kasada

CASE STUDY

Flybuys Australia Achieves Online Traffic Integrity with Kasada

How Australia's most popular loyalty program optimized customer experience while foiling login fraud and account takeover attacks

flybuys

Established in 1994, Flybuys is Australia's most popular loyalty program, helping Australians to enjoy a wide range of rewards and benefits when they shop. Flybuys is committed to serving its 8.7 million active members with new and exciting ways to engage with the program. Flybuys points can be collected across 22 participating brands making up 25% of Australian retail sales including Coles, Kmart, Target, AGL, and Optus. Flybuys also allows members to collect points via its financial, insurance, and travel services partners. Flybuys is a joint venture between Wesfarmers and Coles but operates independently. After 25 years, Flybuys has recently entered an exciting new phase of growth, with a renewed focus on product development and innovation to continuously improve our members' experience.

But with innovation comes challenge. With so much traffic logging into the site via web and mobile, the company had no clear way to determine how much of that traffic was human and how much was synthetic bot traffic. That's an important distinction, as Flybuys was particularly concerned about protecting its login pages from bot traffic and mitigating possible account takeover attacks. Account takeover is a growing concern for Flybuys' online activities, knowing losses topped $5.1 billion in the U.S. alone in 2018, according to Javelin Strategy. Given Flybuys' priority on protecting its members' accounts, the company needed to find a solution to stop bot attacks in their tracks while providing the best customer experience possible.

THE PAIN: No Visibility Means No Control

When Flybuys found itself in the position of not having a clear picture of its online traffic, it had plenty of company. In fact, recent Kasada research 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.

"While we had some internal capacity to monitor user credentials, we needed a better understanding of who—or what—was logging into our online properties," said Anthony Martino, IT Operations Manager at Flybuys. "We were mostly concerned about synthetic traffic, and whether that traffic was being weaponized against us in credential stuffing attacks for account takeover."

> *Kasada worked proactively with us to demonstrate the platform and its immediate value. As a result, back in 2018 Flybuys was the first Coles' business to roll out Kasada. From the moment we switched on the platform, there was immediate feedback on the number of page requests that were bot-driven, and I can tell you Kasada neutralized them from the very first page load request. When a bot attempts to attack us, it ends quite quickly. This has enabled us to provide a secure customer experience without the added friction normally found in other solutions."*
>
> — **PHIL HAWKINS,** Chief Operating Officer, Flybuys

Another way synthetic traffic can be used against a business' online assets is through a distributed denial of service attack (DDoS), in which normal traffic is overwhelmed by malicious automation.

"Multiple businesses had suffered from DDoS attacks, even though they were relatively minor," noted Alex Loizou, Head of Security at Flybuys. "But it was enough for us to start looking for better solutions and that's how Kasada came into view."

THE SOLUTION: Kasada Online Traffic Integrity Solution

Once Flybuys found Kasada for DDoS attacks, the company realized the company could also help protect against other forms of malicious automation such as account takeover and loyalty points abuse, integrated as a single service. They entered into a proof of concept and immediately benefited, moving to full production shortly thereafter.

Kasada provides customers like Flybuys with visibility into all of their traffic, not just the bots stopped. Not only can Flybuys detect bot attacks as they happen but also gain critical insight into real customer traffic to improve the customer experience. Customers also use Kasada's analytics to report accurate KPIs, optimize marketing return on investment, increase sales, and protect their brand reputation and shareholder value.

THE GAIN: See All Traffic and Stop the Bad Bots

Flybuys chose Kasada based on its elegantly simple and superiorly effective technology, experienced team, and surprisingly affordable price. Since implementing Kasada, Flybuys is able to:

- Achieve greater visibility into all of its traffic—human *and* synthetic (good or bad)
- Defend against bot-based attacks, specifically credential abuse
- Reduce the amount of synthetic traffic to the site, resulting in better site performance
- Stop account takeover attacks and protect member information
- Provide the best, most secure customer experience possible
- Neutralize bot attacks from the very first page load request
- Protect its users while providing an optimal experience without the use of CAPTCHAs

> *The level of engagement we get from the Kasada team and the further investigations they have undertaken on our behalf to help us deal with threats has consistently exceeded our expectations. The solution works as advertised with an ease of implementation that is clearly different from the competition. We also appreciate Kasada's behavioral-based approach. Even as we have undertaken re-platforming activities, Kasada has provided a secure, bot-resistant front door to all of our online assets."*
>
> — **ANTHONY MARTINO,** IT Operations Manager
> Flybuys

More About Kasada's Online Traffic Integrity Solution

Kasada's online traffic integrity solution protects companies against the damaging, often underestimated effects of malicious automation across their web, mobile, and API channels. 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.

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 online traffic integrity solution. 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, onboarded 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.