Overview

Fujifilm's deep storage service offering, Permivault was recently rebranded as Dternity, representing little more than a name change. The service utilizes LTO-6 digital tape storage technology, open LTFS standards, and local network connections to provide vendor neutral long-term storage for backup and disaster recovery. While the service uses data tape to provide secure, long-term storage, it operates the same as disk-based cloud services, allowing users to manage and retrieve their files via a web portal. Data is actively monitored, migrated to new tape formats, and easily recalled from storage. Fujifilm states the service performs regular integrity checks and has self-healing mechanisms in cases of failure. The service can also be coupled with a Dternity NAS appliance to manage an onsite tape library, provide low-latency access to onsite tape storage, and automate submission to the Dternity Media Cloud for backup. Either service can be purchased and utilized separately or in conjunction with one another.

Dternity Media Cloud

SERVICE PROVIDER: Fujifilm

WEBSITE: www.dternity.net

PRODUCT RELEASED: 2014

COMPLIANCE: HIPAA HITECH; SSAE 16

SERVICE: Deep storage

INFRASTRUCTURE: Wholly owned

COST: High

Data Management

Files may be submitted to the Dternity Media Cloud via VPN over a CIFS or NFS share or through shipment of drives to Fujifilm's data centers. **Dternity offers a service to transfer data from old data tape formats and other storage media if shipped to Fujifilm.** According to available service documentation, data is not altered, transformed, or separated across the data centers. Files are stored in their original state, as written to tape upon ingest. File integrity checks are reportedly performed at regular intervals and the system automates replacement of corrupt files from redundant copies. System documentation does not specify the mechanism, regularity, or transparency of file integrity verification.

Reporting / Metadata

Dternity Media Cloud provides a web portal through which users may view an index of the files in storage—displaying the contents of your tapes—and retrieve data from storage via VPN or shipment of storage media. Service documentation does not indicate any reporting capabilities at this time. **An improved web portal is scheduled to be released in late 2014.**

Redundancy

The Dternity Media Cloud is positioned as a deep storage archiving and disaster recovery service. One or more copies are replicated to removable LTFS-formatted data tape within 24 hours of delivery. **Dternity Media Cloud does not provide geographic separation of data, copies are stored in one secure data center.** The service should be used in conjunction with other storage services to ensure data is backed up in different regions.

Accessibility

Dternity does not advertise a latency period for retrieval like similar services, such as Amazon Glacier. In disaster recovery scenarios, the service claims data will be available for immediate recovery, with a "99.99% annual uptime". Transfer speeds via a VPN connection will be dictated by the customer's and Deternity's bandwidth, which is not specified in the service documentation. Dternity recommends larger files be retrieved via shipment of storage media.

Security

Data transfers to and from Dternity use the Secure Sockets Layer (SSL) transfer encryption protocol. Fujifilm's experience as service provider of secure storage for medical and government records indicates high-level security requirements for their typical customers.

End of Service

Available product documentation offers no information regarding Dternity and/or Fujifilm's specifications for end of service. The use of LTFS potentially provides customers with storage media that is interoperable with other data tape systems, but the availability of these tapes and data return mechanisms in end of service scenarios is unknown.

Levels of Preservation

	Level 1 (Protect)	Level 2 (Know)	Level 3 (Monitor)	Level 4 (Repair)
Storage	• **Two complete copies that are not collocated**	• At least three complete copies • At least one copy in a different geographic location	• At least one copy in a geographic location with a different disaster threat • Obsolescence monitoring for storage system(s)	• At least three copies in geographic locations with different disaster threats
Data Integrity	• Check file fixity on ingest if it has been provided with content • **Create fixity info if it wasn't provided with the content**	• **Check fixity on all ingests** • Virus-check high risk content	• **Check fixity of content at fixed intervals** • Maintain logs of fixity info; supply audit on demand • **Ability to detect corrupt data** • Virus-check all content	• Check fixity of all content in response to specific events or activities • **Ability to replace/ repair corrupted data** • **Ensure no one person has write access to all copies**
Security	• **Identify who has read, write, move, and delete authorization to individual files** • **Restrict who has those authorization to individual files**	• **Document access restrictions for contents**	• **Maintain logs of who performed what actions on files, including deletions and preservation actions**	• **Perform audit of logs**

Have more questions? We can help.
Contact AVPreserve at info@avpreserve.com