Casper Secure™ Drive Backup

Data is Never Exposed During Backup or Recovery with Casper Secure™

Many companies have implemented full disk encryption to protect data at rest. However, such policies do not guarantee that a company is safe from data breaches. Gaps in security often occur in the backup or recovery process.

For example, one multinational company with a large portion of its workforce working off-site implemented PGP® Whole Disk Encryption. However, the company did not change the backup and recovery procedure that had been in place prior to this security measure.

When an employee's laptop failed, IT sent a static image of what was on the machine when the laptop was first issued to the employee on a USB drive configured to boot. Then the employee restored the image to an unencrypted drive and retrieved data from the cloud - all before encrypting the drive, putting the data at risk.

Casper Secure™ Drive Backup eliminates these security gaps. In one step, Casper Secure creates a complete, fully encrypted image backup of an encrypted Windows system disk in its original encrypted state.

Users have a choice of two kinds of backups: a fully encrypted, instantly bootable clone or a fully encrypted restore-point image backup.

Should the system disk fail or become corrupted, users can recover instantly with the bootable backup or choose a specific point-in-time to restore. Either way, users can be back up and running quickly with encrypted recovery, eliminating a day or more of unnecessary downtime.

With Casper Secure Drive Backup, data is never place in an unprotected state during backup or recovery. Casper Secure ensures users always remain 100% compliant with data security requirements.

Client Highlight

"No matter how you do it, there's nothing as fast as switching out a failed or corrupted system drive with a Casper Secure backup drive. And, since the Casper Secure Backup maintains all of the data in its original encrypted state, our Lab remains 100% compliant with HIPAA regulations."

John MacDonald, Systems Administrator
Neuropsychology and Brain Imaging Lab
Dartmouth College's Geisel School of Medicine

Casper Secure Eliminates Security Gaps

	Data Protection at Backup	Data Protection at Recovery
Traditional Backup Products	Data resides on backup either in unencrypted state or a separately encrypted state, which requires a different encryption key, additional password management, and separate compliance requirements.	Risks non-compliance and data security by requiring data to be restored in an unencrypted state and then separately re-encrypted. The amount of time to re-encrypt a restored disk is directly proportional to the size of the entire disk rather than the amount of actual data restored, resulting in unnecessary downtime, wasted time, and increased costs.
Casper Secure Drive Backup	Data always resides on backup in its original encrypted state. No extra step is required to encrypt data. There are no additional pass words to manage or new compliance requirements.	Provides immediate, encrypted data recovery without risking compliance or data exposure. A bootable backup with all data in its original encrypted state provides users with a zero-downtime recovery option. A fully restorable encrypted backup provides users with shortest possible downtime when data restoration is required as all data is restored in its original encrypted state and no unnecessary time is spent re-encrypting unused areas of a disk.

Future Systems™ SOLUTIONS

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