



Casper Secure™ Drive Backup 3.0 **for PGP® Whole Disk Encryption**

- Reviewer's Guide -

Future Systems Solutions, Inc.
8888 Keystone Crossing, Suite 1300
Indianapolis, IN 46240
Phone: 800.272.5457
Fax: 317.579.3001



TABLE OF CONTENTS

THE PROBLEM

THE PROBLEM WITH WHOLE DISK ENCRYPTION	3
COMPARISON OF EXISTING BACKUP STRATEGIES FOR USERS OF WHOLE DISK ENCRYPTION.....	4

THE SOLUTION

THE SOLUTION - CASPER SECURE DRIVE BACKUP FOR PGP WHOLE DISK ENCRYPTION	5
HOW DOES CASPER SECURE ADDRESS THE PROBLEM OF MAINTAINING A BACKUP OF A WHOLE DISK ENCRYPTED DRIVE?	6
HOW DOES CASPER SECURE ADDRESS THE PROBLEM OF REPLACING A FAILING WHOLE DISK ENCRYPTED DRIVE?	6
HOW DOES CASPER SECURE ADDRESS THE PROBLEM OF UPGRADING A WHOLE DISK ENCRYPTED DRIVE?	6
WHO NEEDS CASPER SECURE DRIVE BACKUP?	7
WHAT ARE THE MOST IMPORTANT ISSUES FOR USERS OF BACKUP PROGRAMS?	7
HOW DOES CASPER ADDRESS THE EASE-OF-USE ISSUE?	7
HOW DOES CASPER ADDRESS THE CONVENIENCE ISSUE?	7
HOW DOES CASPER ADDRESS THE DEPENDABILITY ISSUE?	8
HOW DOES CASPER ADDRESS THE SPEED ISSUE?	8
HOW DOES CASPER ADDRESS THE SUPPORT ISSUE?	8
WHAT MAKES CASPER SECURE DRIVE BACKUP SO SPECIAL?	9
WHAT BENEFITS DOES CASPER SECURE DRIVE BACKUP FOR PGP WHOLE DISK ENCRYPTION PROVIDE?	10
ABOUT FUTURE SYSTEMS SOLUTIONS, INC.....	12
CONTACT INFORMATION.....	13

The Problem with Whole Disk Encryption

Due to increased awareness of identity theft and the need to protect the confidentiality of information, users in greater numbers have resorted to various data encryption technologies to secure their data, including file, virtual disk, and whole disk encryption technologies. While users of file based and virtual disk encryption technologies are able to rely on standard backup solutions to quickly and securely backup and restore their encrypted data, whole disk encryption technologies present new challenges.

More specifically, users of whole disk encryption technologies such as PGP® Whole Disk Encryption are confronted with several seemingly simple, but major problems:

- 1) How do I quickly and securely maintain a complete backup of my whole disk encrypted system without the backup leaving my sensitive data in an exposed, unprotected state?
- 2) How do I replace a failing whole disk encrypted drive with a new one without wasting an entire day performing a laborious and time-consuming restore and re-encryption process?
- 3) How do I upgrade my whole disk encrypted system drive to a larger capacity model without resorting to a laborious and time consuming backup, restore, and re-encryption process?

These problems are best illustrated by looking at the existing backup options available to users of whole disk encryption products. Existing backup products fall into two basic categories: those that operate within Windows and those that operate external to Windows. Both have negative consequences for users of whole disk encryption technologies:

- Backup products operating within Windows create an unencrypted backup of the whole disk encrypted drive. This not only leaves the user's data unprotected, a compliance and confidentiality nightmare, but also necessitates a time consuming re-encryption of the entire disk when the backup is subsequently restored.

For example: Restoration of 100GB of unencrypted data to a 500GB drive is relatively fast, requiring approximately 1 to 3 hours, but re-encrypting the drive requires an additional 5 to 15 hours depending on the speed of the disks and CPU.

- Backup products operating external to Windows perform blind, sector-by-sector backups that copy the entire physical disk – whether data exists or not. While the user's data remains fully protected, this process has several major drawbacks, which make it impractical:
 - No compression is available for the backup; therefore, storage requirements for the backup must be equal to the full capacity of the encrypted drive – whether meaningful data exists or not.
 - Incremental and differential backups are not supported.
 - The backup must be restored to a drive equal to or larger than the original drive.
 - The backup cannot be used to upgrade the available capacity of a drive. If the backup is restored to a disk larger than the original, the result is a copy that is the same size as the original – i.e., the additional space remains unpartitioned.
 - Data restoration is unnecessarily time-consuming.

For example: If a user has a 500GB drive containing only 100GB of data, the entire 500GB must be copied to a backup store, requiring at least 500GB of space and 5 or more hours, depending on the speed of the disks. Likewise, restoring the backup would require an equal amount of time, and if the backup is restored to a 1TB hard disk, the result would be a 500GB copy with the additional 500GB left unused (unpartitioned).

The Problems with Existing Backup Programs for Users of Whole Disk Encryption

Strategy	Disk Space Required for Backup	Time Required for Full Backup	Time Required for Restore	Key Weaknesses
Backup within Windows	Less than or equal to the amount of actual data existing on drive (e.g., less than or equal to 100GB for a 500GB drive containing only 100GB of actual data)	Approximately 1-3 hours per 100GB of data depending on speed of disk(s) (e.g., approximately 1 to 3 hours to backup a 500GB drive with 100GB of actual data)	Approximately 1-3 hours per 100GB of data restored <u>plus</u> 1-3 hours per 100GB of space on restored drive for re-encryption (e.g., approximately 6 to 18 hours to restore and re-encrypt a 500GB drive with 100GB of actual data)	<ul style="list-style-type: none"> ▪ Backup persists data in unencrypted state ▪ Restoration requires a time-consuming re-encryption process after backup is restored.
Backup external to Windows	Equal to full capacity of drive, including any unused space (e.g., at least 500GB for a drive with a 500GB capacity even if only 100GB of actual data exists)	Approximately 1-3 hours per 100GB of disk space depending on speed of disk(s) (e.g., approximately 5 to 15 hours to backup a 500GB drive with 100GB of actual data)	Approximately 1-3 hours per 100GB of disk space depending on speed of disk(s) (e.g., approximately 5 to 15 hours to restore a 500GB drive with 100GB of actual data)	<ul style="list-style-type: none"> ▪ No compression; backup storage requirement must be equal to full capacity of encrypted drive. ▪ No incremental or differential backups. ▪ Restoration must be to drive equal to or larger than original drive. ▪ Upgrading to larger hard disk not possible; additional space not utilized if restored to larger drive. ▪ Unnecessarily time-consuming

The Solution: Casper Secure Drive Backup for PGP Whole Disk Encryption

Casper Secure Drive Backup for PGP Whole Disk Encryption (WDE) is the first and only PC backup solution to confront the problems affecting users of whole disk encryption technology by creating a fully bootable, completely encrypted backup of a whole-disk-encrypted Windows system drive.

As a backup and recovery solution, Casper Secure Drive Backup offers these unique advantages:

- Fast, Completely Encrypted System Backups.** Unlike traditional backup and disk imaging solutions that can produce only an unencrypted backup of a PGP whole disk encrypted PC, Casper Secure Drive Backup creates a backup that persists all of the encrypted data in its original encrypted state. *With Casper Secure Drive Backup, sensitive data stored on a whole disk encrypted drive remains fully protected when backed-up.* In addition, exclusive SmartClone™ technology enables Casper Secure Drive Backup to maintain a complete backup in the same amount of time required by most traditional backup programs to perform a partial or incremental *unencrypted* backup of an encrypted disk.
- Rapid Recovery.** In the event of a hard disk failure, a backup created by Casper Secure Drive Backup can be used as an immediate and permanent replacement for the failed hard disk, or restored to a new hard disk in a single step. No special rescue disks or arduous data restoration processes are required to facilitate recovery, and most importantly, no lengthy re-encryption process is required.
- Convenience.** Casper Secure Drive Backup enables complete system backups to be performed at any time without leaving Windows, so there is never a need to restart the computer or stop work to create a backup. Integrated scheduling permits the backup to be performed completely unattended in the background, and exclusive 1-Click Cloning™ makes even on-demand backups a snap.

The Casper Secure Drive Backup Solution for Users of Whole Disk Encryption

Strategy	Disk Space Required for Backup	Time Required for Full Backup	Time Required for Restore	Key Advantages
Backup within Windows	Less than or equal to the amount of actual data existing on drive (e.g., less than or equal to 100GB for a 500GB drive containing only 100GB of actual data)	Approximately 1-3 hours per 100GB of data depending on speed of disk(s) (e.g., approximately 1 to 3 hours to backup a 500GB drive with 100GB of actual data)	<u>None</u> if backup on bootable storage device; otherwise, approximately 1-3 hours per 100GB of data (e.g., approximately 1 to 3 hours to restore a 500GB drive with 100GB of actual data)	<ul style="list-style-type: none"> Backup persists data in <i>original encrypted state</i> No restoration or lengthy re-encryption process required for recovery. Backup fully updatable while in encrypted state. Backup can be made to drive either larger or smaller than original.

How does Casper Secure Drive Backup address the problem of quickly and securely maintaining a complete backup of a whole disk encrypted system without leaving sensitive data in an exposed, unprotected state?

- Casper Secure Drive Backup creates a complete backup of a whole disk encrypted drive that persists all of the encrypted data in its *original encrypted state*.
- A backup created by Casper Secure Drive Backup remains fully updatable in its encrypted state. Other products require two separate, time-consuming steps to create an updatable encrypted backup.

How does Casper Secure Drive Backup address the problem of replacing a failing whole disk encrypted drive with a new one without wasting an entire day performing a laborious and time consuming restore and re-encryption process?

- A backup of a whole disk encrypted drive created by Casper Secure Drive Backup can be used immediately as a complete and permanent replacement for the original whole disk encrypted drive in the event of a corruption or drive failure – making a separate restore, and most importantly, a time-consuming re-encryption process unnecessary.
- A backup of a whole disk encrypted Windows system drive is fully bootable. In the event of a corruption or system drive failure, the backup can be used immediately to boot and run the computer.
- Systems with support for booting from USB hard disk (USB-HDD) type devices, including most modern laptops and desktop PCs, can boot and run directly from a backup of a whole disk encrypted Windows system drive that is attached as an external USB drive.
- When a system precludes immediate replacement or booting from the backup, a complete backup of a whole disk encrypted drive can be restored without performing a separate, day-consuming re-encryption step.
- A backup of a whole disk encrypted drive can be restored to a new drive that is either smaller or larger than the original.

How does Casper Secure Drive Backup address the problem of upgrading a whole disk encrypted system drive to a larger capacity model without resorting to a laborious and time consuming backup, restore, and re-encryption process?

- Casper Secure Drive Backup can quickly copy a whole disk encrypted drive to a larger drive in the same amount of time as traditional backup and disk imaging programs copy an unencrypted disk, thereby foregoing the need to perform separate backup, restore, and lengthy re-encryption steps.

Who needs Casper Secure Drive Backup?

- Road warriors, SOHOs, and individuals wanting to efficiently maintain a complete, bootable, PGP Whole Disk Encrypted backup of their primary notebook and desktop system disks
- Enterprises whose diversified backup plan includes stand-alone recovery capabilities for PGP Whole Disk Encrypted notebook and desktop PCs
- Users wanting to upgrade their PGP Whole Disk Encrypted system to a new, larger capacity hard disk
- In short, every PC user who employs PGP Whole Disk Encryption technology

What are the most important issues for users of backup programs?

- **Ease of use.** A program that is too complicated to use is of little value. A backup program must be intuitive and easy to use in order for it to be a viable backup or data migration solution.
- **Convenience.** Having a current backup can make all the difference in the world. Unfortunately, backups are often put off or forgone altogether when the computer is needed for other tasks, or worse, forgotten when the task is left as a manual chore for the user. To be a good backup solution, a backup program must free the user from the burden of maintaining the backup as well as permit the backup to be performed at any time -- without disrupting what the user is currently doing on the computer.
- **Dependability.** A backup is worthless if it cannot be accessed or restored when needed. A backup solution must produce a reliable backup that a user can depend on when disaster strikes.
- **Speed.** Backups can never be too fast. If a backup takes too much time to produce, users may postpone or forego a critical backup simply because they are short on time.
- **Support.** Windows systems are complicated, and when things go wrong, support is critical. Timely and accurate help for unexpected problems is essential for any backup program.

How does Casper Secure address the ease-of-use issue?

- Casper Secure Drive Backup utilizes a series of sophisticated wizards that are carefully designed to make the process of backing up or upgrading a whole disk encrypted drive extremely easy, especially for novices. The wizards are engineered to take all of the guess work out of the backup process by guiding a user intuitively through the entire process and automatically managing many of the tasks that might ordinarily make the process too technical or confusing for the novice.

How does Casper Secure address the convenience issue?

- Casper Secure Drive Backup enables the backup of a whole disk encrypted drive to be performed at any time and without requiring a system restart.
- Integrated scheduling and Advanced Power Management features permits automated backups to run fully unattended daily, weekly, monthly, or at any time desired.
- 1-Click Cloning combined with Casper Secure's SmartClone technology enable on-demand backups to start and complete in the shortest possible time.

- Innovative SmartWrite™ technology and Automatic Performance Throttling support ensure maximum performance and full use of the computer while a backup is underway, avoiding loss productivity.

How does Casper Secure address the dependability issue?

- Casper Secure Drive Backup was engineered specifically for Windows and users of PGP Whole Disk Encryption technology.
- With Casper Secure there are never any surprises regarding the validity of a backup. If trouble is encountered during the backup process, Casper Secure records the problem as well as any affected volume, file, and directory in an easy-to-read, comprehensive report.
- Exclusive Automatic Copy Verification support ensures a backup is not corrupted during the backup process by faulty RAM, failing disk, or disk controller interface.
- By creating a fully bootable backup of a whole disk encrypted system drive, Casper Secure not only eliminates the frustration and problems typically associated with complicated data restoration processes, but also makes it extraordinarily easy to test and use a backup should the need arise.

How does Casper Secure address the speed issue?

- Exclusive SmartClone technology enables Casper Secure Drive Backup to maintain a complete, fully bootable backup of a whole disk encrypted drive in the same amount of time required by other backup and disk imaging solutions to perform a partial or incremental *unencrypted* backup of a whole disk encrypted drive.
- AccuClone™ technology virtually eliminates problems caused by poorly engineered or misbehaving third-party drivers and applications as well as the aggressive filtering techniques employed by today's leading antivirus and antispyware implementations that can significantly degrade performance during the creation of a bootable backup.

How does Casper Secure address the support issue?

- Future Systems Solutions support has a reputation for being exceptional, both in response time and quality. The Future Systems Solutions' support team takes its responsibility very seriously. Support requests received from customers are generally answered within hours, not days, and very few individuals require follow-up contacts. The critical nature of the backup process demands that there is a knowledgeable person at the other end of the support request email, fax or phone call, and the FSS team's passion for excellence carries through to the company's support function.

What makes Casper Secure Drive Backup so special?

- It is the first and only backup solution that:
 - Creates a complete backup of a whole disk encrypted drive that persists all of the encrypted data in its *original encrypted state*.
 - Saves time by creating a fully updatable backup of a whole disk encrypted drive in a single step. Other products require two separate, extremely time-consuming steps to accomplish the same goal.
 - Produces a backup of a whole disk encrypted drive that can be used immediately as a complete and permanent replacement for the original whole disk encrypted drive, or restored to a new drive without performing a separate, day-consuming re-encryption step.
 - Provides a near-instant recovery capability for users of whole disk encryption by creating a fully bootable backup of a whole disk encrypted Windows system drive, including a backup that can boot and run directly from an external USB drive.
 - Quickly duplicates a whole disk encrypted drive to a larger drive without requiring a laborious and time consuming backup, restore, and re-encryption process.
 - Creates or restores a whole disk encrypted backup to a drive that is either smaller or larger than the original.
 - Supports fast, encrypted differential backups of a whole disk encrypted drive.
- **Plus...**
 - PGP Administrative Policy Enforcement extends administrative policies defined through PGP Universal Server to the backup process to ensure users do not create a backup that violates company policy.
 - SmartStart™ Wizards make backing up or replacing a PGP Whole Disk Encrypted Windows system drive faster and easier than ever.
 - SmartSense™ Disk Detection jump-starts the backup process by automatically detecting when a new portable disk or existing backup disk is attached to the computer.
 - SmartSense™ Automatic Backups fully automate the process of maintaining a system backup on a portable drive, making it easier than ever to maintain a complete, instantly bootable system backup on an external USB drive
 - Automatic Copy Verification™ ensures backups are not corrupted by faulty RAM, a defective cable, failing disk, or bad controller interface during the backup process.
 - Automatic Performance Throttling support was designed specifically to take advantage of new functionality available only in Windows 7 and Vista, ensures other applications remain completely responsive even while Casper Secure Drive Backup performs a backup in the background.

Casper Secure Drive Backup is the first and only PC backup solution to confront the problems affecting users of PGP whole disk encryption technology by creating a fully bootable, completely encrypted backup of a whole-disk-encrypted Windows system drive.

#

What benefits does Casper Secure Drive Backup for PGP Whole Disk Encryption provide?

Feature	Benefit
Creates a complete, fully-encrypted, instantly-bootable backup of PGP Whole Disk Encrypted Windows system drive.	Stress-free, rapid recovery. In the event of a hard disk failure, the backup created by Casper Secure can be used as an immediate and permanent replacement for the failed hard disk. There is no special rescue disk or lengthy data restoration process required to facilitate a recovery. Users have complete and immediate access to all of the data on their backup. In fact, testing a backup created with Casper Secure is as easy as restarting the computer directly from the backup hard disk.
Creates or restores a fully updatable backup of a whole disk encrypted drive in a single operation.	An updatable backup or restoration of a whole disk encrypted drive no longer requires two separate steps, resulting in a significant savings of time.
Creates a fully bootable copy of a whole disk encrypted Windows system drive that can boot and run directly from an external USB drive.	Provides laptop users with unprecedented security and convenience.
Creates or restores a backup of a whole disk encrypted drive to a drive that is either smaller or larger than the original.	No need to use a drive that is the same size as the original drive. The drive simply needs to be large enough to accommodate actual data – unused space is not backed up or restored.
Creates a backup of a whole disk encrypted system drive that can be tested immediately after its creation by simply configuring the computer to boot from it.	Eliminates worry about the integrity of the backup.
Quickly duplicates a whole disk encrypted drive to a larger drive.	Makes short work of hard disk upgrades, enabling users of whole disk encrypted system drives to upgrade to a larger capacity drive without requiring a laborious and time consuming backup, restore, and re-encryption process.
Creates and removes encrypted and unencrypted partitions from whole disk encrypted hard disks.	Users can create and remove encrypted and unencrypted partitions from whole disk encrypted hard disks without the lengthy and time consuming decryption and re-encryption process normally required.
PGP Administrative Policy Enforcement	Extends administrative policies defined through PGP Universal Server to the backup process to ensure users do not create a backup that violates company policy.
Automatic Copy Verification	Ensures backups are not corrupted by faulty RAM, a defective cable, failing disk, or bad controller interface during the backup process.
AccuClone™ Technology	Exclusive disk imaging technology that not only ensures the backup is usable as a complete and an immediate replacement for the original, but also retains all encrypted data in its <u>original encrypted state</u> .
SmartClone™ Technology	Backups of whole disk encrypted drives are updated in the same amount of time required by other backup and disk

Feature	Benefit
	imaging solutions to perform a partial or incremental <i>unencrypted</i> backup of a whole disk encrypted drive.
SmartWrite™ Technology	Ensure maximum performance and full use of the computer while a backup is underway, avoiding loss productivity.
SmartSense™ Disk Detection	Jump-starts the backup process by automatically detecting when a new portable disk or existing backup disk is attached to the computer.
SmartSense™ Automatic Backups	Fully automates maintaining a system backup on a portable drive.
SmartRelease™	Automatically prepares a portable backup drive for safe removal after a backup.
Integrated scheduling	Backups can be performed automatically on a routine basis, ensuring that backups are always up-to-date. Backups can be performed daily, weekly, monthly, or at any time desired
Advanced Power Management	Increases scheduling flexibility by allowing Casper Secure to wake a computer in the middle of the night to perform a backup completely unattended, and then safely return it back to sleep.
SmartAlert™ Notifications	Notifies users via email when a backup has been completed or only when a backup requires attention for true “set it and forget it” operation.
SmartStart™ Wizards	Make backing up or replacing a PGP Whole Disk Encrypted Windows system drive faster and easier than ever
1-Click Cloning™	Beginning the backup process is one mouse-click away, adding convenience to on-demand backups.
Automatic Performance Throttling (APT)	Designed specifically to take advantage of new functionality available only in Windows 7 and Vista, APT improves responsiveness of other applications while Casper Secure performs a backup in the background.
Solid State Drive (SSD) and Advanced Format Drive (AFD) support	Increases the life expectancy and enhances the performance of solid state and long data sector drives.
USB Boot Capability	Creates a fully bootable copy of a PGP Whole Disk Encrypted Windows system drive that can boot and run directly from an external USB drive
USB 3.0 Support	Ensures maximum performance when backing up to or booting and running from a portable USB drive.
Native 64-bit support	Provides true 64-bit performance on Windows 64-bit platforms, including 64-bit editions of Windows 7, Windows Vista, and Windows XP Professional x64 Edition.

Feature	Benefit
Designed for Windows	Designed from the ground up to run entirely from within the Windows environment so that users never have to stop what they are doing or restart their computer to create and maintain a complete PC backup.
Complete Windows 7 and Vista support	Takes full advantage of start-of-the-art, Windows 7 and Vista innovations such as I/O prioritization, I/O cancellation, and User Account Control.
<p>Works with any hard disk recognized by Windows, including all SATA, eSATA, ATA/IDE, SCSI, USB, and Firewire drives – even hardware RAID arrays.</p> <p>Backups up to 2 terabytes in size.</p> <p>Compatible with all versions of FAT and NTFS.</p>	Wide range of supported hardware assures compatibility and eliminates need to install special drivers. If Windows supports the user's hard disk, Casper Secure will too.

#

About Future Systems Solutions, Inc.

Future Systems Solutions, Inc. (FSS) was founded in 1986 to develop software solutions that enhance the operation of existing systems. The company has worked with and supplied technologies to industry-leading companies, including Symantec, Iomega, and Quarterdeck.

In 1986 FSS became the first company to bring device-independent disk caching to the PC market with the introduction of SpeedCache™. This unique approach to disk caching meant not only superior performance, but also an unrivaled level of compatibility. By avoiding system dependencies, SpeedCache offered true plug-and-play compatibility for any computer system that supported Microsoft's DOS operating system.

In those early days of personal computing, FSS quickly became a premier provider of software solutions for RAM expansion manufacturers and system resellers. In 1987, the company released EME™, a solution designed for computer system manufacturers that needed a way to simulate the emerging expanded memory standard from the more common and less expensive form of expansion memory known as extended memory.

To further enhance the value of extended memory, FSS released version 2.0 of its caching product as SpeedCache+™. Together with EME, SpeedCache+ quickly became a favorite bundle for original equipment manufacturers producing PCs.

In 1989, FSS licensed the SpeedCache+ technology to Peter Norton Computing as a component for the Norton Utilities. With the success of the Norton Utilities, the disk caching technology developed by FSS became second only to Microsoft's SmartDrive (which was bundled with MS-DOS) as the largest distributed disk caching technology for the PC.

In the early 1990's FSS' SpeedCache+ became the premier disk caching utility for the Microsoft Windows environment. In 1992, FSS debuted the first caching technology to enhance multimedia and CD-ROM drive performance on the PC. By 1993, the rave reviews from the PC industry and the growing popularity of SpeedCache+ attracted the interest of Symantec and led to the exclusive licensing of the technology for distribution under the Norton Speeddrive label.

FSS continued to be a key provider of system enhancement utilities to software publishers while pursuing research and development efforts in emerging technologies. In 1996, FSS signed an exclusive licensing agreement with Quarterdeck Corporation and released the first device-independent persistent caching technology for CD-ROM drives. Then, in 1997 FSS licensed its innovative application launch acceleration technology to Symantec Corporation for inclusion in the Norton Utilities, and in 1998, FSS added to its list of technology leading developments with the introduction of DriveSpan™, the first true hard disk spanning utility for PCs.

Also in 1998, FSS introduced Drive2Drive™, a product designed to make backing up existing hard disks and upgrading to new hard disks faster and easier than ever. Designed specifically for Windows 9x / ME, Drive2Drive was the first product of its kind to image an active Windows system hard disk completely within the Windows environment. This advance made it possible for non-technical users to upgrade and backup their system hard disk without the need to create or use a special startup disk, or waste time learning archaic DOS commands.

The next decade saw the emergence of Casper™ as a hard disk backup and upgrading solution designed specifically for users of Microsoft's new operating system platform, Windows XP, and its successors, Windows Vista and Windows 7. Like Drive2Drive, Casper's introduction made it possible for non-technical users to easily create and maintain an instantly-bootable, backup replacement disk for their PC. Technical innovations such as SmartClone™ differential cloning technology were subsequently introduced to make it possible for Casper to maintain a complete backup replacement hard disk for a PC in the same amount of time required by other backup and disk imaging solutions to perform a partial or incremental backup to a proprietary archive. Other innovations such as AccuClone™ disk imaging, Automatic Copy Verification™, SmartSense™ disk detection, and support for creating a fully bootable backup on a portable USB drive continue to make Casper faster, more reliable, and more convenient to use.

In 2009, Casper Secure™ Drive Backup for PGP® Whole Disk Encryption was released. Casper Secure Drive Backup remains the first and only PC backup solution to confront the problems affecting users of whole disk encryption technology. While whole disk encryption ensures sensitive data remains fully secured on a PC, traditional backup programs fail to deliver the same level of security for a backup. Casper Secure solved this problem by allowing users to create an equally-secure PGP whole disk encryption backup that is instantly-bootable and useable as a complete and immediate replacement for the original PGP whole disk encrypted drive in the event of a hard disk failure or corruption.

Contact Information

Future Systems Solutions, Inc.
8888 Keystone Crossing, Suite 1300
Indianapolis, IN 46240
Phone: 800.272.5457 / 317.579.3100
Fax: 317.579.3001
www.fssdev.com

Product Marketing

Marty Rubenstein
mrubenstein@fssdev.com