kasada

REA Group defends its digital assets with the help of Kasada

How a leading digital advertising company optimizes its business decision-making and data strategy by ensuring superior online protection, authentic traffic, cleaner metrics, and better analytics with the help of Kasada's online traffic integrity solution.

REA Group™

REA Group Limited is a leading digital enterprise specializing in real estate. A public company, REA is listed on the Australian Securities Exchange and is an S&P/ASX 200 company. The Group operates Australia's premiere residential and commercial property websites realestate.com.au and realcommercial.com.au as well as market-leading property sites in Asia and other property sites and apps globally.

The key challenge for any online property company is the safeguarding of its listings data while providing excellent customer experiences. Protecting and maintaining control over online assets and ensuring the authenticity of traffic without compromising the customer journey are constant concerns. Defending valuable data against bot attacks and aggressive scraping by commercial research companies and competitors has become essential to succeeding in today's digital business environment. REA prides itself on keeping pace with the rapidly evolving technology and exceeding its audience expectations. In order to strengthen its online defenses against threats to data security while maintaining its online experience, REA was on the look-out for an outstanding online integrity solution.

THE PAIN: Differentiating between genuine and malicious traffic

REA recognizes and strives to stay ahead of two of the most essential challenges facing online enterprises – visibility and protection while maintaining an amazing user experience.

First, without good visibility and clean data, metrics and analytics can be polluted with noise.

"A better understanding of synthetic traffic greatly improves our telemetry and analytics", said Craig Templeton, CISO & GM, Group Technology Platforms, REA. "Having a high level of data integrity is important for our market and audience. By quantifying bot from legitimate traffic, we can have high levels of confidence in our metrics. Traditional bot mitigation products and strategies are not up to the task due to the thriving data acquisition industry."

Second, unsanctioned automation acting against organizations such as REA impose arbitrary costs and impact user experience by consuming resources devoted to serving a legitimate audience.

> *Commercial scrapers have significant resources to devote toward their business. It's difficult to have a data monetization strategy if competitors are able to acquire your data assets for free. At REA, we have committed significant resources towards building value from the data and the insights that we have. It's unreasonable for other actors to leverage, monetize and deriving their own insights on that investment without our consent. A good product must protect our business and growth strategy."*
>
> **— Craig Templeton,** *CISO & GM, Group Technology Platforms, REA Group*

THE SOLUTION:
Quick-to-deploy traffic integrity with Kasada

The REA team knew that traditional defenses such as CDN, WAF, and other cybersecurity bot mitigation solutions would fall short of adequately addressing current online challenges. "At REA we have a policy that you can't deploy a public-facing authentication endpoint without having anti-automation protection," said Templeton.

REA noted that some vendors were offering endpoint authentication without a clear bot mitigation strategy, and thus, requiring internal engineering development and integration time. In Kasada, REA found what they considered to be both a superior product and a passionate service team that could fully support REA's high-performance standards and growth-minded goals. Kasada provided a solution that would not only rapidly deploy and have the capability to fight everyday intrusive bots as well as a plethora of sophisticated commercial scrapers and other elusive actors, without draining engineering and development resources or burdening the end user.

THE GAIN: Improved Insights and Business Growth

REA selected Kasada for its high-visibility traffic integrity solution with a business-growth model that goes beyond marketplace competitors. Since implementing Kasada, REA Group is able to:

- Achieve protection of its online assets while delivering a superior customer experience.
- Ensure authenticity of portal traffic by blocking very sophisticated and persistent synthetic traffic, swiftly and efficiently, at public endpoints.
- Further subvert bot and scraper efforts by also foiling synthetic countermeasures.
- Maintain a below .001% false positive rate without adversely impacting legitimate traffic.

Kasada is more than an anti-bot insurance provider. Rather than mere protection, Kasada supports our business growth. The analytics module provides better insights and visibility stripped of synthetic traffic. We know with Kasada we're looking at real traffic, which means real data and real tools for strategic decision-making and future data monetization."

— **Craig Templeton,** *CISO & GM, Group Technology Platforms, REA Group*

- Provide tech teams with a rapid response capability when confronted with bot attacks.
- Help back-office teams with access to swift, reliable, 24/7 solution support.
- Improved analytics and resulting insights.
- Support the business teams and the organization's growth strategy.

"Kasada's brand proposition is all about giving back control and web integrity, and that's proven to be exactly right. Kasada provides tremendous visibility. When you have visibility, you can make better decisions. You have control over traffic and, therefore, more accurate data. With more and better data, you can correlate with other data sources. Your CISO might have specific tactical use cases, but the chief digital officer, the chief marketing officer, and other revenue-generating parts of the business may also be able to leverage that information to bring growth into your company and support enterprise vision and ambitions."

Kasada and AWS

Since 2015, Kasada has leveraged the AWS Cloud to build and host their advanced bot mitigation solution used in this case study. Kasada integrates seamlessly with AWS services requiring only a single routing change to direct traffic from the AWS Edge to Kasada.

About Kasada

Kasada provides the only online traffic integrity solution that accurately detects and defends against bot attacks across web, mobile, and API channels. With Kasada, internet control and safety are given back to human beings 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.