Multinational PayTV Operator Prevents Content and Service Piracy with Guardsquare

LATAM digital video entertainment leader utilizes Guardsquare's full suite of mobile app protection, testing, and monitoring products.

The Company

With more than 35,000 employees, this Latin American media production and distribution company offers live and on-demand video content through satellite, cable, and the Internet. Their widely popular mobile streaming iOS and Android applications are used by more than 10 million customers across 11 countries in the LATAM region. Through these apps, subscribers can stream live and on-demand local, regional, and international video content, such as premium shows, and different types of sports and movie genres. The company has seen an exponential growth of 107% in new subscriptions throughout 2022, an increase of 2.53 million users.

COMPANY DETAILS

Industry
Media and Entertainment

Privately / Publicly owned
Private

Employees
35,000+

Challenges

- Prevent video content from being pirated
- Protect against video streaming service piracy
- Ensure the security of sensitive data & assets stored in & processed by the apps
- Safeguard against tampering, reverse-engineering, repackaging, and cloning

Solutions

- AppSweep | DexGuard | iXGuard

"We realized DRM and other content protection mechanisms are not the silver bullets in preventing piracy. We've seen how easy it is for someone with a little bit of knowledge to bypass these mechanisms and have access to premium content. We needed to protect our mobile apps from reverse engineering and tampering to prevent attackers from being able to get in and understand how our code works."

— **Mobile Lead,** Multinational PayTV operator

The Challenge

The biggest security challenge the digital media company faces is piracy. Experts estimate that the US economy alone loses $29.2 billion to video content piracy every year. The company leverages a number of content protection mechanisms including encryption and Digital Rights Management (DRM). Content owners and production studios often require third-party streaming services to protect their Intellectual Property (IP) using this technology to prevent piracy. DRM restricts how the content is accessed or used by encrypting the content to prevent unauthorized users from viewing, downloading, or copying the media.

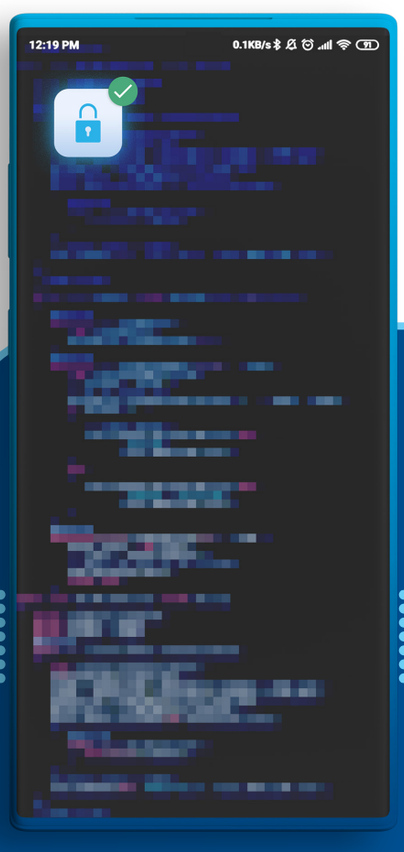
However, this technique does not always provide adequate protection when used on its own, and can be bypassed using a variety of methods regardless of the scheme used whether it's Google Widevine, Apple Fairplay, or Microsoft PlayReady. More crucially, DRM doesn't protect mobile app code or its server communication. Without additional protection at the app level, the company's video streaming apps were vulnerable to attacks using a variety of techniques based on reverse engineering and tampering. Without sufficient code protection, threat actors could gain unauthorized access to the service and content. In addition, they could have executed Distributed Denial of Service attacks (DDoS) on mobile application API endpoints to bring the company's services down. All of these attacks could result in negative impacts on the company's bottom line and brand reputation.

Lastly, the company needed to protect its self-service apps where customers can manage their subscriptions, recharge their account balance, and rent content or games. They needed to make sure sensitive financial and personal data being processed and stored in the app were well protected.

> **"Market proof was a very important factor for us when choosing a security solution. We chose Guardsquare due to its prominent presence in the LATAM market, especially in the financial services industry."**
>
> — **Mobile Lead,** Multinational PayTV operator

The Solution

The company sought to improve the security of its iOS and Android applications by implementing advanced security tools to prevent static and dynamic app threats. Combining code obfuscation and runtime protection mechanisms has made it significantly more difficult for threat actors to tamper or reverse engineer its apps. The company also incorporated a mobile app security testing solution into its development cycle to identify and fix vulnerabilities in the apps' code and dependencies. Lastly, it leveraged a threat monitoring solution to gain real-time insights into how threat actors attempt to compromise their apps, allowing them to make informed decisions and continuously improve their security posture.



After using ProGuard, Guardsquare's open-source Java optimizer, for approximately five years, internal stakeholders were happy with the solution and familiar with Guardsquare's in-depth approach to mobile app security. The company chose Guardsquare due to its comprehensive solutions and market presence in the LATAM region, especially in the highly regulated financial services industry. Guardsquare's mobile app protection, testing, and monitoring products enable developers to integrate security throughout the app development lifecycle. DexGuard (Android) and iXGuard (iOS) provide advanced protection mechanisms for mobile apps through multiple layers of code hardening and Runtime Application Self-Protection (RASP). AppSweep enables developers to find and mitigate vulnerabilities before the app goes into production, while ThreatCast, monitors threats the protected apps face in real-time.

The Results

The company quickly migrated to DexGuard and iXGuard, thanks to their familiarity with ProGuard configurations. Combined with ThreatCast's reporting capabilities, the company saw a significant decrease in apps being run on rooted and jailbroken devices, a telltale sign of suspicious activity.

The certificate pinning and Runtime Application Self-Protection (RASP)'s hooking detection feature, ensure continuous secure communications between the client app and the server. By preventing Man-In-The-Middle (MiTM) attacks from taking place, threat actors can no longer intercept the apps' communication and steal sensitive data such as authorization, authentication, and CDN tokens that can be abused to gain unauthorized access to the service and content. By layering both static and dynamic analysis code protection, their apps are well-protected against tampering and reverse engineering. Finally, Guardsquare's polymorphic approach ensures that the protection configuration is different on each release to reset the clock for the attackers, rendering their previous attack knowledge useless.

> **"After implementing DexGuard, we activated the advanced protection features, like root/jailbreak detection and certificate pinning, and refined the configuration. Later, we conducted two pen tests on our apps, but the pen testers weren't able to break into the app. "**
>
> — **Mobile Lead,** Multinational PayTV operator

With AppSweep, the media company was able to automate its mobile app security testing and continuously improve its security posture by identifying and fixing security issues before the app goes into production. As proof, when the media company conducted pen tests on their fully protected apps, the pen testers could not find a way to break Guardsquare's protections. With ThreatCast, the company has been able to track different kinds of threats its apps face in real-time, such as usage in unsafe environments (i.e., jailbroken or rooted devices) and other tampering attempts (i.e., debugger, hooking). Using these insights, the company has made more informed decisions to improve its security posture and fine-tune protection configurations.

By layering content protection mechanisms such as encryption and DRM with mobile app protection, the company succeeded in achieving more robust protection against content and service piracy. By working with trusted partners, it can spend more time focusing on its business without compromising on security.

"ProGuard had already significantly helped us optimize the size and speed of our Android apps. Although the tool did offer basic name obfuscation, we needed more advanced protection features. DexGuard is definitely a big upgrade from ProGuard. The team instantly felt familiar with the tool, and the migration from ProGuard to DexGuard was quite straightforward. It was an easy sell internally," said the Mobile Lead of the company.

GUARDSQUARE
Mobile application protection

Want to see for yourself how **Guardsquare** can protect your Android and iOS apps against common attacks?

Request a demo

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.