



## **Unified Software Protection: Modern Strategies for Securing Software Revenue**

---

### **OVERVIEW**

Organizations that rely on the sale of software as a revenue stream need to be concerned with maintaining flexible licensing while still preventing piracy. Fortunately, there are solutions available in today's market to address the needs of companies looking to protect their software and control its use. This paper attempts to define some of the challenges independent software vendors (ISVs) face in protecting their intellectual property and ways in which they can maximize the benefits of anti-piracy solutions.

### **TELLING THE GOOD GUYS FROM THE BAD GUYS**

The violation of software licensing, whether intentional or unintentional, equals lost revenue for software vendors, who must work to minimize this loss. However, when implementing software protection solutions, vendors must be careful not to negatively affect customer acceptance with, for instance, the accidental prevention of use for legitimate users or onerous license activation processes.

Often times ease of use and prevention of piracy can act in opposition. Entirely software-based licenses enable the greatest level of flexibility and end user transparency, but cannot provide as strong a measure of security. The environment in which the software operates cannot be considered entirely secure because the license is stored on the machine and not a separate, hardened device. Therefore, software-based solutions do not offer the strongest type of defense against piracy attacks.

The technologies that make up hardware keys (dongles) have advanced greatly since their invention and the concept remains a practical and popular one: a robust, reliable external device that ties the license not to a machine, but to the owner of the hardware key. While hardware based solutions provide the highest level of security available, they can also be considered difficult to distribute and manage. For this reason, these types of solutions are less popular in markets where rates of piracy are low and, for example within enterprise-class software where intentional piracy is a lesser concern.

When deciding to introduce software protection, it is important to consider the nature of the software being sold, the target audience, the intended market and the amount of the existing piracy. Highly specialized software that requires extensive training and support is not likely to have broad appeal on a P2P network and not a likely candidate for software protection, per se. However, these applications do benefit from license management where

number of seats sold and amount of features sold have significant dollars associated with them.

Software-based and hardware-based licensing each have distinct advantages and disadvantages. Implementing a complete protection program should involve either one or a combination of both technologies, used as necessary depending on the market being served. Ideally, a single technology source can be used that offers both software and hardware licenses, allowing a company to maintain a corporate wide standard.

### **THE PROBLEM OF ADVANCED TECHNOLOGY**

The rapid advancement in the availability of high speed Internet access has presented both an opportunity and a problem to software companies. Pirated software can be rapidly disseminated worldwide, quickly and effectively inflicting damage on the revenue streams of software vendors. P2P networks in particular have achieved notoriety in the media for their role in the illegal distribution of music and movies. The same networks are also flooded with illegal copies of high priced software. Needless to say, a pirated copy of *Star Wars III* is going to receive more media attention than a pirated version of TurboTax®, but the problem remains the same. In fact, according to research conducted by SafeNet MediaSentry Services™, one of the most pirated pieces of content in 2005 was not a song or a movie, but a very popular photo editing software program.

Associations like the Business Software Alliance (BSA) and the Software & Information Industry Association (SIIA) are the software industries equivalent of the Recording Industry Association of America (RIAA). Like their counterparts, BSA and SIIA work to thwart the illegal distribution of software. Their efforts, while significant, did not lead to a decrease in the overall percent of software pirated from 2004 to 2005. Unfortunately while the percentage of software pirated held steady at 35%, losses due to piracy increased by \$1.6 billion over 2004, to \$34 billion.

### **KNOWLEDGE IS POWER**

Many software companies are alerted to their piracy problem when they find, much to their horror, that copies of their application are available on P2P networks mere weeks, sometimes even days, after release. Because of their mass appeal, music and movies are usually shared among a broad audience. Software piracy, although less publicized, is also big business. Those with the technology to investigate this problem can see just how rampant the problem is. The internet is filled with countless sites where pirated copies of expensive software can be purchased at a fraction of the price.

Fortunately, monitoring services have been developed that can report not only how much, but where piracy is occurring. The results of “where” are equally important when making decisions about software protection, because certain regions may call for tighter security measures than others. Unfortunately, most organizations do not have access to quantifiable information of this type. Perceptions of piracy rates are often based on anecdotal evidence. Real statistics are often a complete, and often unpleasant, surprise.

The real ongoing value of knowing about piracy is in its ability to allow a company to evaluate and adapt its anti-piracy measures as required. The ability to monitor piracy gives insight not only into the value of software

protection itself, but also allows a company to engage in protection modeling assessments. For instance, the monitoring results can validate or invalidate a decision to use hardware-based protection in geographies where piracy rates are particularly high. Without data on piracy rates software protection decisions are made based on small sample evidence and "common sense" techniques. Monitoring services provide the business intelligence for software protection that allows companies to close the loop between design, fulfillment and ongoing management.

The complex and dynamic nature of online piracy makes effective monitoring challenging. Accurate assessments of piracy threats often require time intensive manual reviews to verify the authenticity of software titles. The continued growth of piracy sites means ISVs must invest in extensive resources in order to conduct piracy monitoring. In addition, factors such as the emergence of open source clients and community supported protocols further the need for dedicated anti-piracy monitoring resources. Covering this expansive universe is not only time-consuming from a resource perspective, but can also be extremely costly.

#### **TIME TO MARKET**

Getting products quickly to market is often a high priority for software vendors. Delays in deployment can be costly and reflect poorly on the software development team. Software protection is typically implemented at the end of the software development cycle, when pressure to get the product to market is highest. This forces developers to require a solution that can be implemented quickly without extensive training or programming. A robust set of developer tools can cut development time while increasing the functionality delivered.

#### **SYNCHRONIZATION**

When implementing software licensing and protection, fulfillment must be considered as well. Software protection solutions almost always involve sending a license, either a hardware key or an electronic license, or even a paper license, to the end user. These licenses need to be tracked and managed. Many companies that engage in ecommerce want to tie licensing back to the same CRM and ERP systems that capture the payment and authorization information.

The extent of back office integration, the amount of licenses being delivered, and the license models being implemented all impact the integration of software protection into an application. Often, organizations make the mistake of deciding on a solution at a business unit level, rather than a corporate level. A product manager or development manager sees piracy having a negative impact on the product and decides to either build or buy some prevention technology. If the results seem effective, particularly in the short run, the owner considers the problem addressed if not entirely solved.

If the decision to protect software is not made at a corporate level the results will be confined to the product using software protection. A company could find itself with a dizzying array of software protection techniques, both home grown or purchased, and all tracked and managed separately. The tracking and management of licenses are often done manually and records are maintained by the software division or business unit. The more divisions there are, the more difficult it is for a company to make decisions or gather information about all their products. It is virtually impossible to have a

standard process for fulfillment and a centralized repository of licenses if each department implements their own protection scheme.

### **REDUCTION OF COSTS**

One of the most important reasons for considering standardization is the cost of fulfillment. The distribution, tracking and management of licenses are all very relevant parts of the licensing ecosystem. Often times they are managed through manual processes which are costly and inefficient. Also, with no uniform methodology for managing fulfillment, sharing and presenting the information collected to those unfamiliar with the licensing technology is difficult. Imagine a company with 15 different reports on licensing statistics, all displaying essentially the same information in various formats. The ability to consolidate reports and make intelligent business decisions based on pertinent licensing information is greatly hindered.

### **BEYOND YOUR EVENT HORIZON**

Complete software protection includes methods for protecting applications beyond your event horizon and after delivery to end users. If a copy of software is successfully pirated, a software vendor is thankfully not powerless to prevent rampant dissemination. Countermeasure techniques used by anti-piracy vendors can stem unauthorized distribution through seamless integration into the piracy networks themselves.

Techniques can be used that prevent would-be pirates from accessing pirated content. They could end up downloading a trial-only version, or be continually queued to download, so the download is never finished. On some networks it is possible to directly interfere in the process of downloading a pirated file, most often resulting in the user abandoning their download attempts altogether.

### **HORSEPOWER**

Achieving maximum efficacy in the reduction of online piracy requires not only sophisticated engineering expertise but also sustained and diligent execution of countermeasure campaigns. Additionally a worldwide reach is necessary in order to make significant reductions in the spread of pirated software. Sheer horsepower and global reach are clearly required. Additionally, countermeasures are also only highly effective when implemented in scale, which requires significant development resources as well as physical hardware infrastructures. If this type of initiative is not in line with the core business of an ISV, undertaking countermeasure campaigns can result in significant monetary investment with little or no tangible return. Fortunately specialized anti-piracy vendors are available to undertake countermeasure campaigns on behalf of ISVs so it is not necessary to allocate excessive resources.

### **SYNERGY**

The overall goal of software protection is to increase revenues. As with many enterprise-wide initiatives, simple objectives can often get lost in the complexities of deployment.

A standard software protection technology also makes implementing a standard fulfillment process simpler. IT can develop a fulfillment methodology to be automated, extended to the channel and most importantly maintained by a single department, thereby reducing the costs of having fulfillment managed by individuals scattered across multiple business units. Tracking and management of licensing information can also be centralized. It is

important to select and implement software protection that can be centralized to allow for the synergistic benefits.

### CONCLUSION

While entertainment content gets most of the media publicity, software faces equally significant piracy challenges. The consolidation of software protection techniques allows companies to reduce the time and effort required to implement and maintain a solution and to allow scalability. Monitoring piracy rates provides quantifiable data and services provide the ability to impact software piracy beyond your event horizon.

Like CRM and ERP, decisions about software protection should be corporate wide initiatives. Taking a unified approach reduces the effort and cost associated with deployment, provides data on efficacy and brings focus to the goal of reducing the revenues lost due to unlicensed use.

### SafeNet OVERVIEW

SafeNet (NASDAQ: SFNT) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property, and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit [www.safenet-inc.com](http://www.safenet-inc.com).



[www.safenet-inc.com](http://www.safenet-inc.com)

**Corporate Headquarters:** 4690 Millennium Drive, Belcamp, Maryland 21017 USA  
Tel: +1 410.931.7500 or 800.533.3958 email: [info@safenet-inc.com](mailto:info@safenet-inc.com)

Phone USA and Canada (800) 533-3958  
Phone Other Countries (410) 931-7500  
Fax (410) 931-7524  
E-mail [info@safenet-inc.com](mailto:info@safenet-inc.com)  
Website [www.safenet-inc.com](http://www.safenet-inc.com)

©2005 SafeNet, Inc. This document contains information that is proprietary to SafeNet, Inc.  
No part of this document may be reproduced in any form without prior written approval by SafeNet.  
SafeNet shall have no liability for errors, omissions or inadequacies in the information contained herein  
or for interpretation thereof. The opinions expressed herein are subject to change without notice.

**Australia** +61 3 9882 8322  
**Brazil** +55 11 4208 7700  
**Canada** +1 613.723.5077  
**China** +86 10 885 19191  
**Finland** +358 20 500 7800  
**France** +33 1 41 43 29 00  
**Germany** +49 18 03 72 46 26 9  
**Hong Kong** +852.3157.7111  
**India** +91 11 26917538  
**Japan** +81 45 640 5733  
**Korea** +82 31 705 8212  
**Mexico** +52 55 5575 1441  
**Netherlands** +31 73 658 1900  
**Singapore** +65 6297 6196  
**Taiwan** +886 2 27353736  
**UK** +44 1276 608 000  
**U.S. (Massachusetts)**  
+1 978.539.4800  
**U.S. (Minnesota)**  
+1 952.890.6850  
**U.S. (New Jersey)**  
+1 201.333.3400  
**U.S. (Virginia)** +1 703.279.4500  
**U.S. (Irvine, California)**  
+1 949.450.7300  
**U.S. (San Jose, California)**  
+1 408.452.7651  
**U.S. (Torrance, California)**  
+1 310.533.8100

**Distributors and resellers  
located worldwide.**