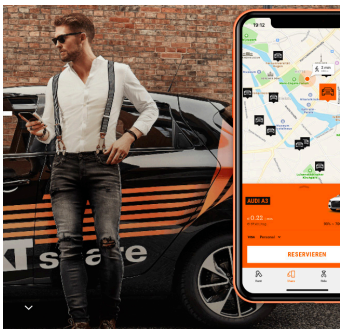
approov
API THREAT PROTECTION

CASE STUDY

SIXT

# SIXT Minimizes the Business Impact of Data Scraping



*"We looked for a solution that could authenticate when API requests were coming from our mobile apps and when they were coming from 3rd party mobile apps..."*

– Nico Gabriel, President, SixtX

Keeping pace with the consumer demand, car sharing has become an increasingly popular alternative to owning — and customers want to use mobile phones to access such services. But mobile API connection data runs the risk of being "scraped" and used by competitors or other third party services. Using Approov API Threat Protection, SIXT was able to lock down control of their API data and build a more secure platform by deploying additional security layers available through Approov.

## The Client

SIXT, established in 1912, was the first car rental company in Germany and is still owned and managed by the SIXT family today. The company has always focused on great customer service and continually improving their offering to meet changing market needs.

There have been significant changes in car ownership and usage patterns recently. In large European cities consumers are choosing not to invest in owning a car but rather take advantage of mobility services, like car sharing. This trend is disrupting the automotive sector — from OEMs to rental operators and all the players in between. SIXT quickly identified these changes as an opportunity to offer mobility services. The company invested significantly in the fast growing car sharing sector, initially with BMW, and more recently as an independent supplier. SIXT Share is now available in most large German cities, with an aggressive road map to rapidly expand services to more cities throughout Europe.

## The Challenge

Like much of the travel industry, car sharing (or ride sharing) tends to attract aggregator companies who offer promotions to help increase traffic and bookings. The design and deployment of APIs has made aggregation even easier but it also has created a significant security risk.

Single API requests can produce large amounts of data and advanced commands can access sensitive functionality. Because car sharing relies on mobile apps for reservations and access to dynamic and up-to-date data on vehicle availability, characteristics and location, SIXT realized that they needed a more secure API to protect their customer data.

> *"In the early days of car sharing, we saw some aggregators popping up and displaying the availability and location of our vehicles. Reviewing our API security arrangements, we realized how straightforward it was to extract this level of data*

©2020 CriticalBlue Limited. All rights reserved. Version 1.1

*and we worried about the possibility that 3rd parties might be able to take a further step and reserve and access our cars via our API," said Nico Gabriel, President, SixtX.*

*"We looked around for a solution which could authenticate when API requests were coming from our mobile apps and when they were coming from 3rd party mobile apps, and that's when we came across Approov. I'd like to emphasize that we are not opposed to sharing data at all, but rather we want to control which data we share and who we share it with - in order to maintain our brand image and direct connection with our customers. Approov gives us that granularity of control."*

## How Approov API Threat Protection Helped

Unfortunately aggregators are difficult to lock down because many enterprise security protocols are based on user authentication using a user name and password. However, in order to access the services that aggregators offer, consumers willingly give up their user credentials. Therefore user authentication protection systems on the API provide very limited security and SIXT understood the risks.

*"Considering the activities of the aggregators, who are effectively accessing our data without permission, you might imagine that legal remedies could be taken to stop them. However, there are complexities around the fact that APIs are endpoints on the Internet and therefore accessible by anyone and around proving the specific hacking techniques that the aggregators are using. We decided to adopt Approov because it adds a high security barrier, is unconnected to user authentication and is frictionless for our customers."*

The SIXT approach was to use Approov to deploy mobile app authentication first, and then to switch on specific security capabilities and optional features over time. The first deployment of Approov brought vehicle availability and location data back under SIXT control, but reservations and
vehicle access could only be done through the SIXT mobile app.

Over time additional security layers were added to the deployment, including:

- Man-in-the-Middle (MitM) detection to ensure that bad actors were not monitoring SIXT API traffic.
- Instrumentation framework detection (for example, Frida) to ensure that hackers were not using these tools to reverse engineer the SIXT mobile app
- Use of the Approov custom claim capability to bind user sessions to tokens to minimize the risk of at-scale attacks.

## The Results

With their API environment now stable and secure, SIXT can choose what data to share with aggregators and at what level. They also have a foundation to continue strengthening their API security and remain vigilant of changes and needs in their business.

## Summary

Maintaining control over company and customer data and ensuring it is secure has become critical. SIXT understands the need to protect API connections is an increasing mobile world. Approov provided them the insurance they needed.

Nico Gabriel also offered advice for others who want to secure their API channels but need a trusted partner to help:

*"You should look for a solid product that brings new levels of protection to your business. However, I'd say that it is equally important that you consider your security vendor as a partner. Of course we want to make decisions and choices about our security arrangements, but we do not want to be security experts. We want to stay focused on being mobility experts instead. The Approov team has been with us every step of the way as we have grown our business, and they have been extremely helpful in both proposing and implementing new levels of protection within our environment. They truly are experts in their field."*


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

©2020 CriticalBlue Limited. All rights reserved. Version 1.1