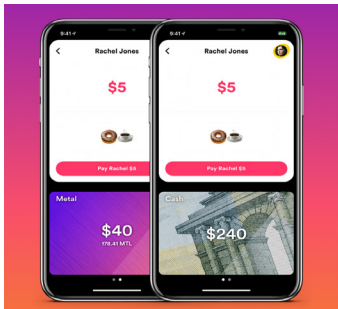


Proactively preventing smart bots from causing financial and brand damage



“The main issue we were facing was bots attempting to communicate with our APIs and attempting fraudulent transactions.”

“Looking at the traffic we’ve been able to counter with Approov and the financial fraud that usually comes with it I’d be willing to guesstimate at least a 10x return on our investment with Approov.”

– Glenn Marien, CTO and Co-founder, Metallicus

Significant changes in financial behavior, such as the move to mainstream use of cryptocurrencies, comes with risk as well as opportunity. Fraudsters typically migrate towards such discontinuities in the market because there they usually find the attractive combination of immature security protocols and opportunities to game the system. As use of the Metal Pay platform grew, so did fraudulent activity and Approov was deployed to identify and block fraudulent transaction requests not coming from genuine mobile app instances.

The Client

Metallicus is a fintech company which started in 2016 with a focus on peer-to-peer payments and anything to do with cryptocurrencies. Their flagship product, Metal Pay, provides users with an easy way to purchase and sell virtual currencies. Metallicus has also built a decentralized network, called the Proton Blockchain, with built-in KYC, asset swaps, DeFi lending, zero gas fees, etc.

Metallicus’s co-founder and CEO, Marshall Hayner, describes the company’s mission as creating the “PayPal of crypto”. Their main customers are people looking for an easy way to buy and sell digital currencies while simultaneously offering the typical features one would expect from a peer-to-peer payment app. Metal Pay offers customers a Cash Wallet that is FDIC-insured through their banking partner, which allows for the purchase, sale, and P2P transfer of over 60 cryptocurrencies. Metal Pay’s target demographic is anyone and everyone, in other words they are democratizing the market. The platform enables people to instantly send money to friends, family, and businesses with just a phone number – with cash and crypto transfers remaining free between Metal Pay users.

The Challenge

Metallicus’s key mission is to empower global access to traditional banking and digital assets. A new generation of customers are attracted to platforms like Metal Pay because they want to learn about everything blockchain technology can offer them while retaining all the existing features of the traditional system that they are used to. Delighting those customers requires a hybrid platform that will seamlessly integrate with both worlds while identifying key revenue streams to enable the business to prosper.

Being in the finance industry, most of the company’s key metrics originate from monitoring fraudulent transactions and identifying appropriate mitigations in each case. Any attack vector in this sector inherently leads to financial loss so it’s crucial

for the business to constantly monitor the activity on their platform.

Once Metal Pay was launched and began to gain momentum and customers, the first signs of nefarious activities appeared. Glenn Marien, Metallicus's CTO and co-founder, explains the situation at that stage:

"The main issue we were facing was bots attempting to communicate with our APIs and attempting fraudulent transactions. This varied from basic scripts issuing API calls to sophisticated full account takeovers (ATOs) impersonating real people. We realized that the security mechanisms we had in place were failing to protect us from this fraudulent activity."

The team recognized that they had no way of knowing whether an API request was coming from an authorized device or not. They needed a secure and reliable way to be able to identify the traffic that was approaching their network so that fraudulent traffic, typically emanating from scripts, bots, modified apps or manipulated apps, could be blocked.

In the most extreme cases the impact of not being able to differentiate genuine traffic sources from automated sources is a financial loss for the company, as well as a frustrating experience for legitimate customers trying to use the Metal Pay platform. If left unaddressed, any financial services company in this situation will start to see their reputation being negatively affected. Glenn picks up the story:

"We quickly realized that we weren't going to be able to solve this problem with traditional measures and knew we were going to have to think outside of the box. Recognizing this while you're experiencing an on-going attack is incredibly challenging for everyone in the business. The entire engineering team was under a lot of pressure to get this solved as soon as possible so we could continue with business as usual."

How Approov Mobile App Protection Helped

When looking for a solution to these problems, a few important things needed to be considered. Firstly, any fraudulent activity due to unauthorized devices impacts

Metallicus's reputation with their partners as well as their customers. Secondly, a crucial consideration is to ensure the impact of any security arrangements on network latency is minimal while making certain all traffic is authorized.

Another layer of complexity was added to the challenge when the team noticed that bots were getting smarter, using cellular networks to act as legitimate devices trying to use their APIs. Brute force mechanisms like blocking a range of IP addresses might slow down the fraudsters for a while but banning cellular IP ranges would mean legitimate users would be affected as well, so that was not an option. This is when it was finally recognized that Metal Pay was going to need a more sophisticated method of countering illegitimate activity from reaching the network.

In addition to the core capabilities of bot detection and mitigation, one of the key factors for consideration was cost, ideally based around a business model which scaled with growth of end user numbers. Approov was identified through a simple web search and the Metallicus engineers were able to get their account set up and the Approov SDKs implemented in their apps in record time.

During the test phase the team were highly impressed with the results they were seeing from Approov. Not only did it counter the fraudulent activity they had been experiencing, it was also able to categorize the activity - allowing the company to make educated decisions on which activity they wanted to address moving forward. The Approov team was also involved in reviewing the implementation and deployment and Metal Pay's "Approov'd" apps were soon deployed live.

"We saw a near total stop of automated scripts reaching our network as a result of deploying Approov. This also meant a significant drop of fraudulent transactions being made by these traffic streams. In addition to that, the data that's being fed to our system by Approov has allowed our compliance team to make informed decisions in certain areas. Turning on Approov and seeing the fraudulent bots hitting our API come to an end was a great feeling!"

The Results

When developing a publicly exposed API it is important to make sure that the clients reaching such APIs are coming

from authorized devices and originating from applications that your company developed. This way you can make sure that legitimate customers are using your platform while offering the best service to them. Now that Approov is fully deployed, the data that is being fed into the Metal Pay system allows the organisation to use those metrics in their anti-fraud system and detect anomalies as they happen. It has become an invaluable tool in the Metallicus internal systems.

Glenn summarizes the benefits:

"In addition to that, the team at Approov is simply incredible and we have nothing but good things to say about them. They're available for any questions we have and even monitor our traffic proactively. Our integration with them was one of the quickest ones we've been able to roll out and the results were visible instantly. Looking at the traffic we've been able to counter with Approov and the financial fraud that usually comes with it I'd be willing to guesstimate at least a 10x return on our investment with Approov."

Summary

Metallicus deployed Approov to stop fraud first and foremost. This was achieved by ensuring that only genuine instances of their mobile, running on uncompromised mobile devices, could execute transactions via their APIs. Now that scripts, bots, modified apps and manipulated apps are blocked, the Metallicus team can get back to focusing on their core activities to satisfy their customers and grow their business. Over to Glenn for a final few words for companies concerned about similar issues:

"It's crucial to be proactive about identifying traffic streams to your business, even if you're not experiencing an attack. Doing so will help protect your business and help you identify what kind of traffic is trying to reach your network. The overall implementation is one of the easiest we've done. The Approov team have done a great job of creating an easy to use SDK and have great documentation that goes with it."



Contact us for a free technical consultation - our security experts will show you how to protect your revenue and business data by deploying Approov Mobile App Protection.
www.approov.io