approov
API THREAT PROTECTION

CASE STUDY

RACING POST

Protecting Proprietary Data

Racing Post relies on controlling access to its racing form data. Loss of that proprietary data means loss of customers and revenue. As the company launched its new native mobile app, Approov API Threat Protection was rapidly deployed to protect their cloud-based mobile API from data scrapers and cloned apps, protecting sensitive data and providing a secure foundation for the creation of additional digital products.

The Client

Racing Post is the authority on racing and betting in the United Kingdom. Their mission, says Stephen Gorton, Technical Solutions Architect, is to "transition from a traditional newspaper business to a multi-channel digital company who puts its customers at the heart of everything we do". They have been successful in achieving this transition in spite of strong competition from the many media companies who are also facing the challenges of transitioning to digital. At the 2013 British Media Awards, the *Racing Post* mobile app was named "Digital Product of the Year" and the iPad Daily Edition won the "Launch of the Year" prize.

Racing Post is now focused on driving content sales and betting through their existing consumer products while growing a sustainable and strong B2B digital business. Once this model is firmly established in the United Kingdom, *Racing Post* will push their digital offering to the international community, broadening their coverage beyond horse and dog racing into other sports.

The Challenge

Given the value of their proprietary data that was now available on the internet, it was not long before the scrapers hit the *Racing Post* app — even behind a private mobile API. The seriousness of losing customers and revenue was becoming a concern.

> ***"We have a substantial number of customers who use our iOS and Android apps for betting." Stephen explained. "We found that there were a number of Android app clones that were attempting to make use of our unique data. We also found a number of sophisticated data scrapers, trying to gather daily and historical information that we generate and make available solely to our app subscribers".***

The problem continued to grow. So the *Racing Post* team began looking for solutions.

"We wanted to secure our data to the point where only our apps could seamlessly access it, but quickly deny any other unauthorized source from accessing our API data content," Stephens added.

The engineering team developed several methods to limit the number of app clones

"It did everything we required. We did not find an alternative and we managed to successfully implement Approov inside our environment in a small amount of time."

– Stephen Gorton, Technical Solutions Architect but found they could not completely lock down access at the level they required to make certain that customers and revenue were retained. They looked at various existing methods but it became clear that any cloner or scraper with good knowledge and resources could breach these systems.

How Approov API Threat Protection Helped

Racing Post had a tough problem to solve and they struggled to find a commercial offering that could provide the level of security that they needed to tackle the more sophisticated attacks.

"We came across approov.io, researched the system, looked at how it works, analyzed its cost-base, ease of implementation into our iOS and Android app codebase, reviewed the documentation, and support processes. It did everything we required. We did not find an alternative and we managed to successfully implement Approov inside our environment in a small amount of time," stated Stephen.

The Approov SDK was integrated into their iOS and Android apps. On the server side a new API was created using the AWS API Gateway so the Approov token check was implemented in an AWS Lambda function and deployed as a Custom Authorizer for the API Gateway. This implementation allowed their API to continue to handle up to 10,000 requests per second.

The Results

Once deployed as a Custom Authorizer, ***Racing Post***'s API Gateway effectively recognized traffic from authorized apps and blocked all requests from data scrapers and cloned apps. So well in fact, that the number of rejected requests has greatly reduced over time as attacks have been unsuccessful.

Following the initial deployment to protect their dynamic racing data, ***Racing Post*** has also successfully implemented an Approov signature check to authorize access to their static data via their CDN edge (Cloudfront & Fastly). Now only their apps can access ***Racing Post*** static data ranging from news to images to referencing static JS/CSS code.

"Because of the success of Approov, we have also created our own in-house static JWT system for our fixed B2B partners", comments Stephen.

"We are now looking at using Approov to generate keys and tokens required for our other secure data systems, using the Approov token as an authorizing method for access".

Summary

Approov provided both the protection ***Racing Post*** needed to secure their valuable data and protect revenue as well as enabling their company to implement additional features to their apps with the peace of mind that their API is secure.

According to Stephen, some of the key points that make Approov the right choice for ***Racing Post*** include:

"The ability to set up a fully functioning test app at zero cost to test."

"Quick support for any queries relating to the service."

"Up-to-date SDK and documentation."

approov

To see Approov API Threat Protection in action and get more information, contact us for a free demo.
www.approov.io