

CDP (Continuous Data Protection)

Managing critical data is no longer just an IT issue. There are legal, regulatory, financial, and compliance consequences for missing or corrupted data. CDP technology eliminates many of the traditional problems associated with data backup. This primer details the evolutionary process leading to the current state of CDP.

Managing information is critical to any business. But some files are more critical than others (e.g. the company's latest financials vs. last week's bowling party pictures). Computers have increased productivity, but have also increased the amount of information we create and manage. Mistakes happen, data becomes corrupted, and malcontents can wreak havoc with your files. Depending on your business, losing a file can be an inconvenience or could bankrupt your company – CDP is one way to help minimize this risk.

The concept behind CDP is to provide a user-accessible, current, versioned copy of a file. Some vendors bundle additional services including offsite storage (eVaulting) into their CDP offering. Most users work locally and then save the file to a shared server. Files in this shared location are then saved daily to removable media (most commonly tape), which is then stored offsite.

This traditional process has three main weaknesses. First, time and resources are needed to retrieve offsite media; and even then, restoring files from tape is not a sure bet. Tapes degrade, and depending on the backup cycle, you may need to restore from multiple tapes to restore a single file. Second, there is a window of time between most backup cycles; meaning that a file lost at 10AM will not be on the previous backup. Third, this process requires staff and perhaps other services (e.g. courier services) to restore a file.

CDP provides continuous backup of files, not just point-in-time backups. This is similar to the autosave feature of Microsoft Word. Additionally, CDP is not application specific, nor does it require the user to configure the backup. Industry experts agree that most users know they should perform file maintenance, but that they don't actually do it. CDP maintains a compressed, versioned copy of each file. Not only is the file compressed to save disk space, but only the document deltas (changes to the document) are stored.

The following example details how CDP works: A user creates a two page document and saves it to a folder managed by CDP. CDP saves a copy of the file in a separate location, compresses it, and versions it. The user then adds three pages to the document and saves it again. CDP will only save the changes – not the entire document. This process not only saves disk space, but provides document level version control. Some other applications may provide versioning functionality, but everyone modifying the document must use it, plus it creates file bloat and these files tend to be corrupted easily.

Storing files offsite is a well accepted practice, but Hurricanes Rita and Katrina illustrated the inherent weakness of this solution. Offsite storage must be close enough to permit timely access to the media when needed. But what happens if your backup data is

destroyed as well? EVaulting provides additional access to your time-sensitive data. This feature moves the files offsite via the internet to a data center. The data center can be located across the country to minimize the risk of natural or man-made disaster.

Studies indicate that between 80-90% of businesses that lose critical data go out of business. EVaulting and CDP must be considered in any business continuity plan.