

SafeGuard[®] Easy - The electronic Fortress

Access Protection and Encryption for Data on
Notebooks and Workstations

Utimaco Safeware AG

Table of Contents

1	Preface.....	3
1.1	Abstract.....	3
1.2	Document Information.....	3
2	The Main Modules of SafeGuard Easy.....	4
2.1	Pre-Boot Authentication (PBA).....	4
2.2	Boot Protection	5
2.3	Encryption.....	5
2.4	Centralized Management.....	6
3	Cost Advantages with SafeGuard Easy.....	7
3.1	"SafeGuard Easy" for the User:.....	7
3.2	"SafeGuard Easy" for IT Managers:	7
3.3	"SafeGuard Easy" for the Administrator:	9
4	SafeGuard Easy – acknowledged worldwide	11
5	Protection of Investment	11
6	Comparison SafeGuard Easy and EFS.....	12
7	Additional SafeGuard® Products.....	13
8	Details of SafeGuard Easy.....	14
8.1	Hard-disk Encryption (incl. hibernation support).....	14
8.2	Encryption of External Data Media.....	15
8.3	Remote Help / "Challenge-Response" Procedure	15
8.4	Group Concept / Central Management.....	15
8.5	Key Management.....	16
8.6	Trial -and-Error Protection.....	16
8.7	Multi-Boot.....	16
8.8	Support of Security Hardware	16
8.9	Feature-optimized.....	16
9	Technical Details – SafeGuard® Easy 4.10	17
10	Further Information.....	18

1 Preface

1.1 Abstract

This white paper describes the features and functions of SafeGuard Easy which, with more than 1.7 million licenses sold, is the most widely sold application for hard-disk encryption and access protection worldwide. SafeGuard Easy works like an electronic fortress by creating a secure environment for users of PCs or notebooks; irrespective of where the notebook or laptop is taken. Whether in the office, on the road, at home - the data on the computer remains protected from unauthorized access and also remains unreadable for third parties should the device be lost or stolen. This is essential protection for valuable electronic information (e-assets), especially on mobile computers.

SafeGuard Easy allows rapid implementation of organization-wide data protection and, due to its durability and low ongoing costs during its life, is a very cost-effective solution. Utimaco Safeware guarantees comprehensive and permanent protection of data through using modern encryption algorithms considered secure by experts.

Furthermore, Utimaco Safeware has had the product analyzed and evaluated by independent organizations. Thus, the effectiveness, security and efficiency of the software is evaluated and certified by a third party. Besides official security certifications such as Common Criteria or FIPS, certifications include also vendor specific evaluations like "Aladdin eToken enabled" or tests in IT-magazines. The Secure Computing Magazine e.g. tested 12 encryption products (09/2002) and evaluated SafeGuard Easy as "Best buy" with an overall rating of 5 stars.

The following chapters show how SafeGuard Easy works and which options the program offers for data protection on PCs and Notebooks.

1.2 Document Information

Version: 4.00.02 final, last changed: 03.10.2004.

Author: Product Management – Device Security.

Copyright © 2004 by Utimaco Safeware AG

All Rights Reserved.

The information in this document must not be changed without express written agreement from Utimaco Safeware AG.

2 The Main Modules of SafeGuard Easy

Using four main modules, SafeGuard Easy creates a secure environment and the user is guaranteed that his data is secured in this electronic fortress wherever the computer is taken:

- Pre-Boot Authentication (user ID and password entry before operating system boot)
- Boot Protection (among other things, virus protection for the master boot record)
- Encryption (for the protection of **all** information on the computer)
- Centralized Management (for enforcement and configuration of uniform security policies on all computers of an enterprise)

2.1 Pre-Boot Authentication (PBA)

The Pre-Boot Authentication (PBA) creates a security area around a computer and can be compared to a defense trench working together with the drawbridge:

In case of a PC, this means that the user has to logon with his user ID and his password before the booting of the computer. Any further information required for booting the computer is derived from the password. None of this information is stored on the hard disk of the computer. Thus, it is made sure that only authorized individuals are able to boot the computer.

Entering the password cannot be avoided. As the Pre-Boot-Authentication works as an autarkic security sub system, it is therefore independent from the operating system; attacks against the operating system are ineffective.

Another potential approach to access a computer is to use a "trial and error" method i.e. repeatedly trying different passwords. If there was human intervention, a guard would soon suspect something was wrong if the visitor did not know the password and gave him several wrong ones instead. In the technical world, this method of attack is called dictionary¹ or brute force attacks². In order to avoid giving the false user of the computer a chance to systematically guess common passwords, SafeGuard Easy, after a definable time limit for typing errors, delays the new entry. After a few unsuccessful attempts, the waiting time between two entries is already up to 20 minutes, thus making it impossible to gain entry using this method.

As an optional extension, SafeGuard Easy supports the user authentication via a cryptographic hardware token (Aladdin eToken) in addition to the traditional UID/password authentication in the PBA. This adds the factor "possession" (the token) to the factor "knowledge" (the password) in the authentication process. Only persons who can present both are granted access. In addition, such a token serves well as key store for PKI certificates e.g. to create e-mail signatures etc.

Effect: Using Pre-Boot Authentication, the first potential wave of attacks on the data in the fortress is blocked!

¹ Dictionary Attacks: At these attacks, it is tried to guess common password by the systematic (alphabetic) going through of word lists (in different and also exotic languages). This is successful with a very high number of PC systems as users like to use known words as passwords (or parts of passwords).

² Brute-force-Attacks: Systematic procedure to go through all (also non-plausible) character and number combinations. Much more slowly than dictionary attacks, but, nevertheless, successful sooner or later (depends on password length)

2.2 Boot Protection

While booting, the operating system (caretaker and coordinator, as it were) is not yet active. Therefore, its security mechanisms are not effective either. In particular the Master Boot Record (MBR) which regulates the ongoing boot procedure is not protected by the operating system. The Master Boot Record is often attacked by one of the most frequent form of computer viruses - boot sector viruses. These are spread by copying themselves into the boot sectors of all systems used (floppy disks and hard-disks). Just through the use of disks, they can "infect" other systems unnoticed. These viruses are able to block, manipulate or delete files and drives.

Thus, the boot protection of SafeGuard Easy brings about two things:

1. "Enforced Booting from the Hard-Disk": The boot protection prevents the computer from being booted by unauthorized individuals using boot media other than that of the hard-disk. This is so important because use of other media (e.g. floppy disks or CR-ROMS) would mean that the booting of the operating system could be avoided and the attacker would be able to give himself administrator rights on the PC and would then have full access to all files.

Using SafeGuard Easy, guarantees that only authorized users are able to boot from a disk.

2. MBR protection: The MBR is particularly well protected. If SafeGuard Easy discovers that the MBR has been touched/manipulated or modified in any way for example by viruses, then it will force the use of the original MBR. At the time of the initial installation, SafeGuard Easy makes a backup of the original Master Boot Record and therefore SafeGuard Easy can use this MBR backup anytime. Thus, SafeGuard Easy effectively protects against boot sector viruses.

Effect: SafeGuard Easy takes away further potential attack opportunities. Attacking tools like MagicDisk which can tear holes in the walls by damaging the operating system become ineffective!

2.3 Encryption

Besides access control, encryption is a fundamental component of SafeGuard Easy. Using encryption, the data on the hard-disk is systematically "encoded". This is achieved by means of a pre-defined mechanism, the "encryption key", and a defined method, the so called encryption algorithm. This procedure is so large-scale that, for outsiders, the data remain unreadable without the "encryption key".

For its products, Utimaco Safeware only uses publicly known, strong and internationally acknowledged standard algorithms. SafeGuard Easy includes the new, extended AES standard with 256 and 128 bit key length as well as IDEA 128 bit among several others. These algorithms have the advantage that their calculation methods are proven and well-known, but the results are unpredictable. Thus, from an encrypted hard-disk, neither the used key nor the original content can be found out.

SafeGuard Easy does not only secure local harddrives, but also removable media such as floppy, ZIP or USB memory sticks. Thus also these media remain secure and protected against unauthorized access in case they are lost.

Effect: By using strong and worldwide acknowledged algorithms, SafeGuard Easy is able to guarantee that the data is protected in the best way possible i.e. even if a notebook or storage media is lost or stolen, SafeGuard Easy customers do not have to worry as their data is kept secret!

2.4 Centralized Management

IT security must not rely on end users actions. Simple and effective methods for software installation and enforcement of security policies are basic requirements which are perfectly met by SafeGuard Easy. It allows itself to be integrated in existing deployment systems, but also provides it's own policy server as an alternative. Scripting interfaces help automating administrative tasks and even if users should forget their passwords, secure methods are in place to help them and regain their productivity quickly.

Effect: Centralized Management ensures, that all doors of your fortress remain closed and security relevant actions only happen on request of the commanding office without requiring him to present locally for his requests.

3 Cost Advantages with SafeGuard Easy

Using comprehensive access protection and the encryption of the entire hard-disk with SafeGuard Easy, organizations (companies and public institutions) can avoid financial losses through stolen data and can meet the data protection demanded by their legislator. With the unique design of the product, an optimal relationship between security and cost is achieved. This is confirmed by more than 1.7 million licenses having been sold up to now.



3.1 "SafeGuard Easy" for the User:

- **Cost advantage 1: Time savings - user training is not needed.**
With SafeGuard Easy, the user only sees the login dialogue after switching on the computer. He logs on before the operating system starts and then, the program does not appear again. As SafeGuard Easy works in the background entirely unnoticed, this mode of function is called "user transparent".
- **Cost advantage 2: Time savings - multiple login to the computer is no longer required.** After a successful initial check on the identity and authenticity of the user (=authentication), login to the operating system can be performed automatically using the Single-Sign-On functionality of SafeGuard Easy.
- **Cost advantage 3: Time savings – no user decisions.**
All data on the hard-disk is encrypted by SafeGuard Easy all the time! And it does not matter where the data is stored on the hard-disk by the user or, implicitly, by the operating system. This saves the user much time as he does not have to take any responsibility for the filing of the data on his hard-disk and he doesn't have to make decisions to protect the data.
- **Performance bonus: Performance of encryption**
Because of the high encryption performance, the user does not notice the encryption (transparency) and is able to work at full speed.
- **Security bonus: Support for encrypted Hibernation**
Especially mobile users often make use of the operating system function "hibernation" (suspend to disk). This function allows freezing the current status of a computer (e.g. by closing the notebook) and restoring it later without having to perform a time consuming boot process. Due to the technical complexity, most disk encryption products do not allow to use hibernation on encrypted disks. SafeGuard Easy not only allows the usage of hibernation, but also encrypts the hiberfile, so that all data remain secure at all times.

3.2 "SafeGuard Easy" for IT Managers:

- **Security bonus: Due to the fact that complete encryption of the hard-disk has taken place on a sector by sector basis, user errors cannot lead to security gaps.** The encryption takes the responsibility for the loss of confidential data away from the user, the administrator and the project manager.
- **Cost advantage 4: Central control and implementation of the security policy**
SafeGuard Easy can be distributed and administered via the network. From a central point, e.g. user-specific rights are defined, filed in configuration files and imported into a computer

without user intervention. This way, an organization-specific security policy can be implemented in departments, business units or in the whole company; completely independent of the individual user.

- Security bonus: Five stars ***** for SafeGuard Easy
Secure Computing Magazine, one of the most popular IT security magazines, evaluated SafeGuard Easy as “Best buy” in a test of 12 encryption products (09/2002). SafeGuard Easy got top ratings (5 stars) for user-friendly operation, performance, documentation, support, price/performance relation and for the overall rating. In addition, SafeGuard Easy was selected as reference product in the Network Computing magazine 04/2003 amongst six tested harddisk encryption products.
- 

- Cost advantage 5: Protection of investment
SafeGuard Easy currently supports Windows 2000/XP and Windows 2003 Server. Older versions support all Microsoft operating systems starting with MS-DOS and even OS/2. Broad platform support, with migrations between different operating systems and SGE versions being achieved smoothly along with the product longevity represents an invaluable protection of investment for the customers of SafeGuard Easy.
 - Cost advantage 6: Low support costs
Due to it's effective design, SafeGuard Easy rarely requires software or policy updates. Thus the maintenance costs for SGE are much less then for other software products in large, productive environments.
 - Cost advantage 7: Training
No end user training is required. The only user interaction with SafeGuard Easy is to enter his user name and password. As no training is required here, this project phase is dropped completely. Therefore, desktop security projects are completed more quickly and more cost-effectively
 - Cost advantage 8: Time savings - external, objective security check
In a desktop security project, the check and evaluation of the security and effectiveness of a software solution is one of the phases which is most difficult to calculate. Few organizations have employees who are experienced in putting security software to the acid test themselves and external consultants are often swamped with this. Utimaco Safeware takes this evaluation off its customers and has had SafeGuard Easy certified by an independent institution according to the internationally valid Common Criteria (CC) regulations. In addition, a certification of the encryption core according to the US norm FIPS 140-2 is currently in progress.
 - Cost advantage 9: Interoperability with security hardware
SafeGuard Easy allows the usage of security hardware such as cryptographic USB token (eToken) or Trusted Platform Modules (e.g. IBM ESS chip). Therefore a higher security level can be achieved by using this hardware. On the other hand, if the hardware already exists in the company, SafeGuard Easy will allow using the hardware more effectively and so ensure a return of investment (ROI) for the hardware more quickly.
 - Cost advantage 10: Time savings by supporting outsourcing
Implementing a security projects with SafeGuard Easy does not require large teams of security and IT personnel to be available. In addition, the configuration and installation of SafeGuard Easy also could be outsourced to an external service provider.

- **Cost advantage 11: Cost and time savings by permanent long-term encryption**
The choice of different and most current algorithms keeps the operating costs low as data encrypted once does not have to be encrypted again for years.
- **Cost advantage 12: Sharing hardware costs with users**
In certain areas e.g. insurance agents, it is common that users pay parts of the costs of their computer hardware and in turn get the right to use this hardware privately as well. The centrally managed part of the computer needs then to remain secured and under the control of the administrator at all times, whereas the user shall have all freedom in the private part of his PC. Such scenarios can effectively be set up with the "Twinboot" function of SafeGuard Easy. Even more, this allows in addition saving the costs for separate boot manager software, since this functionality is already integrated in SafeGuard Easy.

Flexibility bonus

SafeGuard Easy is no isolated solution. The broad portfolio of the SafeGuard product family allows the extension of the disk encryption core by other security modules as demand arises e.g. for SSO to arbitrary applications, usage control of Plug & Play devices, workgroup based data encryption on network drives etc.

3.3 "SafeGuard Easy" for the Administrator:

- **Cost advantage 13: Cost savings using automated installation and pre-configuration**
According to the organization's specific security policy, the administrator prepares the required settings and distributes the software together in combination with the encrypted pre-settings. Then, the installation and initial encryption of the hard-disk(s) can be made without direct intervention of the administrator or user. As no permanent connection to an administration server is required, the costs for the roll-out of a solution with SafeGuard Easy are clearly below the costs of solutions of competitors.
- **Cost advantage 14: Time savings by "deploy and forget"**
After the installation of SafeGuard Easy, the data is reliably protected and normally, there are no further administrative tasks ("deploy and forget"). Settings like password rules or used algorithm are previously defined by the administrator, but can be changed easily if required. As SafeGuard Easy encrypts entire hard-disks or partitions, but no directories, a configuration change is only necessary in exceptional situations.
- **Cost advantage 15: Time savings by remote configuration of client notebooks**
Changes in the SafeGuard Easy configuration can easily be created by "Wizards" and be distributed to the client notebooks using a protected configuration file and a central management console. The administrator is free in his choice of transmission media and can send the configuration to computers without direct access to an administration server even via e-mail.
- **Cost advantage 16: De-blocking possible without sending in the computer**
If users have forgotten their passwords, their computers can be cleared via telephone using the hotline and a "Challenge/Response" procedure. Here, a password is never transmitted in clear text and this help is also possible without network connection of the computer. Further options: e.g. entering an expendable password or switching off the disk encryption is possible without sending in the computer to the IT department or the IT service provider.
- **Cost advantage 17: No organizational instructions for emergency help required**
The emergency help over the "Challenge/Response" procedure is immediately ready for use





without preparation, training or organizational instructions: Calling the house internal help desk is enough to clear a blocked computer. This saves much time and considerable costs both in the implementation of the desktop security project and during its daily operation.

- **Cost advantage 18: Setting up a user pool is possible**
SafeGuard Easy supports up to 15 different user configurations with different user profiles. Thus, an unlimited number of users can work on one computer without having to do without the security of encrypted data.
- **Cost advantage 19: Scripting Interface**
Many repeating administrative actions can be executed in a completely automated way via the new scripting interface of Safeguard Easy. This leaves the administrator more time for complex and higher level tasks.
- **Cost advantage 20: Secure Wake on LAN (WOL)**
Unattended software deployment often contradicts with the requirement to have pre-boot authentication of users, as typically there is no user present to enter a password when WOL occurs. SafeGuard Easy now offers the administrator proper means to perform centrally managed software deployment via Wake on LAN without reducing the PBA security more than absolutely necessary.
- **Cost advantage 21: Compatibility with IBM Rescue and Recovery® (RnR)**
SafeGuard Easy is the first harddisk encryption product, which provides IBM certified compatibility to the backup software IBM Rescue and Recovery and other ThinkVantage Technologies. Rescue and Recovery allows convenient creation and restoration of local backups even by end users. The interoperability of both products ensures that backups are encrypted just as other operating system data and that even a full system restore can be performed without having to do a prior complete decryption of the harddisk. This helps saving time and costs without compromises in security.

4 SafeGuard Easy – acknowledged worldwide

Utimaco Safeware is acknowledged as the best hard disk encryption solution by many decision-makers in top organizations world-wide. Therefore, when looking for a solution to secure data on PCs (desktops and notebooks), SafeGuard Easy is frequently chosen. Over 1.7 million licenses sold make SafeGuard Easy the most successful hard-disk encryption solution world-wide. Many administrators have successfully rolled out big security-projects with SafeGuard Easy. The users of notebooks of SafeGuard Easy customers often do not even know that the data on their computer is protected as the software works so transparently.

■ References

- Dresdner Bank, Allianz Versicherungen (insurance), Deutsche Post, STATOIL Norge AS, KPN Telecom, HYDRO, DBV-Winterthur (insurance), EADS Airbus, Vodaphone (Sweden) Gerling (insurance), R&V Versicherung (insurance), numerous ministries and financial organizations worldwide, including the „Canadian Customs and Revenue Agency“.
- SafeGuard Easy is certified according to the worldwide IT security standard Common Criteria (test level EAL 3). Certification is the testing of the quality and security of the product by an independent institution. The continuous certification of various versions of SafeGuard Easy has been made since 1994. In addition, the cryptographic core of SafeGuard Easy is currently under certification according to the US standard FIPS 140-2. 
- Besides security certifications of independent third parties, also the interoperability with hardware devices becomes increasingly important. Therefore SafeGuard Easy has been designed and certified according to the Aladdin eToken Enabled logo criteria, which ensures interoperability with other eToken enabled applications. 
- The product offers excellent security: During the long-standing success story of SafeGuard Easy (over 10 Years) it has never been necessary to issue a service pack because of a security problem.
- The product is characterized by unequalled stability.
- Secure Computing Magazine, one of the most popular IT security magazines, evaluated SafeGuard Easy as “Best buy” in a test of 12 encryption products (09/2002). SafeGuard Easy got Top ratings (5 stars) for user-friendly operation, performance, documentation, support, price/performance ratio and for the overall product rating. 
- SafeGuard Easy was selected as reference product in the Network Computing magazine 04/2003 amongst six tested harddisk encryption products. 

5 Protection of Investment

The broad platform support and the long-standing existence and stability of the product is a priceless investment protection for customers of SafeGuard Easy. The data of SafeGuard Easy users is protected on computers in heterogeneous environments. During migrations between different operating systems or software version re-encryption of the data is not necessary.

SafeGuard Easy already today allows to make use of a Trusted Platform Module (TPM) chip, as it is found in many modern computer systems e.g. IBM Thinkpad. This utilizes existing hardware in an optimal way and ensures a fast Return of Investment of Hardware costs.

6 Comparison SafeGuard Easy and EFS

For the protection of files and data on computers, several professional encryption programs and cost-effective shareware are available. Since the release of Windows 2000, the Microsoft operating systems have also included protection mechanisms to prevent unauthorized reading of files on individual computers. But PC administrators who have to implement the company's security policy with the help of these protection mechanisms (Encrypting File System (EFS)) are faced with several problems.

Among other things, the PC administrator has to define the following:

- Which data is not worth being protecting?
- Where do the users have to file confidential data?
- How is the key management / recovery regulated?
- etc.

These questions have to be answered, before EFS is activated. Moreover, it has to be tested with every deployment of new software, e.g. of a new application or a security patch for every affected computer to confirm whether the initial configuration is still valid. It is feared that, with day to day pressures, many of these tests and particularly the reactions of them are omitted and so more and more security gaps open up. A high security level can theoretically be achieved with the settings in EFS but this requires detailed preparation and very thorough (and time-consuming) control of the security aspects during the planning and implementation stages. The documentation of the settings is very difficult to start with. To prevent security gaps with every additional installation will, however, prove even more difficult.

New/additional security gaps appear because many applications swap out file fragments and entire files in directories unknown to the user. Therefore, they become available on the hard-disk in clear text without the knowledge of the user. In fact, the protection by the EFS strongly depends on the active participation of the user. He for example has to explicitly name the directories where the confidential files are filed.

Additionally, files required by the system **before** user login **cannot** be encrypted. In the first place, this refers to the swap file, which is particularly security relevant as it contains confidential system data, in addition the boot partition, files in the system directory as well as newly created directories in that. All files in these directories cannot be encrypted! Furthermore to regain access to encrypted data in case a user has forgotten his password is a complicated task, which is anyway only possible, if such a situation has been considered and taken care for from the beginning in the rollout plan.

Conclusion:

Only a program for hard-disk encryption on sector by sector basis like SafeGuard Easy secures all data, no matter where they are on the hard-disk. It relieves both the user and the administrator from actively having to worry about securing confidential data. Besides that, it is only hard disk encryption that can prevent an attacker from booting the computer from CD or disk and making modifications without running the operating system to grant himself more rights for a future login.

If, besides the purchasing costs, the ongoing administration and management costs during operation are considered, SafeGuard Easy, in contrast to shareware programs or EFS, proves to be the more cost-effective and easier-to-handle solution.

7 Additional SafeGuard® Products

SafeGuard Easy works like an electronic fortress which protects the data on a PC or notebook no matter where the computer is located.

Although SafeGuard Easy is the ideal data protection when the computer is switched off ("power-off-protection"), a company may have further security requirements:

- to prevent manipulation of data or configurations on a computer
- when sending files over public data lines,
- when using confidential files within an organization or

For the protection of e-assets, Utimaco Safeware and its partners are offering the following products:

SafeGuard® Advanced Security

SafeGuard Advanced Security consists of seven modules that secure the data integrity, ensure a higher stability of the entire IT infrastructure and decrease internal support costs.

One example is its unique single sign on capability which enables convenient registration of the user to different systems at the same time (e.g. file server, ERP systems). This automated Single-Sign-On saves the user a lot of time.

The Plug & Play management module as another example, allows restricting unauthorized usage of Plug & playing hardware such as USB memory sticks etc. Application Specific Access Rights allow a very fine grained usage policy optimized to the actual needs and environment.

With its comprehensive capabilities, SafeGuard Advanced Security is the ideal tool to assist a company to enforce their organization-wide security policy.

SafeGuard® PrivateCrypto

By using SafeGuard PrivateCrypto, confidential files can be secured with strong AES encryption and password protection. E-mails with encrypted attachments can be sent and therefore it allows you to communicate securely over the internet without the need of a complex PKI infrastructure in the background. Any file can be provided with a password and can easily be compressed and encrypted by a mouse click. SafeGuard PrivateCrypto is integrated into the context menu of Microsoft Windows Explorer and can easily be activated using the right mouse button. Therefore, the program is a useful supplement to SafeGuard Easy.

SafeGuard PrivateCrypto is also available in a Pocket PC version for PDAs.

SafeGuard® LAN Crypt

SafeGuard LAN Crypt enables the access of user groups (project teams, management, personnel department, R&D etc.) to confidential and therefore encrypted data. The files can be stored on different storage media (hard-disks, disks, CD-ROMs etc.) or even on a network server. SafeGuard LAN Crypt is particularly an ideal solution if a workgroup based key management and / or a separation between Windows and security administration is desired.

8 Details of SafeGuard Easy

8.1 Hard-disk Encryption (incl. hibernation support)

With SafeGuard Easy, the hard-disk can be encrypted completely or partition by partition. This means that there is nowhere on the hard-disk(s) where files in clear text are stored. Why is complete encryption so important?

Advantages of complete Encryption of Hard-disks at Sector Level

- user-independent security/ correctness in use:
 - Simple, quick and complete implementation of an organization-wide security policy
 - Critical information does not have to be marked in any way
 - Users do not have to be trained or advised which data is worth being protected.
 - Users cannot store valuable and company confidential data in clear text.
- Negates the need for special actions when hardware errors occur
 - The hard-disk isn't functioning, but can be "addressed" thru the operating system: The hard-disk can be repaired without the necessity to delete the data.
- User-independent security:
 - IT manager do not have to be concerned about where application programs set up directories and files or file fragments. In contrast to Encrypting File System (EFS) in the Microsoft operating systems, administrators and users do not have to set up, supervise and update a security policy for every current and future directory.
- Complete data protection against cloning of hard-disks and against the manipulation of **all** important files:
 - Operating system
 - Temporary files
 - outsourcing files
 - Future files of unknown file formats
 - Files in the early boot phase
 - Main memory image as created during hibernation
- Availability for almost all Office software and hardware platforms
 - Supports all important Microsoft file systems (FAT-16, FAT-32, NTFS)
 - Can be installed on all notebooks and workstations
- Flexible update mechanisms by encryption which can be restricted partition by partition:
 - Operating system and application programs are stored on C:\ in clear text, documents and data of the applications are available in an encrypted form, e.g. on D:\
 - SafeGuard Easy enables automated backup procedures, e.g. upgrades or mirrored hard-disks (catchword "Ghost") of C:\
 - Result 1: company confidential data is protected permanently and without loopholes

- Result 2: modern and cost-saving PC concepts are supported
- Twinboot and Boot Manager options in SafeGuard Easy allow a simple and effective implementation of scenarios which separate between private and business partition and support even more complex "Multi-Boot" scenarios.

8.2 Encryption of External Data Media

As SafeGuard Easy supports all Microsoft file systems, the encryption of external data media like Floppy, ZIP, JAZ disks, USB memory sticks, Compact Flash or SD memory cards is also possible and enforceable. Thus, data on removable media can also be protected and remains secure if the media should get lost or stolen.

8.3 Remote Help / "Challenge-Response" Procedure

For most day to day tasks, SafeGuard Easy offers an efficient help tool. With the so called "Challenge-Response procedure", the system administrator can authorize the following actions:

- De-installation of SafeGuard Easy
- New definition of user password
- Registration and backup of error search
- Allow switching of disk encryption.
- Allow n -number of times a tokenless logon (in case user has lost his token)

The Challenge- and the Response-Code can only be "used" by the system administrator or the user of SafeGuard Easy. Therefore, the transmission of these codes over telephone or fax is not a security issue! A Challenge or Response-Code that has been used once cannot be used a second time.

As additional options for the helpdesk, there exist server based web-interfaces and also a Pocket PC client which allows to generate the response code. Furthermore, the challenge-response process could even be fully automated by adding a biometric voice recognition server from VOICE.TRUST.

8.4 Group Concept / Central Management

Optionally, SafeGuard Easy can be personalized to individual users or templates (group concept). The configuration and administration can conveniently be made from a central point. SafeGuard Easy allows hierarchical delegation of administrative rights. The central policy deployment can either be integrated in existing software deployment tools or make use of SafeGuard Easy's own central management server and network agent.

The scripting interface allows in addition the automatization of repetitive administrative tasks.

The "Secure Wake on LAN" option allows for the first time the combination of centralized, unattended software deployment and secure pre-boot authentication.

8.5 Key Management

No relevant security information such as passwords or used keys are stored on the hard-disk. As the data on the hard-disk cannot be decoded at reading-out or cloning, it is protected from attacks.

8.6 Trial -and-Error Protection

After an incorrect password entry, the response time of SafeGuard Easy increases. By using this method trial and error or brute-force attacks are impossible.

8.7 Multi-Boot

SafeGuard Easy can also be used for the protection of data on a computer, when several operating systems are installed at the same time but in separate partitions. The program also enables you to define partitions that should remain unencrypted e.g. when they are only for private use.

8.8 Support of Security Hardware

SafeGuard Easy takes advantage of modern security hardware such as Aladdin eToken or Trusted Platform Modules (TPM) to meet even highest security demands.

8.9 Feature-optimized

SafeGuard Easy has become increasingly efficient during the course of its development history, nevertheless, it does not include features which are useless in practice. It is a development philosophy to avoid the introduction of features that represent a risk themselves or would affect the system performance. Besides the security mechanisms, the high usability of SafeGuard Easy within organizations has also been an important factor.

9 Technical Details – SafeGuard® Easy 4.10

[System requirements]	
Hardware	PC with Intel Pentium or compatible processor
Operating system	Microsoft Windows XP / 2000 Microsoft Windows 2003 Server Standard Edition
Network	All Windows-supported networks
[Interaction / technical data]	
Third-party suppliers	SafeGuard® Easy is compatible with all typical software distribution systems (MSI packets). Optional fully-automatic, biometric challenge / response helpdesk via VOICE.TRUST Server.
Additional Utimaco Safeware products	SafeGuard® Advanced Security modules as add-ons to support other smartcards, central auditing, Multi- Desktop, SSO, PnP management, Application Specific Access Rights etc. SafeGuard® LAN Crypt for File/Folder encryption. SafeGuard® Easy Web Console for Challenge / Response Helpdesk, with CryptoServer 2000 Hardware Security Module.
Encryption	AES (256 and 128 bit), Rijndael (256 bit), IDEA (128 bit), DES (56 bit), Blowfish-8/16 (256 bit), Stealth-40 (40 bit), XOR (64 bit).
Smartcards	Aladdin eToken Pro for user authentication at pre-boot level. eToken via PKCS#11/CSP interface can also be used for other applications. Other types of smartcard can be integrated via PKCS#11 at operating system level. ³
TPM modules	Integration of security chips that meet Trusted Computing Group (TCG) specifications for: Machine binding of disks, authentication between clients and administration servers, as well as for hardware based key generation. Currently tested for IBM ESS.
Certification	<ul style="list-style-type: none"> • Common Criteria EAL3 • FIPS 140-2 (in evaluation) • Aladdin eToken enabled
Special features	<ul style="list-style-type: none"> • pre-boot authentication before the operating system starts • allows a combination of (up to 8) bootable operating system partitions that are either encrypted or not encrypted • encryption of removable media (diskette, ZIP, JAZ, USB memory stick) • Compatible to IBM Rescue and Recovery • supports hibernation (Suspend to Disk)

³ Also requires a SafeGuard® Advanced Security module.

10 Further Information

If you would like to find out more about mobile security products, please contact your nearest Utimaco Safeware distributor or visit our website:

<http://www.utimaco.com/sg-easy>

<mailto:info.pds@utimaco.de>

Utimaco Safeware AG

P.o. Box 20 26

D-61440 Oberursel, Germany

At the e-mail address: info.pds@utimaco.com one can order an evaluation sheet that helps an organization in quantifying the risks and costs associated with lost or stolen notebooks and desktops.

SafeGuard[®] is a registered trademark of Utimaco Safeware AG.

Microsoft[®], Windows[®], Windows NT[®], Windows 2000[®], Windows XP[®], Windows CE[®] are registered trademarks of Microsoft

Microsoft, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

eToken is a registered trademark of Aladdin Knowledge Systems Ltd.

Rescue and Recovery[™] is a registered trademark of IBM.