

SpyProof!®

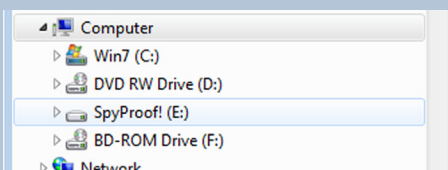
SpyProof! protects sensitive data-at-rest from internal and external threats.

Its intelligent use of virtual disk encryption technology protects important data with little impact on performance. SpyProof! is effective, inexpensive, and easy to manage.

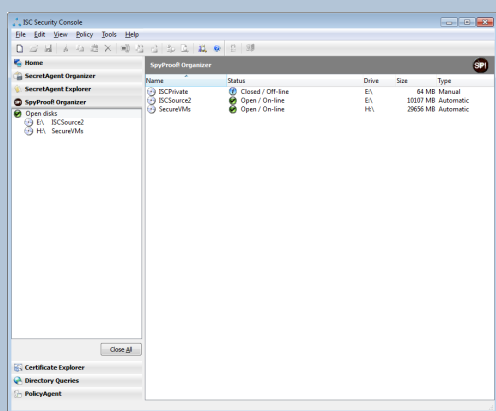
OVERVIEW

Concerned about the security of your sensitive data but find file encryption too time consuming? Imagine a virtual disk drive that automatically encrypts all data written to it and transparently decrypts that data for any application as long as the volume is mounted. Once unmounted, the encrypted disk is completely unreadable by unauthorized users and thieves. That's SpyProof!

SpyProof! enables users to create and manage encrypted virtual disks that provide transparent data encryption. Users must authenticate in order to 'mount' encrypted disks and make the contents accessible. To authorized users and applications SpyProof! disks appear as additional drives; unauthorized users see only random data.



A SpyProof! Volume Mounted as E:



SpyProof! Volume Management Console

DATA AT REST SECURITY

SpyProof! provides superior security for data at rest because

- unmounting a disk erases the disk's key from memory and secures it from cold boot and memory capture attacks
- all disks are automatically unmounted when the system is suspended
- each user can have their own encrypted partition so sharing a computer doesn't mean sharing sensitive data (however, shared SpyProof! disks can be created)
- users can create multiple disks for different classes of information and mount them as needed to decrease the window of data vulnerability

USE AND ADMINISTRATION

SpyProof! is easy for users to understand and simple for administrators to deploy. Users familiar with thumb, flash, network, and external drives intuitively save their files to SpyProof! disks.

SpyProof! automatically mounts specified disks on startup or when resuming from sleep and users can mount other disks on demand. Mounted disks are automatically unmounted when Windows shuts down, the user logs off, or the system enters a suspended state.

The user's system can be configured so that common folders are located on a SpyProof! disk. In such a scenario applications naturally save files to the encrypted virtual disk.

Administrators can pre-create disks for their users. This simplifies the end-user experience while providing administrative control of disk access. SpyProof! is easy to deploy, pre-configure, and requires little support.

ENDLESS POSSIBILITIES

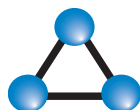
SpyProof! can

- protect laptop computers and physically insecure desktops and servers from security breaches due to loss or theft
- distribute sensitive company documents, movies, or music on a CD/DVD that only a limited number of employees or authorized customers can view
- easily create encrypted backups. Backup the encrypted SpyProof! data files even when the disks are mounted (live backup of in use disks)
- provide secure network storage for users. Users can store an entire SpyProof! disk on a network server and only they and their managers, not system administrators, can access the data
- enable data compartmentalization by giving users an administratively inaccessible storage pool

DAS INTEGRATION

ISC's Document Access Servlet (DAS) allows SpyProof! disks to be protected by 'community of interest' or organizational role certificates. These certificates allow anyone in the community, or those acting in a particular role, to mount the disk. Administrators can easily modify membership and duty rosters without requiring disks to be re-keyed.

Sensitive documents, movies, and music may be securely distributed by copying to a SpyProof! partition and burning to a CD or DVD. Only authorized principals will be able to mount such a disc and access its contents. With DAS, authorized recipients can even be specified after the data is encrypted and burned to disc thereby providing superior protection for data-in-transit.



Information Security
CORPORATION

+1 847 405-0500
sales@infosecorp.com
http://www.infosecorp.com

SpyProof!®

PERFORMANCE

All software-based encryption solutions require additional processing that impacts performance. When accessing data stored on a SpyProof! disk 10-20% of the computer's processor is used and there is a 1-2% decrease in read/write performance as data passes through the SpyProof! device driver. In practice,

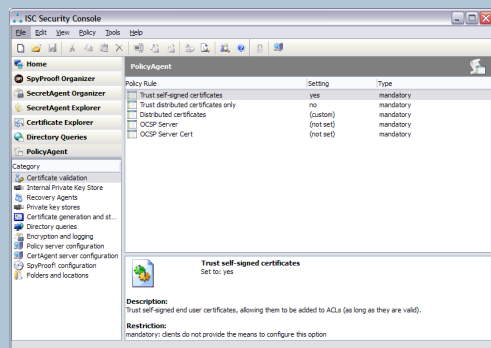
- users do not notice a performance change
- system boot and application load times are unchanged as these system components are not encrypted
- users processing large data sets notice an acceptable change in performance

SECRETAGENT INTEGRATION

SpyProof! includes SecretAgent Reader which provides for the decryption of files created by SecretAgent Enterprise users. When SpyProof! and SecretAgent are installed together, they appear in an integrated environment and share user and security policy settings.

CONFIGURATION POLICIES

PolicyAgent allows SpyProof! administrators to enforce compliance with the organization's security policy. Using a digitally signed security policy file, an administrator can control such factors as the key size used for encryption, data recovery certificates, password requirements, and other common security parameters.



DATA RECOVERY

Encrypting sensitive data is important, but access to organizational information must be ensured. SpyProof! supports optional data recovery allowing one or more designated administrators to mount all encrypted disks either locally or over a network connection. Data recovery can be made mandatory by specifying data recovery agents' certificates in the security policy file. The designated agents will be added to the ACL whenever a SpyProof! disk is created or its access control list is modified.

PKI Support

- **certifications and standards:** certified by DISA's JITC PKE Lab as interoperable with the U.S. Department of Defense PKI. Interoperable with the U.S. Intelligence Community PKI. Internal Path validation module passes the stringent NIST PKITS Certificate Path Validation Test and is "(Federal) Bridge-Enabled."
- **certificate authorities:** functions with any X.509 Certificate Authority. Additional functionality is available when used with ISC's CertAgent, Entrust's Authority, or Microsoft's CA
- **PKI tools:** includes private key, certificate, and CRL management components with integrated certificate and private key storage
- enforces standard IETF PKIX certificate extensions, including keyUsage, basic constraints, and policy constraints
- imports X.509 version 3 certificates from binary, PEM- or base64-encoded ASN.1 DER, PKCS#7 and PKCS#12 files
- generates self-signed RSA, DSA, and ECC certificates for use without a formal PKI
- **private keys:** utilizes Microsoft CAPI/CNG, PKCS #11, Entrust, or its own integrated key store (either on your PC, or on your Windows Mobile device) for private key operations

Technical Details

Suite B	SpyProof! fully supports NSA Suite B ECC algorithms
Bulk Encryption	128/192/256-bit AES-CBC (FIPS 197)
Key Exchange	RSA (up to 16384-bit keys; ANSI X9.31; IEEE 1363; RFC2313) Diffie-Hellman (up to 4096-bit keys; ANSI X9.42-1998; IEEE P1363) ECDH (163/233/ 283/409/571-bit NIST curves in char. 2, 192/224/256/384/521-bit NIST curves in char. p; FIPS 186-3; ANSI X9.42-1988; IEEE P1363)
PRNG	FIPS 186-2 Appendix 3.1; FIPS 140-2 Annex C; NIST SP800-90
Certificate Path Validation	Microsoft CAPI/CNG certification validation RFC5280-compliant internal path validation module
Hardware Support	Supported APIs: PKCS#11, Microsoft CAPI, Microsoft CNG Supported Tokens: DOD CAC, PIV, other smart cards, USB tokens, hardware security modules and biometric devices
Platform Availability	Windows 2000/XP/Vista/7/2003/2008 (32- or 64-bit)
File Systems	NTFS (default) and FAT-32

Standards and Regulatory Compliance

- utilizes ISC's CDK, a FIPS 140-2 compliant (#347) cryptographic module, for all cryptographic operations except for private key operations performed when used with smart cards or third-party private key stores
- satisfies NSTISSP 11, OMB, and GSA acquisition requirements for COTS security and information assurance products
- available through the DAR ESI BPA and GSA SmartBuy programs
- complies with Section 508 of the ADA
- meets HIPAA requirements for securing sensitive medical information

Export Information

SpyProof! may be freely exported to all but a handful of embargoed countries and denied parties under License Exception ENC: ECCN 5D002; CCATS: G025241.