Gourmet Food and Goods Delivery Platform **Protects Its Business Integrity with Guardsquare**

DexGuard provides multilayer protection against GPS spoofing, API endpoint abuse, and fraud.

The Company

Founded in 2017, this Saudi-based online delivery service enables elite customers to order high-end food and consumer goods via intuitive, easy-to-use Android and iOS apps. With more than 12,000 restaurants and stores in the service's network, customers can sample the region's most popular cuisines, book a table at their favorite restaurant, and even have chocolates, flowers, or perfumes delivered to their homes.

The company is committed to delivering the most secure and seamless experience to its hundreds of thousands of customers across the nation. Through their commitment to delivering the most reliable, user-friendly, and secure mobile experience, in the first half of 2023, the company managed to more than double its app installs and grew its revenue by more than 600%.

COMPANY DETAILS

Industry
Retail / E-commerce

Privately / Publicly owned
Private

Employees
300+

Challenges

- Preventing tampering and reverse engineering
- Preventing order and delivery fraud
- Ensuring brand reputation and customer loyalty
- Safeguarding sensitive components in the app
- Minimizing API-endpoint abuse risk

Solutions

- DexGuard

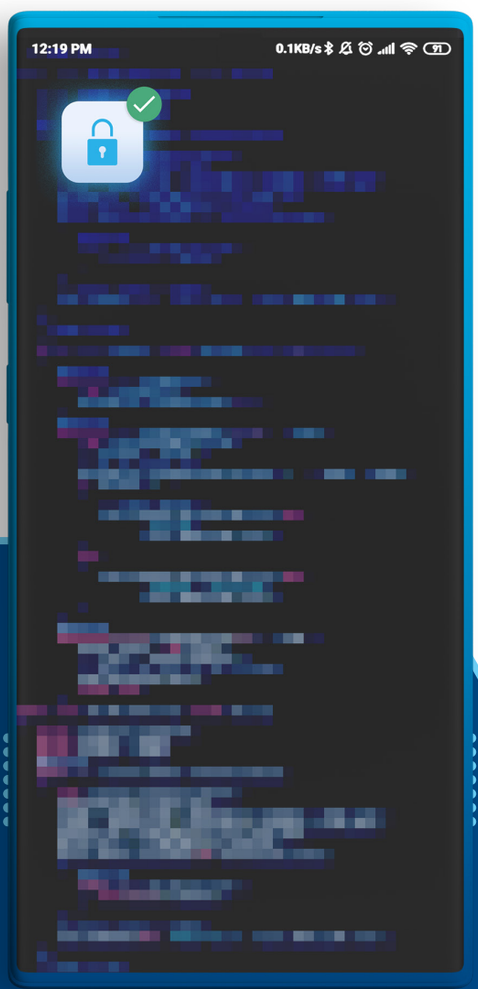
"Trust is the foundation of our business. As the main digital storefront, the security of our mobile apps is one of the most crucial components we need to get absolutely right."

– CTO, Premium food delivery app

The Challenge

The company understood the importance of security and utilized an open-source tool to protect its mobile application from the beginning. However, as the company continued to grow its service offerings, coverage, and user base in the Saudi Arabian market, it increased its emphasis on achieving a more robust mobile app security posture. The security team started to notice security vulnerabilities that were successfully exploited by threat actors that compromised their Android app and the integrity of their service.

> **"Despite the security controls we put in place, hackers were able to tamper and reverse engineer our app. We first realized this when we noticed illegitimate users managed to fake their location by disabling the built-in geoblocking and anti-GPS spoofing feature to commit fraud."**
>
> **— CTO,** Premium food delivery app



The open-source tool they used could only provide simple code-hardening techniques. Consequently, threat actors were able to deobfuscate, modify, and manipulate the code's behavior to commit different kinds of attacks. The security team found several modified versions of their apps available online. More concerningly, they also noticed malicious drivers and couriers being able to fake their GPS location. By doing this, threat actors were able to trick the app into allowing them to accept delivery orders that were far away from them or in busier locations so they could earn more, and even get paid without having to deliver the orders.

"Our security team found that many of the attackers were from outside the regions we serve, meaning they were able to bypass the geoblocking security control we put in place. We knew these observed threats were only the tip of the iceberg of what they could do. We needed to find a more sophisticated protection tool quickly. Left unprotected, we risked further financial losses and potential damage to our brand reputation and loyalty," said the CTO.

The Solution

After thoroughly researching the market for the available options, the company was convinced that DexGuard offers the most comprehensive and advanced protection. The gourmet food and goods delivery company chose Guardsquare also due to its good reputation and significant market presence in the region. This was further supported by suggestions made by their partners in the region.

> **"Guardsquare's reputation preceded them; many of our partners recommended DexGuard for its advanced protection features and track record. Even the AI research tool we used during our market research agreed."**
>
> **— CTO,** Premium food delivery app

The company was drawn to the wide array of static and dynamic code protection features DexGuard offers to combat the tampering and reverse engineering attacks they were experiencing. The security team wanted to layer DexGuard's code obfuscation features (i.e., name obfuscation, data encryption, and call hiding) with its runtime application self-protection (RASP) features (i.e., certificate checks, root, tamper, and hooking detection), to ensure that their Android app's code could not be deciphered and its behavior could not be altered by attackers at runtime.

"DexGuard's comprehensive feature set provides us the flexibility to customize how and which part of our app's code needs to be protected, allowing us to tailor the protection configuration for our use case," noted the CTO.

The Results

Using DexGuard's built-in Protection Report, the company was able to conveniently assess and enumerate the strength of both static and dynamic protections they applied to their app. Using the tailored configuration advice provided by the Protection Report as guidance, they were able to optimize DexGuard's multi-layered defense according to their use case. In a matter of weeks, they were able to fully implement the tool, pass the internal pentesting, and deploy the fully-protected version of the app. Very quickly, the company saw that DexGuard's layered static and dynamic protection was able to effectively prevent threat actors from tampering with their fully-protected app.

“DexGuard’s Protection Report was extremely handy in ensuring that we take into account all the risks associated with our app’s use case. The team was able to easily understand the protection level they’ve achieved, and what else can be done to further enhance the security of our app,” explained the CTO.

They no longer see modified versions of their app and completely eliminated the GPS spoofing problem they previously faced. The development team also utilized DexGuard’s call hiding and data encryption features to fully protect their app from potential attacks on their API endpoints and other sensitive assets inside their app. Thanks to Guardsquare’s polymorphic protection techniques, the company can seamlessly ensure that no two releases have the same protection configurations, essentially resetting the attacker’s clock with every new release. Next, they look forward to implementing into their iOS app, further improving their security posture.

> **“With DexGuard fully implemented, we no longer see any successful tampering or reverse engineering attempts. The protection Guardsquare offers allows us to ensure our brand and service integrity."**
>
> **— CTO,** Premium food delivery app

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 security tools that:**

PROTECT **TEST** **MONITOR**

Guardsquare offers the most complete approach to mobile application security on the market. 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.