



## CodeArmor® Software Protection for Microsoft® .NET

### Your Intellectual Property Can Be Stolen or Tampered With

The sensitive source code that is at the heart of your company's software intellectual property (IP) is critical to your competitive advantage and revenue stream. However, if you develop using C# and deploy your applications on the Microsoft .NET Framework, your source code is easily accessible.

Since .NET applications are partially compiled into an Intermediate Language (IL), novice users can use free tools to decompile deployed applications. The result? Your valuable applications are more vulnerable to malicious tampering, IP theft by competitors and software piracy.

### Active Software Protection for .NET Applications

CodeArmor Software Protection for Microsoft .NET is an automated solution that secures the code within .NET applications from reverse engineering without requiring source code modifications or design changes. Unlike passive .NET protection solutions such as obfuscation, CodeArmor minimizes the impact to your software development lifecycle and doesn't introduce deployment or support complexities. Instead, CodeArmor creates a runtime environment that securely integrates with the Microsoft .NET framework and prevents access to the decrypted code while application executes. The CodeArmor runtime decrypts the .NET code a method at a time, limiting access to code in memory.

### Protects Application Programming Interfaces

Because only the IL code is encrypted and the metadata is retained, interfaces with external applications are not impacted allowing collaborative development environments to still be supported. Organizations can share their IP within Application Programming Interfaces (API) and Software Development Kits (SDK) and still mitigate the risk of losing their code.

### Low Impact Protection Process

Unlike obfuscation approaches CodeArmor is able to encrypt the IL code itself at the assembly level without changing code flow, renaming variables, or requiring developer expertise. This simplifies the integration of protection within a software release and minimizes any impact to customers.

### CodeArmor at a Glance

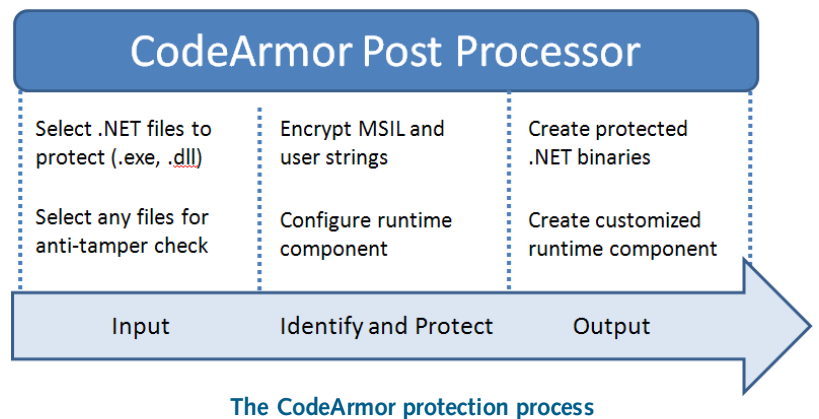
- **Low impact .NET protection.**  
Easily secures existing Microsoft .NET applications without requiring source code modifications or software development resources
- **Granular code encryption.**  
Secure integration with .NET Framework provides method level decryption and minimizes exposure of code in memory
- **Secure sharing of Software IP.**  
Allows organizations to share code in their APIs, SDKs, and ASP .NET applications without exposing valuable or sensitive software IP

**CodeArmor extends protection beyond obfuscation solutions by encrypting the code itself and decrypting a method at a time during execution.**

## Protecting an Application

Through a graphical interface, the user selects the files to be protected or verified, configures the security settings, and initiates the protection process. Alternatively, the protection post processor can be integrated for automation during the software build process using a command line interface. Once the protection process initiates, the CodeArmor post processor analyzes .NET binaries, encrypts the IL code, and create signatures for the files to be verified at runtime. Optionally, user strings can be encrypted as well. The protection process creates encrypted .NET assemblies and a customized secure runtime component.

When the application is executed, the runtime component dynamically integrates with the .NET framework to provide per method decryption capabilities and minimize risk to decrypted code in memory. Although the .NET files are protected, they appear as managed assemblies allowing other applications to reflect off and interface with them.



### About V.i. Labs

V.i. Labs combines piracy business intelligence, anti-tampering and software protection technology to recover sales revenue, prevent the theft of software intellectual property and avert reputation damage. V.i. Labs' patented CodeArmor platform allows software vendors, embedded system providers, and enterprise organizations to harden their applications against theft, gain business intelligence into emerging markets, measure unlicensed use of their software, uncover new revenue streams and increase sales.

#### FEATURES

#### BENEFITS

##### Non-invasive protection

- Intermediate language code is encrypted at the assembly level without impacting application code flow or introducing support dependencies

##### Method level encryption

- Prevents decompiling of .NET assemblies
- Minimizes exposure of decrypted application code in memory

##### Anti-tamper protection

- Prevents tampering of specific application files or resources

##### Protects APIs and SDKs

- Can share software IP with customer and partners without exposing sensitive code

##### ASP .NET support

- Protects Web application code being hosted on third party networks

##### Platform support

- Supports 32-bit and 64-bit applications

##### Leverages the CodeArmor Platform

- Supports unmanaged application components with native protection component
- Works in conjunction with CodeArmor Intelligence to track pirated use of .NET applications and notify vendors and organizations of threats to their software