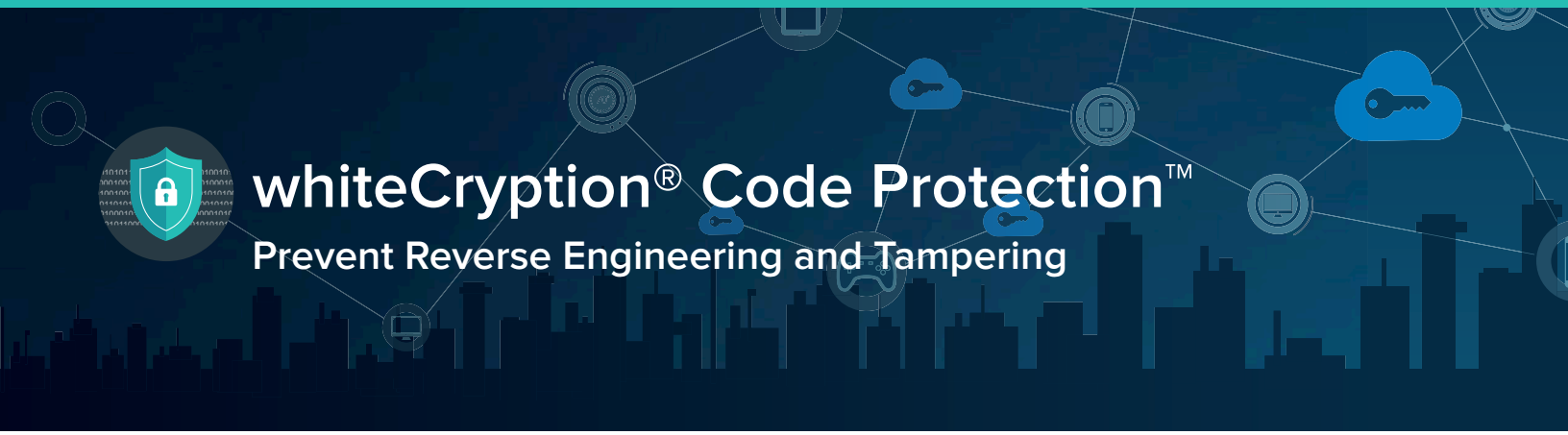

whiteCryption® Code Protection™

Prevent Reverse Engineering and Tampering

BUSINESS BENEFITS

- **Don't Be the Headline.**
  Protect your endpoints from attack, manage risk, and build brand. Prevent loss of revenue and reputation with application shielding.
- **Shield Your Applications.**
  Go far beyond typical code obfuscation with our advanced obfuscation capabilities and leverage our Runtime Application Self Protection (RASP) to keep your source code, and other proprietary information secret.
- **Proven and Easy to Use.**
  Battle-tested Code Protection automatically applies optimized security techniques requiring very few modifications to the source code.
- **Foil Hackers.**
  Shield IoT devices and mobile apps that are outside the firewall and out of your control where hackers can decompile and tamper with them.

EVERY APPLICATION NEEDS APPLICATION SHIELDING

whiteCryption Code Protection provides mobile apps or devices with code obfuscation and Runtime Application Self Protection (RASP), shielding them from decompilers, debuggers, reverse engineering and tampering.

Unsurpassed Code Obfuscation

Significantly more sophisticated than commodity code obfuscators, our advanced obfuscation techniques give you the best protection in the industry while maintaining performance and minimizing memory impact.

Runtime Application Self Protection (RASP)

RASP goes much further than obfuscation by ensuring that any attempt at inspecting or tampering with the application triggers customizable defense actions including program exit, data deletion, logging and real-time notifications.

It's Easier Than You Think

Use Code Protection to profile your application and have it automatically place powerful shielding techniques perfectly designed to achieve your security goals, without tedious, manual, trial-and-error efforts. Moreover, Code Protection will fit into your existing CI/CD workflows through its Command Line Interface (CLI).

USE CASES

Mobile Payment Systems

When money is changing hands, protect the logic behind payments, and prevent malicious external intervention with the application shielding that Code Protection provides.

Healthcare

Protects patient privacy and sensitive medical data, even when the device is in the possession of a hacker.

Media & Entertainment

Ensures Digital Rights Management (DRM) enforcement for highly valuable digital content applications used by millions of users world-wide.

Connected Car

Provides application shielding for critical car components to ensure the integrity of the system and protection of the occupants.

FEATURES

Runtime Application Self Protection (RASP)

- **Integrity Protection.** Using our patented technique, up to hundreds of overlapping integrity checkers protect each other and are automatically added to an application, thwarting attackers.
- **Customizable Defense Action.** When Code Protection detects a threat, it corrupts the program state to cause an exit by default. However, your code can take control to perform any actions.
- **Anti-Debug Protection.** Prevents a debugger from inspecting your application while it is running.
- **Anti-Method Swizzling.** Detects method swizzling in Objective-C programs and prevents potentially unsafe dynamic loading of libraries.
- **API Hooking Detection.** Prevents hackers from attacking a running application.
- **iOS Jailbreak and Android Rooting Detection.** Detects and prevents your mobile app from running in an unsecured iOS or Android environment.
- **Integrity Protection of Android APK Packages.** Provides a set of source code and run-time features that protect APK packages against tampering, including re-signing with a different key.
- **Shared Library Cross-Checking.** Verifies the integrity of shared libraries that your application calls so they cannot be replaced or tampered with.
- **Mach-O Binary Signature Verification.** Prevents macOS, iOS and tvOS apps from unwarranted re-signing that can be used to facilitate piracy.

Advanced Obfuscation

- **Symbol Stripping & Renaming.** Makes it difficult for hackers to make sense out of a program, in case they attempt to use static analysis.
- **String Renaming & Encryption.** Removes some of the clearest signs that hackers use to understand how a program operates.
- **Control Flow Obfuscation.** Provides additional hurdles to understanding what the application is doing.
- **Android Binary Packing.** Encrypts Android applications when they are not being run to protect against static analysis. They decrypt only at runtime.
- **Inlining of Static Void Functions.** Increases the obfuscation level of final protected code.
- **Objective-C Message Call Obfuscation.** Instead of storing method calls in plain text in the binary, they are obfuscated to confuse attackers.
- **Objective-C Metadata Obfuscation.** Since Objective-C executables contain metadata that can aid attackers doing static analysis, metadata is encrypted and only decrypted at runtime.
- **Binary Diversification.** The resulting output file is always different, even if no changes are made to the source file, frustrating hackers.

Easy to Use

- **Fully Automated.** Minimal or no changes are required to the original source code. A few advanced features that require minor modifications to your code may optionally be used and are easy to implement.
- **Code Profiling.** Ensures maximum performance and minimum footprint for protected applications without requiring tedious manual efforts.
- **Security Expertise.** Unrivaled expertise is built-in and automatically applied so you can focus on your application.
- **Module Selection.** Select the modules to protect with our easy-to-use GUI or CLI to optimize safety, footprint and performance.
- **GUI or CLI.** Use the intuitive GUI or the CLI to integrate into existing CI/CD workflows.

Wide Platform Support

- **Operating Systems:** Android, iOS, tvOS, macOS, Windows, Linux, QNX, and others.
- **Languages:** Android Java, C, C++, Objective-C, Swift.
- **Google Play Licensing Service:** Provides a more secure alternative library to the easily decompiled Java library that Google provides to use the Google Play Licensing Service.

Strengthen Your Security with our Complementary Products

whiteCryption® Secure Key Box™
Performs common cryptographic functions in mobile apps, IoT devices, and services while keeping cryptographic keys secure without requiring dedicated hardware security.

Seacert™
Provides trusted identities for your IoT devices, mobile apps, services and users with customized X.509 certificates and a robust PKI infrastructure.