approov
API THREAT PROTECTION

CASE STUDY

Protecting Patient Data While Delivering Agility To Physicians

"Approov plugged an immediate API security hole which pentesting had exposed in our platform, and we calculate that the adoption of Approov will bring us a 10x RoI."

– Tiago Calado, Software Development Manager

The delivery of healthcare services via the mobile channel has been accelerating in recent years but the current pandemic has caused the provision of such services to explode. The ability for physicians to provide healthcare services from flexible locations while accessing sensitive data such as Protected Health Information (PHI) has significant security implications.

The Client

MV is a Brazil-based provider of core healthcare information and management systems. With solutions for hospitals, clinics, health plan operators, radiology centers and public and private health networks, MV has not only become a national leader in the development of health management software, but has built, over more than 30 years of experience, an excellent reputation within the Brazilian health system.

The company provides complete, end-to-end solutions and operates a B2B business model. There are about 2 thousand institutions using MV solutions to offer efficiency, agility, precision and security in the provision of health services. This number grows every year, especially with the expansion of operations in Latin America and the international recognition of MV solutions.

The Challenge

Amongst MV's many mobile apps, the Medic MV app is at the heart of the demand for solutions which can deliver a service which has the required flexibility for physicians under today's conditions.

The Medic MV app is built for physicians of all specialties. It facilitates access to patient information inside and outside of the point of care in order to decrease the difficulty of accessing required medical records, increase the efficiency of communication and facilitate the highest quality of medical workflow.

Tiago Calado, Software Development Manager, provides some context:

> ***"When we developed the Medic app we of course had it and the APIs which service the app pentested. In parallel to the pentesting, one of our pilot customers expressed concerns about giving access to patients' Electronic Health Records on a mobile device."***

Considering the sensitivity of this PHI data and the recent adopted Brazilian Personal Data Privacy Regulation (LGPD), the team already knew that security would be key to reaching their goal of being the number one medical app in Brazil. Even though they

had already implemented many security mechanisms in the app and at the API endpoints, the pentesting results were frustrating because it was clear that there were more weaknesses which would need to be addressed before the MV Medic app could be deployed at scale. Specialist help would be needed.

How Approov API Threat Protection Helped

The pentesting company and MV reviewed the pentest results, during which it was agreed that reaching the required level of protection for PHI data which is accessed from outside of hospitals would require additional security layers. The pentesters were aware of Approov and the MV team recognised that because time was short, they should immediately take a closer look at Approov.

User authentication and TLS encryption was already in place but the application required more; specifically highly effective certificate pinning, man-in-the-middle detection, blocking of scripts and bots attempting to use the APIs, and proof that only genuine app instances can successfully make API requests.

Tiago adds:

> ***"Getting the app and API protection wrong in the MV Medic app was not an option. The recent LGPD legislation means that our healthcare institution customers could suffer from significant fines if we didn't meet our security goals. Those goals are a required differentiator for our sales teams and we had our product launch coming up fast."***

The Results

The MV team engaged with Approov, initially with a technical call and then a trial with the full service. It was obvious that the capabilities and flexibility in Approov were both needed in the Medic app and also impossible to deliver internally.

The Approov trial moved seamlessly into deployment with the MV Medic app trial, and the pentesters repeated their early work, with different, and much better, results this time. The app was now ready for prime time. First however, some specific use cases had emerged in the discussion between MV and Approov and the Approov engineering team implemented these new features so that the solution could be deployed, monitored and managed in the way that MV and their healthcare institution customers expected.

The app has now been launched and is a success on the Brazilan market. Plans included offering it across Latin America and beyond.

Summary

We asked Tiago to estimate the impact Approov has had on their business:

> ***"Approov plugged an immediate API security hole which pentesting had exposed in our platform, and we calculate that the adoption of Approov will bring us a 10x RoI considering lost sales and the cost of an internal development. In fact we are so convinced by the need for leading edge security that we are now planning to add Approov into all of our healthcare apps."***

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