



# **Business Intelligence to Track and Monetize Software Piracy**

**Arxan Best Practices White Paper**



## Executive Summary

Piracy intelligence gathering is the process of instrumenting software with a remote notify mechanism that transmits information about users of pirated software back to the ISV. This data provides your sales team with potential leads, helps your marketing team understand and characterize your particular piracy situation, and helps product management develop effective anti-piracy strategies.

Arxan's business intelligence solution includes both product, GuardIT, and professional service elements that together yield a complete offering for customers.

Our GuardIT product includes remote notify as a standard reaction when software compromise is detected. Remote notify integrates easily into your software application and backend CRM system. It is fully hardened against tampering, spoofing and server-side attacks to ensure it functions reliably and provides meaningful data without placing your CRM data or enterprise network at risk. ISVs have the option of using remote notify as a piracy monitoring system which measures (but still allows) unauthorized use, or combining it with comprehensive anti-tamper measures for strict license enforcement.

### What is your piracy situation?

ISVs lose an estimated 33% of revenue to piracy on average. But what does this mean for your specific business and software title? Real time piracy intelligence from the field – about both under licensed customers and users of counterfeit software – provides data regarding who is abusing your software, where they are located and how they have subverted your license management layer. This data allows you to measure piracy and gather leads for a potential software sale. It also enables improved software protection strategy, and prosecution where appropriate.

#### Did you know?

- Revenue losses from software piracy exceeded \$48 billion in 2007
- In a challenging economy, software users are more likely than ever to underpay for licenses
- While average piracy losses to an ISV are 33% of revenue, some software sees up to 90% unauthorized use

#### There are three components to an effective anti-piracy strategy:

1. Metering - Enforcing terms of software usage through license management, node locking or similar metering solutions
2. Application hardening – Protecting code integrity, preventing theft of intellectual property (IP) and hardening license management
3. Business Intelligence – Gathering real data regarding the who, where and why of pirated software use, through a combination of active tamper detection, covert callback and software watermarking technologies

**Piracy intelligence data allows you to identify underpaying customers and users of pirated software.** GuardIT allows applications to covertly report back unauthorized use or attack attempts to a central server. This information provides leads for your sales team, and allows your product management team to assess the extent and geographical distribution of piracy.

### Recover revenue and refine strategy

Many ISVs feel that piracy can be priced into their software product, and see piracy as a viral marketing channel that builds their software's popularity. This permissive strategy of allowing controlled piracy to build market share can be effective as long as you retain visibility of where your software is being used and how it is being tampered.

GuardIT's remote notify feature can be used to securely transmit piracy, tampering and forensics information from the field to your sales, marketing and product management teams for sales follow up, strategic analysis and performance monitoring. This helps to recapture revenue as well as prosecute where appropriate. Remote notify



can also be used to measure the effectiveness of anti-piracy programs, and to gather business intelligence on how your customers are using your software. For example, usage patterns, and software problems can all be tracked in real time.

## How It Works

Piracy intelligence gathering works in three steps:

### Step 1: Instrumenting the Application for Remote Notification

GuardIT protects applications using a network of Guards that are embedded into the software binary after compilation. Each Guard performs a specific security check, and reacts in a configurable way if a compromise is detected. Remote notification is available as a reaction for checksum Guards (which detect tampering), anti-debug Guards (which detect debugging or virtual execution) and authentication Guards (which detect code lifting, code injection and similar types of unauthorized execution). The remote notify reaction is specified and configured via an XML configuration file or via GuardIT's rich graphic user interface. It is embedded into the application by GuardIT in an automated, post-compilation protection process.

### Step 2: Gathering and Transmitting Forensic Information from the Application

Leverage Arxan's professional services to configure the remote notify reaction to gather and transmit a variety of data specific to your business and application. This would include:

- IP address, MAC address, domain name, email address, username and other user identifying characteristics.
- Time zone, language setting, zip code or locality setting and other geographic characteristics.
- Application hash (to identify strain of hacked binary), type of compromise, area of binary that is compromised, and other application security characteristics

When a remote notification is triggered on the end user's system, this data would be gathered and composed into an optionally encrypted message that is sent back to a specified IP address or addresses. The packet would be camouflaged within normal internet traffic to protect it from being blocked by application firewalls or port scanners.

### Step 3: Aggregating and Filtering Intelligence Data at the Server

Leveraging Arxan's professional services to remote notify messages, out of the box, can be received in one of two ways.

1. Collated into a log file on the ISV's server or Arxan's piracy monitoring server for subsequent analysis
2. Received by a gateway script which runs on the ISV's server or a cloud computing platform such as Amazon Web Services or Force.com, with automated aggregation into Salesforce.com or other CRM systems.

This data provides actionable leads to your sales team, precise vulnerability information to your development team. Forensic information can also be forwarded to law enforcement agencies for appropriate action.

## GuardIT provides robust, reliable piracy intelligence

**Myth:** Remote notify and traitor tracing measures bypass the attention of professional hackers and directly become active at the end-user layer. Thus, it is not necessary to harden them.

**Reality:** Gathering and use of piracy intelligence data directly affects a hacker's ability to profit from counterfeit software, making it a prime target of attack. Many types of attacks are possible:

In contrast to unguarded alternatives, GuardIT's remote notify feature is part of a deep, layered defense mechanism. GuardIT intelligence gathering is robust in the field and very difficult to spoof, alter or disable. You can therefore confidently expect to see adequate returns from the investment in instrumenting your software, setting up a backend and lead processing infrastructure, and related development and testing overhead.

- Simple software tampering can disable an undefended phone-home call
- Server side components of an intelligence gathering infrastructure are vulnerable to exploits such as SQL injection, man in the middle attacks, and denial of service.



- Software can be tampered to send junk information back to the ISV server.
- Unprotected phone home routines can be tampered to craft packets with malformed strings. This can enable a server-side compromise and potential theft of your CRM credentials and all related data – a severe enterprise level compromise with very high breach management costs.
- End to end hardening of the remote notify infrastructure is critical to protect against these threats. In contrast to unguarded alternatives, GuardIT's remote notify feature is part of a deep, layered defense mechanism. GuardIT intelligence gathering is robust in the field and very difficult to spoof, alter or disable. You can therefore confidently expect to see adequate returns from the investment in instrumenting your software, setting up a backend and lead processing infrastructure, and related development and testing overhead.

## Arxan provides a piracy intelligence solution of choice

**Easy Integration with Application.** GuardIT enables the developer to specify an appropriate reaction when tampering or compromise is detected. Remote notify is a standard user-defined reaction, and can be enabled via an easy point-click interface. The information gathered and sent, the circumstances under which a remote notify is triggered, and the destination for the remote notify data are all fully customizable. GuardIT also provides point-click integration with leading license management systems such as FlexLM®, and customization capability for any in-house or third party system.

**Easy Integration with Backend.** GuardIT provides out-of-the-box support for leading CRM solutions such as Salesforce.com®, and easy customization for integration with a backend system of your choice. The backend gateway can be hosted by the ISV directly, or can be implemented with a cloud platform such as Amazon® Web Services.

**Secure cross-platform support.** GuardIT protection integrates easily into native C/C++ or managed .NET/Java applications. Desktop, embedded and server applications, Windows and Linux, 32-bit applications and 64-bit applications can all be secured with GuardIT and be instrumented to report back with piracy and usage data.

**There are a range of strategies to secure software assets, such as:**

- Permissive management via piracy intelligence gathering
- Under-licensing management via secure node locking
- Complete management by deploying comprehensive application hardening

**With GuardIT you can choose freely from this full spectrum of software security strategies, for all types of applications.**

## More Information

Arxan Technologies Inc. is a leading provider of application hardening solutions designed to protect software intellectual property (IP) from piracy, tampering, reverse engineering and any manner of theft. Arxan supports a full range of application protection needs, from commercial software anti-piracy to military grade assurance. Businesses rely on Arxan to fortify software, license management and DRM applications to prevent the loss of billions of dollars to unauthorized use. Founded in 2001, Arxan Technologies has offices in Bethesda, Md., San Francisco, Calif., Dallas, Boston, Chicago, New York and West Lafayette, Ind. For more information about GuardIT and other Arxan products, please visit [www.arxan.com](http://www.arxan.com) or write to [info@arxan.com](mailto:info@arxan.com).

## Notices

Arxan, the Arxan logo, GuardIT, Guard and GuardScript are registered trademarks or trademarks of Arxan Technologies, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. Portions of the information disclosed herein are protected by U.S. Patent No. 6,941,463; U.S. Patent No. 6,957,341; U.S. Patent No. 7,287,166 and Patents Pending. Copyright © 2009

Arxan Technologies, Inc. All rights reserved.

