

Easy and transparent hard disk encryption for notebooks and PCs

The ultimate PC security solution – whether in the office or on the move

Data is one of the most valuable assets that companies and organizations own today. These assets are increasingly vulnerable as mobile computing becomes ever more widespread: Sensitive information is often stored on notebooks and removable media without any firewall protection.

Mobile devices and media—along with the sensitive and valuable information that is stored on them—are especially at risk of loss or theft. A company's management team is responsible for taking all the appropriate steps to protect the organization's data.

SafeGuard Easy provides this protection: No unauthorized user may access the device and read data, or use the device as a tool to enter the company network. If a device gets into unauthorized hands, the data is protected even if the hard disk is removed. The entire hard disk is completely encrypted and a user authentication procedure runs before the operating system boots, providing secure protection.

SafeGuard Easy is truly user-proof. It operates transparently in the background, so end users don't have to undergo training or alter their work behaviors. For security officers, IT managers and system administrators, SafeGuard Easy offers transparent security, easy security policy implementation and simple deployment.

Whether a single laptop or 10,000 PCs need protection, SafeGuard Easy allows easy implementation and enforcement of the IT security policy. In a world where laptops and desktop PCs are lost every day and hackers attack corporate secrets every hour, SafeGuard Easy is a business necessity.

Key benefits**Enhanced security**

- » Perfect protection of PCs and notebooks against unauthorized access
- » Perfect protection of data on hard disks and removable media against unauthorized access
- » No additional costs for erasing data or destroying hard disks in case of sale, disposal or return of leased devices as data is securely encrypted
- » Smooth integration into the existing IT security environment (e.g., fingerprint, TPM chip)
- » Secure protection in each power mode including hibernation and stand-by
- » Certified according to Common Criteria EAL3 and FIPS 140-2

Easy to deploy

- » Easy rollout via network without end-user involvement
- » Easy administration from a central console
- » Reduced help-desk workload through simple reset of forgotten passwords
- » Interoperable with Lenovo's TVT Rescue and Recovery as well as CSS and Computrace

Easy to use

- » Fully automated encryption in the background—no change in working behavior, no user training
- » Proven security solution—more than 4 million laptops and PCs worldwide are protected by SafeGuard Easy

Security

- Pre-boot authentication using password, fingerprint or Token; optionally applicable on up to eight OS partitions:
 - Organization-specific password rules
 - Optional Token or fingerprint authentication
- Comprehensive encryption capabilities:
 - Full or partial hard disk encryption, independent of file system (e.g., NTFS, FAT)
 - External media encryption (e.g., diskettes, Zip and Jaz disks, USB memory sticks)
- Sophisticated and efficient encryption algorithms:
 - AES (256 and 128 bit), IDEA (128 bit) and others
- Secure key management: enciphering key dynamically generated from the password entered—not stored on disk
- Secure hibernation:
 - Encryption of Suspend to Disk mode (hibernation image)
 - Authentication after resume
- Use of TPM chip for encryption key generation and authentication procedure (e.g., IBM ESS support)
- Integrated Boot Manager to support multiple operating systems and/or secured/unsecured partitions on the same device

System administration

- Windows Installer (MSI)-based installation
- Optional central administration console:
 - Queuing and distribution of configuration files to clients
 - Central collection of client settings
- Remote management console for remote client management
- Scripting interface for automating administrative tasks
- Pre-boot event logging
- Secure Wake-On-LAN mode

Easy to use

- Single sign-on to the operating system
- Automated encryption without user intervention
- Efficient algorithms—negligible performance impact
- Secure and powerful challenge/response procedure to reset forgotten passwords without the need for an online connection

Interoperability

- Certified compatible with Lenovo Rescue and Recovery (RnR)—allows RnR to back up and restore data to SGE-encrypted hard disks (even a complete restore of the operating system)
- Compatible with Computrace from Absolute Software to locate stolen notebooks (one of Lenovo's TVTs, new CT version required)
- Compatible with all leading software distribution tools (e.g., LANDesk)
- RSA SID800, Aladdin eToken PRO (32KB, 64KB or NG-OTP) or VeriSign USB token for pre-boot authentication
- Integration of other smartcards via PKCS #11 (additional SafeGuard Advanced Security module required)
- Pre-boot fingerprint authentication on Lenovo PCs and notebooks (5x, 6x Series and external reader)

System Requirements

Hardware

- » PC with Intel Pentium or similar
- » Minimum 25MB free hard disk space
- » RSA SID800
- » Aladdin eToken PRO, Aladdin eToken NG-FLASH and NG-OTP (all with CardOS)

Operating system

- » Microsoft Windows XP/2000 (latest Service Packs)
- » Microsoft Windows 2003 Server Standard Edition
- » Microsoft SQL Server 2000 (SP3) or 2005 for central administration (optional)

Network

- » All Microsoft-supported networks

Certifications

- » Common Criteria EAL3
- » FIPS 140-2
- » NATO restricted
- » Aladdin eToken enabled
- » RSA secured
- » EnCase compatible

Interfaces

- » Scripting API to automate repetitive administration tasks

Standards/ Protocols

- » PKCS #11, AES (256 and 128 bit), Rijndael (256 bit), IDEA (128 bit),
- » DES (56 bit), 3DES (168 bit), Blowfish-8/16 (256 bit), Stealth-40 (40 bit)

Language Versions

- » English, German, French

For full details, visit www.sophos.com