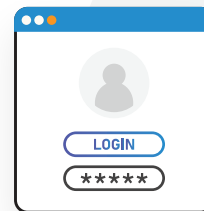
Protect against:
- Credential stuffing
- Fake account creation
- Account takeover

2 Browse & add to cart

Protect against:
- Skewed metrics & analytics
- Poor site performance
- Inflated infrastructure costs
- Web, price, and content scraping

3 Checkout

Protect against:
- Denial of inventory
- Loyalty, reward, and payment fraud
- Promotion abuse

Get Kasada

Kasada has been leading the fight against advanced bots. No management, no maintenance, no rules, and no risk scores - just a simple solution to turn on.

30 min
Deploys within 30 minutes

Easy to use
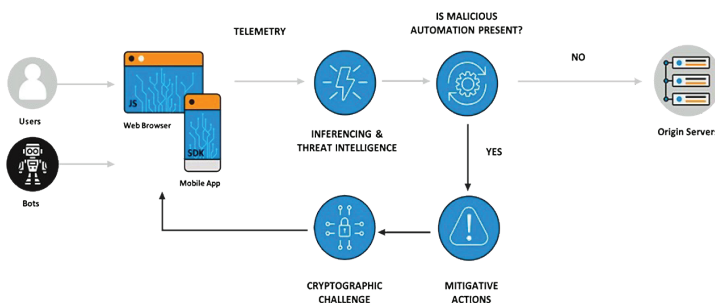
24/7
24/7/365 customer support

Stop bots without a CAPTCHA

Keep your customers happy and improve conversions by removing points of friction - making it easier to create new accounts, log in, and checkout. Kasada works invisibly behind the scenes to stop automated threats, so your customers never have to solve a CAPTCHA again.

How Kasada works

Kasada assumes all requests are guilty until proven innocent. Using telemetry data, threat intelligence, and behavioral data, Kasada accurately detects malicious automation before it enters your site. To remain effective over time, Kasada created its own proprietary language and obfuscation to protect against reverse engineering.

For every one second delay in website traffic, conversion rates drop 7%

Users · Web Browser · Mobile App · Bots · TELEMETRY · INFERENCING & THREAT INTELLIGENCE · IS MALICIOUS AUTOMATION PRESENT? · NO · YES · Origin Servers · CRYPTOGRAPHIC CHALLENGE · MITIGATIVE ACTIONS

Why Kasada

90% more effective

Better protection than rule-based solutions

60% more conversions

Better conversion rates from happier customers

71% IT cost reduction

Lower data center and infrastructure costs

Kasada was implemented in just minutes, and immediately neutralized our flow of attacks. Amazed by how simple and immediately efficient the solution was.

Regan MacDonald, True Alliance

Kasada has been instrumental in the success of our highly visible flash sales.

Senior Director of eCommerce

About Kasada

Kasada provides the easiest and most effective way to defend against advanced persistent bot attacks across your web, mobile, and API channels. With Kasada, trust in the Internet is restored by foiling even the stealthiest cyber threats, from credential abuse to data scraping. The solution invisibly stops automated threats while inflicting financial damage to attackers, destroying their ROI. With the ability to onboard in minutes, Kasada ensures immediate and long-lasting protection while empowering enterprises with optimal online activity. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, please visit www.kasada.io and follow us on Twitter, LinkedIn, and Facebook.