DATA SHEET

Sydney Recovery Gateway

Ransomware Protection for Cloud Storage

Key Benefits

- Recovery deleted files easily from a file system interface
- Easily delete Cloud Storage Versions saving monthly storage costs.
- Support for Cloud and Object Storage Version API's
- Supported partners include Amazon, Cloudian, Wasabi and other 3rd party vendors that support Amazon S3 Version API's
- Out of band Gateway allowing administrative access to all versions of files.
- Recovery tools restoring versions by date to single or multiple buckets.
- Local recovery disk cache may be flash, SSD, SATA or SAS
- Full compatible with the BridgeSTOR NAS Edge Cache and the Coronado NAS Gateway
- Full Active Directory Integration for User Authentication
- Ships as an OVF, AMI or an ISO for installation on physical hardware

The BridgeSTOR Sydney Recovery Gateway has been designed for companies that require protected and secure storage for corporate files. Sydney combined with Cloud or Object Storage guarantees recovery of files attacked by Ransomware by using strict version control native to Cloud Storage.

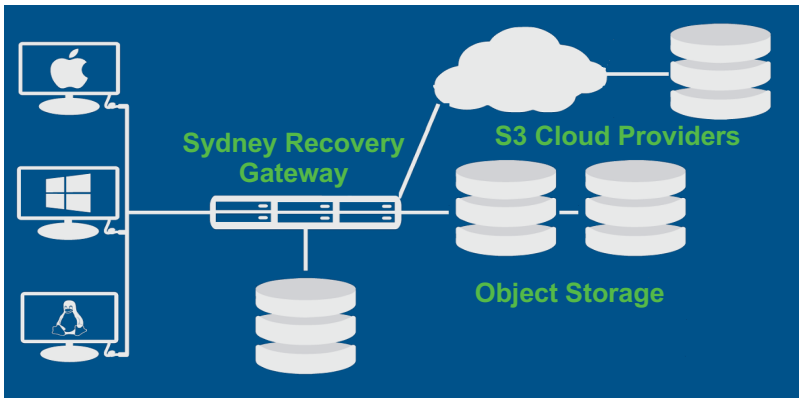
Challenge

BridgeSTOR Coronado and Brooklyn NAS gateways expose SMB and NFS shares to corporate users allowing easy access for shared files in the cloud. File data may be lost by a Ransomware attack, a virus attack or an accidental deletion of a file. Replication doesn't solve the problem as it just replicates the bad data. If not caught in time, backups of the data may also be compromised or not accessible or just too old. Sydney cannot stop the attack from occurring, but it will allow corporations to easily recover data without paying ransom in a fast and reasonable timeframe.

How it Works

Bucket Versioning. Most Cloud and Object Storage vendors support object Versions when creating a bucket allowing an object that is deleted or replaced to become a Cloud Version. All BridgeSTOR NAS Gateways convert files to objects while acting as a storage firewall exposing current files while not exposing Cloud Versions. If an attack occurs, the hackers can only manipulate the current files and have no access to Cloud Versions.

The Sydney Recovery Gateway supplies a secure out of band appliance that communicates directly to the cloud storage. Built on Linux, Sydney includes two mount points one displaying all files and the other display files with versions. The version mount point is limited to reading files/versions, deleting files/versions or copying a version back to the original file name or to a different bucket. Sydney also includes command line tools allowing subdirectories or files to be copied by a date range inside a bucket or completely moving objects from one bucket to another.



209 S. Stephanie Street B276 , Henderson, NV 89012 • www.bridgestor.com