



## CodeArmor® Software Protection for Native Windows

### Protect Valuable Software Applications against Piracy, Code Theft and Tampering

Most application security solutions are designed to secure network elements, encrypt application data, or detect network intrusions. While these solutions provide valuable measures of security, they don't protect the application code and algorithms that comprise the software intellectual property (IP). Attackers can still reverse engineer and tamper with applications — opening the door to financial loss, reputation damage and threats to mission-critical and high value software.

Tackling the problem of software piracy poses an equally difficult challenge. To fight piracy, organizations have traditionally relied on difficult-to-deploy hardware dongles or license systems that then are easily defeated by piracy groups.

### Strong Software Protection Made Simple

CodeArmor from V.i. Labs is an automated security solution that protects applications without requiring source code modifications or design changes. It layers granular Just-In-Time (JIT) decryption, anti-debugging, anti-tampering, and secure run-time execution monitoring to provide comprehensive software protection. Unlike other solutions that must be integrated into the software development process, CodeArmor hardens and protects applications in their executable form — virtually eliminating the need for software development resources or impacting product-time-to-market. Once protected, applications are persistently secured against piracy, tampering, misuse or theft wherever they are deployed.

### How CodeArmor Works

CodeArmor is comprised of three components:

**CodeArmor Post Processor:** A desktop application that automatically analyzes, encrypts, and embeds protection functions into a software application.

**Secure Execution Monitor:** A set of security functions for encrypting and decrypting application subroutines, ensuring application integrity, and monitoring the run-time environment for malicious activity and unauthorized access.

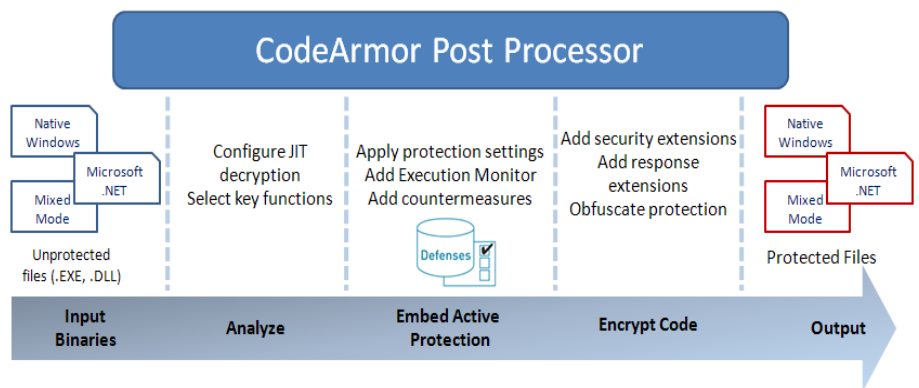
**Application and Security Extensions:** Custom extensions that can be added by CodeArmor to integrate with authorization frameworks, hardware devices, and alternate threat response systems.

### CodeArmor at a Glance

- **Provides simple, automated protection.** Easily secures existing software applications without source code modifications or requiring complex security infrastructure.
- **Ensures application integrity.** Application code operates as it is intended — no matter where the application is deployed.
- **Offers comprehensive security.** Protection includes Just-In-Time function decryption, anti-debugging, anti-tampering, and run-time execution monitoring.

## Protecting an Application

To protect a software application, a user starts the Post Processor and selects the application files (.EXE or .DLL) files to be protected. Using a graphical interface, the user selects specific functions for JIT decryption (e.g., licensing, IP) and configures a protection level. Then CodeArmor automatically starts the protection process. During this time, the runtime monitoring protection logic is embedded and obfuscated within the application binaries along with encrypted functions.



The CodeArmor protection process

## Self-Protected Application

When the protected application is launched, the monitor checks the run-time environment to detect hacker attempts to attach debuggers, insert malicious code, or perform other techniques to capture code. If tampering is detected, the monitor can notify a user, log the event, or halt the executable altogether or a custom response. CodeArmor verifies the integrity of the application statically as well as in memory and decrypts and re-encrypts the sensitive functions as they are called and therefore limits the exposure of these functions in memory.

### FEATURES

### BENEFITS

#### Non-invasive protection

- CodeArmor allows organizations to automatically protect applications without modifying the source code or changing the product design.

#### JIT decryption and granular encryption

- Granular function level encryption allows CodeArmor to focus on the code at risk and minimize impact to application performance and operation.
- JIT decryption limits exposure of application code in memory and prevents a scripted attack.

#### Anti-tampering and secure execution monitoring

- CodeArmor decrypts and then verifies the integrity of specific functions in memory prior to execution to prevent the application from being altered.
- At runtime, CodeArmor continually monitors for threats including debuggers, disassemblers, decompilers to ensure safe execution of the application.

#### Protection for integrated license management

- CodeArmor prevents reverse engineering and the creation of binary patches that defeat licensing systems by hardening the license routines embedded within the application.

#### Leverages the CodeArmor platform

- Can support .NET applications with .NET protection component
- Works in conjunction with CodeArmor Intelligence to track pirated use of applications and notify vendors and organizations of threats to their software