Storage Guardian Remote Backup Restore and Archive Services

Storage Guardian is the unique alternative to traditional backup methods, replacing conventional tape-based backup systems with a fully automated, agent-less (single instance, online solution backing up to Storage Guardian's mirrored, secure, off-site data storage infrastructure. It provides centralized and automated backups of PCs, file and database servers and corresponding immediate online restorations.

Storage Guardian's principal other benefits are:

- Risk reduction – the vulnerability to your organization caused by incomplete backups is virtually eliminated.
- Removing the tedious task of managing the backup and restore process, which more effectively uses management time – Set & Forget
- Disaster contingency - the service has inherent mission-critical disaster recovery capabilities, thereby allowing your company to continue in spite of unforeseen disasters.
- Restore times for accidentally deleted files are dramatically reduced, making your end user more productive.
- Ease of future planning - the Storage Guardian service simply grows as your data volumes increase. Archiving of historical important data is simplified.
- Cost effectiveness - the Storage Guardian service is priced to be competitive with hardware/software offerings trying to address the same issues.
- No capital outlay - the Storage Guardian service is charged on a **monthly-expense** basis.
- Backup up times are dramatically reduced through advanced software functionality, reducing the actual amount of data transmitted to Storage Guardian

Storage Guardian involves the installation of the Agent-less DS-Client software on any Windows system at your premise (Mac and Linux also supported). The DS-Client will connect to the Storage Guardian Data Storage Center via your Internet connection.

Our pricing model is based on the monthly volume, in compressed GBs, stored at the Storage Guardian's Data Storage Center. The greater the volume the lower the cost.

- Minimum monthly charge is for 1 compressed GB (3:1 Compression Ratio Basis
- Monthly rate for mission-critical data backup – immediate restore
- Different monthly rate for historical archive data backup – web portal restore

DS-Client Backup Software for Windows 2000/XP/Vista /2003, 2008SBS - Included

MS SQL (Open & Hot Backups) - Included

MS Exchange / Outlook .pst backup and message level restore - Included

Local storage across LAN Backup & Restore – Included 30-day, No Obligation Evaluation Test Software is included with no Charge training and implementation assistance.

Data Center Facilities

Storage Guardian's data center is a climate controlled, secure environment that is up and running 24x7x365 and delivers the highest level of security, reliability and fault tolerance. The data center sports an advanced HVAC temperature control system with separate climate zones, a sophisticated fire suppression system and multiple battery backups and power generators. Our state-of-the-art physical security features include 24x7 video surveillance, security breach alarms and secure card access.

Our facility is staffed and monitored around the clock, year-round. Our staff are experienced at quickly resolving hardware and software issues. In addition, the latest network and server monitoring technology instantly detects problems and ensures that they are dealt with immediately.

Storage Guardian's data center was designed to be reliable, high-performance, scalable and fault tolerant. Our network backbone is built with Cisco equipment, the world leader in Internet network gear. Every part of the network, from our switches to our routers and firewalls, have a redundant "stand-in" that instantly becomes operational in the event of a hardware failure. As a result, most network problems result in no lost data or connections.

Beyond our edge routers, our network is completely switched and centers around a redundant gigabit fiber backbone. Extra fiber is pre-wired to each row, enabling us to add new capacity quickly and meet additional bandwidth requirements if needed.

The combination of a secure, climate controlled premises, fault tolerant network equipment and scalable, high-capacity architecture ensure that Storage Guardian's data center is optimized for reliable transfer and safeguarding of customer data.

Storage Guardian Remote Backup/Restore and Archive Services:

- Storage Guardian provides an automated and unattended backup process ensuring that data held on PCs, Windows 2000 / XP / Vista / 2003 / 2008 / NetWare ® files servers, Macs, Linux, Vmware and Hyper-V environments and application/database servers is securely backed up and transferred offsite via the DS-Client software.
- Backup data is transferred offsite to the Storage Guardian secure Data Storage Center via a TCP/IP Internet connection.
- Sophisticated data compression technology, including common file elimination and delta blocking, maximize data transfer over the line connection. Compression can average a 3:1 ratio.
- All data is AES encrypted at customer’s site prior to transmission offsite. If dedicated leased line is chosen, then incorporated additional link level security increased.
- Secure Firewall protection is incorporated within the Storage Guardian offering to protect the customer and Storage Guardian network from unauthorized access.
- Storage Guardian provides a easy to use interface that simplifies the backup & recovery process and provides detailed information about scheduled operations.

- Centralized configurations of the Storage Guardian DS-Client software enables a network administrator/IT manager to specify exactly what data is to be backed up, ensuring investment is not wasted by backing up unauthorized or unnecessary information.
- Storage Guardian evaluation client enables accurate size of data volumes and transfer rates prior to full implementation of service.
- A user - definable number of backup versions of files are retained on disk, for immediate online restore.
- Backup data required for legal or audit purposes can be held archived upon request.
- Backup data can easily be selected and restored online without the need to locate and identify tapes.
- Storage Guardian response team is on 24 hour standby to support major data recovery by delivering requested backup data to the customer site.
- In the event of a major customer site disaster, a portable DS-System is delivered to the customer site or to a specified disaster recovery site.
- A Microsoft® and Novell® certified solution

Storage Guardian Service Guide

Storage Guardian is a unique alternative to traditional backup methods, replacing conventional tape based systems with a fully automated online solution. It provides centralized and automated backups of PC's, file servers and application/databases servers with secure offsite storage and immediate online restorations.

DS-Client Software:

The DS-Client software runs on one server that is on the local network. It utilizes standard Microsoft® Windows and Novell® Netware networking resources to connect to the customer's systems that are to be backed up and restored. To backup and restore Exchange® and SQL® servers, the DS-Client uses standard Microsoft® Applications Processing Interfaces (API). The DS-Client must be installed on a Windows® system, either Windows ® 2000, 2003, XP, Vista, 2008. Also DS-Client for Mac and Linux options.

Depending on the customer's network configuration, Storage Guardian may require the customer to set up appropriate permissions on any network resource for required backup and restore capabilities.

The Storage Guardian DS-Client software is completely agent-less making the application easy to deploy and support across the LAN from the one machine.

Installation Configuration of the DS-Client:

StorageGuardian will arrange an FTP server to perform the installation and configuration of the DS-Client software. This will involve configuration of the client settings, defining network address to the DS-

System, registering the DS- Client with the DS- System and entering the customer's specified encryption keys.

Encryption Keys

For the security of customers' backup data, the DS-Client encrypts every file it sends with an encryption key provided by the customer. The files are stored and remain encrypted on the DS-System at all times. The decryption process occurs during the restore operation of the backup data by the Storage Guardian DS-Client. This ensures that all backup data transferred and stored outside the customer location is always encrypted. The Storage Guardian software uses a 256 AES encryption algorithm and can be configured with two encryption keys: Private and Account.

Private Key

The private key is the default; used by individual DS-Client to encrypt backup data before it is transmitted to the DS-System at the Storage Guardian Data Centre. Backup files that are unique to a DS-Client are encrypted using the DS-Client private key and stored in that Storage Guardian DS-Client private area of the Storage Guardian DS-System.

Account Key

For customers with more than one DS-Client, an account encryption key is also defined. The account key is used to encrypt customers' files that are common to multiple DS-Clients connected to the same DS-System. These common backup files are encrypted with the account key and stored in that account library area on the DS-System. DS-Clients that share a Storage Guardian DS-System must be configured with the same account key.

The DS System uses encryption cookie to verify every connection by the DS-Client. Cookies are a piece of code generated using the encryption key, but not the key itself. The DS-Client sends its cookie on every connection requested, which the Storage Guardian DS-System compares with the original received during the initial Storage Guardian Client configuration. This verification process ensures integrity of both private and account keys. After initial configuration, the authentication between DS-Client and the DS-System is transparent.

Both private and account encryption keys can be 8 to 16 alpha/numeric characters and are configured during the DS-Client installation. Encryption keys are stored in the Registry in encrypted form, so that even if you have full access to the DS-Client processor (such as the Storage Guardian Customer Support), they cannot be read. Intentional or unintentional changes to the encryption key will make data stored on the Storage Guardian DS-System unusable.

It is the responsibility of the customer to supply appropriate values for the private and account encryption keys. These values once entered will not be required again except in the case of a disaster recovery situation where the Storage Guardian client must be re-configured.

IMPORTANT: (your company name) is responsible for storing the original encryption keys in a secure location. Loss of the keys will prevent recovery of the DS-Client and the end user's backup data. Storage Guardian has no knowledge of the customer's encryption keys.

Customer Administrator Console - DS-User

The Customer Administrator Console – DS-User is the GUI for the DS-Client and is operated by the customer network administrator to define backup sets and schedules, monitor backup sets and schedules, and monitor backups and perform restores. The Customer Administrator Console DS-User is installed on one or more of the customer's Windows XP®, Vista®, 2000®, 2003®, 2008®, Mac or Linux systems. It will be installed and demonstrated during the initial DS-Client installation and configuration.

DS-User access is integrated into Windows ® network security. Individual user accounts, or groups of users, can be defined and granted authority to perform different levels of the Storage Guardian functions.

Storage Guardian DS-User

All Storage Guardian operations are performed using DS-User. Authority to perform operations can be controlled by defining access to authorized users or groups of users, thus preventing backup and restoration of data by unauthorized personnel.

Backups

Storage Guardian solutions are based on backup sets that define the scope of the backup operation to be performed. Backup sets are executed to perform the specific backup operation and can be executed manually or scheduled to run automatically.

Backup Sets.

A backup set defines the files or databases that are to be backed up. They can include or exclude files or databases by directories, or by filtering the file type. This allows the customer administrator to define backup sets that meet precisely the customer's requirements, thus eliminating the backup of unnecessary data.

In addition, these sets define the number of retained generations, or versions, of files and databases backed up. This enables the customer to selectively restore any of the previous versions of files that have been backed up. The default is set at five generations.

Multiple backup sets can be defined for the same customer system; this feature enables the customer to define separate backups of different types of data on the same system. Multiple backup sets for the same system can also be actioned independently.

A backup set can only include data from a single customer system; one or more backup sets must be defined for each system to be backed up.

Backup sets are defined in a similar manner for Microsoft® Windows and Novell® Netware® file systems and for backups of Microsoft® Exchange and SQL Server. This single interface enables efficient administration of the Storage Guardian Service.

Authorized administrators can manually execute ad-hoc backups, however, the normal method will be to schedule automatic execution of the backup sets.

Open file backup

By default, Storage Guardian will attempt to backup files that are opened, but not locked, by other applications on the customer system. The customer administrator can further configure this functionality, either globally or by individual backup set, to define the method for handling open files and the number of backup re-tries to perform. DS-User provides comprehensive online help information for defining these options.

Files that are completely locked by another application, such as Microsoft Outlook® PST files, will only be backed up using the Message Level Restore Agent available on the Storage Guardian website.

All open files that fail to backup are reported in the activity log on DS-User and in the Storage Guardian status report notifications.

Tiered /BLM Archive Storage

Storage Guardian provides for the long-term archive of non-critical backup data. This is typically backup data no longer required for day to day operations, but required for other business, ie, legal, or audit purposes.

Data archiving is performed by defining and executing additional backup set commands for the appropriate customer file or data bases systems. These archive command sets are typically scheduled to execute on a monthly or quarterly cycle, and complement the regular day-to-day backups.

Archive data generated by these archive command sets is stored in a separate disk area on the Storage Guardian System and is copied to lower-cost media after a customer-defined interval.

Backup Schedules

Storage Guardian has extensive calendar scheduler for automatically executing backup sets. Schedules can be defined to execute backups daily, weekly, monthly, or on a more randomly defined frequency.

Multiple schedules can be defined, and multiple backup sets can be associated with a schedule. Where multiple backup sets are associated to a schedule, the customer administrator can define the number of concurrent backup sets to be executed and the priority in which they should be executed.

DS-User provides a graphical view of the backup schedules. This allows the customer network administrator to quickly view the status of the backups and identify any conflicting or overlapping schedules.

Monitoring Backups

In addition to DS-User a web-portal from the Storage Guardian presents daily management reports on the status of the Storage Guardian service. This web portal includes a summary of scheduled backup, highlights of any errors that may have occurred, and statistical information detailing the quantity of the back up.

DS-User provides extensive monitoring and reporting capabilities for customer administrators. This includes detailed logs of backup activity, and detailed logs of all files backed up, error reports and audit trails for all backup and restore activity.

Initial Data Collection

The primary method of backup is over the TCP/IP network Internet connection between the DS-Client and the DS-System at the Storage Guardian remote off-site data center.

Restorations

DS-User allows the authorized customer network administrator to quickly and easily select and restore data. Data can be restored to a remote system; for example, the administrator could use their desktop machine to restore data from a remote server. Multiple restore operations to separate servers can be performed from a single DS-User instance, making this particularly suitable for a Help Desk role.

There are two methods in which data can be restored. The first is online, where data is restored across the TCP/IP or dedicated line. The second is where the restore data is delivered via a portable Storage Guardian DS-System; this method is used in the event of a disaster or when a large amount of data needs to be restored.

The primary method of data restoration is online. DS-User provides a Restore Wizard that guides the Customer Administrator through the process of selecting and restoring data. The Restore Wizard allows the administrator to search and select files for restore, select the version of the files and choose the target destination for delivery.

Having selected the data to be restored, the Storage Guardian DS-Client delivers the data across the communication network from the DS-System at the Storage Guardian Data Storage Center. The Storage Guardian DS-Client then delivers the data to the specified system on the customer's network. As a part of the operation, all associated security permissions for the data are also restored.

Portable Storage Guardian DS-System Restores

For larger quantities of data, the customer administrator can invoke the Disaster Recovery Wizard to request that a copy of the backup data be copied to a portable Storage Guardian DS-System.

The Disaster Recovery Wizard provides the same level of restore granularity as the Restore Wizard, but rather than restoring the data across the network, it is copied to a portable Storage Guardian DS-System, which is then transported to the customer site. The customer network administrator can then use DS-User to restore the requested data directly from the Storage Guardian DS-Client to the system being restored.

The only data that can be restored from the portable Storage Guardian DS-System is that which was specified when initially requested. If additional backup data is requested then this can be restored either online or by a new request for a portable Storage Guardian being initiated.

IMPORTANT: The customer's encryption key must be made available for the data to be successfully restored.

1