Casper Secure™ Drive Backup for PGP® Whole Disk Encryption

HOW SECURE IS YOUR BACKUP?

A data security strategy is not just about issuing a policy to use whole disk encryption. A strategy needs to make sure that other policies and systems also work well with that encryption.

For example, how can you be sure that every employee keeping a backup is not violating your policy directive by having an un-encrypted backup?

Of course, your company may have company-wide backup and restoration systems in place. However, many times a company has employees that need more. Employees who work in the field, travel, work at satellite offices, or need to respond to clients quickly need a backup and recovery system that is fast and that they can use on their own. Consequently, these employees often resort to other less secure means of backup.

- Are these employees putting your company's data and reputation at risk by creating an un-encrypted backup to fulfill their needs?
- Are they wasting a day encrypting an un-encrypted backup that meets their needs just to remain compliant with company policy?
- Are they needlessly jeopardizing a project by foregoing the type of backups they need to remain productive and to keep the project on time?

Your enterprise needs a solution that allows these employees to make fast and reliable encrypted backups of their data. And if your employees cannot afford to be without their data for any moment, then recovery must be immediate and easy.

CHALLENGES SURROUNDING WHOLE DISK ENCRYPTION POLICIES

Enterprises using whole disk encryption (WDE) technologies such as PGP® Whole Disk Encryption are confronted with several seemingly simple, but major management problems:

1. How can we empower our employees to maintain complete and current backups of their whole disk encrypted systems quickly while keeping their data encrypted and secure at every stage of the backup?

2. When employees' disks fail, how can they easily and immediately access their backup data when they are working out of the main office or traveling and do not have access to office systems or even IT support?

3. When employees need to rely upon their backups, how do we make the recovery process fast to eliminate lengthy downtime while still keeping their data encrypted and safe at every stage of the restoration?

4. How can our employees be confident that their encrypted backups will work when needed? Can our employees be certain that their backups have not been compromised by faulty equipment?

5. When additional disk space is needed, how do we upgrade our employees' hard disks to larger capacities without burdening our IT department? Can our employees upgrade their own systems without resorting to a complicated, laborious and time-consuming backup, restore, and re-encryption process?

HOW CAN YOU MEET THESE CHALLENGES?

Casper Secure Drive Backup. Casper Secure creates an immediately bootable backup as secure as the original drive. All encrypted data is retained in its original encrypted state.

Casper Secure™ Drive Backup for PGP® Whole Disk Encryption

1.

Casper Empowers Employees to Maintain their Own Secure Backup

Unlike traditional backup and disk imaging products that can produce only un-encrypted backups of a PGP® whole disk encrypted PC, Casper Secure Drive Backup preserves all of the encrypted data including all settings and applications in their original encrypted state at every step of the process. This one-step backup saves time and, more importantly, ensures employees remain fully compliant with data security directives when creating backups.

Casper Secure Drive Backup enables complete system backups to be performed easily and at any time without leaving Windows; so there is never a need for employees to restart their computers or to stop working to create a backup.

In addition, creating, updating, and accessing a backup is as easy as attaching a portable drive. And because a Casper Secure Drive Backup creates a backup that remains fully updatable in its encrypted state, an encrypted backup can be updated in the same amount of time required by other backup and disk imaging solutions to perform partial or incremental un-encrypted backups.

With Casper Secure Drive Backup, your employees are able to create and maintain their own secure backups of all of their data, including files, applications and settings.

2.

Casper Secure Drive Backup Ensures Employees are Always Prepared for Hard Drive Failures

A backup created by Casper Secure Drive Backup is bootable and 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.

When a drive fails, an employee can simply boot and run the computer directly from the Casper Secure backup, or the employee can remove the failed drive, replace it with the Casper Secure backup drive, and return to work without delay.

In addition, employees always have complete and immediate access to all of their files and folders on their Casper Secure backup in the same manner as on the original drive.

As a result, your employees can easily and completely recover from a hard drive failure without having to rely on or wait for IT assistance.

Casper Secure Drive Backup ensures there is never a reason for your employees to be unprepared for a hard drive failure even when they do not have access to IT systems or support.

3.

Fast Recovery from Failed PGP® WDE Drives Eliminates Downtime

Accessing a Casper Secure backup is as easy as attaching a portable drive.

Since Casper Secure does not store data in a proprietary format, there is no special rescue disk, no lengthy restoration step, and no time consuming re-encryption process.

By completely eliminating these lengthy processes, Casper Secure Drive Backup will save your employees a minimum of 6 to 18 hours of downtime when recovering from a 250 GB hard drive failure.

Should the original disk fail, the employee can simply boot and run the computer directly from the Casper Secure backup drive and return to work right away.

Casper Secure Drive Backup will save your employees on average an entire day of unnecessary downtime by completely eliminating the lengthy restoration and re-encryption processes required by other products when recovering from a hard drive failure.

Casper Secure™ Drive Backup for PGP® Whole Disk Encryption

4.

Employees always know that their backups will work when needed

Automatic Copy Verification technology brings backup dependability to a new level by automatically verifying the integrity of the backup during the backup process. With Automatic Copy Verification, your employees rest easy knowing that their backups have not been compromised by faulty RAM, a defective cable, failing disk, or bad controller interface.

With Casper Secure Drive Backup, your employees will know that their backup is fully functional with no surprises that the backup has been compromised by faulty equipment.

5.

Upgrading PGP® WDE Drives Is Easy

Casper Secure Drive Backup replaces the overly complex and time consuming backup, restore and re-encrypt process with a simple backup and replace process, so your employees can perform their own hard disk upgrades reducing the burden placed on your IT department.

Casper Secure Drive Backup quickly duplicates a whole disk encrypted drive to a larger drive in the same amount of time that traditional backup and disk imaging programs copy an un-encrypted disk.

"Using Casper simply makes good business practice. No one should risk losing valuable documents, research data, or lesson plans or experience downtime because of a failed or infected hard drive."

--Howard Griffith,
IT Specialist Eastern Washington University

"As an IT security consultant, I recommended Casper Secure Drive Backup to my medical center client. It was the only solution that could meet their requirement of doing bare metal restores of their PGP®-encrypted laptops.

I soon realized Future System Solution covers a segment of the backup market that no other company does and would be valuable to me in my work. Server data backup in most enterprises has its limitations. Rebuilding a workstation from a standard image, restoring data and re-enabling licenses can take several days especially if a workstation runs custom applications. With Casper, I am back in business generating revenue in 15 to 30 minutes. Even better, since it makes a whole disk encrypted copy of my workstation, Casper complies with our corporate security policy and standards."

-- Christophe Henrion,
IT Consultant