iXGuard
GUARDSQUARE

Cutting-edge protection for your iOS apps

Hackers can use easily available tools to disassemble and inspect your iOS applications and SDKs to gain insight into their internal logic. This leaves apps vulnerable to various forms of abuse, including intellectual property theft, cloning, credential harvesting, API key extraction and code tampering.

iXGuard has been designed to protect native (**Objective-C**, **Swift**) and cross-platform (**Unity**, **Cordova**, **Ionic**, **Flutter**, **React Native**, **and other JavaScript-based**) apps and SDKs for iOS against reverse engineering and tampering. iXGuard applies multiple obfuscation and encryption techniques to the code of applications and SDKs and integrates runtime self-protection mechanisms (RASP). The applied layers of protection make it virtually impossible to gain access to their internal logic and to modify their intended behavior.

REQUIREMENTS ▸ ✓ Recent version of Xcode ✓ Bitcode-enabled archive build

Secure development made easy

- iXGuard is a command-line tool that processes and protects iOS applications and libraries. It enables you to fully protect your application or SDK without requiring you to share or alter the source code.
- iXGuard is easy to configure. It can be set up to protect entire applications or specific functions with a single configuration file.
- iXGuard offers built-in support for both native iOS (Objective-C, Swift) and cross-platform applications (Unity , Cordova, Ionic, Flutter, React Native).
- iXGuard provides functionality to help you efficiently and effectively protect your application or SDK: its **In-App Assistant** automatically generates configuration for your application and its **Protection Report** helps you validate and improve your protection setup before release.
- iXGuard integrates seamlessly with Guardsquare's real-time threat monitoring platform, **ThreatCast**. ThreatCast gives you visibility into the actual threats facing your app and enables you to adapt your security configuration to the constantly evolving threat landscape. Free ThreatCast access is included in your Guardsquare license.

iXGuard protects your iOS apps and SDKs against static analysis using multiple code hardening techniques

Name obfuscation

iXGuard obfuscates identifiers to hide semantic information from reverse engineers. Most common reflection constructs are supported out of the box.

Control flow obfuscation

iXGuard hides the original function logic to better shield your applications and SDKs against automated and manual code analysis.

Call hiding

iXGuard hides function call targets to prevent identification of vulnerabilities in the application's code.

Data encryption

iXGuard encrypts strings (encryption keys, API endpoints, tokens, etc.) as well as resource and asset files to prevent sensitive data from leaking.

Arithmetic obfuscation

iXGuard transforms arithmetic statements into more complex but equivalent alternatives to conceal the original computation. The outcome of the transformations is different in every single build.

iXGuard shields your iOS applications and SDKs against dynamic analysis and live attacks using various runtime self-protection mechanisms (RASP)

Jailbreak detection

iXGuard lets you determine how your application should react when it is executed on a jailbroken device.

Debugger detection

iXGuard integrates environment integrity checks that detect the use of debugging tools into your application or SDK.

Repackaging detection

iXGuard makes sure your application has not been repackaged by a third party by performing signature-based checks and by comparing additional fields of the binary with the observed state at compile time.

Method swizzling prevention

iXGuard protects your application or SDK against attempts to modify its behavior through method swizzling.

Code tracing detection

iXGuard detects and prevents code tracing attempts with dynamic binary instrumentation tools.

Hook detection

iXGuard enables your application to detect and prevent attempts by hooking frameworks (i.e. Frida, Cydia Substrate and fishhook) to modify its behavior.