intertrust®

whiteCryption® Code Protection™

Enterprise-grade obfuscation and tamper defense

Datasheet

Secure Systems

Make your software self-defending

Applications are a prime attack target and source of risk for both organizations and users. whiteCryption Code Protection arms your software with proactive security technology so that it can run safely anywhere. Detect and prevent code alterations, guard against static and dynamic analysis, and actively stop hacking. Your data and intellectual property stay secret, software integrity is preserved, and the lifecycle of applications prolonged.

Protect your applications and data

Code Protection thwarts reverse engineering with powerful, multi-layered code obfuscation. It deploys a wide array of advanced protection techniques to prevent static and dynamic analysis and defend against intrusion, malware, and data exfiltration.

Detect and respond to threats

With Code Protection, your application detects when it is running in hostile environments, such as jailbroken or rooted devices, debugging tools, emulators, and other risks. Robust anti-tamper technology protects the integrity of your source code and third-party libraries. Real-time, customizable response actions enable your software to automatically defend itself against discovered threats.

Meet regulatory requirements

Comply with data privacy laws and security requirements set by strictly regulated industries such as financial services and healthcare. Accelerate regulatory approval and testing timelines with proven, comprehensive application protection.

Simplify your application security

Reduce development time and resources with best-in-class protection that easily integrates into your CI/CD workflows. Code Protection analyzes your application and automatically injects powerful shielding techniques that match your security goals and minimize memory and performance impact.

Benefits

Powerful code obfuscation
Patented source code level obfuscation gives you unsurpassed protection while maintaining performance.

Advanced anti-tamper defense
Embed robust tamper detection mechanisms and automated defense response to prevent any attempts at altering or inserting malware into your code.

Accelerate time to market
Bring highly secure, standards-compliant applications to market faster. Fully automated protection easily slots into your existing build cycle.

Widest platform support
Protect native, hybrid, and embedded apps on mobile devices, desktops, servers, and IoT devices.

Comply with regulations
Meet and exceed data privacy and application security requirements while minimizing approval and testing timelines.

Backed by experts
Intertrust's deep software protection expertise guides every step of your deployment.

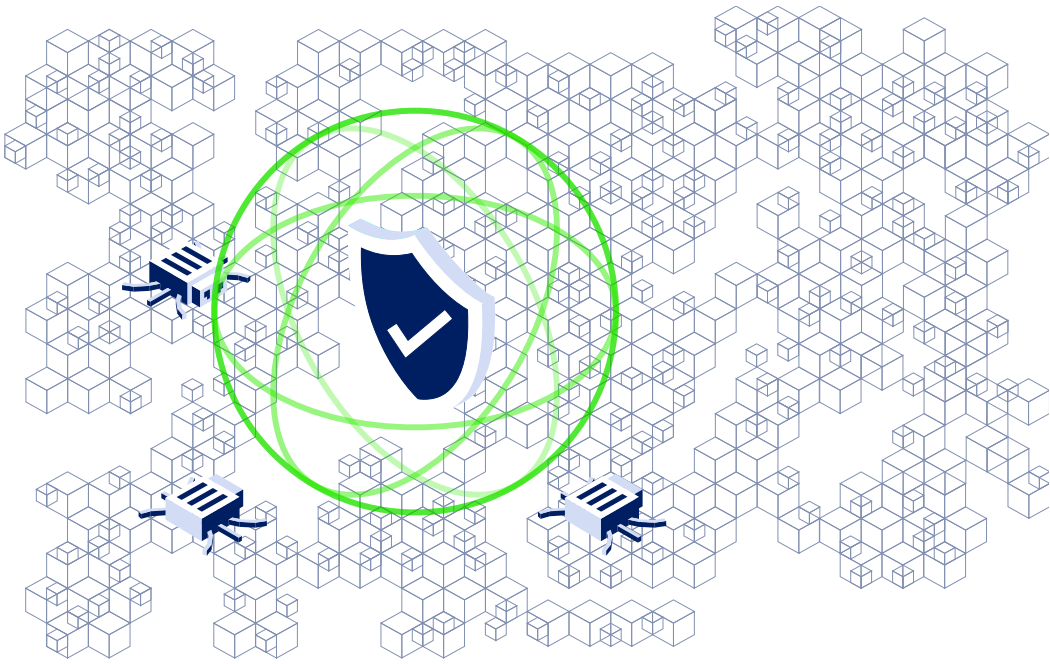
Features

Runtime application self protection (RASP)

- **Integrity protection:** Using our patented technique, hundreds of overlapping integrity checkers prevent code tampering and disabling of application protections.
- **Customizable defense action:** When Code Protection detects a threat, it automatically executes a customizable defense response.
- **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 runtime 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 layered obfuscation and code hardening

- **Symbol stripping:** 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:** Modifies the structure of how subroutines are called to make code more difficult to trace.
- **Binary packing:** Encrypts Android or Linux applications to protect against static analysis, decrypting only at runtime.
- **Inlining of static 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 binary file is always different, even if no changes are made to the source file, frustrating hackers.



Easy implementation that accelerates time-to-market

- **Fully automated:** Minimal or no changes required to the original source code. Fits right into your existing SDLC.
- **Code profiling:** Ensures maximum performance and minimum footprint for protected applications with no manual configuration required.
- **Security expertise:** Deep expertise is built in and continuously improved to stay ahead of changing conditions and customer needs.
- **Full control:** Select the modules to protect 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

- Android, iOS, tvOS, macOS, iPadOS, watchOS, Windows, Linux, QNX, and others.
- Languages: Java, C, C++, Objective-C, Swift, Kotlin for Android.

Comprehensive security solutions

Code Protection is one part of Intertrust's suite of application and IoT security solutions.

- **whiteCryption® Secure Key Box™** provides industry-leading white-box cryptography to secure your cryptographic keys in critical software and apps.
- **Seacert™** provides rich, cryptographically secure identities for IoT devices with customized X.509 certificates and a robust PKI infrastructure.

Start protecting your applications today. For a free all-access trial, visit intertrust.com/code-protection-free-trial

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/whitecryption/code-protection
Contact us at: +1 408 616 1600 | information@intertrust.com

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085