CASE STUDY

Casper Secure™

Dartmouth College's Neuropsychology and Brain Imaging Lab at the Geisel School of Medicine Uses Casper Secure™ Drive Backup to Avoid Loss of Productivity When an Encrypted Drive or Server Fails

» Summary

The Neuropsychology and Brain Imaging Lab at the Geisel School of Medicine relies on Casper Secure Drive Backup and Casper Secure Server Edition to ensure that laptops and servers can be brought back into service immediately with encrypted recovery after a PGP ® whole disk encrypted drive fails.

» The Situation

For several years John MacDonald, the Systems Administrator at the Neuropsychology and Brain Imaging Lab at the Geisel School of Medicine, has used Casper to clone system drives and servers so that these systems could be brought back into service immediately should a drive fail. He supplemented this approach with frequent tape backups. His approach proved itself successful last autumn when the main Windows server crashed. By simply switching over to the Casper clone as the new system drive, the server was back in operation within minutes.

However, because the Lab's faculty and staff are involved with research and testing of clinical patients, the Lab falls under strict HIPAA privacy and security rules. As part of its overall efforts to meet HIPAA compliance, the Medical School adopted PGP whole disk encryption for **all** its Windows desktop and server systems.

Mr. MacDonald worried that the introduction of PGP WDE would threaten his backup and recovery approach. Without a viable solution, it was possible that a staff member could experience at least a day and a half of downtime every time a hard drive failed. And, if a server failed, each of nearly half the staff would experience that amount of downtime. This downtime could cause deadlines to be missed for grant or publication submissions, which could be harmful to both the Lab's financing and the careers of its researchers.

Key Challenges

- The Lab needed the ability to make complete clones of its server drives and laptops that had been encrypted with PGP whole disk encryption.

- The clone had to remain as secure as the original PGP encrypted drive.

- The solution had to ensure a quick, fully-encrypted recovery in the event of a disk failure. It would be too time consuming and risky to first restore to an unencrypted state and then re-encrypt the entire disk.

- The solution had to make it easy to maintain and restore a variety of machines and servers with different configurations.

Complete PC Backup Protection for Users of Whole Disk Encryption

» The Solution

Mr. MacDonald was pleasantly surprised to learn that Casper was available for cloning PGP WDE drives. Casper Secure Drive Backup has all the same functionality of Casper, but it is specifically designed to work with PGP whole disk encryption or Windows® BitLocker® Drive Encryption.

In a single step, Casper Secure creates a fully bootable backup that maintains the original encryption of the drive. There is no new encryption technology to vet, no new password to manage and no time-consuming encryption step to take to encrypt the backup.

Like Casper, Casper Secure backs up everything including the operating system, applications, settings, and all of the data. So if a hard drive or server fails, Mr. MacDonald can boot and run directly from the Casper Secure backup or use the Casper Secure backup as a replacement for the failed drive. Either way, the Lab can be back up and running in minutes without having to re-install an operating system, re-enable licenses of customized applications, restore all the data and re-encrypt the drive.

With Casper Secure, data security directives are always maintained throughout backup and recovery, eliminating the security gaps of traditional backup and recovery systems which rely on users or IT to re-encrypt the new drive.

> *"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, the Lab remains 100% compliant with HIPAA regulations."*
>
> *John MacDonald*
> *Systems Administrator*
> *Neuropsychology and Brain Imaging Lab*

» The Results

Mr. MacDonald implemented Casper Secure on all of the Lab's servers, desktops and laptops. According to Mr. MacDonald, "Casper Secure is simple to use. It takes virtually nothing in terms of time to create a clone because you can start the backup and walk away to do something else."

To Mr. MacDonald, the most important benefit of Casper Secure is the peace of mind it gives him. "I need to put most of my emphasis on preventing downtime since people could be writing grants, doing data analysis or seeing patients. So, recovering quickly from a drive failure is important."

Without Casper Secure, Mr. MacDonald estimates that it could take up to a day and a half to get a machine or server back up and running. He would have to start from scratch when a drive failed by installing and updating the operating system, re-authenticating licenses, restoring data and encrypting the new drive.

According to Mr. MacDonald, downtime is minimal with Casper Secure and there are no security gaps. "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, the Lab remains 100% compliant with HIPAA regulations."

About Future Systems Solutions, Inc.
Future Systems Solutions develops and markets innovative software solutions for the PC. Further information may be obtained by calling 855-5-CASPER or by visiting the FSS website at www.fssdev.com.

Future Systems ™
SOLUTIONS

Complete PC Backup Protection for Users of Whole Disk Encryption