



FREQUENTLY ASKED QUESTIONS

DataGuardian™ Online Backup

1. What backup platforms are supported?*

- Windows: NT 4.0/2000/2003/XP Pro/Storage Server 2003, Small Business Server 2003
- NetWare 4.2/5.1/6.0/6.5
- Red Hat Linux 7.1/7.3/8/9/AS 2.1/ES 3.1
- SUSE Linux 9.1
- HP-UX 11/11i
- IBM AIX 4.3.3/5.1/5.2
- Sun Solaris 7/8/9
- iSeries (AS400) V5R1/V5R2/V5R3

** Current as of 8/1/2006*

2. What are the startup steps for DataGuardian service?

Once you are setup as a DataGuardian customer, you can start to seed your backups. In order to take the initial "full" backup required by DataGuardian, the defer option can be used to send data over a few days during off hours. Alternatively, a mobile vault (server or external hard drive) can be sent to your location to capture the seed, shipped back to IPR to import the seed, and subsequent backups will use DeltaPro technology to ensure the quantity of data backed up is minimal.

3. Will DataGuardian backup Windows Registries?

Yes, it will, but you must explicitly select the Registry/System State backup option. When restoring, you will have the option of restoring your system Registry.

4. Does DataGuardian provide support for NDS?

DataGuardian supports the Novell Directory Service (NDS) under version 4.2/5.x/6.0. During the backup process, the NDS information must be extracted to some temporary files. DataGuardian, at the beginning of the backup, backs up these files. Later, during the restore process, the NDS information is replaced with the original files. The new NDS is active from that point on, and thus the system does not require a reboot.

DataGuardian also supports the Novell Directory Service (NDS) under version 4.1x. During the backup process, the NDS information must be extracted to some temporary files. DataGuardian, at the beginning of the backup, backs up these files. Later, during the restore process, the NDS information is replaced with the original files. The new NDS is active from that point on, and thus the system does not require a reboot.

5. What are the options for the retention of backups?

DataGuardian allows you to define retention schedules that are then assigned to backups. Retention schedules enable you to set both how long and how many copies of a backup should be kept. For example, a daily retention scheme may say keep 10 copies for 14 days; a monthly scheme may say keep 12 copies for 365 days; and a yearly may say keep 3 copies for 3 years. Retentions settings may be set as high as 27 years.

IPR International, LLC

8 Tower Bridge
161 Washington St • Ste 800
Conshohocken, PA 19428
PH 484.533.6800
www.iprintl.com
email: sales@iprintl.com

6. How are open files handled during backups?

Most applications, especially in a network environment, open files in a "shared" mode, which allows any application to read the files even though they were already opened. DataGuardian provides the option to backup any files opened in "shared" mode since the results of an open file read are not guaranteed to provide consistent results. If another application has a file opened in an "exclusive" mode (i.e. other software cannot access the file), then DataGuardian will not be able to open the file for backup. This file will be skipped, and the fact that it was skipped will be noted in the log file.

Optionally, DataGuardian supports two applications to handle open files: Open File Manager (OFM) from St. Bernard Software and Open Transaction Manager (OTM) from Columbia Data Products. Both of these options permit all files to be backed up regardless of how they have been locked. This allows DataGuardian to synchronize and backup email, databases, Intranet applications and all other open files, even if the files are changing during the backup. All critical server data is protected, as open files are neither skipped nor corrupted during backups. This puts an end to corrupted data and logs of skipped open files.

7. How are MS Exchange backups handled?

There is a Plug-in designed as an add-on to the DataGuardian Agent for Windows. It protects data served by MS Exchange Servers version 5.5, 2000 and 2003. This Plug-in provides protection and easy restore of individual messages, folders, or mailboxes. It enables selection of the entire server, individual storage group or stores for either backup or restore. In addition to backup of the database, the Plug-in supports backup of Exchange transaction logs while supporting the single-pass restore. This allows clients to balance the backup and restore speeds with the storage costs for the solution.

8. How are MS SQL Server backups handled?

The MS SQL Application Agent provides online data protection for MS SQL 7 and MS SQL 2000 Servers. In addition to providing all the benefits of DeltaPro, the MS SQL Server Application Agent makes the backup configuration and restore very easy. It allows a simple selection of databases that require protection, only required data is sent to the remote Vault, reducing the costs of the solution. The Application Agent allows backup of either the database or, when full recovery model is enabled, backup of transaction logs, all while reaping benefits of DeltaPro and single pass restore. This feature allows flexibility allowing the user to balance backup and recovery speeds with the amount of data that is stored in order to provide the protection. Restores can be directed to original database; they can be redirected to a user-specified database; or can be "dumped" for use with MS SQL Enterprise Manager.

9. How are databases, such as Oracle, Sybase handled?

Databases have special backup requirements. To properly backup a database, you must be able to take a "snapshot in time" of the database. Traditional database backups are done in one of two ways, online backups via special API functions provided by the database vendor and full database exports to tape/disk. A third alternative is to use special device driver software that allows you to bypass locking issues.

Database APIs (Online Backup) - Some database vendors provide special APIs that support the backup of their databases. For example, the Oracle and Sybase database products can do an online backup if the backup software properly interfaces with their backup APIs. Any update transactions that are applied during the backup process are handled specially to avoid inconsistencies in the backup. The database vendors often supply backup software that will backup their databases to temporary files on disk. For 7-day/24-hour operations, it is common to do an online backup to disk and then use a secondary backup program to backup this data to tape.

Database Export (Offline Backup) - For those database vendors that do not provide online backup capabilities, the database must be shut down. Once the database is offline, the data is copied or exported to a temporary file(s). For databases that are not active all the time, it is common for the database to be shut down and exported to disk and then use a secondary backup program to backup the dump file to tape.

NOTE that the dump file is normally significantly smaller than the database because all the empty space is removed and the work areas/temp areas/rollback areas are not backed up. For instance, a 20-30GB database often produces just a 6GB-dump file.

Even though a dump to tape is feasible (using the internal backup of the database vendor), it is not normally done because it holds "locks" on the database too long which can interfere with performance.

Driver Software (Online Backup) - Optionally, DataGuardian supports Open File Manager (OFM) from St. Bernard Software and Open Transaction Manager (OTM) by Columbia Data Products, both of which permits all database systems to be backed up. It also allows DataGuardian to backup email, Intranet applications and all other open files, even if the files are changing during the backup. All database products are protected by becoming synchronized at the start of the backup and allowing active changes to occur while the backup is going on. As a result, open databases are neither skipped nor corrupted during backups. This puts an end to corrupted database backups.

10. How are Microsoft Cluster environments handled?

The DataGuardian MS Cluster Services (MSCS) Application Agent provides online data protection and integration for MSCS environments. In addition to providing all the benefits of DeltaPro, the MSCS Application Agent makes the backup configuration and restore of virtual nodes extremely easy while offering support for failover and fail-back. Support for remote management of physical and virtual nodes simplifies the configuration and monitoring of the backup solution. The DataGuardian MSCS Application Agent can work in tandem with DataGuardian Exchange and SQL Agents, ensuring that DeltaPro backups of critical file shares and databases are always functional and available.

11. What file types does the DeltaPro algorithm work on?

The DeltaPro algorithm works well on a variety of file types. **NOTE** that the first backup is always a "master" or "full" backup. Subsequent backups take advantage of the DeltaPro Processing scheme. Files that change very little, such as executable files, require virtually no backup activity. Most data files, especially databases, change relatively little during day-to-day operations and therefore lend themselves nicely to the DeltaPro scheme which analyzes for blocks of the file that have changed since the last backup.

12. How do the automatic backup schedules work?

You can schedule backups to run at any time of the day or night, as frequently as you like.

13. How can you administer multiple backups with DataGuardian?

Using the DataGuardian Administrator, a single LAN administrator can setup backups on behalf of other users. The managed system has to be running the DataGuardian Agent in the background, and the manager station running the DataGuardian Administrator connects to the managed system to configure the backup tasks and schedule them remotely.

14. Can you run more than one backup at once?

You may run more than one backup at once on the platforms that support separate instances of an executable program. Operating systems such as Windows NT/2000 support multiple backups at the same time. **NOTE** that NetWare cannot run multiple backup instances.

15. What security is available for your backups?

There are two major security features for DataGuardian. The first is an encrypted authorization feature for every user that connects to the Storage Vault. This protects your data from unauthorized access. An additional option is to encrypt the data before transmission to the Storage Vault. This protects your data both during transmission over the network and while the data is stored on the remote storage server.

16. What communication lines does DataGuardian support?

Because DataGuardian is based on TCP/IP, the underlying physical communication method is immaterial. Thus, local LAN connection, T1, ISDN and Frame Relay, to name a few, are all valid methods for connection between an DataGuardian Agent and a MSV.

The other advantage of using TCP/IP as the network connection protocol is that newer technology will fit transparently into the DataGuardian architecture.

17. Are there any average backup times for remote backups over specific communications lines?

No, there are no "typical" times for communication since there are so many variables involved. The best solution is to run the DataGuardian software in simulated mode, which will determine exactly what data needs to be backed up with the DeltaPro scheme and then estimate the transmission time for that data.

18. Is your data encrypted as it travels over the network?

You can optionally select to encrypt your data on the fly before it is transmitted to the MSV. We support multiple levels up to AES.

19. What do you do if you lose your encryption password?

For your protection, lost passwords can not be recovered.

20. What do you do if your system crashes and you need to restore a backup?

There are two possible scenarios that would follow to restore your backups from IPR.

The first would be used to restore everything using network lines. You would restore your operating system and then the DataGuardian Agent. With the Administrator, you would then restore your data by using the Resync feature to restore your catalogs from the Storage Vault. Then, you would use the Restore command.

The second option would be to request that your backup copied to a mobile vault and have it delivered along with a copy of the DataGuardian software. Then, after restoring your operating system and DataGuardian software, you would then recreate the catalogs and restore directly from the mobile vault disk device.

21. Can I administer and manage my backups remotely from anywhere?

Yes. The Central Control is just a management tool that can sit anywhere on a LAN or a WAN connection and manage backup agents. It utilizes port 808 for this communication between any Agent and a Central Control so depending on your configuration you might need to configure that port on the firewall to pass traffic through. All communication between the Agent and the Central Control is encrypted by default to ensure security.

22. Can I have more than one Central Control?

You can have as many Central Controls as you need. All files and configuration that a Central Control creates or edits, reside locally on the server with the backup Agent. Hence all Central Controls can view exactly the same thing with no synchronization needed.

23. Can IPR see my data?

DataGuardian provides data security for your business critical data via the means of encryption. A Backup agent will first look for DeltaPro changes on a nightly basis. These changes are at the block level. So for example if you changed a sentence in a word document, then only that one sentence is picked up by the backup Agent as the change in the file. Once it has collected all the changes, the backup Agent will then encrypt that information, compress it and send it over the wire to the Vault.

So it is just pieces of the puzzle that are being sent over the wire on a nightly basis so to speak. All the processing is done on the backup Agent and the data is already encrypted when it gets to the vault. The Vault will not restore anything to the Backup Agent without verifying the correct encryption key. There is no way for IPR Technicians to look up an encryption key or be able to break it in any way once a backup agent is set to use encryption. Various encryption types are available all the way up to AES 256 bit.