Hypergrowth Southeast Asian FinTech Company **Prevents Financial Fraud and Bot Attacks with Guardsquare**

Leading digital wallet provider secures top downloaded mobile payment apps with DexGuard, iXGuard, and ThreatCast

The Company

The organization is a leading digital financial services provider in Southeast Asia, founded on a mission of empowering the country's unbanked and underbanked population. Their powerful yet convenient and user-friendly digital wallet iOS and Android apps have helped hundreds of millions of users to make payments, send and receive money, withdraw money, and invest - all straight from the apps. The apps have been the most downloaded financial services app in the country, handling billions of financial transactions annually, and recently experiencing a threefold increase in transaction activities compared to 2021. The organization is committed to delivering the most secure apps that are compliant with the national regulatory and industry standards.

> **"Our business relies heavily on our mobile applications; therefore, it is very important for us to ensure they are properly secured while remaining user-friendly and accessible."**
>
> **— Mobile Front-End Lead,** Southeast Asian hypergrowth FinTech company

COMPANY DETAILS

Industry

Financial services (Digital wallet)

Privately / Publicly owned

Private

Employees

1000+

Customer since

5+ years

Challenges

- Meet PCI-DSS compliance
- Meet the central bank's regulatory compliance
- Maintain performance without compromising security
- Prevent reputational and financial damage due to fraud
- Prevent repackaging and coordinated bot attacks

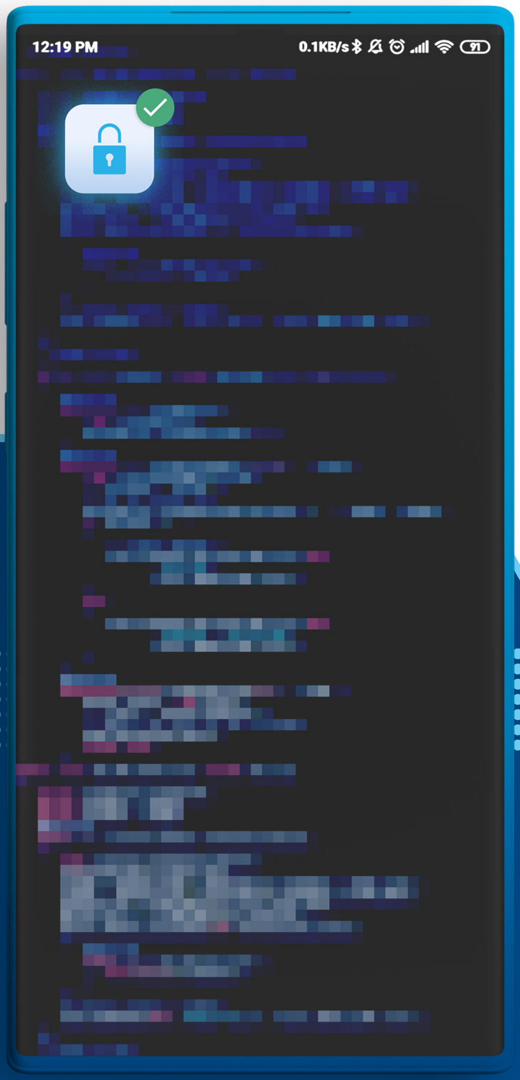
Solutions

- DexGuard
- iXGuard
- ThreatCast

The Challenge

Operating in a highly regulated industry, the organization has to comply with all mandated security compliance requirements from the country's central bank as well as industry standards such as PCI-DSS. Initially, the organization assigned one app security expert to be responsible for the security of their iOS and Android applications. Using open-source solutions, they were able to apply some basic code obfuscation techniques such as class, field, and method obfuscations to protect against static attacks.

> **"Our pentest team found that parts of our apps' control flow, logic, and some API keys were not properly obfuscated, leaving them open to attacks in certain occasions, which can lead to financial and legal consequences. We tried to mitigate this ourselves but it quickly became way too complex for it to be scalable as we grow our business. We needed expert help and we needed it fast."**
>
> — **Mobile Front-End Lead,** Southeast Asian hypergrowth FinTech company



They soon realized, however, that their in-house, DIY approach was unsustainable as they added more features to the apps. This increasing complexity led to more crashes and slowdowns, forcing them to choose between app security and performance. This outcome was problematic as two of the organization's core guiding principles are trustworthiness and user-friendliness. They needed to quickly find a way to balance the two crucial factors in their increasingly popular apps: they sought to apply the highest level of protection without compromising on user experience. Gaps in their security had allowed Account Takeover (ATO) attacks as well as coordinated bot attacks to take place. Without remediation, the organization knew more types and an increased frequency of attacks would occur as threat actors discovered and exploited more attack vectors - which could result in brand reputation damage, financial loss, or legal repercussions due to fraud, and other malicious activities.

GUARDSQUARE
Mobile application protection

The Solution

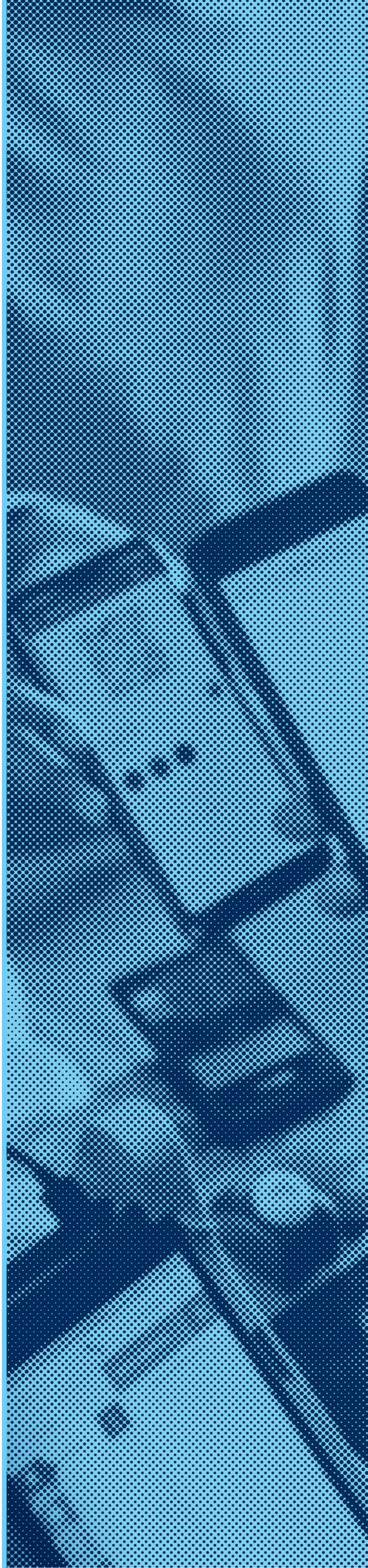
DexGuard and iXGuard were mainly chosen due to their strong reputation in the region, the extensive security features they offer, and partly thanks to the developers' familiarity with Guardsquare's open-source Java and Android app optimizer, ProGuard. The leading digital wallet provider looked forward to applying more advanced code hardening and Runtime Application Self-Protection (RASP) techniques that were not available in their open-source solutions, namely: Control flow obfuscation, data encryption, API call hiding, debugger, and emulator check, as well as root/jailbreak, hook, and tamper detection. These layered security mechanisms provide in-depth protection against static and dynamic attacks.

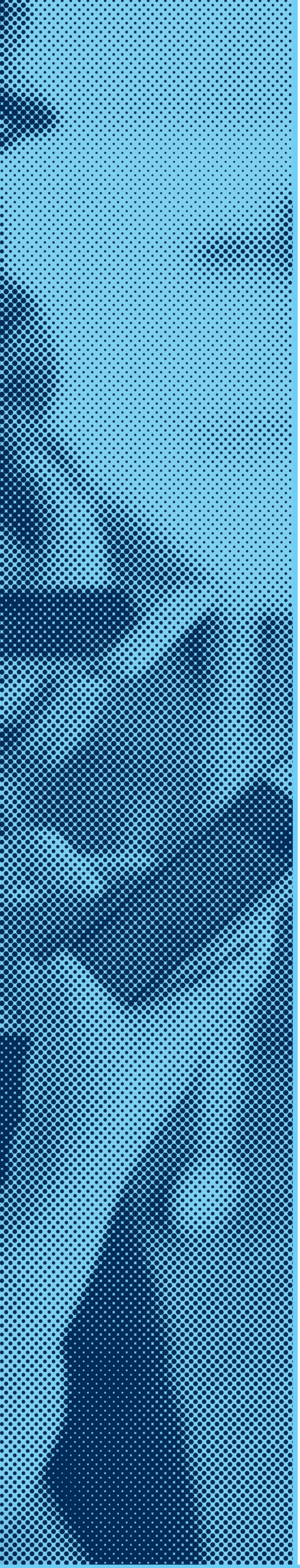
> **"Our engineers were excited to see the breadth of advanced protection DexGuard and iXGuard offer. On top of the control flow obfuscation, data encryption, and other code-hardening techniques we desperately needed, we also layered this static protection with the RASP capabilities to protect against attacks at runtime."**
>
> **— Mobile Front-End Lead,** Southeast Asian hypergrowth FinTech company

Using ThreatCast, Guardsquare's real-time threat monitoring solution, the organization is able to see instantly which runtime protections are getting triggered by DexGuard and iXGuard as their Android and iOS apps are used in production. For instance, they were able to discover that many of their users run their apps on jailbroken/rooted devices and get notified whenever threat actors try to debug or decompile the apps.

The Results

With DexGuard and iXGuard fully implemented, the organization's iOS and Android apps were able to pass internal and external pentesting requirements and achieve the PCI-DSS and central bank's security compliance standards. Additionally, they also received an "A" rating from an independent cybersecurity analysis and certification agency. These results demonstrates a dramatic improvement in the mobile app security and overall security posture they managed to achieve after partnering with Guardsquare. Their digital wallet apps are now fully protected against tampering and reverse engineering without any noticeable impact on performance.





> **“DexGuard and iXGuard did what they were promised to do, and extremely well, at that. Guardsquare’s product, engineering, and support teams have been extremely helpful and responsive in the support tickets we raised. We have been able to achieve and maintain the balance between security and performance on each release."**
>
> **— Mobile Front-End Lead,** Southeast Asian hypergrowth FinTech company

Equipped with ThreatCast, the proactive collaboration between their red and blue, as well as governance & risk teams, has allowed them to maintain a 360° view of the security threats and risks their apps are facing. They do this by complementing their existing SIEM system with real-time insights on environment, app, and code threats gathered by ThreatCast.

Next, the leading digital wallet provider looks forward to leveraging more ThreatCast Premium capabilities such as custom webhooks, rules, and notifications. They are also exploring the use of AppSweep, Guardsquare’s free mobile app security testing product, to find and solve security issues in their Android and iOS apps before production.

“Dozens of our team members actively use ThreatCast on a daily basis. Its handy dashboard has allowed our team to gain a much deeper understanding of which part of our code is being attacked, allowing us to finetune the protection configurations our apps truly need. Additionally, we are now able to more confidently ban or block malicious users thanks to ThreatCast’s user-specific data such as UserID and DeviceID,” said the Mobile Front-End Lead at the company.

PROTECT ········ TEST ········ MONITOR

Do you need help to **protect your apps** against fraud and bot attacks?

Request a Demo

Customer privacy is a top priority for Guardsquare. As a result, we have a policy not to publicly identify customers. The customer has agreed to have this case study published and has reviewed the content for accuracy.

GUARDSQUARE
Mobile application protection

Developer friendly **mobile app sec tools** that:

PROTECT TEST MONITOR

Guardsquare offers the most complete approach to mobile application security on the market. Built on the open source **ProGuard**® technology, Guardsquare's software integrates seamlessly across the development cycle. From app security testing to code hardening to real-time visibility into the threat landscape, Guardsquare solutions provide enhanced mobile application security from early in the development process through publication.

More than 900 customers worldwide across all major industries rely on Guardsquare to help them identify security risks and protect their mobile applications against reverse engineering and tampering.

www.guardsquare.com