kasada

Case Study

AGL secures its business with Kasada

How a leading investor-owned provider of electric energy accelerated its digital transformation planning and ramped up business optimization with the help of Kasada's bot detection and mitigation solution.

agl

THE BACKGROUND

AGL Energy is a leading integrated energy business that operates Australia's largest private electricity generation portfolio, with a total capacity of 10,413 megawatts.

The 180-year-old company accounts for approximately 20% of the total generation capacity within Australia's National Electricity Market, serving 3.7 million customers, including residential, small and large business, and wholesale customers.

As the online economy became increasingly bombarded by rampant malicious bot and scraper traffic in 2017, AGL sought to accelerate its digital transformation planning. In order to ensure that its accounts and IP were solidly protected and its platform fully optimized, the company turned to Kasada.

THE PAIN

AGL was keeping a close watch on growing industry-wide online automated threats that could affect them — such as payment fraud and scraping (some of which was generic scanning, and some was more elusive). The key concerns were to mitigate the risk of backend payment fraud at their payment gateway and to protect pricing IP on their quoting engine.

The company had done a proof of concept with a leading bot manager, largely centered on two business use cases. Firstly, they were looking at where they were exposing pricing information and how to protect its quoting from reverse-engineering on the pricing engine. Secondly, they sought to protect the payment gateway from fraudulent activity.

AGL wanted to avoid a classic legacy scenario wherein relying on blunt controls such as WAF for geo-blocking leads to a constant cat-and-mouse game. The company had found previous providers lacking in effectiveness and in their ability to explain problems, as well as being very expensive.

> *Cleaner traffic means cleaner data. When you stop automated traffic from hitting backend servers, you get a better view of who your customers are and how much traffic is actually human. You get right-sizing on the backend, which gives you a better view of marketing. Prior to Kasada, it was a little bit all over the place. More accurate data enables a better view of site traffic and in turn enables you to work out target segments more effectively."*
>
> **— Heng Mok, CISO, AGL Energy**

THE SOLUTION

To prevent unwanted traffic from reaching the threshold of unacceptable levels, AGL knew it needed to act fast. Kasada provided immediate relief.

“We were about to commence a POC with Kasada when we got hit hard by a large-scale automated attack, said Heng Mok, CISO, AGL Energy. “Slotting the technology in under an actual security incident and putting it through its paces proved what Kasada could do right out of the box. Instead of chasing after constantly morphing bots and scrapers, with Kasada we are able to use the crypto piece to smash that infrastructure—just blow them up. Essentially, we now have a deterrent control that inflicts a whole lot of pain on the bot and scrapers’ backend and on their costs. They move on to an easier target.”

“Additionally, with cleaner traffic we were immediately able to identify poorly written applications and to solidify Request for Comment (RFC) standards throughout our channels,” said Mok. “Another benefit is analytics.”

THE RESULTS

AGL selected Kasada to protect their intellectual property while cleaning up their web traffic metrics throughout their digital transformation. Since implementing Kasada, AGL has realized multiple benefits including:

- Stopping attacks and having the control and flexibility to tune the product during attacks
- Having the ability to take swift and decisive action to remediate, rather than ride out problems with existing and pricey solutions, paying an even higher price later
- Exposing inadequate applications and ensuring RFC standards and best practices, triggering savings that paid for the product for five plus years forward
- Eliminating payment fraud at the gateway by constantly cleaning and washing away bad traffic, improving the customer journey without introducing latency
- Protecting pricing IP on the quoting engine by foiling reverse-engineering price scrapers

> *We've started to put Kasada across all our channels, across API, across mobile, across all the other areas including our customer identity system to protect against credential harvesting. While the initial use cases were business-driven, we've extended Kasada over time, and now it works hand-in-hand with our CDN across our whole digital ecosystem.”*
>
> **— Heng Mok, CISO, AGL Energy**

- Diminishing bot and scraper ROI, thereby immediately improving in-house ROI
- Right-sizing traffic and thus right-sizing backend resources
- Achieving clean data via triaging human versus synthetic traffic, thus enabling better market segmenting and more targeted marketing spend
- Being able to rely on solid, ongoing service and quality support by a solutions partner that proactively reaches out to provide help in shaping roadmaps and ensuring fast, needed outcomes

“The number of transactions and dollar values we saved with Kasada were immediately apparent,” Mok concluded. “We've started to put Kasada across all our channels, across API, across mobile, across all the other areas including our customer identity system to protect against credential harvesting. While the initial use cases were business-driven, we've extended Kasada over time, and now it works hand-in-hand with our CDN across our whole digital ecosystem. With Kasada we are getting the service and outcomes that we need.”

MORE ABOUT KASADA’S BOT MITIGATION

Over 85% of our customers were using other bot mitigation providers prior to contacting us. We stop billions of monthly requests bypassed by systems in-front of us.

About Kasada

Kasada provides the most effective and easiest way to defend against advanced persistent bot attacks across 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.