# Choosing a Best-in-Class Software Protection Solution

## OVERVIEW

Piracy and copyright infringement is a global epidemic that denies software companies their rightful return on investment. Even companies with low piracy rates feel the effects on their revenues. This hurts not only software vendors, but honest paying customers who are often hit with higher prices to compensate for the revenue leakage caused by piracy and license non-compliance. As the number of personal computers and Internet users grow, the incidence of software piracy is accelerating. According to the Business Software Alliance (BSA), thirty-six percent of the software installed on computers worldwide was pirated, representing a loss of nearly $29 billion in 2003. In a highly competitive and escalating threat environment, software companies must find economical but reliable ways to control access to and obtain fair compensation for their products.

The software protection market provides a range of hardware and software products, varying in levels of security, to combat piracy and license non-compliance. Choosing the right level of security depends on multiple factors including the sensitivity or the value of the application being protected and the likelihood of attack. Software-based solutions are typically deployed for lower value applications or to keep honest customers compliant with license terms. Software-based solutions cannot reliably defend against piracy attacks because the environment in which the software operates can never be considered secure.

For these reasons, software developers that are serious about software security or that sell high value software, most commonly use sophisticated mechanisms such as hardware keys or dongles to provide the strongest level of protection against attack. Hardware protection offers strong, physical security that is as visible and reassuring as a deadbolt on a door while requiring minimal handling, if any, on the part of the software user. In addition, hardware protection keys can provide a secure space where information or access to that information can be encrypted and concealed within the key providing an added layer of security.

## HOW TO CHOOSE THE RIGHT HARDWARE PROTECTION SOLUTION

When choosing a hardware copy protection solution, there are several important questions to consider:

- Will the solution fit my evolving business model?
- Will the solution provide positive return on investment (ROI)?
- Will implementing this solution delay my time-to-market?
- Will the solution provide adequate protection against piracy and non-compliance?

**Evolving Business Models:** Software developers are discovering that merely protecting assets against piracy is not enough to remain competitive. To grow business and increase revenue potential, software vendors must support new and innovative licensing models. Demonstration, subscription and pay-per-use models are supplanting standard perpetual licensing models. By offering a flexible suite of licensing models, vendors can meet diverse customer needs and scale as their business evolves. Vendors, who wish to remain competitive by maintaining the ability to upgrade or change licensing models as necessary without re-implementing security, should consider the scalability of the hardware key when choosing a solution.

**Positive ROI:** As the software development industry becomes increasingly competitive there is constant pressure to reduce costs and improve ROI. With the cost of piracy at an all time high, the implementation of a hardware key solution can significantly improve revenues, but software vendors must be careful to choose a cost-efficient solution. The total cost of ownership must be considered, meaning the total cost to obtain, integrate, deploy and manage a security solution. If a solution is reasonably priced, but excessively taxes development resources during implementation or requires excessive management post-deployment, positive ROI cannot be realized.

**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. Because software protection is often implemented at the end of the software development cycle, at the time when pressure is highest to get the product to market, developers require a solution that can be implemented quickly without extensive training or programming requirements. A robust set of developer tools can cut development time while increasing the functionality delivered.

**Strong Security:** Software developers require solutions that include the latest advances in security technology and yet typically, security is not a software developer's core competency. Developers can benefit by relying on the expertise and advice of a trusted software protection vendor when determining which security features will protect their assets most effectively. Finding a respected and experienced software protection vendor allows software developers to focus on what they do best, the delivery of world class products to market.

Of all the decision criteria, security and implementation are two of the most complex points to consider. The security of a software protection solution is of paramount concern because without adequate security, software vendors cannot realize the enhanced revenue streams enabled by deploying an anti-piracy solution. Equally important are new innovations in the area of ease of use and speed of implementation. Through these innovations, software

developers can directly improve time-to-market while leveraging the new evolving business models and reducing the overall cost of implementing a software protection solution.

## SECURE SOFTWARE PROTECTION CRITERIA

With so many competing technologies available on the market today, choosing the right security solution can be a complex and overwhelming process. Software developers must weigh multiple factors when choosing a solution including whether the software vendor possesses the level of expertise required to deliver a best-of-breed solution that will meet both security and cost requirements and protect assets against attacks now and into the future

Security Criteria Check List:

- ☑ Software protection vendor offers security expertise and has a strong history of producing quality products
- ☑ Hardware key uses industry tested, government-approved open standards for encryption
- ☑ Solution provides protection against known hacking threats

### The Importance of Security Expertise

Commercial software protection companies offer state-of-the-art hardware-based solutions that are available off-the-shelf today. These solutions provide software vendors with the benefit of a proven, tested solution. Security is a moving target, therefore software protection vendors must remain ever vigilant and a step ahead of those intent on violating security mechanisms.

Because security is not one-size-fits-all, software developers can benefit by forging a relationship with a security vendor who can serve as a trusted advisor and can help select a solution that will provide the appropriate level of security. The right solution will balance ROI with the level of protection provided against piracy. Multiple factors including the sensitivity or the value of the data being protected and the likelihood of attack must be taken into account when selecting the right security solution. Experience within the industry, product innovation, recognition as a trusted security provider, and a proven track record are important considerations when choosing a security vendor.

### The Latest Advances in Security Technology

Software protection keys utilize encryption to shield vital information from those who are trying to gain access illegally. Therefore, the strength of the encryption is vital to the security of the key. Software vendors should consider hardware keys that utilize the latest technology innovations when the sensitivity or value of information being protected is high and in cases where the threat of attack is substantial.

Although there are different methods of encryption available, the industry now endorses the Advanced Encryption Standard (AES), a FIPS-approved symmetric algorithm selected by the National Institute of Standards and

Technology (NIST), as a preferred algorithm for advanced levels of data security. Because AES has faced intense public scrutiny and is not privately guarded, software developers can have increased confidence when using the algorithm. By using AES, software vendors can be assured their valuable data is encrypted with the most trusted and widely used algorithm in the information security market.

**Known Security Threats**

With advances in computer technology and the cleverness of hackers, cases of piracy are escalating. Even with a hardware key solution in place, software vendors may fall victim to attacks because security is only as strong as its weakest link. Driver replacement or emulation, replay, and brute force attacks are a few of the most popular attacks. To protect against these threats, software vendors must choose a solution that includes the latest innovations and defense mechanisms.

**Driver Replacement or Emulation Attacks:** Although a secure hardware key is a fundamental component of a strong software protection solution, it can be compromised if the method used to communicate to the hardware key is insecure. Drivers used to communicate between the application and hardware key are software based and could be susceptible to a man-in-the-middle attack in which the driver is replaced or emulated. Strong encryption provided by a driver that utilizes a digital signature offers the strongest level of protection against this type of attack. A digital signature serves to authenticate the driver to the hardware key. If the driver is replaced, authentication will fail, and further communication is disabled, thereby preventing unauthorized usage of the software application.

**Replay Attacks:** In a replay attack, the hacker monitors and copies communications as they flow between the hardware key and the application and then replays the communications to compromise the device and gain access illegally to the application. To protect against this type of attack, the hardware key must send random communications to the application so that the hacker cannot discern legitimate from illicit communications and therefore cannot use these communications to compromise the hardware key and gain access to the application.

**Brute Force Attacks:** A common threat to software security, that requires very little skill and much computing power, is a password-guessing attack known as a brute force attack. Each hardware key is protected by a password that is necessary to allow software developers to access and set configurations on the key. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until the one correct combination that works to gain entry to the key is identified. By choosing strong passwords, ones that combine upper and lower case letters, numbers and symbols, and exceed eight characters in length, developers can make it virtually impossible (requiring millions of computing years) for hackers to crack a password. A tamperproof element that locks the key after a defined number of incorrect password attempts can be added to provide further protection against brute force attacks.

These are just a few of the many known attacks and security issues that software vendors face when selecting a security solution. The strength of a security methodology is based upon its ability to protect against exposure to

attack. As technology evolves, security features are challenged over time and new innovations are required to provide a stronger, more secure system that is resistant to attack. An experienced vendor with a proven track record can help software developers stay one step ahead of software pirates.

## EASE OF USE AND SPEED OF IMPLEMENTATION CRITERIA

"Ease-of-use" is a good idea and a popular slogan that many companies use to market their security solutions. However, the true test of ease-of-use occurs during implementation. Because software protection is most commonly added at the end of the software development cycle, developers should look for a solution that can be implemented quickly without extensive training or programming requirements.

The implementation process typically consists of the following phases:

- Learning curve to understand APIs and architecture of the hardware device
- Unit testing and module integration
- Verification of the design

The ease with which developers can perform unit testing, module integration and design verification is greatly dependent upon the initial phase of implementation, therefore developers tools that help simplify the integration processes and shorten the learning curve can greatly enhance ease-of-use throughout the software development cycle.

### The Importance of Advanced Developer Tools

A complex application programming interface (API) that is difficult to use and offers inadequate functionality can cause unexpected delays in all phases of the implementation. Incomplete or poorly written documentation and a lack of samples or tutorials can further exacerbate the experience. Requiring developers to become fully immersed and knowledgeable of the technical details of a security solution unnecessarily increases the time to implement and the possibility of programming errors.

Developers can benefit from a robust set of developer tools that serve to simplify the implementation of license models, security features, and memory allocation. By utilizing a high-level system that maps easily to an API, developers can streamline deployment by using the tools provided to implement numerous complex security and licensing operations that would otherwise need to be designed and implemented individually by the developer within each application.

Developer tools can be used so that the developer needs to perform only a limited number of programming entries. The developer chooses the desired licensing model(s), which can be implemented immediately or at a later time in the field. Through the use of the toolkit, sample code is automatically generated to implement the APIs completely. The tools take defined business license models and implement them within a higher-level API. The developer is not required to spend valuable time assimilating knowledge about the mundane details, memory allocations, and hardware device architecture.

Lastly, advanced developer tools integrate security into the application in such a way that the security elements do not neet to be re-implemented if the license model is changed in the future.

## INTRODUCING SAFENET'S ULTRAPRO SOFTWARE PROTECTION KEY AND BUSINESS LAYER API™

Building on the success of the SafeNet Sentinel SuperPro product, the industry's most widely deployed software protection key, the new UltraPro solution adds significant features that enhance security, ease-of-use and evaluation, and reduce time-to-market for software developers.

### Security Trusted to Protect Over 35 Million Applications Worldwide

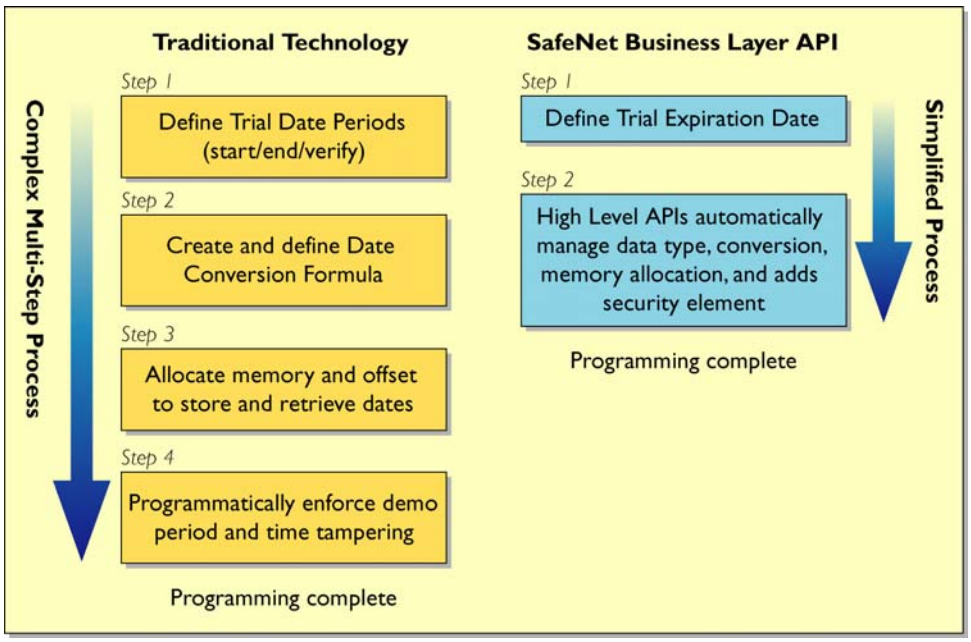
For over 20 years, the Sentinel offering has been the industry's most trusted anti-piracy solution – now protecting over 35 million applications worldwide. With an ongoing commitment to quality products and superior customer service and support, SafeNet delivers the right solutions to help developers defend their applications against the growing rate of software piracy while capitalizing on the revenue opportunities their products afford. Sentinel UltraPro products include the latest technology advances including AES encryption to secure applications against the growing threats of piracy.

### Offering the Implementation Benefits of Business Layer APIs

Demanding time-to-market requirements already cut into software development cycles and the implementation of complex software protection solutions can significantly compound the problem. UltraPro brings the Business Layer API™ framework to the development community, which enables a dramatic reduction in integration time, facilitates on-time project completion, reduces cost, and improves quality by reducing the opportunities for programming errors.

With conventional key technology, a developer must be very familiar with the design of the hardware key and assumes responsibility for numerous programming steps, especially at a low level API, in order to implement a design. SafeNet's new implementation techniques using a Business Level API can dramatically improve this situation by allowing developers to create and implement new business license models in a fraction of the time when compared to competitive hardware keys.

**Table 1: Traditional developer tools vs. SafeNet's Advanced Business Layer API tools**




SafeNet's Business Layer API can decrease a developer's learning curve and time to implement by providing an easy to understand and intuitive interface. Because UltraPro takes standard and developer-defined business license models and implements them with a higher-level API, developers can now focus on their core competency and not waste time with the mundane details and specifications previously associated with deploying a software protection device.

## CONCLUSION

With market competition and the cost of piracy escalating, software companies must find economical but reliable ways to control access to and obtain fair compensation for their products. Software developers must select a software protection solution that will give them a competitive edge in the industry. Some key criteria for making the selection are whether the solution will meet the needs of their evolving business model, deliver positive ROI, integrate smoothly and easily into the application, and provide reliable security.

Of all the decision criteria, security and implementation are two of the most difficult points to consider. The security strength of a software protection solution is a top concern for developers who want to defend against revenue erosion due to piracy. Equally important are improvements in the area of ease of use and speed of implementation that can directly improve time-to-market and reduce the overall cost of implementing a software protection solution.

SafeNet's Sentinel UltraPro solution adds important features that enhance security, ease-of-use, and reduce time-to-market for software developers. UltraPro uses the well-recognized AES encryption algorithm so developers

can be assured their data is encrypted with the most trusted and widely used algorithm in the information security market. In addition, UltraPro features the new Business Layer API™ framework, which enables a dramatic reduction in integration time, facilitates on-time project completion, reduces cost, and improves quality by reducing the opportunities for programming error.

SafeNet products meet the challenges of software and information providers by balancing two critical needs – protection against rising piracy rates and support from creative licensing models to enable new market penetration. UltraPro gives developers the power to speed implementation and time-to-market while still relying on the proven and trusted level of protection they can expect from SafeNet products.

## 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.

SafeNet®
*The Foundation of Information Security*

***w w w . s a f e n e t - i n c . c o m***

**Corporate Headquarters:** 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** email: ***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*
Website *www.safenet-inc.com*

©2004 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 6121 6455
**Canada** +1 613.723.5077
**China** +86 10 8266 3936
**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(Tokyo)** +81 3 5719 2731
**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. (New Jersey)** +1 201.333.3400
**U.S. (Virginia)** +1 703.279.4500
**U.S. (Irvine, California)** +1 949.450.7300
**U.S. (Santa Clara, California**)
+1 408.855.6000
**U.S. (Torrance, California)**
+1 310.533.8100

Distributors and resellers
located worldwide.