

DiskCrypt

Secure • Performance • Cost Effective

DiskCrypt -- Hardware-based Disk Encryption Device

Did you or your corporate suffer from losing sensitive confidential data residing on the hard drive? Do you worry about the consequences of sensitive personal and corporate data falling into the wrong hands? Didn't think you will be the next victim? Think AGAIN!

Consider the following statistics

A typical medium-sized company loses 11 notebooks annually, with an average financial loss of US\$64,000 per notebook.*

*Kensington Technology Group Notebook Security Survey 2001 and 2003 CSI/FBI Computer Crime & Security Survey.

57% of computer crimes are linked to stolen notebooks that were then used to break into corporate computer servers.*

*SC Magazine, May 1999.



DiskCrypt is engineered specifically for those executives who carry important and sensitive corporate data with only limited protection from using the traditional software disk security solutions.



Unlike software solutions from Microsoft EFS, PGP, Pointsec, or Winmagic, we have assembled full security features into one compact 2.5" form factor device that is an ideal replacement of your existing 2.5" notebook disk drive without any hardware and/or software modifications.

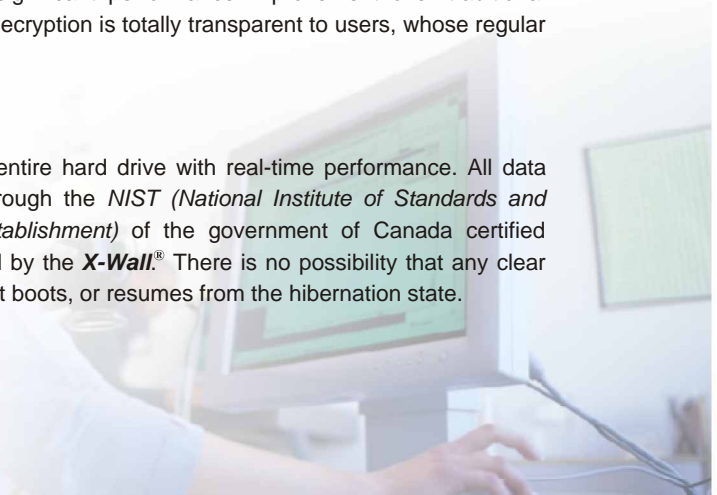
DiskCrypt is a hardware-based disk encryption device that provides cross platform compatibility and significant performance improvement over traditional disk encryption software solutions. It consists of an 1.8" form factor hard disk made by Toshiba and an **X-Wall**[®] real-time encryption module that encrypts every byte and sector of data written into the hard disk, including Master Boot Record (MBR), Operating System, Temp and Swap files. The DiskCrypt is engineered just like an ordinary 2.5" form factor hard disk that can be mounted perfectly to the notebook hard disk compartment.

Significant Performance Improvement

DiskCrypt eliminates platform dependency completely and offers significant performance improvement over traditional software disk encryption solutions. The operation of encryption and decryption is totally transparent to users, whose regular computing behavior remains unchanged.

Military Grade Data Security

DiskCrypt is a hardware-based cryptographic device that encrypts entire hard drive with real-time performance. All data residing on the disk drive (Data-at-Rest) are safeguarded 24/7 through the *NIST (National Institute of Standards and Technology)* of the USA and *CSE (Communications Security Establishment)* of the government of Canada certified industrial strength TDES (Triple DES) cryptographic engine provided by the **X-Wall**[®]. There is no possibility that any clear text be left unencrypted. DiskCrypt authenticates the user every time it boots, or resumes from the hibernation state.



Look at what Gartner says about hardware security

“Hardware is also not invulnerable to attack, but it generally requires much more sophisticated attackers with larger budgets than those that typically succeed against software-only security options. When information is sensitive, valuable or 'must be trusted not to change', hardware has to be part of the solution.”

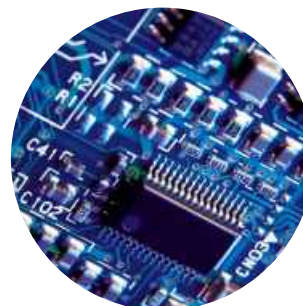
© Gartner Research Note COM-16-5309, 10 June 2002 : “ Software Security is Soft Security: Hardware is required.”

Reduces Total Cost of Ownership

Your Total Cost of Ownership is minimized as no software upgrades and patches are ever required to maintain the DiskCrypt's functionalities. Beside, there is no change whatsoever to your existing IT security infrastructure, which dramatically reduces your IT management overheads. Users of the new DiskCrypt require no training, as installing DiskCrypt is as simple as replacing a 2.5" hard disk.

Free to Dispose

When it's time to dispose a used computer, what would you normally do? Rewrite hard drive multiple times? Smash the hard drive with a hammer? Shred it or simply burn it? With **X-Wall**® real-time encryption technology, you simply pull the KEY, be it a physical key token or a Password. As every bit and byte residing in the hard drive is strongly encrypted, there is no chance that your proprietary information will be exposed.



One or Two Factor Authentications

DiskCrypt offers either one factor or two factors authentication. For those who are satisfied with Pre - Boot authentication with Password control, one factor authentication using PIN/Password may well serve the purpose. When the new DiskCrypt is installed, a power on process will bring you the pre - boot authentication screen from where you get to set your new password and the recovery password. The recovery password setup allows you to recover your disk drive just in case you have forgotten about your password. Two factors authentication, however, involves with using KeyCrypt, an external USB type smartcard token, in addition to the pre - boot authentication password. One must present the KeyCrypt and the password in order to access your disk drive. KeyCrypt is essentially a USB compatible Smartcard device that allows the same flexibility you would have had experienced with the regular Smartcard key management system. You can also set the "recovery password" under two factors authentication for the event that both password and/or KeyCrypt are lost.

Upon successful authentication, the notebook loads the operating system and the user is able to use the notebook as usual. DiskCrypt automatically decrypts and encrypts all the data that is accessed or saved using strong industry standard TDES encryption algorithm, supporting key lengths ranging from 128 bits to 192 bits.

Migration Toolkit - Optional

The DiskCrypt Migration Toolkit enables users to migrate seamlessly from the original hard disk to using DiskCrypt. Simply follow the instructions on the package and you are ready to use your notebook exactly the same way as before. No other modification of the notebook computer is necessary.

Data Recovery Toolkit - Optional

While losing sensitive data may pose great risks, not being able to continue working will result in frustration. The DiskCrypt Data Recovery Toolkit makes periodic and incremental snapshots of the hard disk onto another external drive that the user can store securely. This ensures business continuity and a real peace of mind even in the unfortunate event of a notebook being lost or stolen.



SPECIFICATIONS

Storage Capacity & Speed

- 20 GB
- 66, 100 or 133MB/sec Ultra DMA Transfer Rate

Operating Systems

- Operating system independent
- Tested with: Windows 98, 2000, XP, and Linux

Interface & Mechanical

- Standard 2.5" HDD. Complies to SFF-8200, SFF - 8201, SFF - 8212
- Size: 100(L)x70(W)x9.5m

Encryption Algorithm

- NIST & CSE certified TDES 128 or 192-bit key strength

Authentication Mechanisms

- One factor Pre - boot authentication
- Two factors authentication using both Password and KeyCrypt® USB smartcard cryptographic token

Certifications and Standards

- Designed to meet FIPS140 - 2 Level 2
- CE, FCC

NOTE: Specifications subject to changes without notice.



Enova Technology Corp.

Building 53, #195-57, Sec. 4, Chung Hsing Road, Chutung District, Hsin-Chu County, Taiwan 310, Republic of China

©TEL: +886 (3) 591-0197

©FAX: +886 (3) 591-0204

www.enovatech.net