



software protection made simple.

Software Piracy

Recover Revenue from Piracy with Advanced Technology

Most Independent Software Vendors (ISVs) have invested in license management systems to deter license overuse and inadvertent piracy of their valuable software applications. While these systems provide some measure of protection, they are no match for the software cracking community which has the knowledge and tools to bypass license management functions altogether. Often, hackers use reverse engineering tactics to quickly disassemble and patch software licensing systems – allowing free or low-priced copies to be easily created and distributed globally.

Piracy groups specifically target high-value software (i.e., software licenses costing thousands of dollars per seat) used in manufacturing, modeling, design, test, and other analytical processes. Businesses in emerging countries that use this software to build new products and compete for offshore contracts are fueling this demand at increasing rates. Although ISVs in this space have adopted sophisticated licensing systems designed to prevent piracy (and some have pursued legal interdiction services), none of these solutions have been effective. Licensing systems have been quickly cracked and legal enforcement has been severely limited by weak IP laws in emerging countries.

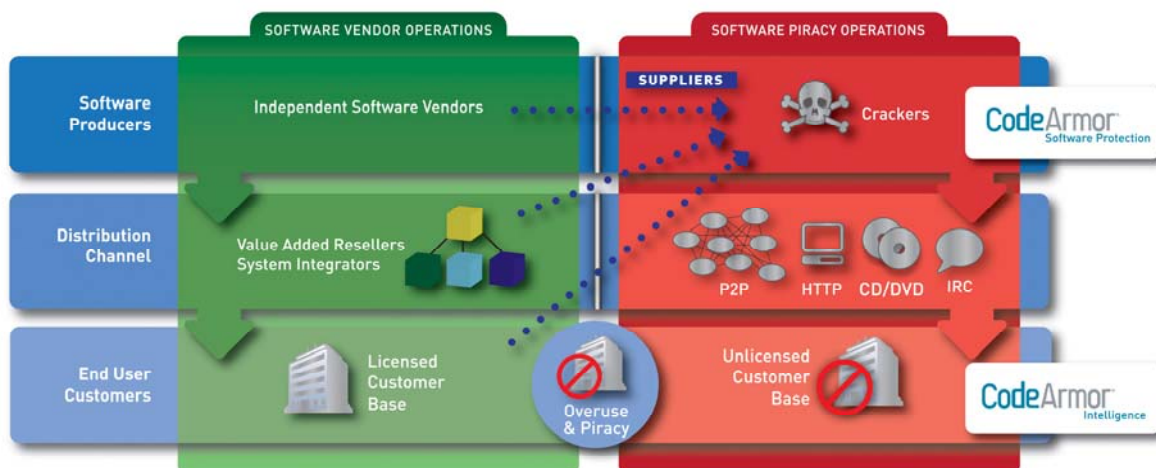
Challenges of the Piracy Distribution Channel

The piracy scene mirrors traditional ISV distribution channels, using an efficient and well distributed framework to make cracked applications available to the masses. Key distribution methods include peer-to-peer file sharing services like BitTorrent, popular search engines or pirate index services like thepiratebay.com, Web and auction sites, and street warez merchants that distribute counterfeit software. This complex and robust distribution channel makes it very easy for infringing organizations to find the cracked software they need to build their businesses. Shutting down any given node in the network does little to stem the flow of cracked applications.

CodeArmor enables ISVs to recover revenue from piracy.

Software Protection is a layered defense against reverse engineering that targets piracy groups and the software cracking process itself.

Piracy Lead Generation identifies the actual end users of pirated software and enables ISVs to recover the license revenue by pursuing them through legal or sales activities.



CodeArmor Software Protection and Piracy Intelligence

The patented CodeArmor® platform offers two products that allow ISVs to deter piracy and gather intelligence on their specific products' piracy activity to recover revenue.

CodeArmor Software Protection is a layered defense against reverse engineering that targets piracy groups and the software cracking process itself. An ISV adds CodeArmor anti-reverse engineering protection into its software release to prevent the embedded Digital Rights Management or licensing functions from being bypassed (bypassing these functions is known as *binary tampering* and is the most common method of enabling an application to be pirated). CodeArmor hardens these functions in the software binaries using code encryption, obfuscation, anti-tampering and anti-debugging capabilities, and extends the time it takes to crack the software – reducing the supply of pirated software and giving ISVs more time to recover revenue. Because protection is added to the software binaries (and not the source code itself), the protection process can be automated, allowing the ISV to focus its efforts on its core competencies and products' functionality.

CodeArmor Intelligence identifies the actual end users of pirated software and enables ISVs to recover the license revenue by pursuing them through legal or sales activities. The CodeArmor Intelligence technology remains dormant unless it detects crack-related tampering, at which point it begins to gather forensic evidence of actual use of the software by the infringing organization. It is a turn-key piracy lead generation solution that can be quickly integrated within existing releases and provides the data needed to quantify the true scope of an ISV's piracy problem. The reporting capability communicates data to the ISV's reporting and lead management database using stealthy and secure communication technology and provides filtering capabilities for large amounts of data to allow forensic data to be organized into sales leads and easily integrated into Salesforce.com and existing CRM systems. CodeArmor Intelligence can be used on its own or combined with CodeArmor Software Protection.

Choosing the Right Approach

Selecting the right anti-piracy strategy depends on a variety of factors including market focus, the type of software, and the maturity of the business and software. **Software Protection** is a sound strategy if there is software IP at risk, compliance and robustness requirements, a new licensing investment, low customer risk to apply or Microsoft .NET is being used. **Intelligence** is a good choice where there is unknown piracy loss and activity, a mature product with many versions, a large complex customer base, the software is used by businesses, and there is a sales presence or legal services infrastructure in place.

Revenue Recovery

While there is no magic bullet to eradicate software piracy, the CodeArmor platform enables ISVs to recover revenue by focusing on the producers of cracked applications or businesses that are using pirated software. Because the pirated software channels are highly distributed, well-organized and robust, they have been impervious to attempts to bring them down. Individual vendors must examine their markets and product offerings to determine whether Intelligence should be implemented before pursuing a Software Protection strategy. In addition to providing strong data on the full scope of a vendor's piracy problem, Intelligence augments existing legal and sales processes by creating piracy leads to directly recover license revenue from businesses using pirated software.