Casper Secure™ Drive Backup

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

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

For example, a 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 data security measure.

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

Casper Secure™ Drive Backup eliminates security gaps in the recovery process. With Casper Secure, users have immediate, encrypted recovery.

Casper Secure backs up everything, including the operating system, applications, and settings, in its original encrypted state. Thus the backup is as secure as the original drive. A Casper Secure backup is instantly bootable so that users can immediately recover from drive failures by simply running their computers directly from the backups. There are no special rescue disks or lengthy restoration and re-encryption processes required.

By using Casper Secure, a user's data is never placed in an exposed or unencrypted state. Users always remain compliant with data security directives, eliminating security gaps in the backup and recovery processes.

Interview 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