kasada

Kasada Bot Detection and Mitigation

The easiest and most effective way to defend websites, mobile apps, and APIs against advanced bot attacks.

Malicious Automation

Bad bots are estimated to make up half of all Internet traffic within the next few years. According to Verizon's 2021 DBIR, 61% of breaches involved credential data; 95% of organizations suffering credential stuffing attacks had between 637 and 3.3 billion malicious login attempts through the year. These trends are accelerating as businesses of all industries and sizes massively shift to a digital approach. Automated threats and malicious automation include the following:

- Credential stuffing and abuse that leads to account takeover
- Fake account creation, login fraud, payment fraud, carding fraud that result in fraud losses
- Checkout abuse, denial of inventory, sniping and scalping that greatly reduce the availability of inventory to legitimate users
- Application denial of service, resulting in service disruption and bringing down network infrastructure
- Data theft and illegitimate content scraping and price scraping fraud and abuse – which can be conducted by competitors or bad actors

Bots Are Rapidly Evolving

In order to evade anti-bot defenses, bot operators continue to evolve their methods. In an attempt to look and act like humans, adversaries use open source DevTools, stealth plugins, anti-detect browsers, and residential proxy networks.

Most Solutions Can't Keep Up

First-generation detection systems rely on IP blocking, device fingerprinting, and rate limiting which have become frustratingly ineffective to detect modern bot operations. They must let automated requests in to look for suspicious activity that fly beneath the radar. It's already too late.

A New and Better Approach

A modern approach accurately identifies and stops malicious automation before it's ever allowed to enter your infrastructure, by detecting malicious automation client-side in real-time by assuming every request is guilty until proven innocent.

Introducing Kasada

Kasada provides the easiest and most effective bot detection and mitigation solution. The Kasada platform 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 and puts 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

Kasada adapts to new threats in real-time. It's resilient to retooling, and strikes back by making attacks too expensive and arduous to conduct.

Client Interrogation

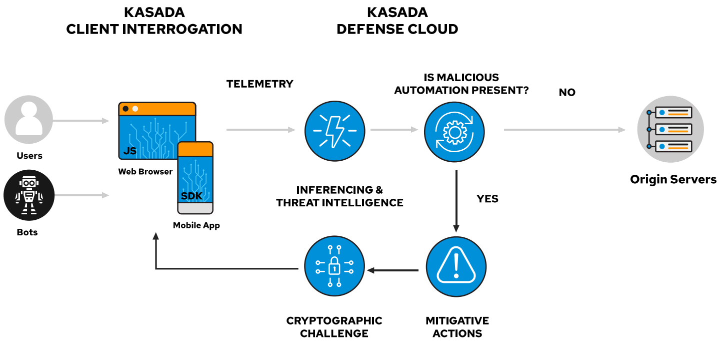
- **Client interrogation** - inspects all client requests for the immutable evidence of automation that bots leave when interacting with applications
  - A client inspection process invisible to humans
  - Looks for headless browsers and automation frameworks
  - Inferencing determines if the request is from a human, bad bot or good bot without having to let requests in
  - Sensors are obfuscated with our own polymorphic method to deter reverse engineering attempts

Mitigative Actions

- **Customizable responses** - designed to deceive bot operators while making bot attacks too expensive to conduct at-scale
- **Cryptographic challenge** - clients must solve an increasingly difficult asymmetric cryptographic challenge as proof of work
- **Fights automation with automation** - expensive work and exhausts compute resources, without the adversary knowing

Threat Intelligence

- **Threat intelligence** – deep analysis of adversarial techniques and traffic patterns by analyzing all request and sensor data
  - Sophisticated data-based models for layered defense
- **Dynamic script injection** - learnings from our data are added to the client inspection process in real-time without the need for code upgrades
  - Allows for instant defense updates and continuous feedback



Benefits of Using Kasada

Kasada has been leading the fight with novel approaches and cloud-based technology to mitigate advanced bots that other security platforms can't:

Time-to-Value

- Immediately detects advanced bots without custom rules or tuning
- Deploys and provides time-to-value within 30 minutes

Long-Term Efficacy

- Stops attacks from the first page load request, including new bots
- Remains effective by frustrating attackers and fighting back

Simplicity

- Easy to use, manage, and integrate into your existing tech stack
- Little to no maintenance is needed
- Invisible to users; no CAPTCHA

Business Visibility

- Cleans up skewed data to enable accurate web metrics
- Provides actionable insights
- 24/7/365 customer support

85%

of our customers were using other bot mitigation providers prior to contacting us

Billions

of dollars protected for eCommerce organizations on a monthly basis

5 Billion

monthly requests stopped that were left undetected by systems in front of us

What Our Customers Say

> *We find Kasada to be one of our most valuable controls within our ecosystem.*
>
> **Benjamin Vaughn, VP & CISO, Hyatt Hotels Corp**

> *With Kasada, we're able to quickly and effectively stop malicious bots targeting our login APIs used across websites and mobile apps.*
>
> **Dick Ward, Head of Cyber Security, Sportsbet**

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.