

Transparent network file share encryption

Unique protection of confidential files against unauthorized insider or outsider access

Most data protection measures are designed to protect against threats from outside the organization, while most in-house risks are usually overlooked or ignored. However, the potential damage caused by the misuse of confidential company data is exactly the same no matter where the threat originates. In almost every organization, valuable information such as business reports, HR documentation, customer data and research results is saved electronically without being protected. The current practice of saving data centrally on servers, multi-site workplace networking, and the use of mobile data media greatly increases security risks. As more organizations outsource their IT departments in an effort to reduce costs, they are faced with increasing data confidentiality concerns as well.

What is needed is a security solution that only allows authorized user groups access to sensitive data across an organization. With security policies in place, even in-house system administrators or personnel from outsourcing companies can be restricted from accessing confidential data.

SafeGuard LAN Crypt uses fully-automated file encryption to provide effective protection for confidential files. SafeGuard LAN Crypt does not force users to change the way they work: The encryption process is transparent and runs invisibly in the background. This means that each user is assigned a unique "key group" based on his profile with which he can read - released files in plain text. Whereas, if those files were accessed by an unauthorized person, he would only see an enciphered, unreadable string of characters.

In SafeGuard LAN Crypt, the roles of Server Administrator and Security Officer are strictly separated, giving it a unique advantage in handling data security. The Server Administrator can still manage the system as usual, but has no means to decrypt any files. To ensure the separation of duties, the keys are managed by the Security Officer who defines the individual access rights for working groups or individual users in accordance with the company's security guidelines.

SafeGuard LAN Crypt provides comprehensive protection for all company data. It is scalable so it can be used in small temporary teams, in departments and project groups, or throughout the organization.

SafeGuard LAN Crypt – Intelligent file encryption.

Key benefits**Enhanced security**

- » Transparent data security for user groups and individual users
- » Encryption on all standard media and in heterogeneous environments
- » Separation of duties between server and security administration
- » Simple implementation of a company-wide security policy
- » Flexible definition of encryption rules for user groups
- » Easy PKI integration and support for certificates, smartcards and USB tokens

Easy to deploy

- » Seamless integration into heterogeneous IT infrastructures
- » Easy, central administration using existing directories or domains
- » No need for additional upgrades to existing IT infrastructure
- » Scalable from individual user groups up to a company-wide rollout

Easy to use

- » Simple to use with integration in familiar working environments
- » Transparent to users, self-explanatory functionality, resulting in higher levels of user acceptance

Key Features/Functionality

Data security

- Comprehensive security solution for preventing unauthorized access to data
- Protects valuable company data and confidential personal information
- Strictly separates server and security administration responsibilities
- Excellent data protection if IT is outsourced because although outsourcing staff can manage the files, they cannot read them in plain text
- Implements tried and tested security algorithms
- User authentication by X.509 certificates
- Supports smart cards and USB tokens

Security administration

- Simple, central installation, configuration and administration through integration in existing IT environments and by using existing directory services or domains
- Uncomplicated integration with existing PKI systems
- Cost-effective and quickly implementable solution; does not need additional infrastructure
- Includes a recovery strategy so that encrypted data can also be accessed in an emergency situation
- Flexible and powerful administration API for integration into provisioning systems and to support business workflows

Ease of use

- Information saved securely by authorized users without any risk of unauthorized access by outsiders
- Persistent encryption
- No need for changes to users' familiar working environments and working habits
- High level of acceptance by users: no additional training required
- No reduction in file server performance: encryption and decryption are completed by an end-point client agent

Interoperability

- Compatible with SafeGuard Data Exchange 5.40 and higher
- Provides secure encrypted file access to authorized anti-malware services (e.g., Sophos)
- Supports Microsoft SQL Server and Oracle databases
- Supports Microsoft Active Directory and Novell eDirectory
- Integration into provisioning systems enabled by administration API
- Microsoft Crypto API integration: the use of Cryptographic Service Providers (CSPs) means that any RSA-enabled components from third-party suppliers (such as smartcards or USB tokens) can be implemented for user authentication
- Aladdin eToken certified

Further information

For more information about Sophos and our complete line of SafeGuard solutions, visit:
www.sophos.com.

System Requirements

Hardware

- » PC with an Intel Pentium processor or a compatible processor

Operating system (32-bit)

- » Windows XP Professional SP2/SP3
- » Windows Vista (Ultimate/Enterprise/Business) SP1/SP2
- » Windows 7 (Ultimate/Enterprise/Professional)
- » Windows Server 2003 R2 SP2 with Terminal Server services
- » Windows Server 2003 R2 SP2 with Citrix Presentation Server 4.5

Operating system (64-bit)

- » Windows 7 (Ultimate/Enterprise/Professional)
- » Windows Server 2008 R2 with Citrix XenApp 6

Supported file server operating systems

- » Microsoft Windows 2003, 2008
- » Novell Netware

Supported media

- » Network drives, local hard disks, CD, DVD, USB and flash memory drives

Standards/ Protocols

- » Authentication: user authentication via X.509v3 certificates
- » PKCS#12
- » LDAP for access to Microsoft Active Directory and Novell eDirectory
- » Encryption: 3DES 168-bit, IDEA 128-bit, AES 128-bit and 256-bit
- » Hash: MD5, SHA-256
- » Tokens: smart cards and USB tokens via Crypto API

Language Versions

- » English, German, French