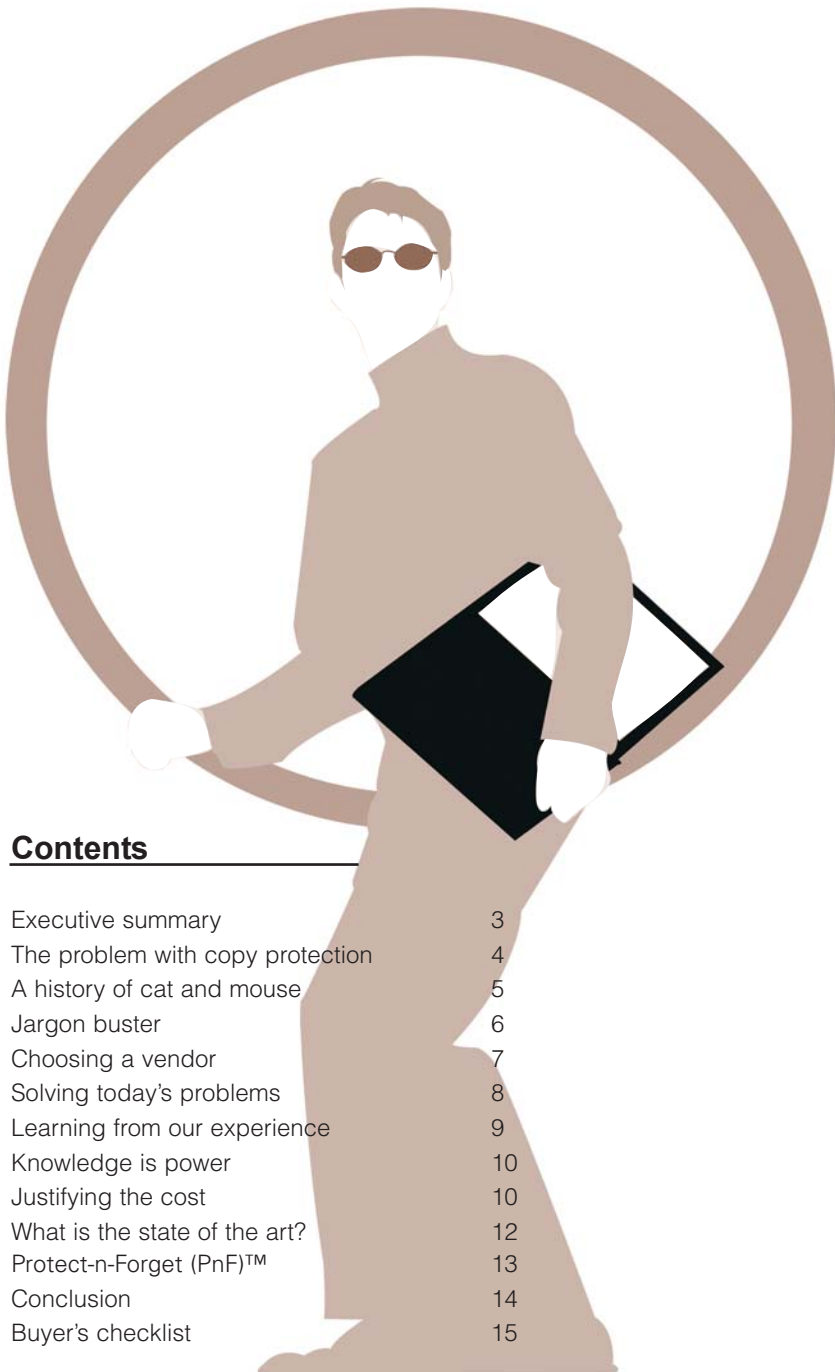




Securing your software

Protecting intellectual property
and the end-user experience



Contents

Executive summary	3
The problem with copy protection	4
A history of cat and mouse	5
Jargon buster	6
Choosing a vendor	7
Solving today's problems	8
Learning from our experience	9
Knowledge is power	10
Justifying the cost	10
What is the state of the art?	12
Protect-n-Forget (PnF) [™]	13
Conclusion	14
Buyer's checklist	15

About The Author



Henry Roberts, CTO, Nalpeiron.

Henry Roberts helped develop one of the first general purpose computers at Monroe Calculator in the 1970s. The thesis for his MSc at the University of South Carolina's graduate school in Computer Science helped Apple Computer to adapt its own copy protection system. Henry's thesis was responsible for defeating Locksmith, a technology that was known for being able to circumvent any copy protection technology on the Apple platform.

After obtaining his MSc in 1981, Henry worked on further Apple copy protection technology at Sensible Software. In 1983 he started his own company, AST, to create custom copy protection solutions.

In 2002 Henry devised a new copy protection technology that led to the development of PRO-Tector and its Protect-n-Forget (PnF) technology. AST and Nalpeiron worked together to produce the new products until 2004, when Nalpeiron acquired AST.

Executive summary

Copy protection is vital for any software development company that wants to preserve its investment. With industry statistics stating that 36% of all software in use is illegitimate, the stakes are high, and companies that fail to mitigate these losses risk losing valuable R&D funds that could hinder their chances to compete in the future. Yet copy protection tools are not all created equal.

Finding a tool that balances ease of deployment, ease of customer use and adequate security can be difficult. Issues such as reliability, support, ease of deployment and ease of use loom large, and any company not considering these factors when purchasing copy protection for their products risks more than ineffective copy protection. Disgruntled customers, high support overheads and irrevocable damage to their corporate image could result.

When considering the ROI on any copy protection tool, purchase cost is therefore not the only figure that should be included in the calculation. These other issues must also be weighed up. Tangible costs such as post-deployment support can be mitigated by choosing the right tools, but there are other, imponderable costs. Using inadequate tools that degrade the customer experience by erasing licenses unnecessarily can damage a company's image and generate bad feeling. The effect of inadequate copy protection tools on ongoing sales can only be estimated in broad terms.

Henry Roberts

The problem with copy protection

Software developers are one of the most threatened species in the world. Apart from the contemporary threats, such as offshore outsourcing and volatile skills requirements linked to a fluctuating hi-tech economy, they face another challenge: the preservation of intellectual copyright.

Software piracy has always been the biggest problem for software vendors. In a profession that relies entirely on intellectual copyright, protecting information is vital for the survival of your business. It is unfortunate for software developers that information is the easiest thing to replicate. Figures from the Business Software Alliance prove it. 36% of the software installed on computers worldwide was pirated in 2003, representing a loss of nearly \$29 billion. The study, conducted for the first time by global technology research firm International Data Corporation (IDC), incorporated major software market segments, including operating systems, consumer software, and local market software. The study found that while \$80 billion in software was installed on computers worldwide last year, only \$51 billion was legally purchased.

Shielding your code

This problem will not disappear, and it leaves software vendors with three options. They can become open source vendors, focusing on services and support for their software products, making the source code available and allowing it to be copied under a GNU-type license. This requires a fundamental shift in business focus and an associated realignment of skills and staff within the organization at a technical and a business level. Secondly, they can do nothing, and watch their sales atrophy. Lower revenues constrain future research and development. In an industry which relies on new features, this is the kiss of death. The third option lets you keep your current business model and maintain your investment. It involves shielding your source code with copy protection solutions, and for software vendors who want to stay alive and grow their business, it is a vital step in the development process.

A history of cat and mouse

The problem with copy protection as a concept is that it creates as many questions as it solves. There are many different types of copy protection working at many different levels. Companies wanting to protect their source code and binaries have a confusing array of options. Part of the reason for this involves the way that the copy protection industry developed. Various techniques evolved over time, often in parallel with each other:

Encoding code: making software secret

Software vendors became more devious, encrypting their code to make it impossible for crackers to disassemble the binary files. This stopped crackers for a short time, but not for very long—they soon realized that although the source files were encrypted on disk, they could not be encrypted in memory because of the performance overhead involved in decrypting code during execution. Software vendors were using loader programs to take the encrypted disk-based file and load it into memory, decrypting it in the process. Once the program was in memory, it was unprotected and therefore vulnerable to the conventional analysis that enabled crackers to strip the copy protection from the source code.

Manual protection—literally!

Copy protection evolved to help software vendors combat an enemy—the software pirate. Because the war against piracy is fought on a virtual battleground, the rules of engagement change frequently as the weapons evolve. In the early days, for example, the weapons used against software pirates were often analogue.

Software publishers would ask questions about the text of the manual accompanying the program, meaning that unless a user had the manual, the software would be impossible to use. Pirates soon got around that problem by photocopying the manuals, until photocopier-proof manuals came along, at which point they had to either become more devious or less lazy, rekeying the manual by hand.

Debuggers proved to be an invaluable tool for the pirates and led to the continuing rise in cracker clubs and the emergence of the warez community, which distributed cracked programs online. While many pirates sold bootleg software for commercial benefit, others cracked and distributed the code as a hobby, enjoying the status associated with being the first to break a particular program's copy protection.

Riding the loader

The discovery that pirates continued to thwart copy protection mechanisms led to yet another stage of development, as software vendors began introducing loaders that sucked parts of the encrypted program into memory separately, on

an as-needed basis. This made it difficult for crackers to analyse the source code using a debugger, because it was never all in memory at the same time. It was difficult, but not impossible. Innovative crackers learned to simply run the

program repeatedly through all of its configurations, examining the decrypted segments as they appeared until the whole binary had passed through the RAM, in a technique known as 'riding the loader'.

The dongle

Using accompanying text to verify the authenticity of the software was only ever going to be a short term solution. Instead, software vendors took the battle to a more sophisticated level. One popular method in the early days was hardware protection, using the dongle. This was a plug-in device that would connect to one of the machine's interface ports. The software would check for the presence of the device before it would run. While effective, dongles were expensive to produce, and so cheaper systems had to be devised.

Jargon buster: Decrypting copy protection terms

Product Activation

A process where an application makes an 'invisible' call to an Internet server to authenticate and license a user, usually anonymously. The end user only has to enter the license code and the activation process creates and delivers the site code to the server and accepts an unlocking key without the input of the end user.

Serial Numbers/ License Codes

When you ship a protected program you will also include a unique number with it called a serial number. This is used to uniquely identify that copy of the software.

Site Code/ Installation ID

These codes are usually generated when a protected program is first run. They are to be used in tandem with a license code/ serial number from the vendor in order to unlock a program.

Unlocking Keys

Using a unique serial number and site code allows the vendor to create a specific unlocking key, usually another string of numbers, that when entered into the vendor's software will allow a protected program to run on a designated PC.

Wrapper/Instant Protection

A software product that encapsulates an executable file by encrypting it. This provides a range of additional functions, such as copy protection to the original file.

SDK

A software developers' kit is a set of tools, APIs, and software code allowing developers to implement solutions within their own software.

Dongle

A hardware key that plugs into the serial, USB, or parallel port of a computer. The purpose of it is to ensure that only authorized users can copy or use certain software applications.

Protect-n-Forget (PnF)[™]

Protect-n-Forget (PnF)[™] technology means that the user can do what they like to their PC and it will not prevent the security from working—even replacing the motherboard or reformatting and reloading Windows.

Cracked/Hacked

A term used where a 'hacker' has reverse-engineered copy protection technology to render it useless.

Choosing a vendor

Although all software publishers face the same challenges from pirates and crackers, the techniques for meeting these challenges will differ according to the nature of your business. Each business is different and should weight up various criteria when deciding on a copy protection mechanism:

Does the technology support your development environment?

Many vendors support only one or two environments, while some of the wrapper solutions will work with anything and don't require coding at all. Remember that the easier it is to protect something, then the easier it is to remove that protection.

Many SDKs require lots of implementation work on the part of the developer, and some require a server configured with technologies such as CGI. This can present problems, especially if sharing a server with your ISP's other customers. Cheaper solutions are likely to require more customization work on the part of the software developer, potentially increasing development costs.

Consider your end users

Many of the more recent SDKs require a permanent or semi-permanent Internet connection to control licenses, making life difficult for many companies' customers. Consider a solution offering a one-off Internet activation process with the ability to work offline afterwards. Such web-based licensing should also be manually accessible using a web-based forms interface to avoid problems accessing built-in activation services across corporate firewalls.

If you are selling to corporate clients, your copy protection technology must cope with multi-PC deployments. Image builds and PC 'lock downs', which are frequent in corporate environments, can cause copy protection to fail.

What is your product's price point?

Automating the licensing process is vital if you are to avoid incurring huge management overheads. Options here include Internet web-based licensing and automated email. If you are selling small volumes, then it would be good to combine the above features with an activation service from the vendor that works out of the box with your SDK on a pay-as-you-go basis to save costs. If your product is a high-cost, low-volume offering, you may want to consider a USB dongle, but evaluate your cost model carefully. Dongles can cost a considerable amount per user compared to pennies for software solutions. We believe the pure software SDKs on the market are just as good and cost less.

Solving today's problems

As technology and distribution media continued to evolve, the market has produced solutions that break down into four main areas.

Each of these solutions offers its own strengths and weaknesses, but all of them have one thing in common: they are still weapons in ongoing cat-and-mouse battle between software developers and pirates, and should be constantly evolving. Beware of copy protection vendors who promise you a totally uncrackable system.

Nevertheless, these systems can help to protect your intellectual property by making it more difficult for pirates to crack them. They can also be used to help control the distribution of your software and offer payment alternatives, such as try before you buy, usage payments, and timed (lease) payments.



Dongles

Considered old hat by most developers, dongles are expensive on a per-product basis because of the extra manufacturing costs involved. They also reduce the flexibility for the end-user. Nevertheless, dongles are still used on more expensive software products where the cost of the protection is in line with the cost of the software, and standard USB key dongles have helped to reduce this price threshold.

For more details about the misconceptions surrounding dongle security, see our quick guide, *The Truth about Hardware Dongles*.



Media protection

The introduction of media such as CD and DVD has led to commercial duplication systems that introduce deliberate errors into the CD during the burning process. These errors contain patterns that can be used by the program on the CD to check that it is being loaded from the original media. While these systems can yield results, they cannot work effectively with online distribution because there is no media involved.

Crackers have also reportedly circumnavigated various generations of this protection, meaning that it must be constantly updated, just like other systems.



SDKs

An SDK is a piece of copy protection code that has been developed for a specific application environment. SDKs are harder to implement than wrapper technology because you must be a developer with the tools that built the original application. They can nevertheless be relatively simple to implement if the correct solution is chosen.

SDKs are stronger and harder to hack than wrappers and much cheaper and more flexible than dongles. They also tend to have more features and integrate with applications much more tightly, allowing for features such as custom screens, for example.



Software wrappers

Evolving from the loader-based mechanisms found in some software protection systems, software wrappers are considered by many developers to be among the easiest products to use, because they are often designed to be easily integrated into any product. However, that ease of use comes at a price. Once cracked, a software wrapper can be countered with an unwrapper that is easy to distribute and run.

Developers should also be wary of future operating system developments when using wrappers. Unless you are sure that your wrapper solution will survive Windows XP Service Pack 2 and future operating system upgrades, for example, you could find yourself with increasing support costs in the future.

Learning from our experience

Rather than making mistakes when evaluating copy protection systems, we want you to learn from our experience—and what an experience! We spent over \$2000 on two copy protection solutions in our search for the perfect solution, but they ended up costing nearly 50 times that much in support costs, customer refunds and lost opportunities.

The first system we chose was a cheaper option. It cost around \$300, plus the extra cost of the web-based forms for Internet authorization. It had most of the features we wanted, but its low price was a false economy. It took days to get the code implemented correctly on our own servers, and when we tried to take the system online for web-based authorization, our security-conscious ISP refused to host the necessary scripts, so we had to modify them. Already operating on razor-thin margins, the supplier was reluctant to offer much support and we often waited for three days for answers to our queries.

Flirting with disaster

The real cost was to our reputation. Even after an apparently successful testing cycle, the live system proved unreliable and customers were forced to re-license their software over the telephone. The copy protection software lost customers' licenses whenever superficial changes were made to the PC (such as a hard disk defragmentation). Our support helpline was flooded with calls, and we had to begin refunding license fees.

Desperate to stop further damage to our image, we eliminated the system and stumbled along with no licensing model until we could find something more suitable. This time we chose a high-end supplier, paying roughly \$900 for the core client product and extra fees for the server components. The code was easy to implement, the support was better, and the product had more features. We thought our problems were solved, but we were wrong!

Our customers were forced to use license codes over 40 digits in length, making them very difficult to transcribe and convey over the telephone. They constantly got them wrong and had to call back. And just as with the first solution, when customers made any changes to their PCs the protection failed, forcing the customer to call our support department and re-license the product.

By this time we had lost around \$100,000 in sales, costs, refunds, development time, and extra support, meaning that the costs outweighed the benefits of having any copy protection at all! Finally we decided to develop our own system. We were determined to solve the reliability issues that plagued other software, and we pledged to make our software easy to deploy and use. We spent two years creating PRO-Tector™.

Knowledge is power

Having considered all of the issues, you will have hopefully narrowed down the list of potential copy protection vendors to a more manageable size. At this point, you should be able to work your way through the shortlist, evaluating the companies according to your criteria.

If the SDK vendor you are evaluating lets you download its SDK for testing, beware. This is how all the hackers access such systems to analyze and crack the software. Serious vendors will never allow this in order to prevent unauthorized users gaining access to their code. It pays to search the Internet, to see if the copy protection has been cracked.

What to ask your copy protection vendor before you buy!

- How long will your money-back guarantee last?
- Is your support in my language?
- Will your protection survive major changes to the hard drive, such as an operating system re-install, a repartition, or a hard disk crash?
- Will your protection survive Windows updates such as XP SP2?
- Will your protection survive the use of Norton Ghost or any other drive imaging tool?
- Will your protection survive the changing of any hardware in the user's PC, such as the LAN card, the motherboard, or the CPU?
- Will your protection survive rebooting in safe or administrator mode and resetting parameters? What about when the administrator locks down the system? Will the limited user's software still work?
- Will your protection survive defragmentation programs?
- Will your protection survive the editing of entries in the Windows registry?
- Will your protection survive the user finding the copy protection files, codes, parameters and changing them to render the security useless?

Justifying the cost: a word on ROI

Many developers and software publishers must justify their investment in copy protection technology, and it can be a very expensive mistake to pick the wrong solution. Before you decide to go ahead and protect your software, you should spend time calculating the costs of buying, implementing, servicing and supporting your chosen solution. Then, weigh these overheads against the estimated revenue that an unprotected product will cost you. As a guide, the Business Software Alliance found that almost 36% of software used in 2003 was illegitimate.

When we used various technologies to protect our software we found that they incurred significant differences in support and usage costs. The less reliable and

stable the technology we used the higher the support costs. These costs determined whether it was worth choosing a technology or indeed choosing to protect our software at all.

Revenue	Cost
30% of total predicted revenue from copy protected product (or total current revenue from unprotected product + 42.87%)	Software purchase cost
	Software integration cost
	Server configuration cost
	Helpdesk support cost
Total ROI = Revenue - Cost	

Calculating ROI on copy protection tools

Support costs were substantially increased due to customer difficulties when using alphanumeric codes. Errors in transcribing these led to almost 30% of customers calling for help in using these both on and offline. Transferring licenses between PCs was also a problem. 20% of customers were forced to call our support line for help with this problem. When they made changes to their PC setup or performed a Windows update or reformatted their hard disks they lost the license altogether and had to call up for another! This affected 30-40% of all customers. In total, the calls to our support lines jumped into the thousands.

Counting the cost

Our cost calculator, developed using set costs for each call based on our own experience, shows the difference in costs between different technologies. We assume 5000 customers, with a support cost of \$5 per call:

Dongle	Wrapper	SDK	PRO-Tector
\$3750	\$28750	\$20000	\$3750

Cost calculation of various copy protection technologies

Notice that, aside from our own technology (PRO-Tector™), the dongle is the only copy protection technology with a relatively low support cost. But remember the purchase cost. Dongles for 5000 clients will cost roughly \$150,000 (\$30 x 5000).

Each technology choice creates different issues. Dongles cost roughly as much as an SDK to implement and support, but the unit cost per client is high. Wrappers often cost less than an SDK to implement, but they can be unreliable and easy to break, which will increase your support costs. Finally, SDKs can be easy to use but sometimes still have reliability issues, which will increase your support costs. PRO-Tector™ technology has the combined benefit of low deployment and support overheads, leading to a better return on investment.

What is the state of the art?

Too many copy protection and volume licensing systems have failed to find the right balance between ease of use and security. Step too far in one direction, and the software becomes so aggressive that it invalidates licenses in reaction to superficial changes to the PC, meaning that software will fail to work after the user updates Windows or reformats the hard disk. Emphasize ease of use at the expense of security, and the software becomes so pliable that users can easily crack it.

For two years, Nalpeiron has been developing a range of SDKs called PRO-Tector™, which can help developers to secure their software while eliminating re-licensing problems. PRO-Tector™ uses a patent pending technology that finds the right balance, protecting both your intellectual property and the end-user experience.

Costing from \$799 with a 90-day money back guarantee, PRO-Tector™ works even if the PC configuration changes. Its Protect-n-Forget (PnF)™ technology even allows the end users to replace the motherboard or reformat their hard disk without invalidating the product license, leading to lower support overheads. Yet at the same time, it is a hardened copy protection tool.

Software crackers frequently use one of the programs that tracks where copy protection software stores your license information so that they can manipulate it. PRO-Tector™ prevents that, because there are no copy protection license files accessible on the User's hard drive. Neither does it store license information in the registry. That means that people seeking to crack your copy protection can't remove all references to your program and infinitely renew free trial periods or restore a removed license. PRO-Tector™ does not require a connection to the Internet to monitor licenses either so it prevents hackers but it doesn't inconvenience the end users.

Integration with your application can take just a single afternoon, and can be done without compromising your design, layout, schema, or coding. Our SDK has over 50 license management functions and is designed to make counterfeiting very difficult. We support Visual Basic, C++ and C#, and Microsoft's .NET platform, along with Macromedia Director and Borland Delphi. PRO-Tector™ also supports many other development languages with a range of comprehensive tools in the SDK.

Protect-n-Forget (PnF)[™]

PRO-Tector's patent pending Protect-n-Forget (PnF)[™] technology solves the problems that other copy protection technologies fail to address. By enabling you to protect your software even in the event of hard disk reformats, Windows reinstalls and system board replacements, the technology provides a robust protection mechanism that won't inconvenience your end users. And with easy registration using either application-based activation over the Internet or via a web page, it is easy to deploy. Protect-n-Forget (PnF)[™] offers a solid return on investment by protecting you from the costly failures of other anti-piracy software solutions. These include:

Unscrupulous end users

One common trick used by less scrupulous software users to get around other vendors' software activation mechanisms is to call and claim that they lost their license due to a system failure or hard drive reformat. Because these vendors' copy protection systems are not designed to cope with these events, they are forced to award a license to these users, costing them significant amounts of revenue.

Software thieves

People will sometimes call a company to claim a refund for software that they have not removed from their system, or will copy the software using a disk imaging system such as Norton Ghost. Protect-n-Forget (PnF)[™] technology prevents piracy via disk imaging and also has a unique tool to check end user machines to ensure that software licenses have been removed.

Unnecessary license invalidations caused by inadequate protection mechanisms

Other software protection mechanisms can invalidate licenses due to superficial hardware or software changes. Windows is a prime example of the failures of most types of copy protection technology deployed today. This forces customers to relicense their software. This damages your company's reputation and drives up your support costs.

Extra implementation costs

Some other protection mechanisms are difficult to integrate into your software and hard to deploy online. Server-based solutions that require you to implement preset scripts often create problems for ISPs who have their own policies on what they will allow to run. If these solutions do not cater for cross-firewall access, your support costs will once again increase.

Conclusion

Wise software publishers will realise that no one thing makes the perfect copy protection product. Buy on the basis of cost alone, and you will find yourself incurring heavy overheads when you try to solve future problems. Focus on ease of use, and you run the risk of inadequate protection from a generic product that suffers from widely-distributed exploits and software patches. Fail to check for reliability, and you may find your software erasing customer licenses, irrevocably damaging your image.



Adopting long-term thinking

The solution is to think holistically. Think in the long term about the ongoing support issues that you will face as your product succeeds. Consider the importance of the customer experience and the everyday tasks that your end users will be carrying out, and ask yourself whether your copy protection software will be able to survive the realities of your customer environment. The PC is a battlefield—and unless your software comes well-protected, your revenue and your corporate image could be a casualty.

About Nalpeiron

Formed in 1991, Nalpeiron (NAL) is a US- and UK-based company. Nalpeiron started as a software developer and management consultancy, but had poor experiences using copy protection technologies leading to support headaches through lost software licenses. The company decided to develop a range of new copy protection technologies to help its customers solve these problems.

Buyer's checklist: essential features in copy protection

Choose these features when creating a supplier shortlist:

Reliability

Buy a reliable SDK-based solution that will not fail when the end user upgrades the PC or uses Norton Ghost and Utilities. Make sure it survives Windows updates, reformats and registry changes.

End-user experience

Internet activation should be complemented by web-based forms for use behind firewalls. Phone and email license key generation tools should also be provided.

Ease of deployment

Your copy protection software should be fast to implement (it should take no more than a few hours), and should offer easy outsourced 'service' based activation and/or your own in-house server options. No extra programming or setting up complex scripts on ISPs or painful coding to make API calls to components.

Portability

It should be easy for the end user to move between PCs using USB drives or web-based license storage.

Controllable

Easy for you to control end user installations and to offer refunds using 'Proof of Removal' tools.

Concurrency

The product should make it easy for corporations to use software with floating network licenses, and it should facilitate work on PCs that have been locked down by the administrator.

Granularity

Feature controls should allow you to manipulate individual code modules, allowing you to switch features on and off. It should be possible to 'weigh' these modules in terms of value when you sell them.

Comprehensive platform support

Copy protection software should support all Windows versions, and a wide range of development platform support.

Flexible licensing

The copy protection software should be licensable to you in a way that suits your business goals. Royalty-free licensing enables you to maintain the same copy protection tools as your software becomes more successful without incurring financial penalties.

Money-back guarantee

Don't be caught out by software that doesn't deliver on its promises. Get a money-back guarantee to show you how confident your vendor is in its software, and to reduce your financial risk.

For more help with your copy protection purchasing decisions, please read our free selection of quick guides, available at www.nalpeiron.com/downloads/.

- Quick guide: *The truth about dongles*
- Quick guide: *Product activation explained*
- Quick guide: *The benefits of copy protection to different departments*

Contact us now for a free 20 minute obligation-free consultation (normally \$100) to discuss your project and to get impartial advice on the best solution for you. Email us now at consult@nalpeiron.com with your contact details and we will schedule a call with a consultant.



Royalty free solutions for flexible and reliable licensing, activation and copy protection.

Nalpeiron US Office:
11707 S. Beechwood Rd.
Leavenworth
IN 47137
USA

Nalpeiron UK Office:
44 Market Square
Witney
OXFORD OX28 6AJ
United Kingdom

www.nalpeiron.com

Copyright 2005 Nalpeiron.
PRO-Tector and Protect-n-
Forget (PnF) are
trademarks of Nalpeiron.
All other trademarks
belong to their
respective owners.
E&OE.