



CTERA for Data Archiving

Identify inactive data with AI. Execute a governed data lifecycle management workflow.

Enterprise NAS environments hold more inactive data than most IT teams realize. CTERA analysis found that only about 10% of an organization's data was accessed in the last 90 days. Most data sits in primary storage at primary storage prices, without a documented retention record and without a governed process to manage cool and cold data.

CTERA provides an AI-based approach to data archiving to help organizations adopt intelligent and automated data lifecycle management processes.

The Cost of Unmanaged Data Growth

- ✓ **Primary storage bills grow as cold data accumulates**
Most unstructured data becomes inactive within months of creation. Costs compound each month with no business justification behind them.
- ✓ **Ad-hoc approaches create compliance liability**
Manual scripts, informal file moves, and third-party tools leave no audit trail and no enforceable retention policy.
- ✓ **Inactive data widens the ransomware attack surface**
Files accessible via SMB or NFS remain vulnerable to encryption and exfiltration regardless of age. Cold data expands the attack surface.
- ✓ **Identifying what to archive is an administrative bottleneck**
Archiving requires data knowledge. Without intelligent tooling, IT teams need to access and sift through logs, metadata, and storage reports across large, distributed environments to make archiving judgements. This manual identification process cannot scale.



97.5%

The percentage of files not modified in over one year*



9.9%

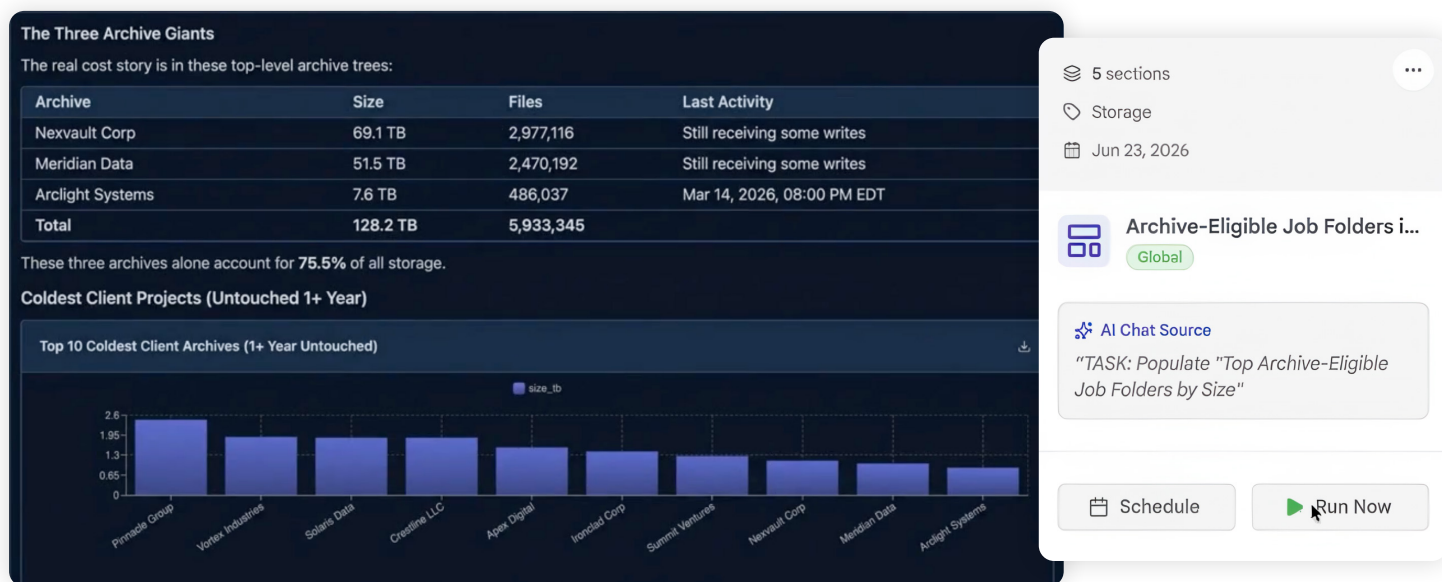
The percentage of an organization's data typically accessed in the last 90 days*

What Data Archiving Should Deliver

1 Automated Identification Without the Manual Efforts

The biggest obstacle to archiving at scale is determining which files & folders qualify. AI-driven analysis automatically surfaces archive candidates, based on age and usage patterns, across the entire environment.

How CTERA Delivers: CTERA InsightAI scans the environment and returns a ranked list of archive candidates. Archive Operators review the output and select what to move. CTERA Archive executes the transfer. AI handles the analysis. The operator makes the call.



2 Lower Storage Costs

Moving cold data to lower-cost tiers such as object storage, cloud archive, or on-premises alternatives reduces primary storage expenses. The addition of reporting gives IT the visibility to plan capacity, justify budgets, and allocate costs by team or workload.

How CTERA Delivers: CTERA Archive moves inactive data to lower-cost cloud tiers — including Amazon S3 Glacier Instant Retrieval and Azure Blob Cool and Cold — or affordable on-premises object storage. Customers can also use CTERA Secondary Data Services licensing. Storage reports display the primary-versus-archive split for capacity planning and cost allocation.

3 A Chain of Custody for Every Transfer

Archiving without documentation creates compliance problems. Each transfer needs a complete record that tracks who initiated the move, the data that was transferred, and the move location.

How CTERA Delivers: CTERA Archive logs every archive and restore operation with operator identity, source, destination, reason, file count, size, and timestamp. Logs are exportable for compliance reporting and legal discovery.

4 Retention That Fits the Regulatory Environment

Not all archived data carries the same regulatory weight. Some organizations need administrative flexibility including the ability to adjust retention periods or remove files when required. Other organizations need strict enforcement.

How CTERA Delivers: CTERA Archive supports two configurable retention modes. Enterprise mode enables select users with the right permissions to permanently delete files, which is useful for organizations with internal enterprise policies, but not legal or regulatory obligations. Compliance mode prevents modification or deletion of archived content for the duration of the retention period. For tamper-proof immutability, CTERA Vault adds WORM (write once, read many) protection via S3 Object Lock on certified storage nodes – blocking unauthorized modification, encryption, or deletion.

5 Protection Against Data Exposure and Ransomware

Inactive data left accessible via standard file protocols expands the ransomware attack surface. Archived data should be isolated from the vectors that put active data at risk.

How CTERA Delivers: CTERA Archive removes data from standard SMB and NFS access, shrinking the attack surface. The Archive Operator role governs who can access archived content – reducing vectors for malicious encryption, corruption, or exfiltration.

How CTERA Data Archive Works



Set Up

The administrator creates Archive Cloud Folders in the CTERA Portal, selects the target storage tier – ideally lower cost cloud storage service or on-premises object storage, sets the retention mode and period, and assigns Archive Operator roles.



Identify

CTERA InsightAI scans the environment and returns a ranked list of archive candidates. Archive Operators review the output and select the files or folders to move. AI handles the analysis. The operator makes the call.



Archive

The CTERA Archive wizard collects the destination folder, the reason for archiving, and initiates the transfer as a background job. Administrators can set up optional views of archived data for users.

The screenshot shows the 'Archive to Vault' wizard interface. The top navigation bar includes icons for Destination, Confirmation, Deletion, Archiving, and Summary. The 'Archiving' step is currently active. The main content area displays 'Archiving Completed Successfully' with the message 'Your files have been successfully archived.' Below this, a 'Summary' section lists: Items: 6, Total Size: 122.7 MB, Destination: IA-Archive (global admin), and Reason: Old Large Files. At the bottom, there is a link to 'Archive Logs' and a 'Download Report' button.

How It Works, Continued...



Govern

Archive Logs maintain a running chain of custody throughout the retention period. Storage reports display the primary-versus-archive split for capacity planning and cost review. Retention policy enforcement runs continuously.



Restore

Archive Operators process restore requests through the CTERA Portal. Every restore logs the same operator accountability as the original archive – identity, destination, reason, and timestamp. Administrators can restore archived content, including at a file level.

Restore from Archive

Destination

Confirmation

Restore

Summary

Restore Destination

Select a destination folder where you want to restore the selected files from the archive.

Destination folder:

Original Location

Original Location

Custom Location...

Enter reason for restoration...

Continue

Cancel



AVAILABILITY

CTERA Archive and CTERA InsightAI are available as part of the CTERA Intelligent Data Platform. Contact CTERA sales for details and a free assessment of your data environment to determine potential cost savings from archiving and switching to CTERA.

See how CTERA Archive and CTERA InsightAI can bring intelligence and accountability to your data lifecycle management.

GET A FREE ASSESSMENT



CONTACT US

CTERA.COM

info@ctera.com

USA: (917) 768-7193

Intl: +972-3-679-9000



 your files.

 your cloud.