



**XENCARE SOFTLOCK**  
A Smart System Protection with Minimal Overhead



## White Paper

First Edition (August 2008)  
Copyright © 2007-2009 XenCare Software. All rights reserved.

## 1. INTRODUCTION

At present, we are constantly facing sophisticated, targeted and financially driven threats to computer. To counter these threats, we have lots of System Protection Software and Antivirus available in the market. Most of these protection software are getting more and more heavyweight (in complex configuration settings, performance overhead, less ease of use, cost of use etc.) to cope with the ever changing army of threats. If you are annoyed at the complexity of these products comparing to their effectiveness, XenCare SoftLock can be the best choice for you. XenCare SoftLock is a lightweight, simple yet powerful protection for your Windows computer. It is a virtual lock system which, when turned on, thwarts all suspicious activities no matter who tried to do it: a normal program or a threat (Virus, Spyware, Malware, Adware) from inside your computer or over the network. This virtual lock system is superior to other similar products in terms of both ease of use and low CPU overhead. Even a naive desktop user can protect her system by the single click lock mechanism of XenCare SoftLock.

## 2. XENCARE SOFTLOCK: BACKGROUND

Let us use the analogy of a house to represent a user's computer system. There are lots of advanced electronic security systems with complex features and closed-circuit cameras with streaming live view on a website so that user can even monitor the cc-view of her house from anywhere. But nothing replaces the faithful lock at the main entrance of the house. Similarly there is a number of such computer System Protection products in the market which are very rich in features, and are truly effective only if the user is smart enough. But they are not without pitfalls. They can be heavyweight with high CPU consumption or advanced user interface that makes an average user confused to set up the optimal settings. User then needs to go through a gigantic user manual or FAQ pages or post queries to the vendor.

XenCare SoftLock provides a simple locking mechanism to protect the computer by a single click lock/unlock feature with fewer configuration settings and an attractive yet simple user interface. You can use XenCare SoftLock to lock your computer down during usual usage period and unlock when setup related tasks are to be done. SoftLock keeps its constant eyes on what is going on inside your computer, even inside the most restricted areas of Windows kernel. It monitors access requests to program files like executables (.exe and .com), Dynamically Linked Libraries (.dll), drivers and some others. It gives you Proactive Security [1, 2, 3, 4, 5], because it does not care which program is performing suspicious activities on your system: it does not use any threat definition look-up (Reactive security). Whenever any program tries to create or modify any sensitive file (binary files) on your computer, XenCare SoftLock will force the system to stall the activity before it even occurs and notify you. You can always unlock the system, install new program and lock the system again.

SoftLock provides the following Key features:

- Stops any threat, even yet unknown ones.
- Needs no threat definition database.
- Needs no periodical update.
- Protects creation, copying and modification of all .exe, .dll, .com, .ocx and .sys files.
- Presents the user a simple tool for safety.
- Uses low memory and performance overhead.
- Protects start-up program list

#### **a. SAFETY FROM UNKNOWN THREATS: PROACTIVE SECURITY**

Proactive security means stopping threats even when you have not yet encountered it, or have not known of it previously. It is all about dealing with ever evolving pattern of threats while also keeping overall cost much small. Proactive security believes that prevention is better than cure, where cure may be the event of getting updated antivirus after someone has already suffered devastation. A proactive security system does not depend on scanning a file for determining if it is a known threat. It will monitor the system for any suspicious activity, and stall it immediately. This approach is called Security 3.0 [1].

XenCare SoftLock provides the user with proactive security by locking the system from unpredictable damages inflicted by intelligently designed threats. In order to cause serious harm to any system a threat, in most cases, need to copy or modify binary files in crucial system areas without the consent of the system owner. SoftLock prevents these damages with the underlying philosophy of Security 3.0 by not depending on any system scanning process. Since binary file alteration and copy are denied in a SoftLocked system, it acts as the faithful old lock at the main entrance of the house.

#### **b. NO THREAT DEFINITION DATABASE**

Antivirus software products typically use two different approaches to provide protection:

- Examining (scanning) files to look for known virus signatures from a virus dictionary, and
- Identifying suspicious behavior from any computer program which might indicate infection.

Most commercial antivirus software products use both these approaches with an emphasis on the virus dictionary approach. The ones with virus dictionary approach need heavyweight signature databases and sometimes become an overhead for the system. XenCare SoftLock does not need any kind of such threat definition database.

#### **c. NO PERIODIC UPDATES REQUIRED**

As SoftLock does not depend on threat definition database, no periodic update is required for it to stay effective. SoftLock will always protect the system from unwanted modifications of binary files which are generally caused by viruses and Malware.

#### **d. PROTECTION FROM UNWANTED BINARY FILE MANIPULATION**

Any kind of binary file manipulations is blocked by SoftLock. If the user wants to do that manipulation intentionally, or if she wants to run a program which may do such manipulation, she can unlock the system and go on with her intended task. Locking and unlocking is a simple one-click procedure. SoftLock also monitors entry to startup program list. So, it is also not possible for a program to register itself to the startup list without the consent of the user.

#### **e. SIMPLEST TOOL FOR SAFETY**

One of the strengths of SoftLock is its simplicity. It is a very simple tool for system safety. It does not depend on the knowledge and expertise level of the user. For more detailed

control over system protection user can resort to the most feasible antivirus product. But almost all antivirus products have so detailed configuration and interaction options that most users either become confused with them, or fail to extract the full effectiveness of such a product.

XenCare SoftLock provides the user with a small number of customization options and a self describing, user-friendly and intuitive user interface. Users can easily enjoy the full effectiveness of SoftLock without being bothered about nitty-gritty system details. Additionally, SoftLock covers a vast portion of system safety though it is so simple (from user point of view). However, it must be noted that XenCare SoftLock is not an antivirus, and it will never fulfill the purpose of an antivirus. Nor will it ensure total security of the system. It will complement the antivirus software by providing the proactive part of system security.

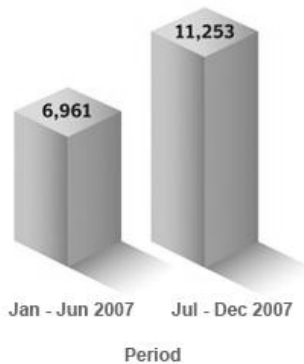
#### **f. LOW SYSTEM OVERHEAD**

It is evident from the previous points that SoftLock is a very simple and lightweight locking mechanism for desktop systems. It just monitors and blocks unwanted binary file modifications and stops any programs to go to the startup list. Since XenCare SoftLock needs no on-demand or on-access file scan, it makes almost no overhead to your system performance.

### **3. SECURITY: SITUATION OVERVIEW**

In modern computing environments, security is one of the most important issues. It should be the highest priority to make sure that a computer always executes safe instructions to maintain privacy, data integrity and safety of computational resources. Systems are connected to networks (the local networks) and networks of networks (the Internet). Due to this inevitable connectedness, the presence of outside attackers and intruders trying to destabilize the computing environment or steal valuable information is obvious. The most common way to achieve those things is to find some exploitable hole and then inject some computer instruction that can be executed internally. Theoretically, there will be always security vulnerability, and there will always be a possibility that someone will be trying to push some bad stuff exploiting that vulnerability. Then it's up to the user/computer to deal with those bad stuffs. Most of the users are not expert and, for example, they can innocently double click on an email attachment to accept those bad stuffs. Or sometimes Operating System or some running program automatically welcomes those bad stuffs because of exploitable security hole in a certain application or Operating System itself.

For the past few years, Symantec (Symantec Internet Security Threat Report) has observed a significant increase in the number of new malicious code threats targeting users and computer systems. As of the end of 2007, the number of malicious code threats that Symantec had identified stood at 1,122,311. Of this total, 711,912 threats were identified in 2007 alone, a 468 percent increase over the 125,243 threats identified in 2006 [\[1\]](#).



**Figure 1 Site-specific Vulnerabilities**  
**Source: Symantec Corporation**

*(During the last six months of 2007, 11,253 site-specific cross-site scripting vulnerabilities were documented, compared to 6,961 between February and June in the first half of the year.)*

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	United States	31%	30%	1	1	1	1	1	1
2	2	China	7%	10%	3	5	2	2	4	2
3	3	Germany	7%	7%	2	2	3	7	2	3
4	4	United Kingdom	4%	4%	9	6	7	3	12	5
5	7	Spain	4%	3%	4	19	15	9	9	4
6	5	France	4%	4%	8	13	6	11	7	6
7	6	Canada	3%	4%	13	3	5	4	35	7
8	8	Italy	3%	3%	5	10	11	10	6	8
9	12	Brazil	3%	2%	6	7	13	21	3	9
10	9	South Korea	2%	3%	15	4	9	14	13	10

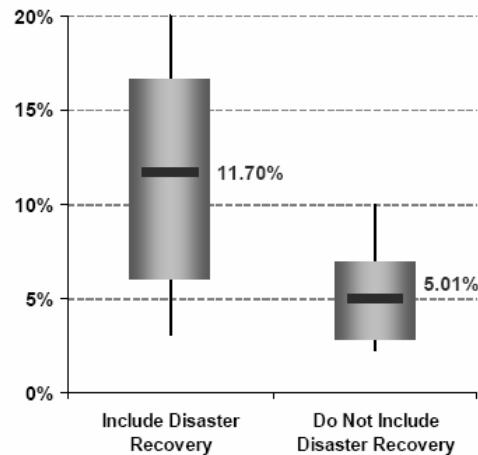
**Figure 2 Malicious activities by country**  
**Source: Symantec Corporation**

*(Symantec Global Internet Security Threat Report trends for July–December 07 Volume Xiii, published April 2008) [6]*

When Adware, spyware and misleading applications are included, Symantec speculates that the ratio of non-malicious software to malicious software being distributed may be reaching a tipping point. In this current condition and with rational anticipation, it can be said that currently available security measures can no longer be effective enough in near future. We need some effective yet simple solutions at this point of current security situation. XenCare SoftLock is the first one of a series of such security products from XenCare Software.

#### 4. SECURITY TRENDS: PRESENT AND FUTURE

Security spending by the enterprises has been growing twice as fast as the Information Systems spending. Still security threats are not completely annihilated and as a matter of fact security is not getting any better compared to the huge amount of costs. System owners, in spite of the hopelessness of further spending, are compelled to increase the security budget to acquire the top-ranked security products by big vendors to fight the threats in ad hoc basis. Since real progress in security should reduce security spending, the additional high costs, though spent fighting the attacks and threats, do not indicate any real security.



**Figure 3 Disaster Recovery Budget Comparisons**  
**Source: Gartner (April 2007)**

*(Note: Data is from Gartner Consulting Worldwide IT Benchmark Service and Gartner Information Security Research Service.)*

Gartner's (Gartner Consulting Worldwide IT Benchmark Service and Gartner Information Security Research Service) latest data shows that the average enterprise is spending more than 5% of the IT budget on security and close to 12%, if disaster recovery spending is included. This amount of spending already exceeds the typical amount spent on all forms of liability insurance by the typical enterprise. However, Gartner has seen little or no correlation between enterprises that spend the most on security and enterprises that are the most secure. While there are definite areas that require additional investment, there are just as many areas of security that can be done more efficiently. This weak correlation between security spending and security level makes the security community all around the globe think about the next generation of security which has been named Security 3.0. To deal with changing threats, changing business environments and continuing budget pressures, enterprises must become more effective and more efficient at protecting customer and business data by adapting the new generation of security measures.

The conventional idea says that the security threats and attacks are completely unpredictable and security is always being in a reactive mode. Over the years, threats have become matured by taking various forms like viruses, worms, denial-of-service attacks, Malware, spyware, Trojans etc. The approach to fight these threats has been reactive ("*oops, new threat - buy new solution*") over the past couple of decades of Security 2.0. Antivirus, anti-spyware and other security products come up with this reactive approach. They keep signature of known threats to database and can only detect and neutralize those known threats. They are needed to be updated periodically to

ensure intended security. So an unknown threat can always cause devastation to the system under such approach, no matter how vast its definition database is.

XenCare SoftLock comes to the scenario with a vow to provide a powerful security mechanism to systems at a very low cost in terms of price, complexity and CPU overhead.

## 5. SECURITY MYTHS: COMMON MISCONCEPTIONS

There are a number of common misconceptions about computer security among users. Users do not know how much vulnerable their systems are while they are thinking that they are safe. Some of the most common wrong ideas are given below as examples.

### I. Since I've installed an antivirus product, I am safe

**Wrong!!!**

Because:

- a. There are always vulnerable spots in a system and there is no universal solution for threat protection. As computer viruses are the intricate workings of intricate minds, they are not subject to any fixed rules. So no particular antivirus product can guarantee 100% protection.
- b. Findings of Kaspersky Lab Virus Research [7] show that there are relatively few products available in shops or on the Internet which offer even close to 100% protection. The majority of products are unable even to guarantee 90% protection. And this is the main problem before the antivirus industry today.

### II. No new virus/spyware can get through to my system, since I have antivirus:

**Wrong!!!**

Because:

- a. antivirus products are based on signature and smart viruses can change their signatures on the fly and same virus can have millions of instances with millions of signatures.
- b. Because of the unimaginable scale and speed of today's Internet, malicious programs propagate so quickly that most antivirus companies fail to release updates as quickly as necessary to minimize the amount of time the users will potentially be at risk. As a result, users often receive updates after they are already infected.
- c. Very often viruses and Trojans are written in a way which enables them to hide their presence in the system and/or to penetrate the system so deeply that deleting them is a complex task. Unfortunately, some antivirus programs are unable to delete malicious code and restore the data which has been modified by the virus without causing further problems.

### III. I have firewall; no one can see me

**Wrong!!!**

Because:

- a. A fully closed firewall would prevent applications from accessing information on the other side of the firewall. Thus, it is necessary to carefully open holes in firewalls that are very small and restricted (hence the term *pinhole*). In computer

networking, the term **firewall pinhole** is used to describe a port that is opened through a firewall to allow a particular application to gain controlled access to the protected network. Leaving open gaps in a firewall exposes the protected system to malicious abuse.

- b. Trojans can get into the system when users are browsing the web and create a back door in their system, go undetected and work well behind firewall.

#### **IV. I use strong passwords; no one can get to my data**

**Wrong!!!**

Because:

A key logger can capture user's password and send it over to a person who can grab user's private data including bank information.

#### **V. I have five different solutions for safety; I am more protected**

**Wrong!!!**

Because:

It's not about how many solutions one have, it's about if they address adequately all the threats one is exposed to.

## **6. XENCARE SOFTLOCK: HOW IT CREATES VALUE**

XenCare SoftLock is a lightweight, simple yet powerful protection for your Windows computer. It is a virtual lock system which, when turned on, thwarts all suspicious activities no matter who tried to do it: a normal program or a threat (virus, spyware, Malware, Adware) from inside your computer or over the network. Some types of file (for example, the executable files with .exe extension on Windows) are capable of providing instructions to the Operating System. XenCare SoftLock works very closely with the operating system and listens to requests that other programs make to the OS. Whenever any program makes a request to create or modify such a file, XenCare SoftLock forces the OS to refuse the request. Thus, it is impossible to modify files of sensitive types when your computer is in locked state.

Threats are evolving every second. To cope with this change, conventional protection software (antivirus, anti-spyware etc.) needs constantly update their definition database. But no matter what a threat is, it (in almost every case) needs to modify/access binary files on your system in order to do harm. However, by monitoring file access requests, XenCare SoftLock can invariably stop every program, be it a threat or not. Besides monitoring file access requests, XenCare SoftLock also watches other sensitive portions of Operating System. It prevents programs from automatically making another program (or itself) initiate when Windows boots up.

This smart approach has many promising advantages:

- No threat definition is needed: absolutely no one is allowed to perform suspicious operation on your computer when it is locked.
- As a direct consequence of the previous point, no regular periodical update of XenCare SoftLock is needed to retain its effectiveness. It will remain as useful as ever against evolving threats once you install it.
- Since XenCare SoftLock does not need to scan files, it makes almost no overhead to your system performance.
- In case you unknowingly launch a malicious program with administrative privileges, XenCare SoftLock can still thwart the program from doing any damage to your system.

However, XenCare SoftLock is no replacement to your antivirus program. It is intended to complement the existing antivirus or anti-spyware programs by protecting unforeseen threats.

## 7. XENCARE SOFTLOCK: FUNCTIONAL OVERVIEW

XenCare SoftLock user interface provides the user with a management control panel for a small number of customization which simplifies the system protection. There is provision for single-click lock/unlock. The following functionalities makes SoftLock an ideal locking tool for all level of users ranging from naive to extremely advanced ones.

### a. CONFIGURE YOUR XENCARE SETTINGS

Using the configuration panel user can do the following things:

- XenCare SoftLock can be activated at the system startup, or not.
- Event notifications can be shown in system tray balloon, or event notification can be disabled.
- Lock/unlock system monitoring i.e. the modification and creation of sensitive types of files.
- Lock/unlock protection of startup programs list.
- Lock/unlock the system during scheduled Windows Update.



**Figure 4 Configuration Panel of XenCare SoftLock**

### b. LOCK/UNLOCK YOUR SYSTEM

A single click on “Lock this system” option in the tray menu enables the SoftLock. SoftLock can be disabled similarly with a single click on “Unlock this system” option.

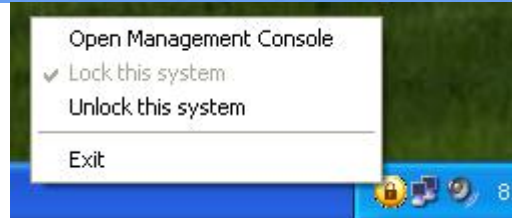


Figure 5 Single click Lock/Unlock Mechanism

### C. TRACK SYSTEM ACTIVITIES: VIEW LOG

User can see the log of activities like process launching, blocked attempts of modification of binary files etc. in the system activities log panel. Events are also recorded in a text file for user if she wants any further diagnosis.



Figure 6 XenCare SoftLock System log

## 8. XENCARE SOFTLOCK IS NOT AN ANTIVIRUS

As stated previously, XenCare SoftLock is not an antivirus or anti-spyware which works based on some wild list dictionary approach. It is a *smart and cool* solution that does not have to be updated regularly in order to retain its effectiveness. Installing XenCare SoftLock once will make the system safe from malicious machine instructions to be executed.

Antivirus software is a computer program that attempts to identify, neutralize or eliminate malicious software. Antivirus is so named because the earliest examples were designed exclusively to combat computer viruses; however most modern antivirus software is now designed to combat a wide range of threats, including worms, attacks, Trojan horses and other Malware.

In the virus dictionary approach, when the antivirus software looks at a file, it refers to a dictionary of known viruses that the authors of the antivirus software have identified. If a piece of code in the

file matches any virus identified in the dictionary, then the antivirus software can take one of the following actions:

1. Attempt to repair the file by removing the virus itself from the file,
2. Quarantine the file (so that the file remains inaccessible to other programs and its virus can no longer spread), or
3. Delete the infected file.

To achieve consistent success in the medium and long term, the virus dictionary approach requires periodic (generally online) downloads of updated virus dictionary entries. As vendors of antivirus software get information about some virus spreading in "the wild", they include information about the new viruses in their dictionaries. An emerging technique to deal with Malware in general is white listing. Rather than looking for only known bad software, this technique prevents execution of all computer code except that which has been previously identified as trustworthy by the system administrator. By following this default deny approach, the limitations inherent in keeping virus signatures up to date are avoided. Additionally, computer applications that are unwanted by the system administrator are prevented from executing since they are not on the white list. Since modern enterprise organizations have large quantities of trusted applications, the limitations of adopting this technique rest with the system administrators' ability to properly maintain the white list of trusted applications. As such, viable implementations of this technique include tools for automating the inventory and white list maintenance processes.

If we get back to our analogy of a house, the contrast between an antivirus product and XenCare SoftLock will be more evident. Basically, antivirus is something like getting a big wanted list of all bad guys from all law enforcement agency, and putting a guard outside your house telling him don't allow anyone to get in my house from that list, no need to add lock on your front door. Whereas, XenCare does not depend on the correctness of the list of effectiveness of the guard, rather locks the front door, and unlocks it when needed.

XenCare SoftLock steps ahead of white listing method by making dictionary approach out of date and giving user the full control over the security system without the necessity of gigantic databases of wild lists.

Even so, XenCare SoftLock is no replacement of an antivirus, at least not yet. In the house analogy, the lock will stop new bad guys about who the guards outside are not yet informed about.

## 9. COMPARATIVE ANALYSIS OF SYSTEM PERFORMANCE

### **System Environment:**

**Processor:** Intel Pentium 4 CPU 3.00 GHz

**RAM:** 256MB

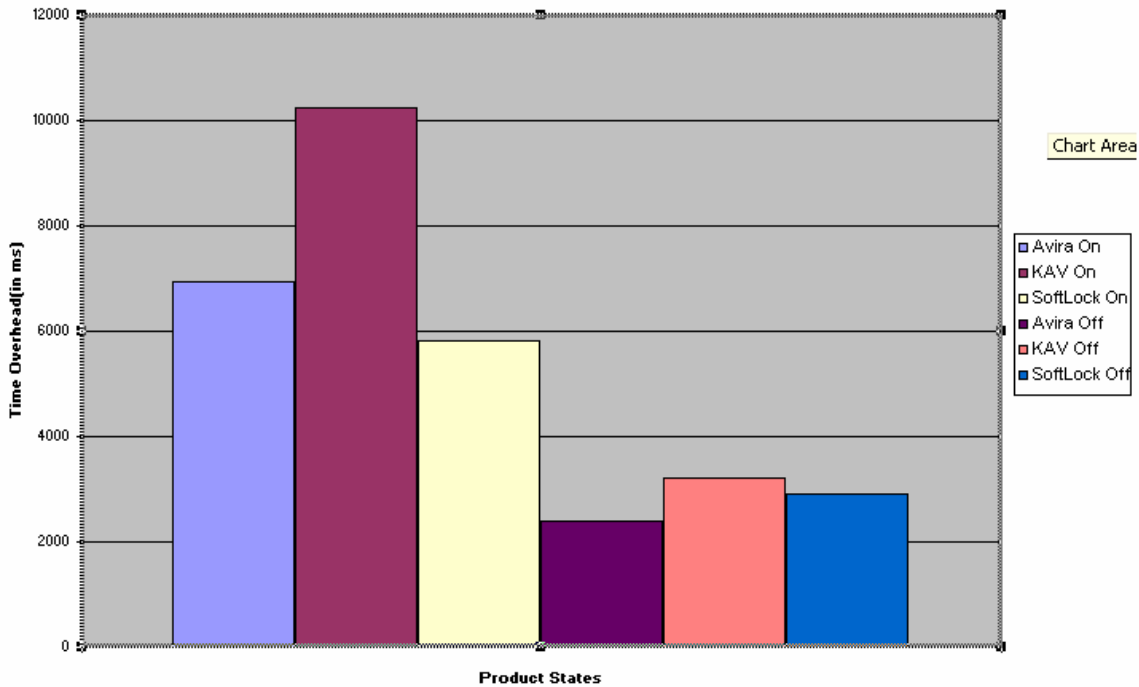
**OS:** Microsoft Windows XP with Service Pack 2

**Test Description:** A folder of 1.28 GBytes was copied from one folder location to another folder with the command line copy option. The copy start time and end time was recorded to measure the

time taken to copy the files in the folder. The time recorded below is on Milliseconds. The time overhead is calculated based on Clean System timing.

	Avira On	KAV On	SoftLock On	Avira off	KAV Off	SoftLock Off	Clean System
Run1	101593	78516	100360	99515	97063	98219	97375
Run2	105625	100516	104640	100125	103156	100719	102360
Run3	101156	111234	101515	98375	97500	97875	88656
Run4	106468	137766	103828	98687	102265	101875	98687
Average:	103710	107008	102586	99175	99996	99672	96770
Time Overhead	6940	10238	5816	2405	3226	2902	0

**Comparative Analysis of System performance in different Security Products**



**Figure 7 A Comparative Analysis**

**10. BECAUSE XENCARE CARES**

The problem of security threats is magnified by the changing intent of attackers. The viruses of the previous days, written by amateurs, exhibited destructive behavior or popped-up screen messages and infections were obvious to the users. Modern viruses are often written by professionals,

financed by criminal organizations. It is not in their interests to make their viruses evident. Their purpose is to create bot-nets or steal information; consequently, they are often well-hidden. If an infected user has a less-than-effective antivirus product that says the computer is clean, then the virus may go undetected. Even major antivirus products have failed to detect programs containing malicious behavior. XenCare SoftLock can make these antivirus products pilfer proof by simply keeping the system free from suspicious computer instructions. XenCare SoftLock cares for your system. That is why it is the best lock for the main entrance to your computer system.

## 11. CONCLUSION

Bundled with cutting-edge technology, proactive security from any external threat, and unmatched security expertise with kernel-level detection – that's XenCare. With years of research and development, XenCare promises to make the IT arena safer than ever but still allows you to manage your PC as you like. XenCare Software builds its solution for the future using few patent pending technologies to provide proactive protection. Future security solution for the 21<sup>st</sup> century should protect system from threats that hasn't been seen yet. XenCare SoftLock is just a step forward to that direction.

## 12. REFERENCES

[1] *Security, Risk and Compliance Scenario: Fighting New Threats, Enabling New Business*: John Pescatore, Ray Wagner

[2] *Trip Report: Security & Risk Management* Gartner Symposium/ITxpo

[3] *Secure Business Operations: Redefine Security*: White Paper from [http://www.unisys.com/public\\_sector/](http://www.unisys.com/public_sector/)

[4] *Towards Proactive Computer-System Forensics*: Phillip G. Bradford, Marcus Brown, Josh Perdue, Bonnie Self

[5] *Active Security—A proactive approach for computer security systems*: Gerhard Eschelbeck

[6] [\*Symantec Global Internet Security Threat Report trends for July–December 07\*](#)

[7] [\*The contemporary antivirus industry and its problems\*](#): Eugene Kaspersky