appdome

CUSTOMER CASE STUDY

Grupo Financiero Monex

Global Foreign Exchange Bank Chooses Appdome to Secure its FX Trading App

CUSTOMER OVERVIEW

Grupo Financiero Monex is a global foreign exchange (FX) company, headquarted in Mexico City, that specializes in international transactions and payment services for commercial clients. The group is one of the world's largest providers of commercial foreign exchange, delivering 850,000 annual transactions including international payments and foreign exchange, representing an annual volume of over $100B.

The *Monex Móvil* app allows users to access their accounts, execute FX trades, wire money to other bank accounts and communicate with their financial advisor.

CHALLENGE

Seeing an increasing threat to mobile apps, and mobile banking apps in particular, the Monex infosec team, on the direction of the CIO, made several proactive recommendations to strengthen the security of the *Monex Móvil* app. Once all the new requirements were documented, Monex looked for the best industry solution to implement their new security template. Key in their evalution were fast time to market, having and maintaining zero-day support for ever changing threats, working with only one vendor, and avoid having to cobble together different solutions.

GRUPO FINANCIERO monex

SOLUTION

Appdome, together with Mexico City based partner Incident Response Team SA de CV "Shield Force", worked closely with the Monex infosec team during an extensive Proof of Concept period. The Appdome Mobile Security Suite, was the **only** solution that was able to satisfy all the security requirements and passed several penetration tests with flying colors. The fact that Appdome's no-code solution allowed the bank to provide instant protection against all known and future threats, without increasing the workload of the - already stretched - mobile dev team clinched the deal.

With Appdome, Monex was able to quickly and easily protect *Monex Móvil*, against any attempts of mobile fraud, account takeovers, ransomware, identity and credential theft, credential stuffing and other backend network attacks.

> "Monex Grupo Financiero has always made it a priority to offer the highest level of security to our clients in the financial services and products we offer. That is why we have decided to partner with Appdome, so that we can ensure that all of our transactions meet the highest standards of quality and security demanded by the market."
>
> -- Luis De la Vega, CIO at Monex

APPDOME MOBILE SECURITY SUITE

Monex secured the *Monex Móvil* app with the Appdome Mobile Security Suite in just minutes with no coding required. The suite includes:

ONEShield™ App Hardening – Comprehensive mobile app shielding and hardening solution that prevents dynamic analysis, tampering, modifying, debugging or interfering with the app's workflows as well as blocks emulators and simulators.

TOTALCode™ Obfuscation – Complete code obfuscating solution that prevents static analysis, obfuscates the entire binary, native code and non-native code/libraries, SDKs and frameworks in the app, protects control flows and strips debug information in the app.

TOTALData™ Encryption – AES-256 Data-at-Rest Encryption for all data stored by the mobile app, in the app sandbox, SD Card and file system, as well as encryption for app preferences, app secrets, XML and other strings, resources and DEX files (Java classes).

OS Security Integrity – Prevents the app from running on rooted and jailbroken environments, root hiding, root and jailbreak tools, and hacking and cheat engines that rely on root and jailbreak.

MiTM Protection – Protects all mobile data in transit from network-based attacks with active man-in-the-middle detection and prevention, including forged certificates, malicious redirection or proxies as well as adds secure certificate pinning and client certificates (for bot prevention). Dozens of enforcement options are available.

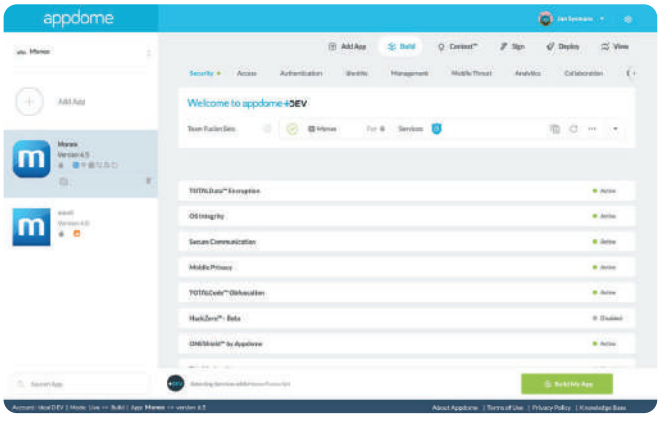
Mobile Privacy and Data Loss Prevention – Protects mobile end users' data and prevents data loss by preventing malicious keyloggers, restricting screensharing, screenshots and recording.

GUARANTEED OUTCOME AT A FIXED COST

The Appdome solution is a zero-development, fixed cost solution, which offers developers and DevSecOps teams a guaranteed mobile security outcome.

Monex is enjoying the following benefits with Appdome:

- A Certified Secure solution that protects the people and businesses that rely on *Monex Móvil* to complete their foreign exchange transactions and wire money between different accounts.
- Protecting all user data everywhere that it's stored in the app, as well as in memory, and in transit (between the app and the bank's servers).
- Preventing hackers from using debuggers, static and dynamic analysis and other forms of reverse engineering to learn how their mobile banking app functions.
- Securing its mobile banking app without impacting release cycles (Fast time to market) or increasing their budget (lowest budget impact).
- CI/CD integration into the bank's build system to ensure that the apps are protected build-by-build, release-by-release.



ABOUT APPDOME

Appdome's mission is to protect the mobile economy and the people who use mobile apps in their lives and at work. Appdome's industry defining no-code mobile security and solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new mobile security, mobile threat, mobile fraud and enterprise authentication, access, UEM/MDM/MAM and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.

appdome

CUSTOMER CASE STUDY

Airfox banQi

Securing the mobile apps of a leading digital challenger bank for emerging markets

CUSTOMER OVERVIEW

Airfox is digital challenger bank for emerging markets with offices in Boston and São Paulo. Airfox is owned by Via Varejo, the largest retailer in Brazil. Under the brand name banQi, Airfox developed an affordable, easy-to-use, transparent, and empathic digital financial services hub for underserved Brazilians and their families to manage, save, and build their wealth and financial life. Unlike incumbent banks and other fintechs, banQi is a neobank that provides users with a complete digital banking experience. Users are able to create a free mobile bank account in minutes. The banQi app has 1M+ downloads.

CHALLENGE

A key part of Airfox's strategy is to use advanced mobile and digital technologies to offer flexible and innovative mobile banking services with a high degree of velocity. As part of this strategy, Airfox relies on the banQi mobile platform to reach millions of otherwise inaccessible customers who use the banQi mobile app for all their banking needs.

Airfox needed to solve two primary challenges, both of which are critical to its growth and success.

(1) Protect the banQi app against cybercriminals who make their living by attacking mobile banking apps with the goals of stealing mobile user data or accessing financial transactions or breaching backend systems.

(2) Develop and release its mobile app quickly in order to stay ahead in the highly competitive Brazilian market.

SOLUTION

The mobile engineering team found that building mobile app security in-house was time consuming, complex, and had the potential to delay future product releases of the banQi app.

Appdome's no-code, mobile security platform enabled Airfox to implement mobile app security in the banQi mobile app in minutes and address their two primary challenges.

As a result, the app is protected against any attempts of mobile fraud, account takeovers, malware, ransomware, identity and credential theft, credential stuffing and other backend network attacks. This protection includes zero-day protection against new threats like Ghimob, a Remote Access Trojan, identified in late 2020 that specifically targets Brazilian banks.

"Being able to develop and releases new features quickly is key for a fintech challenger like Airfox/banQi. However we need to do this securely. There are always new threats out there and we need to be ready for these immediately.

Appdome gives us the trust and confidence that the banQi app is certified secure and that our users are protected from malware, fraud, thefts and more. One less thing for us to worry about as we prepare to provide mobile banking services to underserved communities in other emerging markets."

Emanuel Moecklin, CTO at Airfox

APPDOME APP DEFEND PACKAGE

Airfox secured the banQi app with the Appdome App Defend package in just minutes with no coding required. The package includes:

ONEShield™ App Hardening – Comprehensive mobile app shielding and hardening solution that prevents dynamic analysis, tampering, modifying, debugging or interfering with the app's workflows as well as blocks emulators and simulators.

TOTALCode™ Obfuscation – Complete code obfuscating solution that prevents static analysis, obfuscates the entire binary, native code and non-native code/libraries, SDKs and frameworks in the app, protects control flows and strips debug information in the app.

TOTALData™ Encryption – AES-256 Data-at-Rest Encryption for all data stored by the mobile app, in the app sandbox, SD Card and file system, as well as encryption for app preferences, app secrets, XML and other strings, resources and DEX files (Java classes).

OS Security Integrity – Prevents the app from running on rooted and jailbroken environments, root hiding, root and jailbreak tools, and hacking and cheat engines that rely on root and jailbreak.

MiTM Protection – Protects all mobile data in transit from network-based attacks with active man-in-the-middle detection and prevention, including forged certificates, malicious redirection or proxies as well as adds secure certificate pinning and client certificates (for bot prevention). Dozens of enforcement options are available.

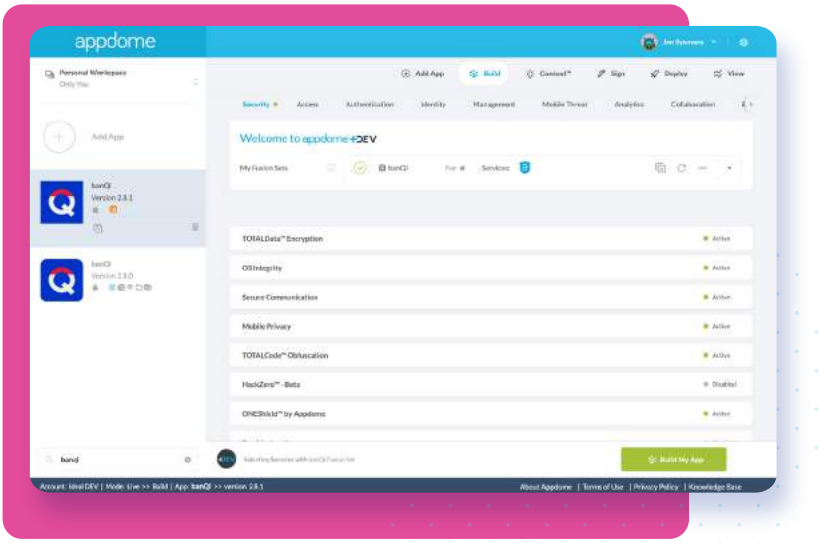
Mobile Privacy and Data Loss Prevention – Protects mobile end users' data and prevents data loss by preventing malicious keyloggers, restricting screensharing, screenshots and recording.

GUARANTEED OUTCOME AT A FIXED COST

The Appdome solution is a zero-development, fixed cost solution which offered Airfox a guaranteed mobile security outcome for the banQi app.

Airfox is enjoying the following benefits with Appdome:

- A Certified Secure solution that protects the people and businesses that rely on the banQi app to do all their mobile banking.
- Protecting all user data everywhere that it's stored in the app, as well as in memory, and in transit (between the app and the bank's servers).
- Preventing hackers from using debuggers, static and dynamic analysis and other forms of reverse engineering to learn how their mobile banking app functions.
- Securing its mobile banking app without impacting release cycles (Fast time to market) or increasing their budget (lowest budget impact).
- CI/CD integration into the bank's build system to ensure that the apps are protected build-by-build.



ABOUT APPDOME

Appdome's mission is to protect the mobile economy and the people who use mobile apps in their lives and at work. Appdome's industry defining no-code mobile security and solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new mobile security, mobile threat, mobile fraud and enterprise authentication, access, UEM/MDM/MAM and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.

appdome

CUSTOMER CASE STUDY

Banco Pichincha Peru

Peruvian Commercial Bank Chooses Appdome to Secure its Mobile Banking App

CUSTOMER OVERVIEW

Banco Pichincha is one of the largest private banks in Latin America with 1.8 million customers, and over $4 in both assets and deposits, with operations in Ecuador, Peru, Colombia, and Panama.

PROBLEM

Cybercriminals are stepping up their attacks on mobile banking apps, especially as more end-users conduct and manage financial transactions using their smartphones during the pandemic.

In light of the desire for mobile banking, partly accelerated by the need for social distancing, Banco Pichincha Peru released its first mobile app, *APP Banco Pichincha Perú*, in July 2020. A key requirement for this release was that the app would meet a set of stringent security requirements.

SOLUTION

With the help of Appdome's platform and mobile security expertise, and Appdome's Peru based partner Aggity Perú, the bank was able to satisfy all its security requirements without sacrificing the release schedule. With Appdome, Pichincha was able to quickly and easily protect their mobile app, connections, data and users against all mobile threats, hacking attempts, mobile fraud, account takeovers, ransomware, identity and credential theft, credential stuffing and other backend network attack.

And with Appdome Certified Secure, the bank now has the trust and confidence that its app is protected with the features needed for their business. In additional the bank can reduce both time and expense spent on penetration testing and vulnerability scans.

"As a financial institution, it's crucial that our mobile app be secure. But we also needed to release the app in a timely manner. Our customers were eager to start mobile banking and with Appdome's help and support, we were able to release a certified secure app quickly without adding to the workload of our mobile development organization or integrating multiple third-party security solutions."

Erick Alencar Rios, Head of Digital Channels at Banco Pichincha Peru."

APPDOME APP DEFEND PACKAGE

Banco Pichincha Peru secured the *APP Banco Pichincha Perú* mobile banking application with the Appdome App Defend package in just minutes with no coding required. The package includes:

ONEShield™ App Hardening – Comprehensive mobile app shielding and hardening solution that prevents dynamic analysis, tampering, modifying, debugging or interfering with the app's workflows as well as blocks emulators and simulators.

TOTALCode™ Obfuscation – Complete code obfuscating solution that prevents static analysis, obfuscates the entire binary, native code and non-native code/libraries, SDKs and frameworks in the app, protects control flows and strips debug information in the app.

TOTALData™ Encryption – AES-256 Data-at-Rest Encryption for all data stored by the mobile app, in the app sandbox, SD Card and file system, as well as encryption for app preferences, app secrets, XML and other strings, resources and DEX files (Java classes).

OS Security Integrity – Prevents the app from running on rooted and jailbroken environments, root hiding, root and jailbreak tools, and hacking and cheat engines that rely on root and jailbreak.

MiTM Protection – Protects all mobile data in transit from network-based attacks with active man-in-the-middle detection and prevention, including forged certificates, malicious redirection or proxies as well as adds secure certificate pinning and client certificates (for bot prevention). Dozens of enforcement options are available.

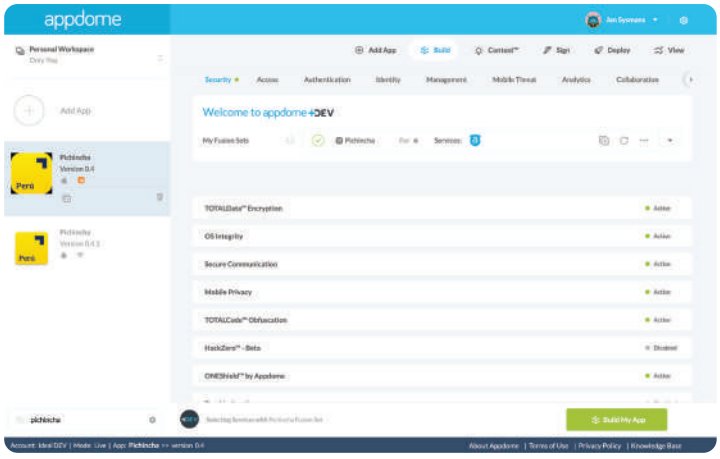
Mobile Privacy and Data Loss Prevention – Protects mobile end users' data and prevents data loss by preventing malicious keyloggers, restricting screensharing, screenshots and recording.

GUARANTEED OUTCOME AT A FIXED COST

The Appdome solution is a zero-development, fixed cost solution which offerec Banco Pinchincha a guaranteeed mobile security outcome.

The bank is enjoying the following benefits with Appdome:

- A Certified Secure solution that protects the people and businesses that rely on the Banco Pichincha mobile app to complete e-commerce and financial transactions.
- Protecting all user data everywhere that it's stored in the app, as well as in memory, and in transit (between the app and the bank's servers).
- Preventing hackers from using debuggers, static and dynamic analysis and other forms of reverse engineering to learn how their mobile banking app functions.
- Securing its mobile banking app without impacting release cycles (Fast time to market) or increasing their budget (lowest budget impact).
- API integration into the bank's build system to ensure that the apps are protected build-by-build, release-by-release.



ABOUT APPDOME

Appdome's mission is to protect the mobile economy and the people who use mobile apps in their lives and at work. Appdome's industry defining no-code mobile security and solutions platform uses a patented, artificial-intelligence coding technology to power a self-serve, user-friendly service that anyone can use to build new mobile security, mobile threat, mobile fraud and enterprise authentication, access, UEM/MDM/MAM and more into any Android and iOS app instantly. There are over 25,000 unique combinations of mobile features, kits, vendors, standards, SDKs and APIs available on Appdome. Over 200+ leading financial, healthcare, government, and m-commerce providers use Appdome to consistently deliver richer and safer mobile experiences to millions of mobile end users, eliminating complex development and accelerating mobile app lifecycles.