

Casper Secure™ Drive Backup 4.0 for Full Disk Encryption

The Only Backup and Recovery Solution for Users of Drive Encryption Technologies

Casper Secure Drive Backup is the first and only PC backup and recovery solution specifically designed for users of Symantec PGP® and BitLocker® Drive Encryption technologies.

In one step, Casper Secure creates a complete, fully-encrypted backup of the system drive in its original encrypted state.

With Casper Secure, users have the ability to recover instantly with a bootable backup or to choose a specific point-in-time to restore. Either way, users can be back up and running in minutes, eliminating a day or more of unnecessary downtime and reducing the burden on IT.

Casper Secure Drive Backup eliminates the security gaps associated with other backup and recovery systems by ensuring that data is never exposed during the backup and recovery processes.



Casper Secure's Unique Advantages

Fast, Complete Encrypted Backups

- Users maintain a complete system backup without ever putting data at risk. With one click, Casper Secure Drive Backup creates a fully encrypted backup of an encrypted Windows system disk in its original encrypted state.
- Users never need to decrypt their system drive to create a complete backup or rely on the backup software to separately encrypt their data. With Casper Secure Drive Backup, there are no new passwords to remember or manage.
- Users have their choice of two kinds of backups: a fully encrypted, instantly bootable backup replacement (clone) and a fully encrypted restore-point (image) backup.¹

Rapid, Encrypted Recovery

- Casper Secure eliminates the separate data restoration and re-encryption steps required by other drive imaging and backup solutions.
- A Casper Secure bootable backup can be used as an immediate and permanent replacement for a failed hard disk or restored to a new drive in a single step. Casper Secure can even produce a backup that can boot and run directly from an external USB drive for immediate recovery.
- Casper Secure's SmartRestore™ provides easy, one-step support for restoring an encrypted backup. And by adding the Casper Secure Startup and Recovery Environment directly to the backup device, a restore-point backup can be restored by simply booting directly to the backup device-completely eliminating the need for separate recovery media.

100% Compliance with Existing Security Directives

- Casper Secure Drive Backup eliminates the security and compliance risks associated with other backup and recovery solutions.
- All data is backed up in its original encrypted state; so there are no new passwords to manage and there are no new security protocols or encryption technologies to vet.
- With Casper Secure, data is never placed in an unprotected state during backup or recovery. That means that all backups created, maintained or restored by Casper Secure maintain 100% compliance with enterprise-wide security directives and HIPAA requirements.

Simple to Use and Convenient

- Innovative technologies such as SmartStart™ and SmartRestore™ make creating, maintaining, and restoring fully encrypted backups easier than ever. Integrated Scheduling and SmartSense™ technology allow users to automate the backup process so that the backup is kept current without a user having to give it a second thought.
- With Casper Secure, complete system backups can be performed at any time without leaving Windows, so there is never a need to restart a computer or stop work to create a backup.

Easy Upgrades

- Casper Secure makes it extraordinarily easy to safely and securely replace an encrypted system drive with a larger hard drive for increased capacity or with a faster Solid State Drive for increased performance.
- Casper Secure quickly duplicates an encrypted drive to another drive without requiring a laborious and time consuming backup, restore and re-encrypt process.



Casper Secure Drive Backup 4.0 Data Sheet

TECHNICAL HIGHLIGHTS

- Makes a complete backup of an encrypted Windows system drive that maintains the original Symantec PGP or BitLocker encryption of the system drive.
- Creates a fully bootable copy of encrypted Windows system drive that can boot and run directly from an external USB drive.² A bootable backup can also be used as a permanent replacement for a failed system disk.
- Copies an entire hard disk or selected partitions and volumes.
- Supports cloning and restoring images of larger hard disks to smaller hard disks.
- Runs entirely from within the Windows environment with easy-to-use wizards for copying, imaging, creating, and removing encrypted and unencrypted drives.
- Resizes partitions during the cloning process to make full use of larger hard disks.
- SmartClone™ technology dramatically reduces the time required to maintain a backup.
- SmartWrite™ technology ensures maximum performance and full use of computer while performing a backup.
- SmartStart™ wizards simplify the process of backing up or replacing a Windows system disk.
- SmartRestore™ provides easy, one-step support for restoring a system from a backup.
- SmartSense™ disk detection automatically detects when a new portable disk or an existing backup disk is attached to a computer.
- SmartSense™ automatic backup functionality fully automates the process of maintaining a system backup on a portable drive.
- Integrated scheduling allows backups to be scheduled daily, weekly, monthly or at any time desired.
- SmartResume™ technology provides support for safely resuming an interrupted backup to another disk or image file backup when a soft failure occurs.
- Automatic Backup Retention policy provides automatic management of image backups.
- SmartAlert™ Notifications notify you via email when a backup has been completed or only when a backup requires attention for pure “set it and forget it” operation.
- Automatic detection and support of solid state and Advanced Format Drives for increased life span and enhanced performance.
- 1-Click Cloning™ permits routine backups to be performed at any time with a single click.
- Automatic Copy Verification™ ensures copies are not corrupted by defective RAM, cables, disks, or controller interfaces.
- Automatic Pre-Image Verification ensures all data on the source drive is accessible before overwriting a bootable backup.
- AccuClone™ technology ensures a true copy with all encrypted data in its original encrypted state.
- SmartRelease™ automatically prepares a portable backup drive for safe release after the backup has been completed.
- Advanced Power Management support increases backup flexibility by waking computer to perform a backup and then automatically suspends, hibernates or powers-off the computer completely unattended.
- Runtime controls allow you to quickly change power management and notification options after a backup is underway.
- Scripting Support allows custom interface design, operation and integration within an enterprise.
- Supports GPT and MBR partitioning.
- Supports all drives including SATA, eSATA, ATA/IDE, SCSI, USB, Firewire, and hardware RAID arrays.
- Fully supports all versions of FAT and NTFS.
- Supports systems using either UEFI or BIOS firmware.
- Allows advanced disk management tasks, including create and remove encrypted and unencrypted partitions, change the active partition, change a drive letter assignment, replace damaged or missing boot records, and more.

SYSTEM REQUIREMENTS

- Supports Symantec PGP Desktop version 9.6x or later and Windows BitLocker® Drive Encryption for NTFS volumes on all 32-bit and 64-bit editions of Windows® 8, Windows 7, Windows Vista®, Windows XP, and Windows 2000 Professional
- 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.



¹Disk image file backups and related functionality supported only when running on Windows 7 and later.

²Requires computer with BIOS support for booting from USB hard disk type devices.

