



## Cloakware Security Suite

Software protection and anti-tamper solutions for government and defense

### KEY BENEFITS

- **Effective security** – defends against reverse engineering, tampering and scripted attacks
- **Inseparable security** – baked into the application, not wrapped-on after the fact
- **Renewable security** – automatable updating of keys, software and security measures
- **Automated tools** – enable rapid development and deployment of security capabilities
- **Proven scalability** – protect one deployment or produce millions of secure products

### KEY FEATURES

- Data transformation
- Control transformation
- Key hiding
- White-box cryptography
- Integrity verification
- Anti-debug
- Code encryption

### SUPPORTED PLATFORMS

- Windows® XP/Vista, Windows Mobile
- Mac OS X (≥ 10.3), iPhone/iPod® touch
- Linux-ARM/MIPS/PPC/ST40
- Symbian™-ARM
- VxWorks™

## Proactively protect sensitive software and data outside your trusted network

In business, software attacks and intellectual property (IP) theft mainly pose a threat to a company's bottom line. In government, the stakes are much higher. IP theft and sophisticated software hackers pose significant threats to national security and defense, personal privacy, and military effectiveness on the battlefield where lives are on the line.

### Your software is at risk

Pervasive threats to software security include reverse engineering, software tampering, copying, and automated attacks which can be launched across a network or on an attacker's desktop. The successful security strategy against these threats is a multi-dimensional approach – data security, network security and software protection. Software applications protected using Cloakware Security Suite can be deployed on untrusted hosts and in hostile environments such as the Internet, concealing proprietary algorithms and secrets, including cryptographic keys, embedded in the software.

### Automated software protection

Cloakware Security Suite is a collection of automated tools that enable developers to protect their application code against reverse engineering, tampering attacks, and automated attacks. Cloakware's security techniques provide application protection through data and control flow obfuscation, anti-debug, White-box cryptography, integrity verification and executable encryption. Cloakware Transcoder™, Secure Signer and Secure Packager deliver Cloakware's security techniques by integrating into a customer's software build process, and embedding application protection directly at the source code level.

### Effective security

- > Defends against reverse engineering and tampering attacks.
- > Creates software diversity to protect against scripted attacks.
- > Enables you to easily tune performance for optimum security within device constraints.
- > Makes security inseparable from the software during development—a much more secure approach than those that only wrap the binaries right before shipping.
- > Independently audited by customers, academics and ethical hacking service providers.

## ABOUT CLOAKWARE

Cloakware provides innovative, secure, proven software technology solutions that enable customers to protect business and digital assets in enterprise, consumer and government markets. The company has two main product lines: Cloakware Datacenter Solutions help organizations meet Governance, Risk Management and Compliance (GRC) objectives for privileged password management while ensuring business continuity and the security of mission-critical data and IT infrastructure. Cloakware Consumer Product Solutions protect software and content on PCs, set-top boxes, mobile phones and media players. Protecting more than one billion deployed applications today, Cloakware is the security cornerstone of many of the world's largest, most recognizable and technologically advanced companies. Headquartered in Vienna, VA and Ottawa, Canada, Cloakware has regional sales offices worldwide.

## CONTACT INFORMATION

### Corporate Headquarters

Cloakware Inc.  
8219 Leesburg Pike, Suite 350  
Vienna, VA, USA 22182  
Tel. +1.703.752.4830

### Canada

Cloakware Corporation  
84 Hines Road, Suite 300  
Ottawa, ON, Canada  
K2K 3G3  
Tel. +1.613.271.9446

[www.cloakware.com](http://www.cloakware.com)



## Easy to use

- > Integrates directly into your product build process; automated tools enable rapid deployment of security capabilities.
- > Security techniques are easy to enhance and quick to upgrade in field deployments.
- > Does not affect program functionality and is invisible to legitimate users.

## Broad platform support

- > Cloakware protects software on more than one billion devices including PCs, set-top boxes, mobile handsets, portable media players and more.
- > Supports all major platforms including Linux, Macintosh, Windows, Symbian, and proprietary embedded devices for a range of chipsets including ARM, MIPS, x86 and PPC, allowing you to build and deploy applications in your environment and on the open computing platform of your choice.

## Cloakware Transcoder™

The Transcoder is a command line utility that transforms source code into mathematically modified source. Transcoded applications are functionally identical to the originals but are highly resistant to reverse engineering and tampering attacks. The protected application reliably executes on open computing platforms without special hardware or additional software. The Transcoder also uniquely links anti-debug, integrity verification and White-box cryptography with code transformations to deliver integrated and layered protection that is far more secure than individual techniques alone.

## Cloakware White-box cryptography

Cloakware's White-box Cryptography implements standard cryptographic algorithms in a way that hides critical keys in environments where hackers can observe cryptographic operations in complete detail. Popular, trusted ciphers like RSA and AES are among the most thoroughly studied algorithms, making them particularly vulnerable targets for attacks such as lifting keys from memory. Cloakware's White-box cryptography ensures that critical keying data is not revealed—even during cryptographic operations.

## Cloakware integrity verification

Knowing that your code has not been tampered with is a crucial element of establishing security. Cloakware's Integrity Verification resists hacker attempts to modify the original program by creating encrypted vouchers that store a signature of the original application. The Integrity Verification run-time library uses the voucher to detect tampering of the application. Integrity verification can also ensure the authenticity of externally-signed modules that interact with the application, including components of the operating system. Integrity Verification continuously verifies signed components "in memory" to ensure that they are integral at all times. If integrity is compromised, developer-configured failure paths and anti-tamper actions are taken.

## Cloakware code encryption

The final step to application security is encrypting the application executable to prevent static analysis. Cloakware's Secure Loader provides a range of options for encrypting the executable or specific critical functions, and authenticating this code at runtime before decrypting it directly into a memory location.