SafeNet | SENTINEL SOFTWARE MONETIZATION SOLUTIONS

Defending Against the Triple Threat to Intellectual Property

A White Paper for Software Publishers & Intelligent Device Manufacturers

WHITEPAPER

Contents

Overview

Technology and innovation have never moved faster and most of it involves software in one form or another. From off the shelf packaged software products, to software offered as a service from the cloud, to intelligent hardware devices in the data center, in your home, or in the palm of your hand – software now drives it all.

The companies that develop these products have invested countless hours and dollars in research and development and in writing software code. The code that drives these software products and intelligent hardware devices contains trade secrets and is valuable Intellectual Property (IP). If not properly protected, this IP may easily be compromised causing irreparable damage to a company brand, its ability to compete, its revenue, and the experience provided to its customers.

This paper discusses the triple threat to intellectual property and explains the forms that IP attacks take. It also explains the consequences of inadequate protection, and presents best practice examples of how successful publishers are using commercial software rights management solutions to proactively protect their intellectual property investments and increase revenues.

The Triple Threat to Intellectual Property

Attacks on Intellectual Property (IP) come in a variety of forms including:

- Software piracy
- Reverse engineering & theft of trade secrets
- Code tampering

Each of these poses a serious threat to software revenue and future innovation for software publishers and intelligent device manufacturers.

Software Piracy

The most obvious example of IP compromise is Software piracy. Also known as illegal use and theft, piracy is the unauthorized duplication and/or distribution of copyrighted computer software; an act that infringes upon the legal rights of the software publisher. According to the Ninth Annual BSA Global Software Piracy Study conducted by IDC and IPSOS, 42% of software was pirated in 2011. While worldwide revenue losses due to software piracy were $63.4 billion, up from $58 billion in the preceding year. [i]

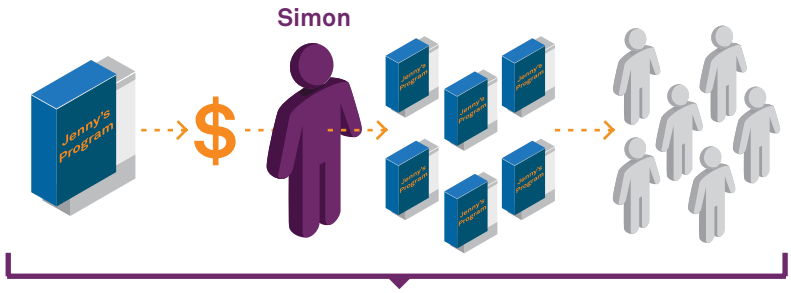
Whether intentional or not, a vast amount of intellectual property and revenue is lost to piracy each year and diverted from software companies and local governments. Revenue that otherwise would be reinvested in R&D to develop and improve legitimate software programs simply does not reach software publishers.

A software piracy scenario is depicted in the figure below. Someone purchases a license to use one copy of your software program and makes multiple copies which are then illegally shared or sold to others.

---

i, BSA Report (The BSA Global Software Piracy Study, conducted in partnership with IDC and Ipsos Public Affairs), http://portal.bsa.org/globalpiracy2011

SOFTWARE PIRACY



Simon buys one copy of Jenny's Program, then makes illegal copies and distributes

"A majority of the world's personal computer users—57%—admit they pirate software."

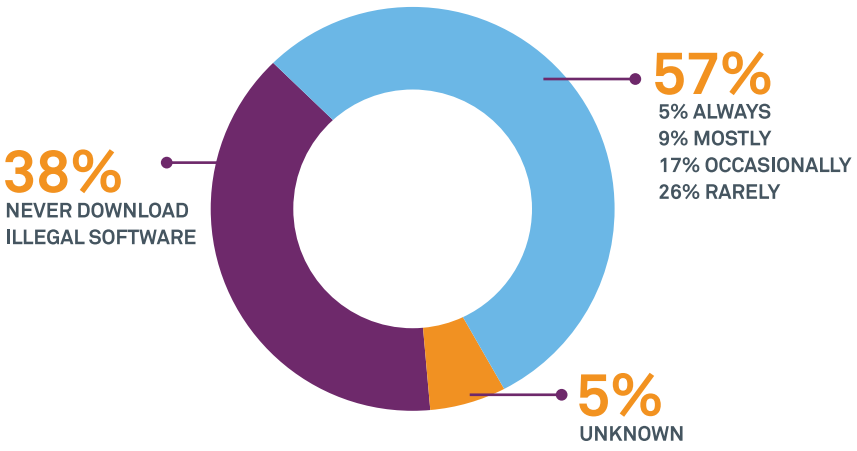
Most organizations equate software piracy to intentional theft; however, software piracy also includes overuse of legally-licensed software, whether intentional or inadvertent. One example of inadvertent overuse is when a company purchases and is licensed to use a set number of software seats, but actually uses more than they are entitled to use.

Although most end users today are aware that unauthorized use and duplication of software is illegal, many show a general disregard for the importance of treating software as valuable Intellectual Property.

In fact, according to the Business Software Alliance (BSA), "A majority of the world's personal computer users—57 %—admit they pirate software. That includes 31% who say they do it 'all of the time,' 'most of the time,' or 'occasionally,' plus another 26% who admit they pirate, but only 'rarely'. Fewer than four users in 10 (38%) say they 'never' acquire software that is not fully licensed." [ii]

GLOBAL SELF-REPORTED PIRACY

Q: "HOW OFTEN DO YOU AQUIRE PIRATED SOFTWARE OR SOFTWARE THAT IS NOT FULLY LICENSED?"



BSA Report (The BSA Global Software Piracy Study 2011, conducted in partnership with IDC and Ipsos Public Affairs)

---

ii, BSA Report (The BSA Global Software Piracy Study, conducted in partnership with IDC and Ipsos Public Affairs), http://portal.bsa.org/globalpiracy2011

SafeNet Survey Reveals:

- Forty-eight percent of software companies have lost revenue due to software piracy
- Seventy percent say copy protection to prevent piracy is one of their biggest challenges
- Only 58 percent employ proper protection and compliance enforcement to combat piracy

Clearly, this is a problem that concerns software publishers. More than 48% of software developers responding to a recent SafeNet survey indicated that they had lost revenue due to software piracy. And an overwhelming seven in ten (70%) indicated that copy protection to prevent piracy is one of their greatest challenges.

In spite of the acknowledged revenue loss and the high level of awareness regarding the risks of piracy, it is surprising then, that only 58% of developers reported that they employed proper protection and compliance enforcement mechanisms to combat piracy efforts.[iii]

The Impact:

Lost revenue: Developing a software application involves a major investment of time, money and effort. Software piracy (including illegal network licenses and unfulfilled upgrades) denies you the revenue you deserve and harms your paying customers, who ultimately bear the cost of illegal use of your products.

Less Innovation: Piracy limits your ability to be competitive, leading to higher-priced, less advanced products for your customers.

Piracy harms your end users: Copyright infringement not only hurts the software industry, it also has negative consequences for the end user. Here are just a few of the common-sense reasons users should avoid pirated software:

- No access to technical support
- Lack of product documentation and warranties
- Content may be incorrect or outdated
- Software may contain viruses or be defective or corrupted
- Difficult or impossible to upgrade
- Expensive lawsuits and/or significant penalties

"Since January, BSA has settled a number of cases of unlicensed software – including eight cases representing a value of more than $2.5 million. The companies involved in these cases are effectively denying copyright owners the rights to compensation for their hard work and intellectual property."

-Jodie Kelley, SVP Anti-Piracy & General Counsel, Business Software Alliance

The Solution: Copy Protection & License Enforcement

A well planned and executed strategy to fight piracy and illegal software use is a key business practice in a strong market, and it becomes even more critical in a difficult economic environment.

Software publishers can employ either reactive or preventative measures in order to counter piracy and illegal use:

Reactive Measures

Many software publishers do nothing to secure their software from illegal use. Instead, they rely on software license agreements and copyright law to protect their software. However, these control mechanisms do not prevent a user from intentionally copying the software and distributing it. Nor do they prevent intentional or inadvertent overuse. If a publisher believes their software has been pirated or used illegally, the power of reactive methods lies only in the legal remedies available to software publishers against software pirates.

Watchdog groups like Federation Against Software Theft (FAST), the Software Information Industry Association (SIIA), the BSA, the World Intellectual Property Office (WIPO) and others are doing their part to educate users and drive legislation that protects software publishers.

---

iii , 'The State of Software Monetization' Survey, commissioned by SafeNet and the SIIA Oct/Nov 2012 http://www2.safenet-inc.com/smsurvey/index.html

"In mature markets, only 20% of those who admit they frequently pirate software say the risk of getting caught is a reason not to do it. In emerging markets, the figure is even lower — just 15% of pirates appear to be concerned about the risk of getting caught. This suggests there is a need to ramp up enforcement to send a stronger deterrent signal to the marketplace."
-Global Software Piracy Study 2011

The BSA, which also investigates, prosecutes, and litigates cases of reported software piracy, recently worked on behalf of Adobe, Autodesk, Microsoft, Quest, and Symantec to settle eight software piracy cases. According to Jodie Kelley, BSA's Senior Vice President of Anti-Piracy and General Counsel, "Since January, BSA has settled a number of cases of unlicensed software – including eight cases representing a value of more than $2.5 million. Using pirated software – even if unknowingly – has the potential to expose a company to devastating legal, financial, and security risks. The companies involved in these cases are effectively denying copyright owners the rights to compensation for their hard work and intellectual property."[iv]

Even though these high profile piracy prosecutions receive plenty of attention, there is still a troubling lack of incentive among admitted pirates around the world to change their behaviour. According to the most recent BSA piracy report, "In mature markets, only 20% of those who admit they frequently pirate software say the risk of getting caught is a reason not to do it. In emerging markets, the figure is even lower — just 15% of pirates appear to be concerned about the risk of getting caught. This suggests there is a need to ramp up enforcement to send a stronger deterrent signal to the marketplace." [v]

While legal action does have value, it can be very costly, and as evidenced by the most recent BSA report, because it is inherently reactionary, it cannot be relied upon to prevent the problem.

Proactive Measures

There are numerous technology-based preventative measures that software publishers take to combat piracy and illegal use.

Some publishers begin by employing more secure code-writing practices.

Others write their own protection & licensing code. Publishers who rely on their development staff to write homegrown protection and licensing code usually have limited security expertise, limited resources to maintain the security code and stay ahead of hackers, and limited results.

Publishers who rely on their development staff to write homegrown protection and licensing code usually have limited security expertise, limited resources to maintain the security code and stay ahead of hackers, and limited results.

Many software publishers trust the expertise, strong security, and license enforcement found in commercially-available software rights management (SRM) solutions to fight piracy and illegal use. Using a commercial protection and licensing solution can result in faster time-to-market, in addition to initial cost savings in implementation and lower cost of ownership when compared to homegrown licensing.

The most powerful commercial solutions employ software- and hardware-based locking and license enforcement. Software protection keys and hardware (USB) keys each have their own distinct advantages and should be considered depending on the specific goals and needs of the software publisher and the needs of their customers. For example, if the publisher delivers their software electronically, then software-based protection and product activation is generally the best method to implement. If the end-user customer requires easy access to the protected application with portability between computers, then it is likely that they will select hardware-based protection.

There are a number of additional issues that need to be considered when selecting the type of proactive software protection and licensing to use, including the level of security required, distribution methods, portability, software price, and more. Software rights management solutions are a proven method for helping to prevent software piracy and secure software revenue.

---

iv, BSA Press release: http://www.bsa.org/country/News%20and%20Events/News%20Archives/en/2012/en-08212012-US.aspx
v, BSA Report (The BSA Global Software Piracy Study, conducted in partnership with IDC and Ipsos Public Affairs), http://portal.bsa.org/globalpiracy2011

Best Practice Case: TAISA

Sentinel HASP HL Protects TAISA High-Value Preventative Maintenance Software from Piracy and Illegal Use while Significantly Boosting Sales

Technical Applied International S.A. De C.T. (TAISA), established in 1974 and based in Mexico, is the leading creator of preventative maintenance software deployed internationally.

"We started with home-grown software protection, but with the passage of time we realized that the solution we had was too simple to protect our software from piracy and losses."
-Pablo Seeliger, TAISA

The Business Challenge

With the creation of their PM Software, TAISA launched a unique product architecture that relied on the maintenance equipment at three facilities and on three disks: a master disk and two more for backup, all of which required anti-piracy protection. With a growing market demand for PM Software and increased competition from companies in the United States, TAISA's homegrown software rights management solution was no longer enough to prevent piracy. They needed something more robust and secure.

"Since our PM Software was developed, there was always the need to protect it," said Pablo Seeliger of TAISA. "We started with homegrown software protection, but with the passage of time we realized that the solution we had was too simple to protect our software from piracy and losses." After realizing the need for more comprehensive IP protection, TAISA tested several software rights management products for compatibility and robust security.

The Solution

After testing Sentinel HASP, Seeliger was convinced that HASP would provide the security required for TAISA's software. HASP easily integrates with TAISA PM Software so the software will not run without the HASP key, preventing unauthorized use, as well as providing IP protection and multiple licensing options.

"Sales after the implementation of HASP increased remarkably, to such an extent that today we could not conceive further developing our PM software without HASP."
-Pablo Seeliger, TAISA

The Results

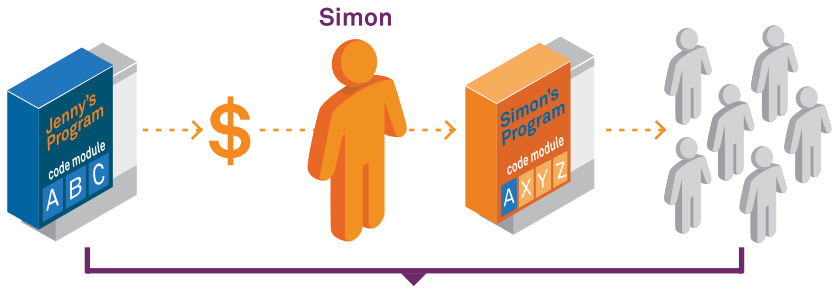
"Without HASP, our losses in sales could have been 20 or 30 percent," explained Seeliger. Not only is TAISA able to protect its software product with complete certainty, but the implementation of the HASP keys allows TAISA to create two versions of its software: a single-user version and a network version which allows multiple users to access the software. Sentinel HASP allows TAISA to protect its software once and deliver it to customers in many formats – increasing sales. "Sales after the implementation of HASP increased remarkably, to such an extent that today we could not conceive further developing our PM software without HASP," Seeliger said.

Implementing Sentinel HASP has also allowed TAISA to confidently expand market reach into countries such as Venezuela, Colombia, Argentina, and Spain.

Reverse Engineering & Theft of Trade Secrets

Software publishers invest a significant amount of resources in research and development of their products, writing code and creating intellectual property that serves as a key advantage and differentiator over competing software and software-driven intelligent devices. Intellectual Property (IP) represents the vast majority of a typical software company or intelligent device manufacturing company's market value. During challenging economic times, competitive pressures naturally increase as companies become more aggressive in trying to win business. With competitive espionage becoming more and more common, your valuable software IP—containing code, algorithms, application data files, and trade secrets—are at risk of prying eyes, reverse engineering, theft, and copycatting by competitors.

REVERSE ENGINEERING & THEFT



Simon extracts trade secrets from Jenny's program code to use in his program code and sells it

Thirty-three percent of global respondents to a recent SafeNet survey believe that reverse engineering and theft is having a major impact on their businesses.

An overwhelming 63% of respondents see code protection to prevent reverse engineering as being a challenge.[vi]

The Impact:

Loss of competitive advantage: through reverse engineering and theft of trade secrets.

Loss of revenue and damage to brand reputation: due to a proliferation of gray market copycat software and software-driven hardware devices.

SafeNet Survey Reveals:

- Thirty-three percent believe reverse engineering and theft has a major impact on their business
- Sixty-three percent see code protection to prevent reverse engineering as a challenge

The Solution: Protect valuable IP against reverse engineering and theft

In these economic times more than ever, it is essential for you to solidify your competitive advantage. As competition increases, it is important to protect that advantage by implementing methods to secure your products from reverse engineering which could lead to theft of valuable IP and trade secrets. If you secure your trade secrets and source code from prying eyes you gain market share by maintaining and continuing to grow your competitive advantage.

Software solutions not only consist of executables and DLLs, they also contain data files which may be of even greater value than the software applications themselves. In many cases, these data files contain highly sensitive information and IP which also must be secured against theft, and copycatting by competitors.

A commercial software rights management solution featuring automatic file wrapping technology provides powerful intellectual property protection against reverse engineering through file encryption, code obfuscation and system-level anti-debugging — ensuring that algorithms, trade secrets, and professional know-how embedded in the software are secured against hackers.

Guarding Intellectual Property protects your competitive advantage and revenue.

---

vi, 'The State of Software Monetization' Survey, commissioned by SafeNet and the SIIA Oct/Nov 2012 http://www2.safenet-inc.com/smsurvey/index.html

Best Practice Case: Virtual Surveillance

Sentinel HASP Halts an Attack in Progress, Protecting Virtual Surveillance Hardware and Software Systems from Reverse-Engineering and Theft

Virtual Surveillance designs and markets digital video surveillance systems used for the surveillance and protection of multi-site operations. The company also produces motion analytics software including motion detection, digital trip wires, object left-behind or removed detection, etc. Virtual Surveillance provides integration with existing alarm systems and alarm triggering capabilities based on any motion event detected in a video feed by its software.

With the imminent threat of a hack underway, speed in implementation was of the essence.

The Business Challenge

Originally, Virtual Surveillance produced their copy protection in house. However, their homegrown protection made it difficult to move the software license to a different machine, or to copy it. For instance, if someone were to use one of the readily-available tools to spoof the MAC addresses of network cards, they could continuously re-use a single software license key. Their worst fears became a reality when they discovered a breach in security. Someone was attempting to reverse-engineer both their hardware and software products.

With the Sentinel HASP key on their side, Virtual Surveillance was able to quickly protect their software before the threat could manifest itself into actual theft.

The Solution

This attack led Virtual Surveillance to Sentinel HASP. The software is spread across many different applications, each of which is dependent on an ASP.Net web service used for sharing media, such as video and snapshot images. This method enables the synchronization of media across various machines and users, requiring an access code to obtain the information.

Due to the security requirements for these applications, having a closed network is an absolute necessity. By creating a system using HASP keys to protect access to the ASP.Net web service, Virtual

Surveillance is able to create a single point of failure, rendering the other applications useless. The web service performs real-time checks to the HASP key during each call. If the HASP key were not present, the key would throw an error to the client application, rather than fulfilling the desired request.

With the imminent threat of a hack underway, speed in implementation was of the essence. SafeNet provided quick and simple instructions, along with a sample C# code which they were able to modify. With the Sentinel HASP key on their side, Virtual Surveillance was able to quickly protect their software before the threat could manifest itself into actual theft.

"HASP gave us the tools necessary to fully protect our software, so we could focus more time on our customer's needs. Our total cost in protecting our multi-million dollar development effort from a known threat was less than $300, including development time and overnight shipping both ways." ***-Eric Burcham, CTO, Virtual Surveillance***

The Rewards

After less than two hours of development time and a quick on-site update, Virtual Surveillance was able to completely protect their multi-million dollar development effort from a known reverse engineering attack that was underway. The cost to them, had the hacker succeeded, would have been incalculable.

"The keys themselves," noted CTO Eric Burcham, "cost a thousand percent less than the time and effort we would have spent coding our own equally formidable protection, and manually generating and keeping track of activation keys for our customers."

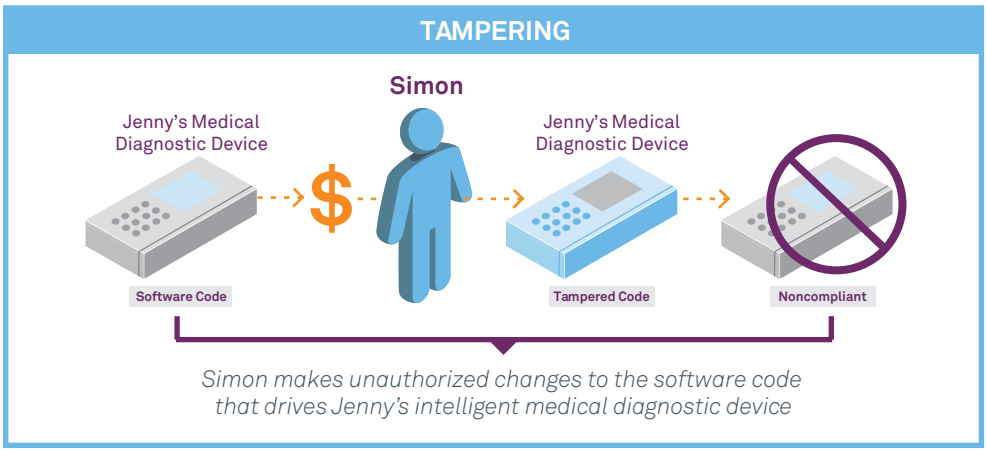
As a small company providing a highly specialized turnkey solution for a rapidly changing and elitist market, Virtual Surveillance needed to protect their assets. Burcham further stated, "HASP gave us the tools necessary to fully protect our software, so we could focus more time on our customer's needs. Our total cost in protecting our multi-million dollar development effort from a known threat was less than $300, including development time and overnight shipping both ways."

Tampering

While theft of trade secrets can be catastrophic, for many ISVs and intelligent device manufacturers, code tampering can be equally devastating. Both scenarios have great potential to damage overall market share and therefore decrease revenue potential.

Tampering occurs when someone gains access to your software code and makes a change to how the product functions. It's important to realize that tampering can be intentional and malicious, or accidental and with good intent. Accidental tampering by an end user usually goes undetected until the damage is done and it is too late.

In the good intent example below, we consider a piece of medical diagnostic equipment. The internal software is designed to control how diagnostic tests are run. Perhaps an end user somewhere thinks the system is slow and decides to tamper with the software code just enough to speed up calculations by 20 percent. Mission accomplished—they are now able to test more patients per day. No malicious intent whatsoever.



While theft of trade secrets can be catastrophic, for many ISVs and intelligent device manufacturers, code tampering can be equally devastating. Both scenarios have great potential to damage overall market share and therefore decrease revenue potential.

What they may not know is that by speeding up the calculation process, they are speeding up a process that needs the extra time to meet several medical industry regulations. Subsequent tests run on the equipment are inaccurate. Who gets the negative press and resulting drop in sales? Not the user who messed with the equipment. Not the hospital. It's the manufacturer of the medical equipment and/or the software vendor that will be cited for having faulty software.

The Impact

The solution may no longer meet business goals: As a consequence of tampering through code manipulation, the software and equipment may no longer satisfy the business goals for which it was intended.

Unexpected results: Tampering with the software embedded within a device can change how the device functions and produce tainted system output.

Lost revenue: Tampering with code could potentially provide users with access to features they have not paid for.

Damage to brand reputation: Regulatory compliance issues can do irreversible damage to your brand and product reputation.

The Solution: Tamper Protection

Without the proper encryption and code obfuscation protection technologies, intelligent device vendors are unknowingly leaving their code vulnerable to tampering.

By effectively controlling access to software source code, software publishers and intelligent device vendors can protect revenue and safeguard the integrity of their brands and products by preventing product tampering, reverse engineering, and IP theft.

Without the proper encryption and code obfuscation protection technologies, intelligent device vendors are unknowingly leaving their code vulnerable to tampering.

Best Practice Case: Leading Packaging Industry Manufacturer

This case example deals with a leading manufacturer that develops software-driven equipment to process end-to-end packaging of liquid consumer food products such as milk and orange juice. The software that runs their packaging equipment is programmed to comply with dozens of public health and safety regulations.

The company's IP protection concerns center around controlling access to the software running the machines and limiting the ability to tamper with key parameters that control processes such as pasteurization. This packaging industry manufacturer uses a combination of SafeNet Sentinel RMS and EMS software monetization solutions to protect their software code from being accessed and tampered with and to strictly control who can change the parameters that control the packaging equipment.

Conclusion

The research data shows that large numbers of software publishers worry that their business is negatively impacted by not protecting their IP. The research also overwhelmingly indicates that not nearly enough ISVs have implemented the proactive defensive measures required to ensure that their intellectual property is protected.

If software companies are worried about the damage that compromised software IP can have on their brand, their ability to compete, the customer experience, and their revenue, why then aren't they protecting it?

We suspect these software publishers either don't have the bandwidth, the support needed from the top, or that they've not yet experienced an IP disaster. The levels of detriment vary. Software piracy results in revenue leakage over time; however, the effects of reverse engineering and tampering can be catastrophic and have the potential to change a business over night. It is very difficult to recover such losses.

Finding ways to decrease and prevent software piracy, reverse engineering, and tampering with the intellectual property found in software code has widespread benefits. The end user is assured that the programs they use are as the publisher intended, and as such are afforded appropriate support and warranties. The software industry is paid for producing quality products, stimulating a competitive market and further product development.

But halting piracy requires the combined efforts of consumers, software producers and government. Some of the most successful efforts involve educational programs coupled with enforcement which has been shown to work in North America and Europe.

Beyond this, software publishers need to take proactive and positive steps in the form of implementing Software protection strategies to defend their intellectual property against illegal use, copying, theft, and tampering.

As the best practice examples illustrate, a field-proven software protection and licensing solution is an effective means of guarding against the triple threat to IP to preserve copyright, combat piracy and thwart competitive espionage and tampering. What many do not realize is that software rights management can also be a forward-thinking profit strategy to increase sales, reduce costs, boost competitive advantage, and enhance market reach.

About Sentinel Software Monetization Solutions

Easy to integrate and use, innovative, and feature-focused, the SafeNet family of Sentinel® Software Monetization Solutions are designed to meet the unique license enablement, enforcement, and management requirements of any organization, regardless of size, technical requirements, or organizational structure.

Software Licensing Products & Services: An award-winning suite of hardware, software, and cloud-based licensing solutions for protecting software applications from piracy, overuse, or code manipulation in order to maximize profitability and protect competitive intellectual property (IP).

Entitlement Management Products & Services: A feature-rich entitlement management system offered hosted, as a service, or for on-premise installation, for enabling software publishers to streamline and easily manage all operational tasks associated with software licensing.

SaaS Licensing & Management Services: A CODiE award-winning software licensing and entitlement management service architected from the ground up to support the unique catalog definition, provisioning, control, and usage tracking challenges of SaaS and other cloud service delivery.

Software Monetization Professional Services: A full suite of consulting and implementation services to help you define, align, and deliver a licensing strategy that meets the business objectives and operational processes unique to your organization, regardless of where you are in the lifecycle of your licensing project.

Try Sentinel solutions for free!

View more information on SafeNet Sentinel Software Monetization Solutions
http://sentinelvideos.safenet-inc.com/

JOIN THE CONVERSATION

Sentinel Online
safenet-inc.com/sentinel

Twitter
twitter.com/LicensingLive

LinkedIn
linkedin.com/groups?home=&gid=2878111&trk=anet_ug_hm

Sentinel Video Cloud
sentinelvideos.safenet-inc.com/

LicensingLive
licensinglive.com

BrightTalk
brighttalk.com

Contact Us: For all office locations and contact information, please visit **www.safenet-inc.com**
Follow Us: www.safenet-inc.com/connected