Product Insight

Do "standard tools" meet your needs when it comes to providing security for mobile PCs and data media?

Author Utimaco Product Management – Device Security

Version 4.30.00 final, last change 14 August 2006

Document Information SGE430-RAU-0806-EN

utimaco® safeware

Table of contents

1 Introduction 3
2 Comparison 4
3 Appendix 1: Limitations of "simple" standard tool solutions 8
4 Contact information 9

1 Introduction

Modern PCs, notebooks and desktops running Windows XP offer a multitude of options to provide a certain level of security "out of the box". Many companies use them to protect their clients. (Security solutions that use operating system functions to protect PCs and mobile data media against misuse are called "standard tool" solutions in this document.)

Examples of this kind of solution includes: BIOS password, hard disk password (special hard disks necessary), Windows Encryption File System (EFS), etc.

At first glance the "standard tool" solutions appear to meet companies' basic needs for security, user-friendliness and ease of administration. However, there is a whole range of requirements that cannot be met with solutions implemented with "standard tools".

The checklist below is intended to help companies determine the extent to which a solution that uses "standard tools" can meet their security requirements. The "checkpoints" contain a selection of the requirements that Utimaco has recognized as important over its more than 20 years of experience in providing IT security for companies.

For each requirement the "standard tools solution" is compared with the solution that SafeGuard Easy offers. SafeGuard Easy is a product in Utimaco Safeware AG's SafeGuard product family that has been specially developed for protecting mobile PCs and data media against misuse. You will find a comprehensive description of the requirements that these solutions meet, and the functionality of SafeGuard Easy, in "Security of Mobile PCs and Data Media", which you should read as a supplement to this paper.

2 Comparison

Checkpoint	For the security of our clients and data media it is important that…	Which solution do standard tools offer us and what aspects of it should we take note of?	What solution does SafeGuard® Easy offer us?
1	… all user data saved on the local hard disk, such as Word or Excel documents, and emails, is protected against being viewed by unauthorized outsiders, if the notebook or hard disk is stolen or copied.	Variant 1: EFS The Encrypting File System (EFS) performs transparent, file/directory (folder)-based encryption within the Windows operating system. Here you should note: 1) The system administrator must activate and configure EFS. 2) Users must be trained to save their data in the correct directories or encrypt it. 3) If a user would like to protect specific individual confidential files, they must deliberately activate encryption for the relevant file or directory via Windows Explorer (right-hand mouse button). Variant 2: BIOS password Variant 3: hard disk password	SafeGuard Easy transparently encrypts the entire hard disk for users ("transparent encryption"). The user has no need to perform any particular actions to ensure the confidentiality of their data if it is lost or stolen. See Appendix 1. See Appendix 1.
2	… user data saved on removable media is protected against being viewed by unauthorized outsiders, if the media are stolen or copied.	EFS: 1) Only a small number of removable media permit EFS encryption (only the ones that have been formatted with the NTFS file system). The majority of removable media uses the older FAT file system and so remains unprotected. 2) Encryption with EFS requires the user to perform additional steps. 3) If EFS is in use it is not possible to force the encryption of removable media at a central location: it is left to the user.	1) SafeGuard Easy can completely encrypt any removable data medium, no matter what file system it uses (excluding CDs/DVDs, for which there are other SafeGuard solutions). 2) For the user, SafeGuard Easy works completely transparently so the user does not have to perform any additional actions to protect their data. 3) It is possible to force the encryption of removable media at a central location, thus ensuring that data can be saved on a data medium without being unprotected.
3	…temporary copies of confidential user data in system files are also always encrypted, and so protected, no matter what the user does.	EFS: 1) Users must be trained to encrypt their data before saving it. 2) Before temporary copies of the edited files can also be encrypted, it is necessary to find out where this temporary data is saved for each application. The user must take responsibility for including these	1) The users do not need training to use SafeGuard Easy. 2) With SafeGuard Easy all data saved on the hard disk is always encrypted, invisibly ("transparently") for the

		locations in encryption. 3) Copies of the confidential data that the operating system also saves in the swap-file cannot be encrypted with standard tools. As an alternative these files can be deleted automatically when the operating system is shut down. However this means that even more time is lost by the deletion process. When a notebook enters hibernation mode, a memory dump image of the RAM is saved on the hard disk. The operating system does not protect these files by encrypting them.	user. 3) Since SafeGuard Easy always encrypts all data on the hard disk, it is not necessary to make special arrangements for temporary files or the swapfile, to ensure their confidentiality. In addition SafeGuard Easy is one of the few solutions currently available in the market that also fully protect the notebook in hibernation mode, because SafeGuard Easy also encrypts the hibernation files.
4	… no harmful programs are imported onto the clients via removable media.	Operating system settings: Certain types of harmful program import can be prevented with standard tools by assigning suitably restrictive user rights. These include, for example, forbidding the execution of scripts or installation packages. However, there are also some types of import, such as the running of EXE files, that cannot be prevented with standard tools. Consequently the importing of data remains a threat.	If SafeGuard Easy is configured in such a way that only encrypted data media can be read, it is impossible for harmful programs to be "sneaked in" to the system via (plain text) data media. More powerful protection can be provided using modules available in SafeGuard Easy's stablemate SafeGuard Advanced Security. With them it is possible to specify whether individual file types can be created or run on a case-by-case basis, no matter what import/export mechanism is in use (and therefore also email etc.)
5	… after booting from external media (for example, CD), direct hard disk accesses cannot be used to install harmful programs such as viruses or trojans, change access rights to files or to spy out local password data via dictionary attacks.	Operating system settings: An experienced administrator using standard tools can recognize some forms of these attacks, and set up obstacles to them, for example by only using signed drivers or by using domain accounts instead of local user accounts, etc. However, even if all the functionality provided by these standard tools is used to the full, it is not possible to fight off all the threats that can be caused by external booting since it is still possible to change data	SafeGuard Easy generally makes external booting with concurrent access to the plain harddisk impossible and consequently thwarts attempts to get round the operating system. It does so by completely encrypting the entire hard disk including the operating system, and

		directly on the hard disk.	integrating that with user authentication before the operating system even boots (PBA: pre-boot authentication). Consequently SafeGuard Easy offers complete protection against the installation of harmful programs, changes to access rights or the spying out of local password data.
6	… our clients are always protected, no matter what the current operating state is.	Variant 1: EFS System data cannot be encrypted with standard tools. Access rights only apply when the system is running, and not at all if the system is booted using an external medium. RAM images such as the swapfile or the hibernation file remain unencrypted, in plain text. This means that the protection provided by standard tools cannot prevent someone from reading secret data such as keys, passwords, or confidential documents that are currently being edited, from this memory dump image (such as swapfiles or hibernation files). Variant 2: BIOS password Variant 3: hard disk password	The protection provided by SafeGuard Easy means that attacks during the boot process or in hibernation mode are generally made impossible. It does this by completely encrypting the entire hard disk including the operating system, and integrating that with user authentication before the operating system even boots (PBA: pre-boot authentication). See Appendix 1. See Appendix 1.
7	… the user authentication is extremely reliable.	Operating system logon: To increase the reliability of user authentication it is also possible to introduce, alongside the "knowledge" factor (the password), a second factor, "property" (a smartcard or token). Although hardware tokens of this kind can be integrated, this necessarily requires the use of Active Directory and a PKI in the background. Even then, however, the operating system itself is not protected from being changed from outside.	When SafeGuard Easy is in use, a hardware token can be integrated as a second factor for authentication (and with Aladdin eToken this even applies during PBA). Additional systems such as Active Directory or PKI are not required. However, if these kinds of systems have been implemented, SafeGuard Easy can use the token jointly with them.
8	… we minimize the effort and cost needed to define, implement and update our security guidelines to ensure the confidentiality of locally-saved data.	EFS/Windows Administration: When EFS is in use, standard Windows Policies are used to configure security settings. However the settings that need to be made for encryption are fairly complex.	With SafeGuard Easy all that is needed is a few, simple policy settings that rarely need to be changed since, quite simply, the entire hard

			disk or removable medium is encrypted.
9	… the encrypted data saved on the client is not lost for ever if the user forgets their password.	EFS/Windows Administration: It is necessary to set up recovery accounts when EFS is implemented. The operating system's recovery procedures are complex and in practice require an online connection to the client if there is no recovery administrator on site.	SafeGuard Easy provides a simple challenge/response procedure for resetting forgotten passwords, even over the telephone. There is no need for an online connection.
10	… the users can still get back to work again as quickly as possible, if they forget their password when they are on the move and can only contact our helpdesk by telephone – without connecting to our corporate network.	EFS/Windows Administration: To reset a forgotten user password you need an online connection or a local administrator.	SafeGuard Easy provides a simple challenge/response procedure for resetting forgotten passwords, even over the telephone. There is no need for an online connection.
11	…defective hardware can be replaced, or leased devices can be returned, without time-consuming deletion of any confidential data saved on these devices (their hard disks).	No solution available using standard tools: Data on hard disks must be destroyed with special wipe tools to ensure that there is no confidential data left behind (even in temporary or system files). It is not enough to simply delete files or format hard disks as there are data recovery tools and companies that can recover the data.	Hard disks can be passed on without special processing. As SafeGuard Easy encrypts all contents, there is no compromise on confidentiality.
12	… users can keep their data confidential from other colleagues even if several users work on the same PC or server.	EFS: This requirement can be met with EFS if a user specifically encrypts the data that they want to keep confidential.	SafeGuard Easy is designed to globally protect end devices and mobile data media. For this reason, it encrypts hard disk partitions and not individual files. To ensure that data in working groups remains confidential, you should use SafeGuard LAN Crypt or SafeGuard PrivateDisk in Utimaco's SafeGuard family.

3 Appendix 1: Limitations of "simple" standard tool solutions

This section goes beyond what has already been said above to describe the limitations of various other "standard tool solutions" when it comes to security:

BIOS password:

Setting a BIOS password provides no real protection for the data on a hard disk since:

- The data on the hard disk remain in plain text. You can get round the protection simply by taking the hard disk out of the computer and installing it in a different one.
- Removing the battery from the computer resets the BIOS to its original state (without a password).
- Central mechanisms for password administration such as password rules or help if users forget their password are not available.

Hard disk password:

Setting a hard disk password offers only limited protection for the data on the hard disk and a hard disk password can only be used in limited circumstances since:

- The data on the hard disk remain in plain text. Taking apart the hard disk or resetting the password, both services provided by data recovery companies, for example, gets round the protection.
- Not all hard disk and BIOS types support this procedure.
- There are no central mechanisms available for password administration such as password rules or help if users forget their password.

Trusted Platform Module (TPM):

Some modern computers have a built-in security chip (TPM). This chip is something like a fixed built-in smartcard. It is used to perform certain cryptographic operations for key management, for applications.
However, it needs special applications to do so: it is these applications that use the services provided by the TPM. Just because the chip is present in a computer does not in any way give you extra security!
SafeGuard® Easy already uses the TPM chip today for certain operations in its key management system to optimize security on these modern platforms. SafeGuard® Easy and TPM are mutually-complementary technologies.

Windows Vista BitLocker Drive Encryption (BDE):

For comparing SafeGuard products with Vista BitLocker Drive Encryption Utimaco provides a dedicated white-paper. In general BitLocker has certain restrictions that make it less interesting for enterprise use e.g. missing removable media encryption, token authentication or challenge/response recovery. Future SafeGuard solutions will integrate BitLocker as one option in it's security management and extend it to an enterprise ready comprehensive solution.

4 Contact information

For further information please contact your local Utimaco Partner or visit our website.

Utimaco Safeware AG
Hohemarkstraße 22
DE-61440 Oberursel
Germany
Phone: +49 (61 71) 88-0
Fax: +49 (61 71) 88-10 10
Info@utimaco.com
www.utimaco.com