The Secant Sentinel Technology Newsletter

DROPBOX...NOT A PROBLEM, RIGHT?

With the advent of BYOD (Bring-Your-Own-Device), many organizations have turned a blind eye to employees' use of consumer-class services such as Dropbox, GoogleDrive, SugarSync and Skybox to sync files between desktops, laptops and all the mobile devices they haul around. In fact, the use of these services is likely even more prolific than you realize. But just how secure is the data stored with these types of services?

Dropbox has had numerous well-publicized security breaches including: users' files becoming publicly accessible for several hours due to an authentication bug; user names and passwords stolen and used to gain access to unencrypted stored files; users' email addresses hacked from a Dropbox employee's unencrypted document and used to generate a spam flood potentially loaded with malware.

Dropbox is not alone in security shortcomings. GoogleDrive users *really* need to read the fine print. Here's how serious they are about the security of your data as noted in the privacy policy of the GoogleDrive agreement: "When you upload or submit content to [Google] services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, communicate, publish, publicly perform and distribute such content."

Here are some serious questions to consider about the use of these services:

- Do you even know what data is leaking onto these services and thus no longer on your network and subject to your security protocols?
- Do you have sensitive or confidential data that is subject to regulatory or non-disclosure compliance that *could* be stored on Dropbox?
- What damage would your organization sustain if the contents of these Dropbox accounts were made public?

So maybe you are rethinking that blind eye? But let's look at why users turned to Dropbox-like services in the first place. Has this ever happened to you?

- Need access to a file that is on another device or network share while you're on the road?
- Forget your presentation which is on your company laptop and you show up to the meeting armed only with your smartphone?
- Can't email a file to a colleague because it's too large?
- Need to collaborate on the same set of files with colleagues which generate multiple revisions?

These are valid productivity and mobile-user requirements, but you need to maintain control and security of your data. Secant is pleased to announce an alternative to these consumer-class services. Introducing SecantSTOR Sync.

The Secant Sentinel Technology Newsletter

SecantSTOR Sync is built for business and brings you the convenience of cloud storage with file synchronization without sacrificing security or IT control. Synced files are encrypted both in transit as well as “at rest” with 448-bit Blowfish encryption. We never see your data and neither will anyone else. User accounts are integrated with your Active Directory so your password security is enforced.

SecantSTOR Sync puts synced files back in your IT control ensuring adherence to your company security policies. Your Sync administrator can manage which types of files can be synced, review login activity and which devices are connecting, as well as view directory and file structure of synced folders.

Users get the productivity gains they require by accessing files from anywhere, from any device…even offline! Files can be synced between all their devices; they can collaborate on the same set of files and share large files securely.

Please contact us to learn how you can regain control of your data with SecantSTOR Sync!