

Secure Backup & Fileshare

WHITE PAPER ON SECURITY

The Secure Backup & Fileshare solution was developed in 1999, and is the leading web-based operating software for online data backup, storage, file sharing, large file transfer and ubiquitous access. Secure Backup & Fileshare's features allow customers to remotely backup, store, and access critical information more easily, reliably and efficiently than ever before - with the highest levels of security and availability.

Secure Backup & Fileshare acts as an "insurance policy" for protecting important data, allowing customers to automatically backup critical files from their computer systems -- and simply "plug in" to the Internet -- to access and use their data much the same way they obtain everyday utility services.

SECURITY

Network and information security is considered to be of the utmost importance in delivering the Secure Backup & Fileshare storage applications and services to customers. Network and information security are core differentiators of our offering. From our personnel to our technology and policies, security is built in to every aspect of our operations and solutions. We apply a 'Defense in Depth' security model, which addresses security from many different perspectives. These include:

- 1) Privacy Assurance and Administrative Security
- 2) Physical Security
- 3) Firewall, Access Control, Hacker-Cracker Defense
- 4) Strong Factor Authentication
- 5) Encryption

Privacy Assurance and Administrative Security – Access to the physical site and machines where Secure Backup & Fileshare data is stored is actively restricted to only key staff members who have a need to be present. Our systems are secured in a multi-layer fashion that grants rights (from physical to virtual access) to a subset of personnel.

Physical Security – The level of physical security for Secure Backup & Fileshare data is equal to or better than Telco-grade and US Government-grade security. Physical operations are serviced by four independent high-speed Internet connections, and have redundant power supplies that can run independent of the local power grid for more than 45 days. Access to our hosting site is restricted to those personnel who have been placed on an access control list by the security manager. Personnel onsite must present identification credentials and then successfully be authenticated through 2 biometric scanners before entrance to the interior portion of the structure is granted. At that point, security staff must escort personnel to the locked areas where data servers are located. Security staff logs each access event. Roving guards in conjunction with a sophisticated closed circuit television network actively monitor the entire facility. The hosting facility is unmarked; attack and bomb proof, weather resistant, and meets US Government secure facility criteria. The site has redundant utilities (power, water, cooling, etc.) in order to allow unlimited length operations at full strength for an unlimited period of time in the case of system failures in the supply of outside utilities.

Firewall and Access Control – Best practices are employed in the firewall and access control systems. Defense is provided by our use of cutting-edge firewall technology and managed security services provided by a dedicated security monitoring team. Our network architecture assures that only limited Internet protocol (IP) addresses are exposed over the Internet. Although our network utilizes multiple servers on our back-end, only specific IP addresses allow users through our firewall. In other words, even though each machine has its own internal address, the world outside our perimeter can never access (or 'resolve') them. Attempts to maneuver around or through the firewall using unauthorized addresses are rejected, logged through an intrusion detection system, and investigated by the security team.

Strong Factor Authentication – All users of Secure Backup & Fileshare must possess a current username/password/domain combination. Without all three data elements, a person will not be granted access to the Secure Backup & Fileshare online data access site. Anonymity is not permitted, nor do we have a 'public folder' area. All Secure Backup & Fileshare users must be registered to utilize the service.

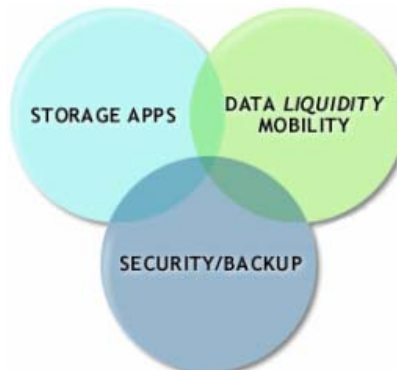
Secure Backup & Fileshare from Cbeyond offers optional additional strong factor authentication methods:

- **Asynchronous** - *Mandylion Labs* asynchronous authentication token that allows an end user to auto-generate and store truly random, cryptographically strong passwords.
- **Synchronous** - RSA Secure ID tokens in conjunction with the RSA "Ace Server." * *This application will be integrated to customer domain upon request.*

In all Secure Backup & Fileshare authentication scenarios, user logins are encrypted using SSL (Secure Sockets Layer, 128-bit encryption). Secure Backup & Fileshare usernames and passwords that are stored on our databases are always encrypted.

Encryption – Users transfer encrypted files using SSL over HTTP and FTP – thus essentially doubly-encrypting private user data. Secure Backup & Fileshare files remain encrypted at all times on our servers and can only be decrypted when downloaded and saved by the user. Users can optionally choose to implement US Government standard AES Triple DES encryption (256 bit key) for Secure Backup & Fileshare data stored on our servers.

OPTIONAL – Users are allowed to choose AES Triple DES encryption from the backup client. In this selection, a user encrypts data prior to transmission for transfer over the Internet to our storage locations. If chosen, this option requires the use of a Secure Backup & Fileshare software client for decryption of any recovered user files.



The Secure Backup & Fileshare solution displays expertise in the intersection of storage applications, mobility, and network security.

Disaster Recovery

Disaster Recovery is the mitigation of data and infrastructure loss in the event of a catastrophic event. Several standard procedures are performed to assure that the risk of data loss and system downtime are minimized if disaster strikes:

- 1) Multiple sites are maintained from which Secure Backup & Fileshare services can operate. If a single site is destroyed or otherwise rendered incapable of functioning, we can operate out of alternative operational sites. Furthermore, each site contains a 100% redundant infrastructure so there is no single point of failure within a single data center.
- 2) Each file stored is copied on Telco-grade disk drive systems and double-backed up to tape, making data loss virtually impossible. Tapes are stored offsite in a facility designed for secured archival storage of data tapes.
- 3) Live data is replicated asynchronously in at least two sites around the globe. US customers' data is replicated on both the East and the West Coasts.
- 4) Virus scans are conducted on the main system servers on a routine basis. Data stores are self-contained and do not allow any malicious programs stored on our systems to execute and initialize.
- 5) Finally, all of the Secure Backup & Fileshare proprietary software is kept under strict configuration control. Upgrades are thoroughly tested before promoted to a live data center and third-party software is kept up-to-date on a regular basis.

Overall, we feel that the Secure Backup & Fileshare solution maintains the highest level of security in the industry and a disaster recovery standard that assures protection of our customers' data while it is in our care.



Please send any additional inquiries to: customer.care@cbeyond.net