



Is Anti-Piracy/DRM the Cure or the Disease for PC Games?

ByteShield™ White Paper # 0005

Is Anti-Piracy/DRM the Cure or the Disease for PC Games?

ByteShield™ White Paper # 0005

0. TABLE OF CONTENTS

1	Introduction	2
2	How Did We Get Here?	3
3	Where we go from here?	5
4	References	16
5	Appendix A: PC Gamers' DRM Charter	17

1. INTRODUCTION

"Only customers hate DRM, pirates remove it"

This is how one developer summed up the current state of software protection from piracy. Anti-piracy, in the form of Copy Protection, Digital Rights Management (DRM)¹, Intellectual Property laws and legal enforcement, has for decades tried to prevent illegal usage of PC games. Yet, the evidence clearly shows that piracy continues to grow and frustrate vendors while anti-piracy frustrates both users and vendors. Vendors' increasingly desperate anti-piracy efforts have aggravated customers - sometimes the inconvenience caused has resulted in such great customer pressure that game vendors have given up trying to protect their PC games at all.



Visit almost any PC Games portal forum, or blog these days and you'll probably read or see (video) expletives documenting the frustration of many game users with most anti-piracy systems. Visit most developers and publishers and you'll probably hear horror stories about piracy, lost revenue and unintended consequences of current anti-piracy technology.

In summary, the current state of anti-piracy in the PC game industry is:

1. Many continue to debate whether piracy of digital content equals lost sales but the real question to ask is 'how much of piracy would turn into sales if piracy were prevented?' Of course nobody knows and different people have different estimates but most people would agree that the answer is unlikely to be at either extreme - i.e. 'all piracy is lost sales' or 'no piracy is lost sales'. Given piracy rates for certain games and software, the proportion does not need to be large before the impact is significant to publishers and developers. For example, describing the PC game market as "the most intensely pirated market ever," Crytek CEO Cevat Yerli's assessment is, "for one sale there are 15 to 20 pirates and pirate versions." AutoDesk has publicly stated similar numbers for AutoCAD. If only 1 of every 10 illegal copies turn into sales, revenues would double.

2. The goals of IP protection are both to increase copyright holders revenue and to prevent people who aren't going to buy games/other software from playing/using them unless publishers enable free, full-feature trials as part of their marketing to ultimately encourage purchases.
3. Even if we accept that DRM¹ has reduced some types of illegal copying it has largely failed to protect vendors' legitimate rights because they are rapidly cracked. If it is extremely easy to circumvent the protection, many amateurs will do it. If the protection is more challenging, some people will not be able to get around the DRM and some of these will actually purchase the game/software, rather than find it on a torrent site. While virtually all DRM solutions have been cracked, the piracy problem may well have been even larger if all games/software had been distributed unprotected.
4. DRM has contributed to destroyed customer relationships and trust by impinging, inconveniencing and even impugning honest customers.
5. Annoyed and hostile gamers publicly vent their outrage and fury on game suppliers and DRM suppliers via portals, blogs and message boards.
6. Impacting honest users tends to shift their sympathy towards the pirates rather than the developers and publishers. In effect, onerous DRM legitimizes piracy – because with pirated copies you avoid the hassles DRM imposes. We have heard of honest users using a cracked version because it is easier to run but purchasing a legitimate copy that is kept unopened in order to be an 'honest' user and of some users who just won't buy a game because it has intrusive DRM.

How did technologies and efforts designed for the benefit to the industry instead become the enemies of the software business? And how do we fix it?

This whitepaper draws from multiple sources across the PC Games industry to answer the questions, 'How we got here?' and 'Where we go from here?' It acknowledges that the piracy problem would have been much worse without the industry's past and existing efforts but presents two key goals that are needed now:

1. A new and effective technology approach to software activation management, IP protection and anti-piracy without the user unfriendliness of DRM
2. To re-establish trust and a balanced relationship between game developers/publishers and their customers

The ByteShield thinking and new approach to software protection achieves these goals and by doing so may become the software industry's and the users' best friend! Though we know of no other vendor taking the same approach, there may be one or more, and we expect others to try to emulate this approach to paint a better future for the PC games industry.

2. HOW DID WE GET HERE?

Software, like some other intellectual property (IP), has both the advantages and disadvantages of being digital. The low cost of goods (COGS) advantage of almost costless replication is also a disadvantage as a piracy enabler—you can keep it and also make



¹ DRM overlaps with software copy protection to some extent, however the term "DRM" is usually applied to creative media (video games, music, films, etc.) whereas the term "copy protection" tends to refer to copy protection mechanisms in computer software. In this paper we will collectively refer to them as "DRM".

perfect copies. In the beginning, software was purely an enabler of hardware sales and uniquely applied to that hardware. As hardware was standardized (PC hardware in particular), software value was recognized separately from hardware and software piracy became economically motivated. Protection against piracy was initially hardware based (CD required in the PC CD drive, dongles, other media that inhibited reproduction) but over time these approaches were understood and defeated. The industry learned that it could not prevent copying so it tried to manage compliance with licenses. For greater protection (and COGS reduction) various software protection methods were introduced and later collectively called Digital Rights Management (DRM). Some DRM systems set out to also protect developers trade secrets - modern software applications and games are often huge investments in algorithm development and coding. Developers and publishers recognized that to maximize their return on investment, they must protect their trade secrets and prevent piracy.

However, most DRM technologies primitively restrict, inconvenience or harass legitimate customers. This has caused a growing consumer backlash against game products that employ DRM, often expressed in anti-protection arguments by three separate groups:

1. Honest users who have paid for a product but are inconvenienced by usability issues or inconvenienced with copy protection or DRM systems
2. Pirates who steal software and often claim to be fighting evil corporate monsters but really just don't want to pay for products, they can use free
3. Activists who use a moral argument against any kind of protection.

To a large extent the clumsiness of DRM alienates honest users and, in their eyes, even legitimizes piracy – some honest users buy a game to be legitimate then apply crackers' patches to remove the DRM, or just play a pirated version of the game. For software (including game) developers and publishers, Copy Protection and DRM have been a lousy trade-off between the degree of impact on their honest customers and the degree of protection afforded to their software (and their revenue). A never-ending battle to stay ahead of the "bad guys." has had the unintended consequence of impacting the "good guys" and every time a new technique is developed to protect games from piracy, hackers are ready and waiting to render it ineffective, often within just a few days. Some DRM technologies have even been extended to 'spy' on users and report back illegal usage with sufficient information to locate and legally address pirate usage – an approach that has obviously further deteriorated trust and the relationship between vendors and users.

Neither Copy Protection or DRM technologies, nor the legal efforts of the BSA (Business Software Alliance), Software & Information Industry Association (SIIA), ESA (Entertainment Software Association) and ELSPA (the Entertainment & Leisure Software Publishers Association of the UK) and others, have actually achieved their intended purpose of reducing worldwide PC software piracy rate. The BSA's latest report (May 14 2008) says that in 2007 worldwide piracy increased by 3% (to 38%) and software company losses increased by 20% (to \$48B). ShackNews reported (June 27, 2008) that Cevat Yerli, CEO of Games Developer Crytek, estimated that PC gaming piracy currently could be 15 to 20 pirated PC games for every 1 legitimate PC game. Of course the problem may have been even greater without these legal and technological approaches but most Copy Protection and DRM approaches have proven relatively easy to crack - patches to overcome most are freely available on the Internet. The result is innumerable unauthorized downloads/installations and significant lost revenue, a poor reputation for DRM and lots of customer bad will.

How is it that this modern industry has got itself into such a mess? There are many causes starting from the basic digital characteristics of software but including proliferation of cracking technology (debuggers, disassemblers, decompilers to name a few 'tools of the cracking trade'), the knowledge and skills, as well as the willingness to apply them. Others include the software industry's reliance on legal approaches, its lack of understanding of how crackers work and the resulting poor DRM technological approaches to inhibiting piracy, its distance from customers due to multi-tier supply chains as well as its willingness to compromise the honest user's experience. Why do software companies continue to buy DRM solutions which don't work? The answer is hubris, lack of alternatives and fear of upsetting customers even more – the thinking is that users have got used to the status quo even though they are impacted by it – but do not make the user experience any worse! A new alternative via a new approach is desperately needed.

Coincidentally, other IP industries have since been impacted by the shift to digital distribution. While software was first out of the gate, music, video and others have or are suffering the same effects and, in general, have learned little from the software experience. They too started with hardware copy protection (e.g. worldwide CD zones), then moved to software protection technologies (e.g. fingerprints) and dependence on legal approaches. The music industry has been decimated by digital technology and the Internet and still analysts are downgrading the entertainment industry saying digital downloads of movies and TV shows pose a huge threat to profits from DVD sales.

At the same time, some current software industry trends are exacerbating the problem, as greater online distribution of software and content leads to greater opportunity for, and impact by, piracy. Another trend is that the Internet enabling user feedback to be increasingly vocal and widely heard and has raising expectations for greater flexibility in how software/games are evaluated, purchased and used - customization of software feature sets for their specific needs, and business models that maximizes their convenience and return on investment (e.g. perpetual licenses, rental licenses, SaaS delivery, etc).

For software developers and publishers meeting these protection and flexibility needs without damaging the customer experience has so far proved a distant dream. The industry simply hasn't had a solution - a new approach is urgently needed to address this industry wide failure.

3. WHERE WE GO FROM HERE?

Recognize that the anti-protection argument is really an anti-piracy one; if piracy didn't exist then software companies wouldn't need protection but it's unrealistic to expect piracy to cease so protection will continue to be needed. Therefore developers and publishers in any IP-based industry must:

1. allow consumers' expectations for fair use of a purchased product,
2. meet consumers' complex and evolving future needs within a relationship of trust, and
3. protect their investments with perceived fairness.



This sounds difficult but can be as simple as using ByteShield. Developers that do not address the problem will likely suffer increasing piracy and lost revenue and/or deteriorating customer relationships.

So how do we do it? We could try to 'fix' DRM? But with the public antagonism towards DRM, it has come to stand more for "Digital Restrictions Management" or "Dumb Relationship Management" than "Digital Rights Management" so we believe the industry should instead develop in a new direction. One that approaches the problem with a solution which puts the users back where they belong - as the focal center of developers' attention and business models - rather than starting, or appear to be starting, by assuming users are criminals. Assume 'innocent till proven guilty' rather than 'guilty till proven innocent' - trust but verify, trust first, verify second but don't inconvenience honest customers to do so.

The industry should adopt this new approach to achieve the following 4 objectives, in order to obtain the benefits noted under each, while addressing all the limitations and including all the learning from the experiment that has been DRM.

The 4 Major Objectives and the benefits of each:

- I Achieve protection for at least the significant revenue earning part of a game's lifecycle**
 - Greater revenue to developers/publishers by decreasing piracy
- II Establish trust between game developers/publishers and customers**
 - Openness and transparency
 - Simplicity of use
 - Avoid changes to users PC
 - Responsiveness to users
- III Provide new benefits to customers**
 - Completely portable and flexible reinstalls and activations
 - Ability to back-up game on a DVD
 - Flexible and dynamic licensing
 - Ability to buy games online or offline
 - Automatic compliance with the software license
- IV Provide new benefits to developers/publishers**
 - No impact on development team
 - Flexible and dynamic licensing
 - Control number of active installations per sold copy
 - Control of release date
 - Ability to offer full feature trial versions
 - Turn attempted unauthorized usage into sales opportunities
 - The game can be available on CD or as a download using the same protection scheme
 - Disable game if charge backs or refund occur
 - Reduced costs for support services and update/patch delivery
 - Compatibility with existing systems
 - Direct communication channel with the end users
 - Increase effectiveness of sales channel
 - Remote management control

How to achieve these objectives is explained in detail below:

To do this we need a different and better technology than so far available for DRM. There may be other alternatives to achieve this and certainly we do not claim that there are not other systems that could replace DRM and provide these new benefits – but at this time we are unaware of any other systems capable of doing so. Therefore we address below how we achieve these objectives with our ByteShield Software Activation Management – to illustrate that the solution is real because the technology already exists.

I. Achieve protection for at least the significant revenue earning part of a game's lifecycle

In effect ByteShield's technological approach to protecting software acknowledges that any protection created by man can eventually be cracked by man given sufficient time, effort and hardware. The real issues are the number of hurdles involved, the time to overcome each, whether they must be overcome one at a time or can be programmatically overcome. Conventional software protection technologies (Copy Protection/DRM) are often based on only a few hurdles and usually cracked quickly. In contrast ByteShield's Software Activation Management (SAM) has high numbers of multiple hurdles, including removal of small but critical pieces of the code it protects and replacement of them at run-time. A cracker is forced to find and 'fix' one piece at a time. Even if a cracker can 'fix' each independent and different hurdle, each one will take a certain amount of time and if there are 1,000, 10,000 or even 100,000 pieces of code need to be 'fixed', one by one, then the total cracking effort required will simply be too great to be worthwhile. ByteShield protection has, to our knowledge, never been cracked - about a year ago, a unit of the US Department of Defense invested 2 months in trying to crack ByteShield and, as far as we can tell, they did not succeed (the results are classified).

For a software activation management system to have some strength against the crackers it will require a Remote Server and:

- Binary Separation – Maximizing the difficulty for the cracker requires that the whole installation is not visible in one piece. The game, on a CD or download, is delivered incomplete. Legitimate code items (literally 1000s in a medium sized application) have been stripped out and replaced with seemingly good code. The removed code is put in a Security Module (SMOD) which is delivered upon activation. To make the application work again, the removed code must be present. This is very time consuming for a cracker to work around or to spoof (simulate).
- Atomic License Checking – Since the application will not run without the SMOD, which can only be received from the server, it would be self-defeating for the cracker to delete or tamper with the call to the server. Thus, the cracker cannot avoid the server verifying the identity of the local installation.
- Repeated Verification - licenses are checked at intervals set by the developer/publisher.
- Unique Installs - While the seed for the SMOD is created when the publisher secures the application on a ByteShield server, every instance of an SMOD is unique.
- Mutation - The SMOD can be set to mutate (change) every time the application is started or by any slower rate (including never). This makes it very difficult to create a protection removal tool since the target is changing.

Summary: ByteShield believes protection is valuable if approached our way i.e. extremely large effort to crack, no or minor impact on honest users and

no impact on PC game and software developers. ByteShield’s technology not only achieves this novel approach to providing the strongest software protection available but does so with extremely low or no performance impact on the execution speed of the protected software.

II. Establish trust between game developers/publishers and customers.

Having depleted trust as a consequence of clumsy, or “draconian” as some gamers say, DRM the game industry has to recover from a negative position. One advantageous trend is that delivering games via download puts developers/publishers much closer to their customers, often linked directly rather than through a supply chain.

An excellent step forward is the “PC Gamers’ DRM Charter© Talkjack 2008”, published June 22, 2008 and reproduced in the Appendix to this ByteShield Whitepaper with permission from the author. Jack summed up the situation succinctly, “*I believe that DRM in PC games is typically imposed upon paying customers to limit customer’s freedom with the game they have purchased in order to make more money for big business. That might be reasonable if the DRM methods being used were respectful and fair to customers, but this does not appear to be the case any longer.*” And he went on, “*The technical methods currently being used with PC games have become offensive, frankly, to paying customers. In a later article I will investigate more deeply the reports of DRM systems like StarForce and possible SecuROM causing damage to customer’s computers*”. You will notice that Jack is not supporting or endorsing piracy in any way but his point #16 sums up the current customer relationship – honest users are feeling that they are regarded as potential thieves, and not as valued customers. The following table lists all Jack’s Charter points and compares how DRM in general and ByteShield User Control handle them - we are using our own product to prove the point that Jack’s Charter can be met.

The following table is long but it addresses all 16 of Jack’ charter points. We have included all of Jack’s very good points in order to address each individually for completeness but, in summary, they fall into four areas:

- Openness and transparency
- Simplicity of use
- Avoid changes to users PC
- Responsiveness to users

PC Gamers’ DRM Charter	DRM Software	ByteShield Software Activation Management (SAM)
<i>1. Stop covertly installing DRM software on a customer’s PC.</i>	<i>Dishonest, malicious software, such as viruses and spyware, install themselves covertly and offer no removal mechanism in Windows control panel. Most DRM software is covert.</i>	ByteShield is open about how our solution interacts with the customer’s computers. ByteShield only installs standard Microsoft drivers.
<i>2. Print clearly on the packaging (or on the download site) the name and logo of the DRM system you licensed and bundled with the game.</i>	<i>Most games which include DRM do not announce this fact on the box – usually gamers get a nasty surprise when they find imposed restrictions upon them not presented at time of sale.</i>	ByteShield agreements with game developers and publishers insist that the packaging, EULA, installation manual and start of application clearly call out SAM to allow customers to make an informed choice. ByteShield does not impact honest users so it is not a sales disadvantage.

<p>3. Remove DRM when it is no longer necessary. If sales have tailed off six months after the release of a game then the DRM is no longer protecting your income, so it is no longer required.</p>	<p>Most DRM systems are built into the software and the only way to remove them is to issue a patch. The availability of such patches would teach the crackers how to automatically remove the DRM on other software so this is unlikely under DRM systems.</p>	<p>With ByteShield developers/publishers have complete flexibility to 'throttle' back or entirely remove the activation management at any point. License parameters can be changed or ByteShield can push out a reinstall without any protection.</p>
<p>4. Do not modify your customer's PC by installing applications that run constantly.</p>	<p>Many DRM systems run even when the game is not running, slowing down the gamers' PCs and risking unnecessary conflicts with other programs.</p>	<p>ByteShield never runs unless the game is running.</p>
<p>5. If you require a user to connect to the Internet in order to 'activate' a single player game, then do so in such a way that their hardware or software firewall protection do not need to be lowered just to allow your traffic through.</p>	<p>Some DRM systems require a customer to open ports purely to activate a game and therefore put users PC's at risk of being compromised by hackers.</p>	<p>While a standard Internet connection is required occasionally by ByteShield, there is no need to lower the firewall or other protections.</p>
<p>6. Do not disable or ignore the keyboard and mouse when your game is loaded. Most people do not want to sit staring impatiently at the screen waiting for the EA, NVidia and numerous other animated logos and movies to finish playing.</p>	<p>Some DRM systems do this but more commonly some game developers do this for themselves and their supporting advertisers. A good idea is to enable the escape key to jump to the main menu and avoid adverts you've seen on previous game startups.</p>	<p>ByteShield never disables or ignores keyboard or mouse.</p>
<p>7. Do not use corrupt registry keys or secret files created in a way which violates the rules of the operating system simply to prevent a customer from deleting your files or keys. See point 1 above about providing uninstall options in control panel.</p>	<p>Some DRM systems (e.g. TalkJack says SecuROM) do this.</p>	<p>ByteShield never corrupts registry keys and never violates the rules of the operating system. ByteShield recognizes that the users must be able to manually empty folders and tidy their registry without special software or hacker-style techniques.</p>
<p>8. Do not repeatedly scan the CD or DVD in the customer's PC while the game is playing. By all means check gamers have a valid disk when they start the game, but then leave it alone. All you are doing is driving customers towards sites like GameCopyWorld to get no-cd patches for games, which make gaming a better experience.</p>	<p>Some DRM systems do this - it wastes electricity and causes unnecessary wear and tear on customer's PC drives. Eventually it can cause the operating system to step down the performance of the customer's drive permanently.</p>	<p>ByteShield goes even further and never requires the CD or DVD in the customer's PC and never scans CDs or DVDs. Protection mechanisms that require the CD or DVD to be in the drive every time a game is run inconvenience honest customers.</p>
<p>9. When someone uninstalls your game from their PC, always uninstall all traces of DRM software from their machines, and do so in a clean fashion.</p>	<p>Some DRM systems do not remove all traces, sometimes they even deliberately leave remnants behind.</p>	<p>ByteShield agreements with publishers require that SAM completely disappears when the game is uninstalled.</p>

<p>10. Do not install device drivers secretly.</p>	<p>Some DRM systems (e.g. TalkJack mentions StarForce) install hidden device drivers on the user's PC, which may conflict with other software. It has also resulted in damaged CD/DVD drives. When the protected game is not in use then the DRM has no right to be active.</p>	<p>ByteShield only installs standard Microsoft drivers and is inactive when the game is not in use.</p>
<p>11. Do not refuse the game to start just because the customer has perfectly valid software such as drive emulators or Microsoft Process Explorer on their machines or in memory.</p>	<p>Some DRM systems detect whether the gamer is using the software to run a pirate copy of the game. However, just because they have got that perfectly legal software installed on their machines does not mean they are actually stealing the game that the DRM is protecting.</p>	<p>ByteShield does not detect or take any action if drive emulators or Microsoft Process Explorer are present.</p>
<p>12. Answer your tech support emails about DRM. Be helpful.</p>	<p>Some developers immediately assume that any DRM errors imply attempted piracy and treat paying customers like suspected thieves until they can prove otherwise.</p>	<p>ByteShield generates extremely few support calls. Those ByteShield receive are promptly handled.</p>
<p>13. A customer should never be required to download and install DRM system updates in order to get a game to work.</p>	<p>Some DRM systems do this (e.g. TalkJack cites Tages and Vista, StarForce and Spellforce2).</p>	<p>ByteShield client is automatically updated to not cause inconvenience to customers.</p>
<p>14. If you are going to require a customer to key in long codes of letters and numbers then print them clearly.</p>	<p>Some Games use hard to read fonts such (e.g. TalkJack cites Spellforce 1), where customers could not tell I's and 1's, 0's and O's apart and then force them to retype the whole thing if they make a typing mistake. Others 'hide' the code inside the packaging e.g. TalkJack cites Starcraft budget edition. He also advises not to print the code on the back of a manual in ink which rubs off on the customer's thumb when they are readying, such as Neverwinter Nights!</p>	<p>Using ByteShield the publisher generates Digital Activation Codes (DACs) which users input at the time of activation. DACs are similar to 'product keys' that most DRM systems use but have 2 major advantage over product keys: 1. DACs are entirely random and independent of hardware so can be shorter, easier to deal with. 2. DACs are not hack-able by random code generation because of remote server detection. DACs can be provided to users in any length and in various ways, such as on a sticker or in an email.</p>
<p>15. If you are going to require customer's to go online to activate their software then do not impose draconian limits on the amount of times they can do so.</p>	<p>Most applications, including games, already use the Internet for updates so it is natural to also use the Internet for activations. Many DRM systems have limitations on how many activations they allow, e.g. TalkJack says Mass Effect offers three activations only.</p>	<p>The ByteShield system controls the number of users, not the number of installations. Therefore, end users are not constrained from installing on multiple machines.</p>

<p>16. If a customer is unable to activate their game because their activation code has been used by a pirate with a random key generator, then you should be helping your customer, not forcing them to jump through hoops.</p>	<p>Some Game developers/DRM systems force users to scan and email their receipt or take a photo of their game packaging.</p>	<p>Since ByteShield activation codes (DACs) are completely random, a pirate will not be able to find a legal code. Any automated random string generation attempts are detected by the ByteShield server and blocked.</p>
--	--	---

Table 1: Comparison of DRM and ByteShield Software Activation Management against PC Gamers’ DRM Charter

Adding to Point 3 some have also asked about disaster scenarios; “what happens when ByteShield turns off its servers, moves over to a new system or goes out of business?” The answer is that after a given time period (or in the event of ByteShield disappearing), ByteShield will, in such cases, assist the publisher and/or developer to change the ByteShield Software Activation Management protection from limited usage to free and unlimited usage.

Another great example is game developer Stardock’s “The Gamer’s Bill of Rights”, published August 29, 2008. Stardock CEO Brad Wardell believes the reason that PC gaming has declined today is an unwillingness of PC software manufacturers to treat their customers with respect and he has codified his ideals into the following, “*We the Gamers of the world, in order to ensure a more enjoyable experience, establish equality between players and publishers, and promote the general welfare of our industry hereby call for the following:*” His ten points are reproduced in the first column of the table 2 below.

ByteShield’s point by point view is in the second column but even though “The Gamer’s Bill of Rights” is incomplete, it’s a good start and excellent to see a game developer recognizing the inadequacies of DRM. **The most important item missing in the list is the right to easily move the game to a new PC, a 2nd PC or to lend it to a friend.** It is also key to recognize that developers being asked to fulfill these gamers’ rights, need to protect their own rights at the same time – i.e. to prevent theft and lost revenue. To fulfill all of “The Gamer’s Bill of Rights” is readily possible but requires the strongest of protection mechanisms; otherwise the crackers’ task just became much easier.

The Gamer’s Bill of Rights	ByteShield Software Activation Management
<p>1. Gamers shall have the right to return games that don’t work with their computers for a full refund.</p>	<p>ByteShield enables this because any installation can be instantly disabled and refunded with no fear of theft</p>
<p>2. Gamers shall have the right to demand that games be released in a finished state.</p>	<p>ByteShield agrees but this is a developer decision</p>
<p>3. Gamers shall have the right to expect meaningful updates after a game’s release.</p>	<p>ByteShield agrees but this is a developer decision</p>
<p>4. Gamers shall have the right to demand that download managers and updaters not force themselves to run or be forced to load in order to play a game.</p>	<p>ByteShield agrees but with respect to the game this is a developer decision. However, in certain circumstances (e.g. bug fix versions, virus protection) this should happen automatically to minimize support issues (for users and developers) but with full information of what is happening supplied to the gamer</p>
<p>5. Gamers shall have the right to expect that the minimum requirements for a game will mean that the game will adequately play on that computer.</p>	<p>ByteShield agrees but this is a developer decision</p>

6. Gamers shall have the right to expect that games won't install hidden drivers or other potentially harmful software without their express consent.	ByteShield already makes this promise in this Whitepaper
7. Gamers shall have the right to re-download the latest versions of the games they own at any time.	ByteShield agrees and ByteShield enables this because any installation can be deactivated in combination with permitting a re-download
8. Gamers shall have the right to not be treated as potential criminals by developers or publishers.	ByteShield already makes this point in this Whitepaper
9. Gamers shall have the right to demand that a single-player game not force them to be connected to the Internet every time they wish to play.	ByteShield offers this but it's implemented at discretion of game developer but online connectivity is becoming ubiquitous because of the benefits it affords users – always on, always up-to-date, always connected, etc. and that many publishers now offer online games for which online connectivity is a prerequisite to play. ByteShield is simply taking advantage of this modern situation to enable copyright protection along with multiple user benefits such as 'unlimited activations'. If ByteShield is used an occasional internet connection is needed but this is a necessary component of balancing the rights of both copyright holders and honest users without all the other limitations of DRM systems
10. Gamers shall have the right that games which are installed to the hard drive shall not require a CD/DVD to remain in the drive to play.	ByteShield already makes this promise in this Whitepaper

Table 2: ByteShield Software Activation Management vs. Stardock's "The Gamer's Bill of Rights"

Summary: Customers do recognize piracy as a problem for developers/publishers and generally accept that license activation be controlled - as long as it doesn't inconvenience them. In general Software Activation Management must be simple and automatic, requiring no end-user intervention, enable enhanced customer support, offer non-intrusive remote updating and renewal through a centralized license manager that manage protected software. In short ByteShield Software Activation Management addresses and overcomes all these shortcomings of DRM.

III. Provide new benefits to customers

- Completely portable and flexible reinstalls and activations - purchasing a software application or a game should include the ability to use it anywhere and be easy to reinstall after a hard drive crash or upgrade to a new computer. It should also permit lending it to a family member or a friend – as long as usage is in line with the license e.g. one activation at a time. This is crucial to our product and why we view ByteShield as considerably more end user friendly than other solutions. End users can install the game/software on an unlimited number of computers and keep on adding installations, as hardware changes or system crashes etc. occur. The real item to control is not the number of installations; it is how many of these installations can be used, at the same time. Thus, with ByteShield, the permission to run moves from one PC to another, seamlessly. The publisher can decide, per activation code:
 - How many users will be allowed
 - How many active installations each user will be allowed
 - How quickly the permission to run moves from one user to another and from one computer to another

- **Ability to back-up game on a CD** – back-ups of game can easily be burned.
- **Flexible and dynamic licensing** - achieve by using software activation management to generate custom licenses on-the-fly in little to no time, even allow users to choose and pay for only the specific software features they want.
- **Ability to buy games online or offline** – ongoing updates are now typically distributed online whether the original purchase was online or offline – vendors generally offer both and their anti-piracy solution needs to support both online and offline distribution.
- **Automatic compliance with the software license** – Audits not necessary.

Summary: ByteShield Software Activation Management meets all these customer friendly objectives and achieves all these benefits.

IV. Provide new benefits to developers/publishers

If they have not already done so, developers and publishers should recognize that developing sophisticated software protection and activation management tools capable of implementing this strategy is beyond the scope of most developers' in-house capabilities. Just as game development is a specialty so is software protection. So choose a sophisticated specialist and ensure that the chosen tool has no impact on development team productivity (the protection should be applied post-development and QA), has a low entry cost (based on developers/publishers revenue so that even small publishers can realize the benefits) and meets the criteria outlined in this whitepaper.

- **No impact on development team** - to minimize time-to-market the software protection solution should not disturb the product development life cycle at all and allow staff to focus on their core competencies like programming and product management, and not be additionally burdened by protection tool education, continual maintenance to keep the software protection up-to-date, or repeated development cycles and product versions to accommodate custom license requests. This can only be achieved using a solution that completely separates protection from development processes. Furthermore the protection process needs to be highly automated and fast so that it is easy to protect the binaries of new releases, updates and patches, even in frequently changing distributions.
- **Flexible and dynamic licensing** - increased competition demands increased product differentiation. This can be achieved by using software activation management to generate custom licenses on-the-fly for a particular customer in little to no time, turning specific features on or off to create multiple versions and attractive purchase options that appeal to increasingly broad and more segmented markets. In other words, product managers need to be able to quickly and actively bring products to market the way that customers want to buy—without using engineering resources to re-code each new flavor—thereby boosting that bottom line.
- **Control number of active installations per sold copy** - the standardized client/server interaction lets the publisher control the number of active instances per user. You can have a widespread variety of licensing options, which are all customizable by the publisher and even interchangeable between games by simply changing the rule set on the server. One game can be allowed to run on several computers, or only one at a time.
- **Control of release date** – and even the targeted hour, without any risk of illegal copies appearing on the Internet. The target game can be distributed in advance of the release date while the publisher retains the control to activate the product

on the servers at a specific date and time. Because the ByteShield platform must download vital pieces of the game, the target game is incomplete (and thus can not be cracked or illegally distributed) until the publisher decides to enable registration and downloading of security modules. This method ensures there will be no illegal copies in circulation before the game is available on the shelves at retailer while preventing retailers from breaking their agreements and releasing copies before the sanctioned launch date. It also avoids huge spikes in game downloading at release date.

- **Ability to offer full feature trial versions** – Today users sometimes download a pirated version of a game to see if they like the game before they actually buy it. By offering a full feature version of the game protected with ByteShield the publisher can allow the users to try it before they buy. Publishers can achieve mass distribution of full feature trial versions with full control over use, without fear of piracy. Sales teams can see who is actually using the game. For evaluation campaigns, this saves time and enables deeper insight into buyer behavior. The sales pipeline can be based on user behavior while ensuring user privacy.
- **Turn attempted unauthorized activations into sales opportunities** – if the software is copied to a different machine, it will startup and but not work unless the license activation is moved by the owner or a new license is purchased.
- **The game can be available on CD or as a download** - with exactly the same software activation management.
- **Disable game if charge backs or refund occur** - sometimes users purchase via credit card and download the game then call the credit card company to stop the payment. Charge backs can be a significant problem – easily discouraged if the vendor can disable playing of that game. Game need also to be disabled at full refunds.
- **Reduced costs for support services and update/patch delivery** – a user-friendly solution require far less support calls and a protection system which automatically pushes out mandatory updates/patches reduces costs.
- **Compatibility with existing systems** – a software activation management solution needs to be compatible with e-commerce platforms, e-stores or SaaS games portals, CRM, ERP and billing systems. Integrating systems allows for 24*7 license fulfillment.
- **Direct communication channel with the end users** - direct, regular channel to communicate to end users for automated electronic upgrades, license management & monitoring, up-sell potential.
- **Increase effectiveness of sales channel** - publishers get sales and inventory information pinpointed to particular resellers and outlets. This makes it possible for the channel management team to assess where the sales channel is working to satisfaction or not and thus be able to take corrective measures immediately.
- **Remote management control** – ByteAdmin enables publishers and developers to manage their licenses themselves with the following features:
 - General License Control - Publishers can use many different license types (e.g. full feature trial, try to buy, rentals, rent to buy, floating or not, subscriptions or purchase) with full time period control (e.g. 8 hours, 30 days, perpetual, a specific start date/time and end date/time) or the number of launches or a combination of these parameters. This is especially useful for pre-release products that need to be tightly controlled prior to commercial release. Publishers also control the number of installations, activations, concurrent users (even across multiple offices in multiple locations) and off-line runs. For downloads, this provides infinite

flexibility. For CDs, it provides the opportunity to offer the end user an easy way to change the license.

- Individual License Control – Publishers have control of each license’s parameters on the fly e.g. if a user pays by credit card, downloads and then calls the credit card company to block the payment, that user can be shut off. Your customer service can use the database to help users with forgotten passwords, downloads if the CD is lost etc.
- User Friendly Activation Codes - ByteShield’s codes are random, un-hackable and can be uncomplicated.
- Use Activation Codes To Get Sales Channel Data - By inserting a sales channel (for example, a store chain) identifier into the activation code, publishers get up-to-the-minute sales data for that channel.
- Customize All ByteShield messages – Publishers can customize e.g. an illicit copy of the application/game can open with a prompt asking the end-user to chose a legit license, so creating a new sales opportunity.
- IP Group Control - Publishers can exclude certain IP groups, if so desired.
- Activation Reports - Publisher has access to license activation reports.
- Automate Mandatory and Optional Updates - Publisher can save time by providing mandatory (e.g. patches) and optional updates through the central server. The ByteShield server can even be used to remove ByteShield protection.

Summary: ByteShield Software Activation Management meets all these developer friendly objectives and achieves all these benefits.

4. REFERENCES

1. Linde, A. Crytek CEO Estimates 20 PC Game Pirates for Every One Legitimate Buyer, ShackNews.com, June 27, 2008, <http://www.shacknews.com/onearticle.x/53357>
2. Talkjack, a gamer and blogger. Is DRM killing PC games? (Part 1) - PC Gamers' DRM Charter, June 22, 2008, Coventry, UK, <http://talkjack.wordpress.com/2008/06/22/is-drm-killing-pc-games-part-1/>
3. Talkjack, a gamer and blogger. Is DRM killing PC games? (Part 2) - StarForce, July 19, 2008, Coventry, UK, <http://talkjack.wordpress.com/2008/07/19/is-drm-killing-pc-games-part-2/>
4. Talkjack, a gamer and blogger. Is DRM killing PC games? (Part 3) - Securom, November 1, 2008, Coventry, UK, <http://talkjack.wordpress.com/2008/11/01/is-drm-killing-pc-games-part-3/>
5. Wardell, B. Stardock announces "The Gamer's Bill of Rights", Stardock, August 29, 2008, <http://www.stardock.com/about/newsitem.asp?id=1095> and <http://www.edge-online.com/blogs/the-gamers-bill-rights>
6. Faylor, C. Stardock Rates DRM Complaints, Revises Gamers Bill of Rights, ShackNews, October 15, 2008, <http://www.shacknews.com/featuredarticle.x?id=1026>
7. Alexander, L. Ubisoft: PC Piracy 'Cannibalizes' Console Sales, Gamasutra, October 8, 2008, http://www.gamasutra.com/php-bin/news_index.php?story=20567
8. SafeDisc, Wikipedia, <http://en.wikipedia.org/wiki/SafeDisc>
9. SecuROM, Wikipedia, <http://en.wikipedia.org/wiki/SecuROM>
10. StarForce, Wikipedia, <http://en.wikipedia.org/wiki/StarForce>
11. Simmers Against Securom (SAS), <http://www.the-sas.org/>
12. Reclaim Your Game <http://reclaimyourgame.com>
13. The Prism <http://www.the-prism.com>
14. Case, L. Piracy, Copy Protection, and the Evolution of PC Gaming, ExtremeTech, March 3, 2008, San Francisco, CA, <http://www.extremetech.com/article2/0,1697,2271706,00.asp>
15. Swiderski, A. A History of Copy Protection, Next Generation, Bath, UK, http://www.next-gen.biz/index.php?option=com_content&task=view&id=10800&Itemid=2
16. Kuchera, B. Ubisoft DRM snafu reminds us what's wrong with PC gaming, ars technica, July 20, 2008, <http://arstechnica.com/news.ars/post/20080720-ubisoft-drm-snafu-reminds-us-whats-wrong-with-pc-gaming.html>
17. Lawton, C.; Charney, B. EA Relaxes Rules on Installing 'Spore', Wall Street Journal, September 19, 2008, <http://online.wsj.com/article/SB122178384121054773.html>
18. Spiess, K. Mass Effect's DRM angering many - Game can only be installed three times total, in some situations, NeoSeeker, June 20, 2008, Toronto, ON, <http://www.neoseeker.com/news/8256-mass-effects-drm-angering-many/>
19. BlueSteel, a gamer and blogger. Bioshock DRM Partially lifted, July 4, 2008, <http://bluesteel.coffeecommmander.net/?p=38>
20. Thang, J. Bioshock Install Limits Removed, IGN, June 20, 2008, San Francisco, CA, <http://pc.ign.com/articles/883/883281p1.html>
21. WhiskeyAlpha, blogger. SecuROM ARGH!!!!!!, bit-tech.net Forums, June 21, 2008, UK, <http://forums.bit-tech.net/showthread.php?t=153266>
22. Business Software Alliance (BSA). 5th Annual BSA and IDC Global Software Piracy Study, May 2008, Washington DC, http://global.bsa.org/idcglobalstudy2007/studies/2007_global_piracy_study.pdf
23. Software & Information Industry Association (SIIA). SIIA Anti-Piracy 2007 Year in Review, February 2008, Washington DC, http://www.sii.net/piracy/yir_2007.pdf
24. Lamoureux, T; Brill, R; Joshi, A. Is Unlicensed Software Usage Hurting Your Bottom Line?, KPMG, September 2007, Mountain View, CA, <http://www.sandhill.com/assets/pdf/SLCSurveyReport2007.pdf>

APPENDIX A: PC GAMERS' DRM CHARTER

Source: "PC Gamers' DRM Charter", published on June 22, 2008 by, [Talkjack](#), a UK gamer and blogger who plans to update the Charter from time to time – for latest version see the blog.

1. Stop the practice of covertly installing DRM software on a customer's PC. Dishonest, malicious software such as viruses and spyware install themselves covertly and offer no removal mechanism in Windows control panel. You should be open about what you are doing to customer's computers. Always list the DRM software in Control Panel so that users can uninstall it at will, knowing that the game requires it.

2. You are quite happy to smother the box with logos, copyright notices etc. for companies who contributed to the software on the game disc. You should print clearly on the packaging the name and logo of the DRM system you licensed and bundled with the game. This will allow customers to make an informed choice when they purchase your product, and not have a nasty surprise when they get home and find you have imposed restrictions upon them which were not clearly available at the time of sale.

3. Instill confidence in your paying customers by removing your DRM when it is no longer necessary. After all, if sales have tailed off six months after the release of a game then the DRM is no longer protecting your income, so it is no longer required. It won't cost you much to do this as customers will gladly download your patch at their own expense.

4. Do not modify your customer's PC by installing applications that run constantly. Your DRM system should only be running when your game is running. Otherwise you are slowing down the gamers' PC and risking unnecessary conflicts with other programs they have purchased. You should not be stealing their CPU time and electricity when they are not using your product.

5. If you require someone to connect their PC to the Internet in order to 'activate' the single player game they have purchased then do so in such a way that they do not need to lower their hardware or software firewall protection just to allow your traffic through. If you require a customer to open ports purely to activate your game then you are putting their PC's at risk of being compromised by hackers. Recognize that most of your customers are not PC experts, just people who want to play.

6. Do not disable or ignore the keyboard and mouse when your game is loaded. Most people do not want to sit staring impatiently at the screen waiting for the EA, NVidia and numerous other animated logos and movies to finish playing. If they press the escape key then let them jump to the main menu without wading through adverts beforehand. By the 10th time they have loaded the game you customers will not be watching with interest, but with boredom and animosity.

7. Do not use corrupt registry keys or secret files created in a way which violates the rules of the operating system simply to prevent a customer from deleting your files or keys. It is their PC not yours, and they should be able to manually empty folders and tidy their Windows registry whenever they want, without needed special software or hacker-style techniques to do so. See point 1 above about providing uninstall options in control panel. See my upcoming article on Securom about how this messed up my data backups.

8. *Do not repeatedly scan the CD or DVD in the customer's PC while the game is playing. This technique wastes electricity (you eco-criminals, you) and causes unnecessary wear and tear on customer's PC drives. Eventually you could cause the operating system to step down the performance of the customer's drive permanently. By all means check gamers have a valid disk when they start the game, but then leave it alone. All you are doing is driving customers towards sites like GameCopyWorld to get no-cd patches for games, which make gaming a better experience.*

9. *When someone uninstalls your game from their PC, always uninstall all traces of DRM software from their machines, and do so in a clean fashion. Do not leave remnants behind anywhere.*

10. *Do not install device drivers secretly. It is not your PC so stop installing hidden device drivers on it which may conflict with other legal software that the customer owns. If the customer is not using your game at the time then you have no right to be monitoring what discs they are using in their drives, or what applications they are running. (See part two of this article to read about StarForce and the CD / DVD drive issues with Starforce drivers.)*

11. *Do not refuse the game to start just because the customer has perfectly valid software such as drive emulators or Microsoft Process Explorer on their machines or in memory. By all means detect whether the gamer is using the software to run a pirate copy of your game. However, just because they have got that perfectly legal software installed on their machines does not mean they are actually stealing the game you are supposed to protect. This practice is tantamount to treating all these customers as criminals, not just those who really are pirating your game.*

12. *Answer your tech support emails about DRM. Be helpful. You are supposed to be helping your paying customers, not treating them all like suspected thieves until they can prove otherwise. Do not ignore customer emails to tech support. JoWood, this means you! I have been waiting 2 years for a reply about Spellforce 2 not running because of some unknown error with your DRM system.*

13. *A customer should never be required to download and install DRM system updates in order to get a game to work, e.g. Tages and Vista, Starforce and Spellforce2. If you are causing this much inconvenience to your customers then you are killing the fun of a gaming session and losing reputation and future business.*

14. *If you are going to require a customer to key in long codes of letters and numbers then print them clearly. Do not use hard to read fonts such as Spellforce 1, where customers could not tell I's and 1's, 0's and O's apart and then force them to retype the whole thing if they make a typing mistake. Do not hide the code inside the packaging such as Starcraft budget edition. Do not print the code on the back of a manual in ink which rubs off on the customer's thumb when they are readying, such as Neverwinter Nights!*

15. *If you are going to require customer's to go online to activate their software then do not impose draconian limits on the amount of times they can do so, e.g. Mass Effect. If you are going to refuse to activate a paying customer's game, making it unusable then the game is not fit for purpose because it cannot be played, and your customer should be able to return it as such. You could just as easily reduce piracy by allowing three installations a month for each key code, not three activations period as you do currently.*



ByteShield, Inc.
3240 Lyon Street
San Francisco, CA 94123-1857, USA
+1-415-420-6636
+1-415-931-1185 Fax
www.byteshield.net

16. If a customer is unable to activate their game because their activation code has been used by a pirate with a random key generator, then you should be helping your customer, not forcing them to jump through hoops. Do not force them to buy a scanner to scan and email their receipt, plus buy a digital camera to take a photo of their game packaging. What will you do next, force them to take a photo of themselves holding both receipt, game box, disc, manual and copy of today's newspaper? Just apologize for the inconvenience, give them an RMA code and ask them to freepost you the unusable game for a free replacement. Or give them a letter instructing them to take the game back to the shop for a free replacement, and give them a voucher off a future purchase of one of your games by way of an apology, and to cover their travel costs. Or how about giving them a free electronic copy of an old game from your back catalogue to cheer them up?

© Talkjack 2008. All rights reserved. Reproduced by ByteShield with permission from the author. The most up to date version of this charter can be found on Talkjack's blog, which is [available here](#).



ByteShield, Inc.
3240 Lyon Street
San Francisco, CA 94123-1857, USA
+1-415-420-6636
+1-415-931-1185 Fax
www.byteshield.net

The information contained in this whitepaper represents the current view of ByteShield Inc. on the issues discussed as of the date of publication. Because ByteShield must respond to changing market conditions, it should not be interpreted to be a commitment on the part of ByteShield, and ByteShield cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. BYTESHIELD MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of ByteShield.

ByteShield may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from ByteShield, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 ByteShield Inc. All rights reserved. ByteShield is a registered trademark of ByteShield Inc in the United States and/or other countries. All brand names, product names, or trademarks belong to their respective owners.

This White Paper is one in a series of ByteShield white papers. The ByteShield white papers can be found in the Collateral section on the www.byteshield.net web site.

To learn more about how ByteShield Software Activation Management solutions can help you manage and secure all your PC games and PC applications effectively, please visit our web site www.byteshield.net or contact us at:

ByteShield, Inc.
3240 Lyon Street
San Francisco, CA 94123-1857, USA
+1-415-420-6636
+1-415-931-1185 Fax
sate@byteshield.net