

## Cisco Continuous Data Protection for Files

### Back Up Your Most Valuable Data: Current Work Files

For most knowledge workers today, the eight-hour workday is a thing of the past. Clicking away at laptops and desktops, these individuals work at home, in the office, and on the road—at all hours of the day and night. According to some industry experts, the work they generate makes up 60 to 70 percent of all corporate data. And it's all increasingly vulnerable to data loss and corruption.

It's no surprise, then, that the protection of laptop and desktop data has become a top priority in many businesses—especially law firms, medical practices, and consulting firms, where lost data can significantly affect productivity, customer satisfaction, and, ultimately, revenue. Losing key business information not only hampers productivity but also creates application outages, project delays, and diverted resources. Re-creating lost data can consume large amounts of time, and depending on the source, some data may not be recoverable at all. Any incident that causes a loss of important business information will likely result in lost opportunities and increased costs.

What's more, it's no longer enough to back up this data periodically. The most valuable files are usually the ones that users have worked on most recently. Companies backing up data only once every 24 hours risk losing eight or more hours of their employees' most recent—and therefore most valuable—output. Instead, businesses need a continuous, real-time backup and recovery solution that enables users to roll back to various points in time.

Most analysts, including Enterprise Strategy Group, agree that performing only a periodic backup leaves data at risk, and they find that this is a major concern among the IT professionals they survey.

Once critical laptop and desktop data is captured, companies need an efficient and cost-effective way to manage it. They need to determine its value to the company and apply appropriate corporate policies for retention and storage. Doing so helps a business prepare itself for any data protection and retention scrutiny it may face from auditors and/or regulators.

### Get a Simple, Powerful Backup and Recovery Solution

The answer to these very real concerns is a simple yet powerful solution: Cisco® Small Business Network Storage Systems (NSS) and Cisco Continuous Data Protection (CDP) for Files software.

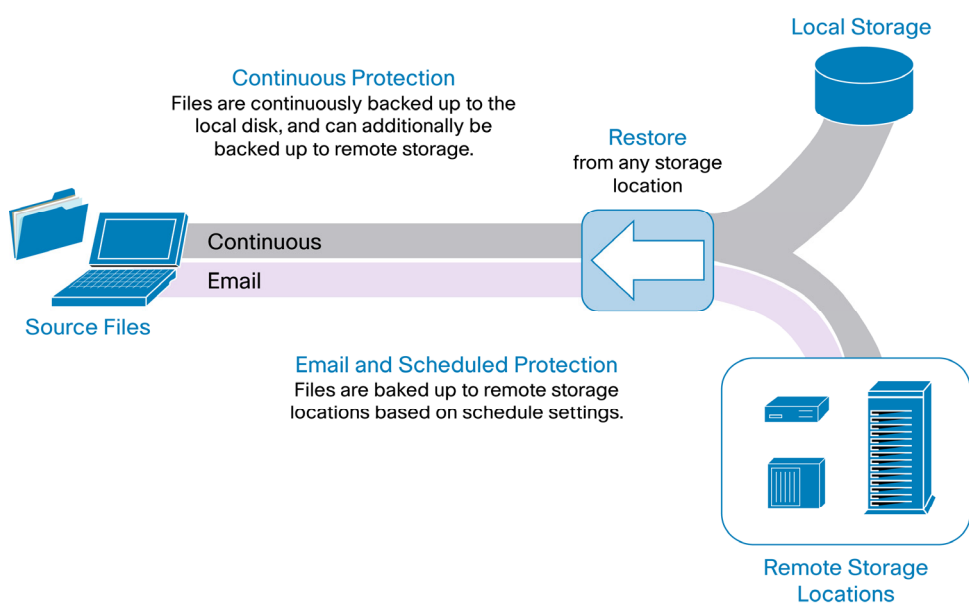
- **The Cisco Small Business NSS storage solutions**, such as the new Cisco Small Business NSS2000 Series desktop storage device, provide easy-to-install, centralized backup and storage for up to 75 employees, with up to 4 TB of data. Because the storage is networked, employees can easily share files and locate backed-up files from any device. Additionally, the NSS allows for drive “mirroring” and encrypted data storage, for superior data protection.
- **Cisco Continuous Data Protection for Files** provides real-time, continuous data protection designed specifically for laptops and desktops. Instead of waiting for a scheduled interval—typically 24 hours—it backs up users' most important files the moment they are saved, in real time.

## Take Advantage of This Major Breakthrough in Data Protection

Until now, the relatively few companies that systematically backed up their laptop and desktop data could do so only on a periodic basis, usually every 24 hours. This method did more than leave end users' more recent and valuable work unprotected. It also created complex issues, such as the need to manage backup windows, protect open files and databases, and handle the heavy impact backup operations have on production systems.

In contrast, Cisco Continuous Data Protection for Files continuously and automatically safeguards all changes to important data--with no involvement from IT administrators. Furthermore, it does so effortlessly and transparently--even, in some cases, eliminating the backup window. See how Cisco CDP for Files backs up data in the diagram below:

**Figure 1.** Overview of Cisco Continuous Data Protection for Files



Cisco Continuous Data Protection for Files:

- Backs up your most important files the moment they are saved
- Provides a real-time, continuous data protection solution for file servers and user endpoints, effortlessly and transparently, without administrative intervention
- Enables you to specify as many as three target backup/replication areas for high-priority files to help you capture every save of a file when it occurs, for protection against file corruption or loss
- Takes advantage of rapid disk-to-disk protection and restore capabilities to minimize the backup/recovery window
- Optimizes recovery point objectives (RPO) and recovery time objectives (RTO), and helps control costs through increased user productivity
- Retains data files for predefined lengths of time and assigns a version to each copy of a file to facilitate date-based restore
- Is easy to implement and manage, and runs transparently in the background with a light footprint

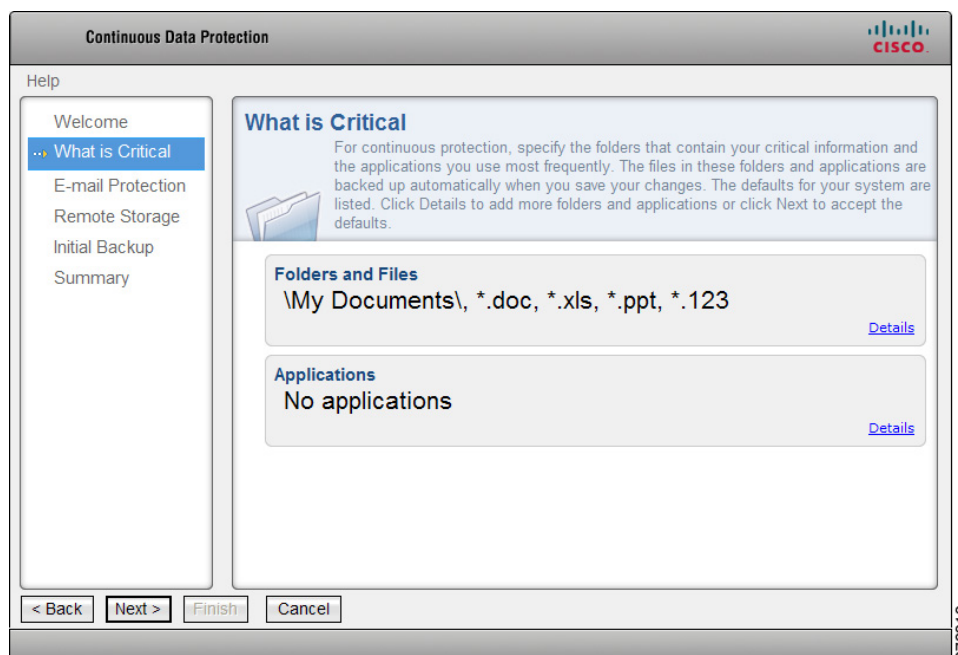
- Works with multiple backup/replication targets (local disk, network-attached storage device, web)
- Automatically manages the local backup target area as a pool with a configurable size, deleting old versions to make room for new ones

The Cisco NSS2000 and NSS3000 Series Network Storage Systems are desktop storage devices that are easy to install and manage. You can install the device yourself simply by plugging it into the switch and running a simple wizard, or, if your business is looking for advance setup and optimization, you can have a Cisco partner customize the drives and RAID settings to provide optimal performance for your needs.

### How Cisco CDP for Files Works

Covering desktops, laptops, and workstations, Cisco CDP for Files captures all changes made to existing files and stores the modifications in a preconfigured repository on the Cisco Network Storage System. Cisco CDP for Files can restore any file up to the last saved change. The below screenshot of Cisco CDP for Files, shows how you can select files and folders and applications will be continuously protected.

**Figure 2.** Use the What is Critical page to specify the files and folders that you want to protect



Users install small data protection agents on the computers they want to protect and follow a wizard to configure the repositories. They then select the locations where the data will be saved. Users can configure a local repository that resides on the same computer that is being protected as well as on the Cisco NSS to provide the ability to recover both accidentally deleted files and entire disk volumes.

For mobile laptop users, Cisco CDP for Files stores changed files in the local repository continuously, sending them to the NSS automatically when the employee reconnects to the corporate network. Mobile workers can easily back up or retrieve files from the NSS device while they are working remotely by logging in through a secure VPN router. The NSS repository is an additional level of protection in case something happens to the laptop to make local recovery impossible.

When selecting a location for the local repository, users also choose the appropriate amount of space to consume. Larger-capacity allocations enable the Cisco CDP for Files software to retain more versions and modifications to the data. You may want to collaborate with your IT Partner to determine how much data should be retained to prevent data loss.

In addition, the software can designate retention policies for specific files that are protected. The files and associated changes cannot be altered or deleted during the specified retention period. By preventing any changes to the files, the software protects the data against human error and viruses that may attempt to delete certain files.

When a restore is necessary, an IT professional or the user searches through the local repository to see if a recent, good version of the deleted file exists. The software interface displays the name of the file and the creator, size, and timestamp of the captured change. With older files, or if the local repository was also affected by a disruption, the repository on the NSS can be searched to restore the files.

## Conclusion

Cisco Continuous Data Protection for Files is like an insurance policy, protecting against data loss and providing a much higher degree of protection than daily backup systems and user-managed manual backup processes can offer. Employees no longer have to risk losing a day's worth of work, because files are backed up continuously. With its flexibility to store data both locally and remotely, Cisco CDP for Files benefits all users in an organization.

For more information visit: <http://www.cisco.com/go/smallbusiness/storage>.



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)