kasada

Why Bot Management Needs To Be Reimagined

When a bot attack isn't stopped by your bot management vendor, why are you as the customer held accountable?

While security and tech professionals accepted these problems as the status quo, we've been determined to find a better way.

If you're tired of fighting the bots on your own, or just have questions about how our solution works, feel free to get in touch with me or a member of our team to see Kasada in action.

Sam Crowther
Founder,
Kasada

1 Reactive in blocking automated threats

Rule-based, static defenses will never be agile or quick enough to respond to retooling and reverse engineering.

2 Too expensive and difficult to use

Requires full-time expertise to configure, manage, and maintain (rules, policies, risk scores, response types).

3 Doesn't offer long-term protection

Effectiveness wanes quickly as defense upgrades are rolled out slowly, but only take days to bypass, creating a never-ending cycle.

4 Negatively impacts UX and conversions

Reliance on CAPTCHAs and visual challenges add friction while the bot operators easily work around them.

5 Inhibits the visibility into your data

Shows only what threats are blocked leading to slow responses, false positives, and difficulty troubleshooting.