Maximize Employee Productivity and Mobility

We live in a fast-paced world. So how do your employees access and share files on the go?

File sync technology has made it possible for employees to access and share files from virtually anywhere. Unfortunately, **the use of consumer-grade file sync services, such as Dropbox, Microsoft OneDrive, and Google Drive, jeopardizes corporate data**. The cost to organizations that mishandle data varies depending on the industry – but in all cases it is significant.

The benefits of file sync technology are great, but consumer-grade file sync services are not appropriate for the workplace. Therefore, it is imperative that organizations adopt a **business-grade file sync solution that is both easy to use and secure**.

MicroData SecureCloud syncs corporate data, allowing users to access and share critical files and folders from their computers and mobile devices. **With SecureCloud, users are able to work from virtually anywhere.**

SecureCloud is full of features that make it easy for users to securely share and work with others. Users have various options for sharing with internal and external parties, can control the files and folders that they have shared, and set policies for the ways in which they are accessed.

All of this combines to form an intuitive and seamless user experience.

And MicroData's SecureCloud gives administrators **total control over their corporate data.** A comprehensive dashboard, rich reporting, and granular controls makes it easy to manage an entire instance of SecureCloud. Coupled with **military-grade encryption**, **custom or unlimited retention**, **remote wipes**, **continuous backups**, and **rapid restores**, SecureCloud sets the standard for business-grade file sync.

Key Features

- Business-Grade file sync enabling secure access from any device
- Secure and easy file sharing
- Backup and restore features preventing data loss
- File Server Enablement enabling automatic secure sharing of server data
- Active Directory integration. Use the same login you already use at the office
- SSAE 16 / DOC Certified
- HIPAA Compliant with BAA available
- 99.999% reliability!

Secure, Automatic Continuous Backups

An on-premises backup solution is smart, but so is having a second, off-site solution. MicroData's SecureCloud gives you a simple, **highly reliable solution for backing up your critical data whether on a server or on a key computer.** Just install the agent, identify the data to be backed up, and then rest easy as everything else is automatic. You can access your SecureCloud backup data anytime from any web browser.

Simple and Affordable

- FREE 30-day trial
- Month-to-month agreements. Cancel anytime.
- No minimum numbers of users.

Call today to get started!
978.921.0990

Silver
Microsoft
Partner

MicroData SecureCloud Sync & SecureCloud Backup

SecureCloud Sync, Monthly

	1-10 users	11-25 users	26-50 users	51+
SecureCloud, Managed. 50GB per user[1]	$10.00	$9.35	$8.70	$8.00
SecureCloud, Unmanaged. 50GB per user[2]	$9.00	$8.55	$8.10	$7.65

[1] Managed SecureCloud includes installation of client on all covered machines, setup of Team Shares, and unlimited Help Desk phone and email support for SecureCloud.

[2] Unmanaged SecureCloud includes basic setup and detailed administrative & user instructions

MicroData SecureCloud Backup, Monthly

	Standard	Managed[1]
Price per computer, includes 500GB compressed de-duplicated storage space	$40	$49
250GB compressed de-duplicated storage space	$20	$29
Additional storage space, per 100GB	$9.00	

[1] Includes installation, configuration, and daily operational checks

Special Discounts are available for any MicroData Essential, Select, or Complete Care customer

---

Frequently Asked Questions about SecureCloud

- **What platforms work with SecureCloud Sync?**

  SecureCloud Sync works with PC, Mac, iPad, iPhone, Android, and Windows Phones

- **What is File Server Enablement and why do I want that?**

  If your company has a server, FSE allows you to securely allow sync and share access some or all of your server data. Users don't need to use a VPN connection or software. Your office users continue to save and work with data in the same locations and don't need a SecureCloud Sync client. Remote users (and guests you designate) can work with data from any Internet enabled device.

- **How do we share files?**

  It's easy. From any user's machine that's running SecureSync, simply right click on the file and share it. Users will get two options; a *Public Share* and a *Secure Share*. A Public Share creates a URL which may be pasted into an email, most commonly, and emailed to anyone.

  For more security and control, the user may also select a Secure Share, where the recipient is specified; the recipient must create a guest account; and the downloads may be restricted, monitored, and timed out.

- **How does SecureCloud Backup work?**

  Any Server, PC, or Mac may be backed up. Configuration consists of designating the files and folders to be backed up and then the backup process happens seamlessly and continuously in the background.

  Recovery and restore of files is easy with web browser access. Files can be recovered either on a bulk basis or by time window. File version backups are also available and this is very helpful with **Ransomware** and **Cryptolocker**-style attacks where a single click allows all backed up files to be returned to the immediate pre-attack state.

- **How is Security Manged?**

  If your organization has a Windows Server, users can simply log in to SecureCloud with their regular Windows password once and then the sync connection is remembered. For non-Server environments, secure encrypted login access ensures safety of your data.