

How to protect data against theft and ensure that it remains confidential – no matter where it is stored

Stored information is one of a company's most important assets. As more confidential and valuable data is carried around by staff members, it is more important than ever to protect sensitive enterprise data. The tried-and-trusted protection provided by a company's central firewall is no use for mobile clients.

Mobile clients (e.g., laptops, netbooks, PDAs) and removable media (e.g., USB memory sticks) are particularly vulnerable to loss or theft, which makes them a weak spot in modern IT infrastructure. Companies need a security solution that can not only protect them against this threat, but also ensure that no unauthorized persons can access their saved data or the rest of their IT infrastructure.

This white paper introduces SafeGuard Enterprise 5.40, an innovative solution from Sophos that fulfills all the requirements a company could have for protecting confidential data on mobile PCs and data media.

How to protect data against theft and ensure that it remains confidential – no matter where it is stored

SafeGuard Enterprise enables seamless integration in the existing IT environment

SafeGuard Enterprise (SGN) protects data against theft or loss, and ensures that it remains confidential, no matter where it is stored.

SGN's underlying architecture was developed with the aim of enabling seamless integration in the existing IT environment, while ensuring that neither the security administrator nor the users of the security solution are restricted in their daily work.

With the central administration and reporting functions in SGN, the administrator can implement the security guidelines on all devices at any time, from one central console, and then audit the protected environment. Because of SGN's transparent operation, the end user is not restricted by the additional security provided by SGN and needs no special training.

SafeGuard Enterprise's combination of transparent data medium and file encryption (Smart Media Encryption), together with its keyring management, achieves levels of flexibility in protecting data media

and the information saved on them that until now could not be obtained in the market.

The portfolio of SGN's authentication methods for users is constantly being extended, permitting the integration and use of existing smartcard and PKI structures, or providing an easy way for a company to change over to them if required in the future.

SafeGuard Enterprise is the result of Sophos's many years of experience in the IT security industry. The product was developed in accordance with current standards and has a modular structure. These factors ensure it has the highest level of interoperability and flexibility for any future upgrades.

All of SafeGuard Enterprise's functions are designed for use in professional business environments and can be managed from a central console. SafeGuard Enterprise does not require any new user accounts or devices to be set up. It uses the information present in Active Directory instead. The Management Center is designed for multi-platform tasks, allowing both PCs and other mobile devices to be managed simultaneously from one console.

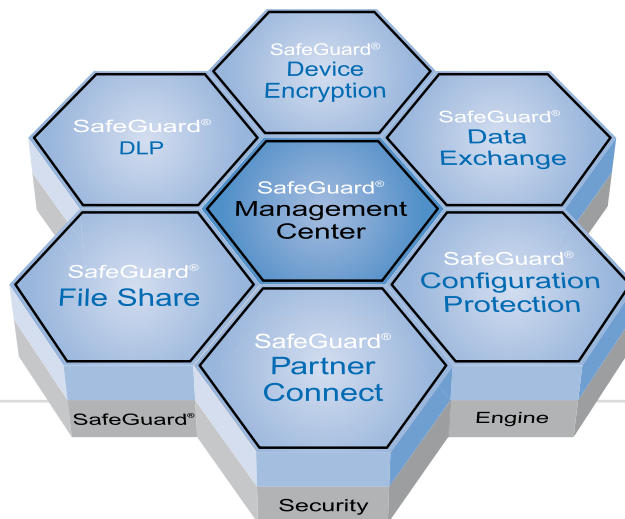


Figure 1:
SafeGuard
Enterprise
Overview

SafeGuard Management Center

The Management Center is the central controlling module in SafeGuard Enterprise. Its primary tasks include:

- » In a centralized manner, creating and administering security guidelines (security policies) in modular, inheritable units
 - The SafeGuard Management Center efficiently creates policies even in large-scale environments.
- » Distributing policies to all SafeGuard Enterprise clients via direct, secure Web Service Communication (SOAP)
 - The SafeGuard Management Center ensures that central policies are implemented quickly on the clients.
- » Re-using existing infrastructure data by optionally importing it from Active Directory
 - The SafeGuard Management Center does not require any additional new user or machine administration; instead, it uses existing information. As an alternative to Active Directory import, auto registration may be used. This option does not require any directory system to be in place. Furthermore, the SGN Management API provides a second alternative for machine/user import and allows SGN to be linked to any provisioning or directory system (e.g., Novell eDirectory) via customized scripts.
- » Logging and reporting status and licensing information in a centralized manner
 - The SafeGuard Management Center provides information about network procedures that impact security issues and facilitates the provision of proof to government bodies that end devices have been encrypted (e.g., regulatory compliance in the United States).
- » Administering certificates and smartcards
 - The SafeGuard Management Center uses existing PKI infrastructures if they are present, but this is not a requirement.
- » Providing the option of role-based administration (e.g., Security Officer and Audit Officer)
 - The SafeGuard Management Center provides a simple method of achieving a division of power between the network administrator and the security administrator for encryption or other administrative roles.
- » Monitoring the health status of SafeGuard Enterprise Management Servers via an optional Management Pack for Microsoft System Center Operations Manager (SCOM) 2007
 - In large IT infrastructures that are monitored with SCOM 2007, this monitoring can be extended to SafeGuard Enterprise. For details, see the separate white paper on this module.

SafeGuard Device Encryption

The SafeGuard Device Encryption (SG DE) module and the Management Center are the main modules available in SafeGuard Enterprise. The Device Encryption module protects end devices (e.g., PCs, notebooks, netbooks and PDAs) and any other type of exchangeable memory media. This module is the successor to SafeGuard Easy.

Its primary tasks include:

- » Encrypting any data saved on local or external data media
 - SafeGuard Device Encryption protects data if the device or data medium is lost or stolen. Because it runs transparently, users can simply continue working with their usual applications such as Microsoft Office. The SafeGuard software automatically ensures that all the saved data is secure.
- » Providing transparent sector-based encryption (volume-based encryption)
 - SafeGuard Device Encryption ensures that all data is encrypted (including boot files, swapfiles, hibernation files, temporary files,

- etc.) without requiring users to adapt their working habits or even worry about security. This method is typically used to share encrypted media exclusively within the company.
- » Providing transparent file-based encryption (Smart Media Encryption, which is covered by the SafeGuard Data Exchange module described below)
 - SafeGuard Device Encryption ensures that all data is encrypted (apart from the boot medium and directory information) with the advantage that optical media such as CDs/DVDs can also be encrypted, and that data can be exchanged with external computers where SafeGuard is not installed (if the policy allows this to happen).
 - » Providing flexible keying management
 - SafeGuard Device Encryption allows encrypted removable data media to be exchanged quickly and easily within specific user groups. It also facilitates recovery procedures in an emergency (e.g., a hard disk that will no longer boot can be inserted in a different computer on which the appropriate key is present).
 - » Delivering the latest graphical 32-bit pre-boot authentication (Power On Authentication [POA]) before the actual operating system starts up, and supporting biometric fingerprint authentication with single sign-on to Windows before booting
 - SafeGuard Device Encryption reliably prevents the operating system from being manipulated from outside and also protects against the use of password hacking tools. SafeGuard Enterprise POA provides an adaptable graphical user interface with full Unicode support for Asian languages and support for an extensive range of authentication hardware (e.g., smartcards, tokens, fingerprint). SafeGuard Enterprise also uses Windows accounts and passwords in its POA. This removes the need for separate user management for POA, which many competitor products still require.

- » Integrating Windows Vista BitLocker Drive Encryption (BDE)
 - SafeGuard Device Encryption provides central management of BitLocker clients within the SGN Management Center, together with native SGN clients. It extends BitLocker using file-based transparent encryption for removable media.

SafeGuard Data Exchange

The SafeGuard Data Exchange (SG DX) module transparently encrypts all kinds of removable media, and allows access to these media via password even on computers where no SafeGuard software is installed. All its functions and keys are centrally managed by the SafeGuard Enterprise Management Center .

When the SafeGuard Data Exchange module is used in combination with SafeGuard Device Encryption, it adds important functions to the removable media encryption capabilities:

1. Encrypted media can be used outside the organization. Users can optionally define their own keys or passwords for removable media, or the files stored on those media, and then exchange these keys or passwords with their business partners. These keys are then also stored on the central SafeGuard server for backup purposes, or can be assigned to other users by the administrator for recovery or sharing purposes.
2. By policy, a mix of plain-text and encrypted files on the same media may be allowed.
3. Optical media such as CDs/DVDs and Blu-ray discs may be encrypted with the DX module.
4. The Portable component of the SafeGuard Data Exchange module can also be stored on the data medium. This allows encrypted removable media to be used on computers where SafeGuard Enterprise is not installed. The keys generated with SafeGuard Portable can also be imported into a user's keyring so they can be used in SafeGuard Enterprise.

Consistent, strong password rules and failed logon delays are also implemented for the portable functionality.

Optionally, the SafeGuard Data Exchange module can be deployed in standalone mode without requiring the SafeGuard Management Center. Using SafeGuard Data Exchange as a standalone solution is particularly suitable for customers who want to implement removable media encryption (SG DX) across the board, but only want to install hard disk encryption (SG DE and SG DX) on specific clients (e.g., all notebooks).

SafeGuard Configuration Protection

SafeGuard Configuration Protection (SG CP) prevents the PC from receiving potentially malicious code and provides data leak prevention by restricting unauthorized export of confidential data via certain communication ports or peripheral devices. All its functions are centrally managed by the SafeGuard Enterprise Management Center.

Besides read/write restrictions on ports such as USB, FireWire, WLAN or Bluetooth, just to name a few, the administrator can also configure policies based on device types, file types or even individual peripheral devices. For the latter, there is an easy-to-use tool provided (the SafeGuard Auditor) that scans the clients on the network and centrally reports all actually or formerly connected peripheral devices as whitelist input for the policy.

SafeGuard Enterprise Security Engine

The SafeGuard Enterprise Security Engine is the basis for every cryptographic operation. It has been developed to meet all current standards with the specific aim of achieving optimum flexibility and security. The SGN Security Engine ensures that:

- » Powerful encryption algorithms are present on all the supported platforms, including device drivers.
- » All the standards, algorithms and protocols relevant for this purpose are made available centrally.
- » Security certificates (e.g., FIPS) are applicable across these components.
- » New algorithms (e.g., customer-specific or country-specific algorithms) and crypto hardware (e.g., smartcards or tokens, Trusted Platform Modules) can be connected to SafeGuard Enterprise easily and effectively.

Boston, USA | Oxford, UK
© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any
form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM