kasada

DATA SHEET

Challenging the Economics of Automated Attacks and Giving Control Back to Human Beings

The Sudden Shift to Digital Business

The world's businesses have abruptly and massively shifted to a digital approach to support work from home as well as online shopping, banking, and life in general. The resulting surge in online activity, concomitant with a huge increase in web and online traffic, has given bad actors boundless opportunities to launch malicious bot attacks, including data scraping, account takeover, and distributed denial of service (DDoS).

In fact, multiple research surveys show that malicious automation accounts for a sizable percentage of login attempts in general—40% and greater, depending on the industry. That statistic is backed up by Kasada research, which shows that 86% of Australia's top 250 websites failed to detect a script loading the login page and 90% failed to prevent an automation tool from submitting credentials. Meanwhile, global security and business leaders still need to protect their companies' most fundamental assets: customers, brand, and IP as well as to defend revenue, margin, and stock value.

The companies winning the battle against malicious automation and synthetic traffic are choosing an easy-to-implement, low-maintenance solution with a low total cost of ownership (TCO) that unequivocally demonstrates immediate and long-term efficacy on web, mobile, and API channels. They're choosing Kasada.

Introducing Kasada

Kasada is an online traffic integrity solution that protects your company against the damaging, often underestimated effects of malicious automation across your web, mobile, and APIs. Kasada offers a cloud-based service along with an embedded, immersive 24/7 customer support via an "always on" chat channel, putting no extra maintenance burden on your internal team.

Unlike alternative solutions that provide incomplete, easy-to-detect, and inefficient bot mitigation tools (which are not only costly to deploy and maintain but also add friction and latency to the user experience), Kasada:

- Makes bots, not humans, do the work, by cleverly deterring synthetic traffic with a cryptographic challenge that makes it arduous and expensive for bots to continue their attacks, while remaining imperceptible to (and requiring no action from) end users.
- Is extremely efficient, easily implements within minutes, and demonstrates clear ROI across multiple departments.
- Is highly effective, delivering the best detection and lowest false positive rates in the market today.

How Kasada Works

Using proprietary techniques, Kasada presents a myriad of obstacles to frustrate and disrupt the operating model of bot attacks, preventing hackers from using automation and challenging critical aspects of the attack process.

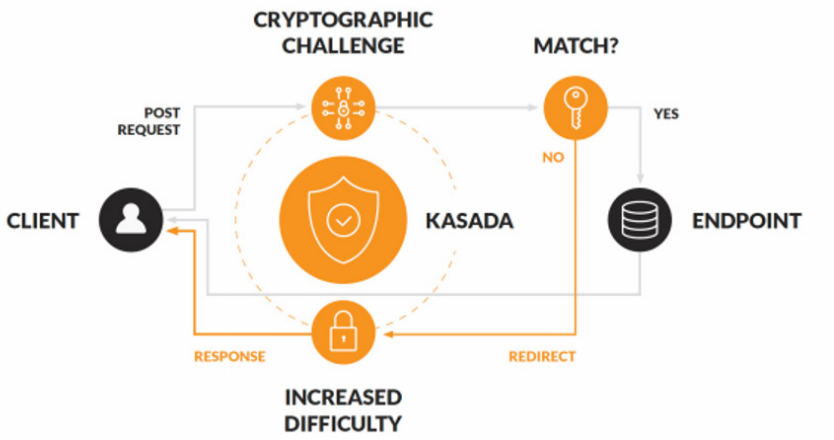

Figure 1: How Kasada Works

Kasada is architected as an alternate origin for sensitive application components. Sensor detection technology with advanced Javascript inspection processes immediately detects bots and categorizes them as benign or malicious. A cryptographic browser-based challenge is used as a proof of work that exponentially increases the difficulty level with the number of abusive requests over time, therefore exhausting the CPU resources of bad bots, without informing the attacker. This forces the attack to permanently cease, as its ROI inevitably collapses. Not only does Kasada neutralize the attack long-term, but also prevents the bot operator from quickly retooling or attacking other targets, as all CPU resources have been exhausted. Fraudsters then stay away from Kasada-protected properties, as it costs them virtually unlimited resources trying to break in.

Primary Use Cases

Kasada efficiently and effectively combats all types of login fraud and scraping fraud:

DATA & LOGIN FRAUD

Credential stuffing, account takeover, fake users, financial fraud, credit card checking, fraudulent payment testing, credit card skimming, game hacking, ad click fraud, denial of inventory, service disruption and denial of service attacks, malware infection, bringing down of vital network infrastructure, and more.

SCRAPING FRAUD

Data theft and illegitimate content scraping, ticket scalping, auction abuse, stock value manipulation, competitive data scraping, industrial espionage, brand extortion, mass dissemination of spam and fake news, fake reviews, spam, opinion manipulation, and more.

Benefits of Using Kasada

Kasada has been leading the fight with novel approaches and cloud-based technology to detect and mitigate the maelstrom of malicious traffic that other security platforms can't:

ALMOST IMMEDIATE TIME-TO-VALUE:

- Stops attacks from the first page load request
- Offers time-to-value within 30 minutes
- Inexpensive to install and manage: cloud-based, no hardware required
- Can be deployed selectively for specific use cases or lines of business

FRICTIONLESS CUSTOMER EXPERIENCE:

- Invisible to end users
- Virtual zero false negatives
- 0.001% false positives
- No CAPTCHA
- Complements most existing fraud solutions
- CDN-agnostic

LONG-TERM EFFICACY:

- Provides world-class obfuscation
- Delivers immutable evidence of automated attacks
- Offers continuous mitigation
- Optionally penalizes attackers

BUSINESS VISIBILITY

- Completely removes malicious bot traffic, enabling accurate marketing KPIs

What Our Customers Say

At Hyatt, our purpose—we care for people so they can be their best—informs all business decisions, including our technology investments. When evaluating technology providers, we selected Kasada's solution for its innovative architecture and its immersive 24/7 customer service that is best characterized as 'embedded.' As a global hospitality brand that welcomes travelers from all over the world, it's critical that we collaborate with technology providers that understand our immediate and long-term imperatives, and we truly value the way Kasada's product further strengthens our technology systems and platforms that our guests use every day."

— BENJAMIN VAUGHN
Vice President and Chief Information Security Officer, Hyatt Hotels

Since Kasada is implemented in line, we scrutinized its performance and business impacts on our online activity. Not only has its false positive rate remained below 0.01% since inception, but we never had a missed attack to report. As for our customer experience, we were expecting some increased latency, but Kasada, in fact, surprised us with just the opposite. It offloaded all synthetic traffic and improved our customer experience."

— KEN KENNEDY
Group Head of Digital, True Alliance

The entire team was so amazed; we had never seen such fast, immediate ROI on a security tool. In just under 30 minutes, we set-up, turned on, and stopped the attack. It was an out-of-the-box experience with instant results. Kasada is a partner that has overdelivered."

— NIKITA PINCHUK
VP Global Engineering, PointsBet

We'd love to demonstrate the Kasada difference to you; please request a demo today.

About Kasada

Operating globally since 2015 and trusted by enterprises worldwide, Kasada gives internet control and safety back to human beings through its category-defining traffic integrity solution for web, mobile, and APIs. With Kasada, even the stealthiest cyber threats are foiled, from login to data scraping across web, mobile, and API channels. Scalable up to multi-billion-dollar companies, onboarding in just minutes, and designed to deliver clear ROI in multiple departments, Kasada's solution invisibly defends and enhances critical business assets while ensuring optimal online activity, with immediate and lasting web traffic security. Kasada is based in New York and Sydney, with offices in Melbourne, San Francisco, and London. For more information, visit www.kasada.io.