Full Drive Encryption's Total Cost of Ownership

Companies implement full drive encryption to comply with privacy regulations or to protect their secrets and reputation. While careful consideration goes into choosing the right encryption technology, its total cost of ownership is often underestimated. A study by Ponemon Institute noted that the cost of the software license and maintenance contract is only a "small fraction" of its total cost.

Downtime and productivity costs that occur when an encrypted drive fails or becomes corrupted are often unaccounted for as they were relatively small before full drive encryption was implemented.

With full drive encryption, employees now experience days of downtime when a drive fails. For recovery, IT must not only restore the image, apply updates, restore data, and re-encrypt the drive but also ensure that all data is safe-guarded throughout the process.

If the employee is on site, the average downtime is two days; if he is off-site, it can take longer. As a result, the employee cannot work: co-workers must wait, revenue opportunities get missed, and client meetings are unproductive. One study estimated it costs a company $1,750 for each day of downtime when a drive fails.

Casper Secure™ Drive Backup is the only backup and recovery solution specifically designed to reduce the TCO of drive encryption technologies such as Symantec (PGP®) and Windows® BitLocker® Drive Encryption.

By creating a complete image of an encrypted drive in its original encrypted state, **Casper Secure** provides secure, end-to-end backup and recovery without ever placing data in an unprotected state. This allows the end user to have immediate, encrypted recovery without the need for IT support.

Most importantly, this means that a company can eliminate unproductive downtime caused by encrypted drive failures.

The ONLY Backup and Recovery Solution Designed for Full Drive Encryption

Including **Casper Secure Drive Backup** as part of your enterprise's backup and recovery tool set offers these unique advantages for endpoint encryption:

- Eliminates the downtime and productivity costs associated with full drive encryption
- Provides complete, encrypted recovery within minutes
- Eliminates security gaps at backup and recovery
- Maintains 100% compliance with security directives.

He needs Casper Secure

Backup and recovery systems in place prior to implementing full disk encryption are often inadequate. Here is one example of the impact a drive problem can have on an organization. It is an automatically generated reply we received from an IT contact at a prospective healthcare company.

> *"I am dealing with a non-functional laptop and currently awaiting a replacement device. During this time, I will have limited access to email and applications. In the meantime, please continue to copy me on all correspondence but also copy both Jennifer and William (below). I should be fully operational late afternoon tomorrow (Tuesday) or Wednesday morning at the latest."*

Future Systems™ SOLUTIONS

Casper Secure™ Drive Backup

The **Only** Backup and Recovery Solution for Encrypted Drives

Casper Secure™ Drive Backup

Key Advantages of Casper Secure Drive Backup

- **Only Backup and Recovery Solution Designed Specifically for Symantec (PGP®) and Windows® BitLocker® Drive Encryption technologies** — completely eliminates the unnecessary downtime and security and compliance risks associated with other backup and recovery products.
- **Safe, Secure, Fully Encrypted Backups and Recovery** — ensures all of data remains in its original encrypted state during and after endpoint backup and recovery. *With Casper Secure Drive Backup, data is never placed in an exposed or unencrypted state.*
- **Complete System Backup Protection** — maintains a complete, instantly bootable backup replacement or image file backup for an encrypted Windows system drive. Users have peace of mind knowing that they are prepared for any data disaster whether a drive has failed or files have become corrupted.
- **Rapid Recovery** — eliminates the arduous data restoration and lengthy re-encryption steps required by other drive imaging and backup solutions. A bootable backup created by Casper Secure Drive Backup can be used as an immediate and permanent replacement for the failed hard drive or restored to a new drive in a single step.
- **Effortless Restoration** — provides easy, one-step support that enables end-users to restore a failed Windows system drive from a backup. Casper Secure Drive Backup automatically locates available backups, the user chooses which backup to restore, and Casper Secure does the rest. Casper Secure will even seek out backups from multiple locations.
- **Ensures 100% Compliance with Existing Security Directives** — since all data is backed up in its original encrypted state, there are no new passwords to manage, and more importantly there are no new security protocols or encryption technologies to vet. With Casper Secure, the backup is guaranteed to be as secure as the original.
- **Reduces Total Cost of Ownership for Full Drive Encryption** — users can quickly recover on their own without IT support, saving days of downtime and eliminating the loss of productivity associated with drive failures and corruptions.

SYSTEM REQUIREMENTS

- Supports Windows® BitLocker® Drive Encryption, Symantec Endpoint Encryption (SEE), Symantec Encryption Desktop (SED) version 10.x, or PGP® Desktop version 9.6x or later on all 32-bit and 64-bit editions of Windows 10, Windows 8, Windows 7, Windows Vista®, and Windows XP (SP3)†
- 500MB available hard disk space
- 512MB RAM (1GB or more recommended)
- Backup device (additional internal or external hard disk drive) for bootable backups. Image file backups can be stored virtually anywhere, including on drives containing other files or remotely on a network attached storage device.

For More Information:

Future Systems Solutions, Inc.
8888 Keystone Crossing, Suite 1300
Indianapolis, IN 46240
Email: enterprisesales@fssdev.com
Phone: 1-855-5-CASPER

† Windows BitLocker Drive Encryption is currently supported only for drives using software encryption formatted with the NTFS file system. BitLocker hardware encrypted drives and BitLocker encrypted drives that are formatted with the FAT file system can be copied only in their unencrypted state. Encrypted cloning and imaging is currently supported only for drives encrypted with software-based drive encryption. Self-encrypting drives (SED), including Opal compliant and Windows BitLocker eDrive compliant drives, may be copied in their encrypted state only when software encrypted.