

42%

OF SOFTWARE  
IS OBTAINED  
ILLEGALLY  
WORLDWIDE

COMMERCIAL  
VALUE OF  
SOFTWARE  
STOLEN

\$63.4  
BILLION



It's your code. Protect it.

The first, and still the most feature rich, Java and Android application hardening and obfuscation tool protects your applications from reverse engineering, tampering, unauthorized monitoring and compromise.

Enterprises, software vendors, and manufacturers, healthcare and financial services firms have all come to recognize a simple truth: Reverse engineering, monitoring, and modifying managed code is a common, well-understood practice and, with the right tools, extremely easy to do.

DashO provides enterprise-grade protection, significantly reducing the risk of piracy, intellectual property theft, tampering and data loss and corruption.

## Development Process Integration

*DashO provides reliable, flexible, and scalable deployment options to accommodate everyone from agile start-ups to automated manufacturing processes.*

**Multiple Configurations** – Standalone GUI, Ant integration, or command line.

**Dedicated Live Support** – Our support engineers are experienced programmers whose job is to make you successful. They'll take the time to chat or speak with you live on the phone.

**Incremental Obfuscation** – DashO allows you to release obfuscated patches without rereleasing the entire application.

**Cross-Assembly Obfuscation** – DashO extends renaming and other protections across multiple and distinct binaries.

**100% Java Compliance** – From Windows to Mac to Android, we've got you covered.

**Cross Platform** – We support all Java applications from Swing-based apps to J2EE apps with Spring/Hibernate to Android.

## Instrumentation & Injection Platform

Introducing complex production defense behaviors, reporting practices, and alerts can, for the first time, be automated through DashO's powerful injection and instrumentation libraries. Development teams do not need to be burdened with writing this additional logic nor do compliance teams need to audit each application development team's implementations. DashO can ensure consistent, transparent, and auditable injection of debug, tamper, expiry, and other runtime behaviors.

## Application Security – Enterprise Application Risk Management

*Application security and risk management cannot be a "one size fits all." Decades of working across industries have helped make DashO readily configurable to ensure effective controls without complicating development or compromising application quality and performance.*

### Advanced obfuscation transforms include:

**Patented Renaming** – Our patented induction overloading takes renaming to a new level of obfuscation.

**Control Flow** – Effectively thwarts machine translation without compromising performance or quality.

**String Encryption** – Our work with various defense departments makes our approach secure, performing and legal for export.

**Built-in "Smart" Obfuscation** – Provides optimized support for Spring, Hibernate, JSP and other frameworks.

### Real-time production defenses and monitoring include:

**Anti-debugger detection** for mobile and desktop offering real-time defensive measures, alerts and reports, and extensions to support integration with preferred IT and system monitoring consoles.

**Shelf Life** triggers absolute and relative expiry behaviors that include custom behaviors, notifications, and reporting. These are suitable for evaluations, beta releases and application inventory management.

**Tamper Defense** protections against malicious modification of runtimes to prevent counterfeiting, piracy, and the introduction of malware.

**Watermarking** – Track unauthorized copies of your software back to the source by embedding data such as copyright information or unique ID numbers.