CASE STUDY

Moving From A Web To A Full API Platform Requires New Security Solutions

"Knowing what is calling your API is a necessary element to protect your mobile channel against scripts and bots trying to negatively impact your revenue streams."

— Alexandre Branquart, CIO/CTO

Deindeal is one of the largest e-commerce portals in Switzerland and is part of the Ringier group. The company has received numerous awards for its business, including the prestigious Swiss E-Commerce Award. Following the acquisition of MyStore, Deindeal has been able to extend its strong market position throughout Switzerland. Its range of products includes exclusive brand products, travel deals and local deals - all with high discounts.

The Challenge

Deindeal's e-commerce business has grown fast, covering an increasingly wide range of product sectors, and the rising use of their mobile apps. These factors created a realization that the underlying platform, based as it was on web technologies, needed to be upgraded to keep pace with the business growth.

One of the primary architectural changes which the company decided to implement as part of the upgrade project was to move to an API based platform.

Based on previous experience, Deindeal is very familiar with the threats associated with bots scraping valuable data from websites. Exfiltrated data such as catalog product availability and pricing can be used by competitors to undercut market prices, directly impacting revenue and profitability. Bots can also affect revenue because they can spoil the buying experience for genuine customers through automation of account onboarding, account takeover through credential stuffing activities, or high speed bidding for limited issue items.

As the company evolved its platform architecture, the team was very conscious that the introduction of APIs might expose the business to a new range of automated attacks via bots or scripts. Alexandre Branquart, CIO/CTO & Co-Founder, picks up the story:

> ***"Having a WAF with bot detection built-in worked well for us when we had a web based platform. The browser gives you some context to help you to spot bad bots. Moving to APIs means that you have no context through which to identify automated traffic. It was clear that a new security solution would be needed for our API based platform."***

Further, the team recognised that the web and mobile API endpoints would need different solutions so they started to research the alternatives. App hardening/obfuscating was initially considered a good option but it was recognised that this approach protected the app but did not protect the servers to which the app connects. Behavioral API

traffic analysis was also considered but it was felt that it would be better if automated traffic could be identified at the edge of the network, as early as possible in other words. Therefore the conclusion was reached that a methodology which could prove the presence and authenticity of the mobile app at the point of the API request was the right answer.

How Approov Mobile Security Helped

Approov was added to the Deindeal platform to specifically ensure that only genuine mobile app instances could use the API. This was directly to address the risk of scripts impacting revenue by impersonating app traffic - in order to scrape product data and then buy up high demand items, or to commit other fraudulent acts.

The company took the view that making the Approov token check at the edge of their network was the right approach so that 'bad' traffic could be filtered out as early as possible. This meant implementing the check in the Cloudflare CDN, making use of Cloudflare workers. It was possible to leverage the work of another Approov customer who had already completed a Cloudflare integration as described in this blog post.

Alexandre commented on the team's experience of working with Approov:

> ***"The documentation is excellent, even though the developers didn't need to read it a lot of the time! Other than the product itself, the other aspects of the Approov solution we really appreciate are the real-time analytics, the Command Line Interface (CLI) tool and the deep security knowledge of the support team. We felt that we were in very capable hands."***

The Approov SDK was dropped into the Deindeal native apps and the solution was deployed in short order. In order to gain confidence in the solution, tokens were monitored for a couple of weeks but traffic was not blocked if the token was invalid. This is recommended good practice and once it was clear that everything was working as predicted, blocking was turned on.

Over the air updates have been used to adjust various aspects of the Deindeal security policy - this is 100% in the control of each Approov customer and determines what constitutes a good app and what constitutes a good app runtime environment.

Deindeal continues to grow its business and already has plans to release more apps towards new market sectors such as takeaway food order and delivery, and other B2B opportunities.

We asked Alexandre to summarize the Approov experience for others:

"Approov makes sense. It addresses a specific need for the mobile channel. It's easy to use, easy to implement and it has a great team behind it. I recommend that you try it!"

approov
mobile security

Find out more about Approov Mobile Security
www.approov.io