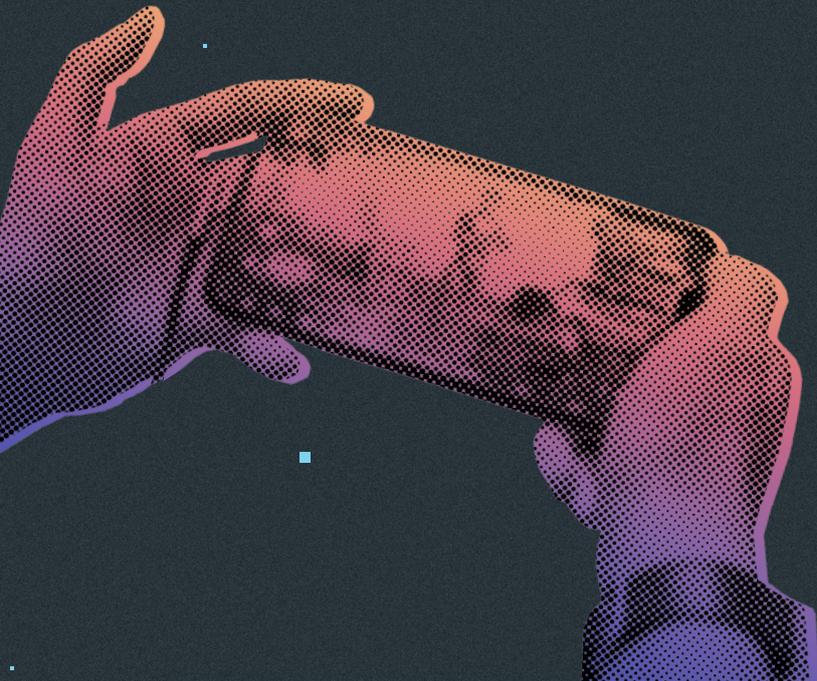


Mobile Gaming Security

Protect valuable revenue streams and maintain user trust with state-of-the-art app security



Mobile games are popular ways to relax and find a competitive outlet. These games also provide their makers with valuable revenue streams. In fact, mobile games accounted for a whopping **72% of overall mobile app spending in 2020**. But many mobile games are not sufficiently secured and are at risk for security breaches and financial losses.



 BAD ACTORS CAN:	
	Cheat & make it easier for others to cheat
	Build & distribute tweaks
	Undermine in-app revenue streams , such as ads or microtransactions
	Access sensitive user information
	& more

With tens of billions of dollars on the line,  apps makers **cannot afford to ignore security.**





The solution: Guardsquare

Protect valuable revenue streams:

Raises the bar against cheating, creating fake apps, diverting revenue streams, or otherwise defrauding app makers of hard-earned income. Code hardening makes it difficult to take advantage of apps.

Defend against the most common mobile risks:

Reverse engineering and tampering are two of the top 10 most prevalent security risks, according to OWASP. Guardsquare's application shielding technology protects against them.

Build user trust and loyalty:

Seamlessly deploy security best practices to both protect your gaming and entertainment apps and to provide users with a sense of fairness, fun, and trust in your apps.



iOS, Android and multi-platform Unity support

OUR APPROACH:

Code hardening:

Hardening the code at various levels throughout the application protects against static analysis. Multiple layers of obfuscation make code resistant to both automated and manual analysis.

Runtime Application Self-Protection (RASP):

RASP mechanisms monitor the integrity of the apps and their environment in real time. When a threat arises, the apps can terminate the attacker's session, display security notifications to the user, and more. RASP also ensures communication between the mobile app and server is secure.

Built for video games:

Guardsquare products are built for the needs of the video gaming industry.

Video games have extremely low performance impact tolerance. Guardsquare products provide effective, out-of-the-box default configurations and allow for protection tuning that enables you to avoid performance bottlenecks without compromising security.

Video games are under constant scrutiny of reverse-engineers. Unprotected games usually get hacked on day 0. However, attacks sometimes take place weeks after the original game release. Even the strongest protections eventually get defeated.

Guardsquare products acknowledge this and provide a high degree of polymorphism in mobile game protection. With every new release, the code hardening, runtime checks, signature, quantity, and position are changed – effectively resetting the clock on attackers.

Video games are often built using commercial game engines. Unity, one of the most popular gaming engines for mobile, adds metadata in your game application that reverse-engineers can use. Guardsquare DexGuard and iXGuard protect the Unity metadata file so that attackers cannot leverage this information to reverse-engineer your game.

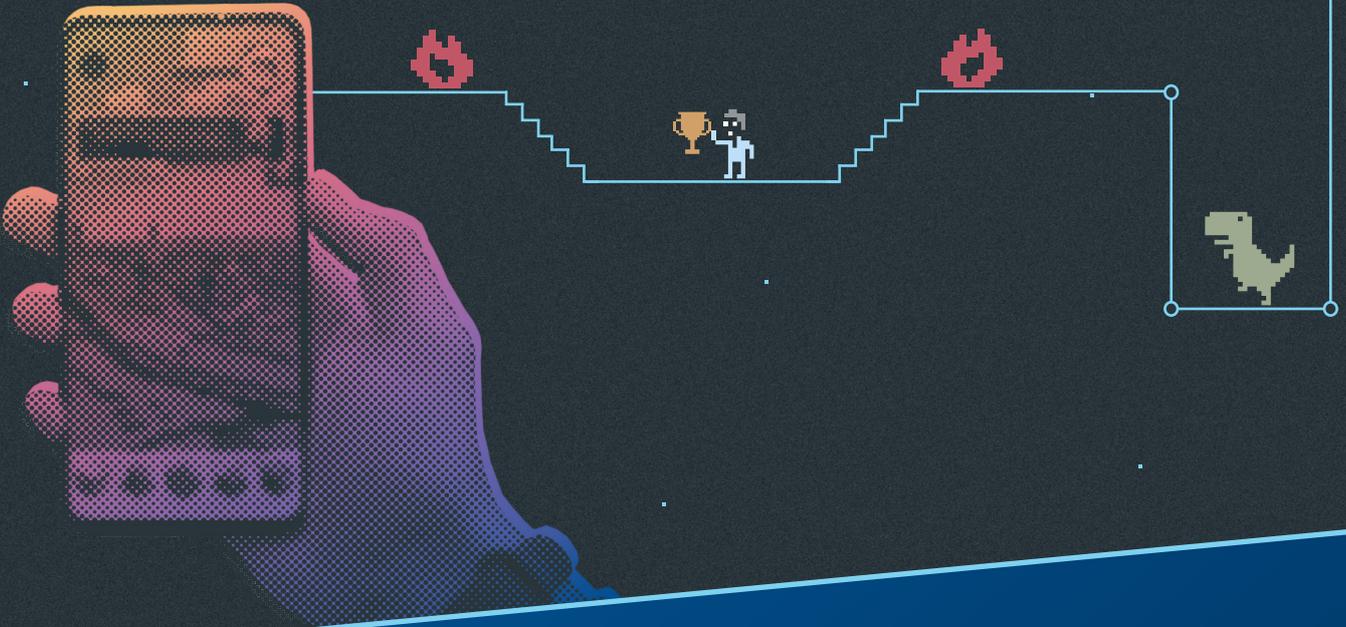


Our products



Verified Solution

 DexGuard	 iXGuard	 ThreatCast
 Android	 iOS	 Android  iOS
<ul style="list-style-type: none"> Code hardening Runtime self-protection Protection of native & cross-platform apps App optimization Unity support 	<ul style="list-style-type: none"> Code hardening Runtime self-protection Protection of native & cross-platform apps iOS app optimization maintained Unity support 	<ul style="list-style-type: none"> Mobile app security console for real-time threat monitoring Get actionable insights Integrate security into the development lifecycle



The creators of ProGuard®

Want more information?
Reach out to [schedule a demo](#)

[Connect with an Expert](#)

 **GUARDSQUARE**
Mobile application protection