White Paper

CTERA Global File System

June 2025

ctera your files. your cloud.

Table of Contents

Introduction

It’s 6 a.m. in London. A global product launch deadline looms, but the design files the European team needs are trapped — fragmented across different regional storage silos. Meanwhile, engineers in San Francisco and Tokyo are working on parallel revisions without seeing each other's updates. Conflicting versions, missed deadlines, and frustrated teams all point to a systemic failure: traditional NAS and legacy storage infrastructures cannot meet the demands of a distributed, always-on enterprise.

While teams scramble to meet global deadlines, IT is fighting its own uphill battle. Traditional NAS was never built for this scale or speed. Storage is fragmented, costly, and hard to manage. To avoid running out of space – an issue that has caused real business disruptions in the past – IT overbuys capacity “just in case.” But the data keeps piling up. “Do we really need to keep all of this rarely accessed data?” they ask. “Does anyone realize how expensive NAS storage really is?” The team is stuck in a cycle of constant monitoring, reactive upgrades, and manual capacity-planning.

Organizations worldwide are recognizing that delivering seamless, secure and high-performance access to unstructured data – anywhere, anytime – is a strategic necessity. A Global File System (GFS) is no longer just “nice to have”; it’s the foundation for digital operations in the modern enterprise.

CTERA’s GFS is engineered to solve this challenge, delivering local performance with global consistency, powerful AI protections, military-grade security, built-in compliance, and future-ready enterprise intelligence capabilities.

What is a Global File System (GFS)?

A Global File System (GFS) enables organizations to centralize, protect, and collaborate on unstructured data while delivering a local file access experience anywhere in the world. It bridges the gap between centralized cloud storage and distributed workforces, ensuring users can access and collaborate on files quickly, securely, and without disruption.

Unlike traditional file servers or legacy NAS systems that were designed to serve a single location, a GFS spans geographies, clouds, and edge devices, delivering a unified view of enterprise data under a single namespace.

In short: A GFS makes it possible to access "any file, anywhere, anytime" while enhancing performance, control, and security.

Key Requirements

With all the changes described above, it should come as no surprise that a GFS must address a diverse set of requirements. Let's look at the key ones:

Global name space: Users should be able to access any file from any location – subject to their access rights. Therefore, each file should have a unique "global name," and a GFS should decouple physical location from logical file names. Distributed access: A GFS solution must provide reliable access to files on a fully synchronized dataset – regardless of where the employees are working across the globe. Providing seamless remote access may involve deploying "access points" (aka CTERA Edge Filers) to facilitate site access to the cloud or leverage desktop applications or a feature-rich web UI to achieve.

Enterprise collaboration: Employees often collaborate, creating and sharing files regularly. Traditional file-based collaboration relies on storing a file on a shared server and then enabling access to others. This typically requires involving a system administrator to set the appropriate ACL for designated files. A more modern collaboration method, such as file sync & share (FSS), allows users to set desired collaboration attributes to specific files or folders and then invite others to share them. A GFS should support both traditional and next-generation file-sharing methods.

Mobile and remote work support: Many enterprises have adopted a "bring your own device" (BYOD) policy, allowing employees to access corporate assets using mobile devices, including laptops, smartphones and tablets. A GFS should enable employees to access files from their preferred device, whether at home or on the road. This may require installation of software apps on users' laptops or mobile devices.

Security: With files created and accessed by a geographically distributed organization, and often stored on externally hosted cloud infrastructure, security is paramount. A GFS must encrypt files both "at rest" – wherever they are stored – and "in transit" while they are sent across a corporate network or the internet. Users attempting to access files must first be authenticated via corporate directory services (e.g., AD, LDAP) and granted access according to defined access control lists (ACL).

Flexible/Hybrid cloud storage: A GFS should support any storage combinations that enterprises choose, including a "private cloud" hosted within a data center, a public cloud, or a dedicated virtual private cloud (VPC) hosted by one or more service providers. Furthermore, a GFS should enable seamless transitions from one storage target to another, preventing vendor lock-in. The chosen storage targets should not impact how users view and access their files via the GFS.

Central scalability: Demand for storage, particularly file storage, continues to grow rapidly. A GFS should support the effortless expansion of storage space, taking full advantage of either private or public cloud storage resources.

Edge scalability: The growth of the central storage pool should not impact users at the edge. They should have access to any file and be able to view all files available to them, regardless of their device's storage capacity. True edge scalability requires a highly efficient edge database (DB), not a full copy of the entire metadata DB, which would create performance bottlenecks and massive storage demands.

Precision controls: A GFS must offer administrators toolsets to ensure data is accessible and synchronized only where necessary, not just for governance but also for device and connection efficiency. To fully leverage multi-cloud flexibility, controls must also be in place to write blocks to specified object storage. Global File Locking should be equally precise as well, not a blanket feature, but one thoughtfully deployed in workflows that truly require it.

Operational efficiency: Techniques such as WAN optimization and caching ensure fast and secure file access throughout the distributed enterprise. Compression and deduplication both globally and at the edge, maximize the efficient use of provisioned storage.

Third-party integrations: A GFS must be compatible with enterprise platforms like Varonis, Sentinel, and Splunk to maintain organizational cross-system SIEM reporting.

Data protection: Files embody significant portions of knowledge, employee output, and corporate intellectual property. Protecting data stored in files is therefore a top priority. Data protection is an umbrella term that covers a variety of processes. These include backup and restore tools to safeguard files from external disasters or user errors; antivirus (A/V) utilities to protect files against malware; and ransomware and exfiltration prevention mechanisms to stop attacks before they succeed. A GFS solution should offer data protection tools that are both built-in and integrated via third parties.

Enterprise data intelligence: Advanced reporting and metrics on GFS activity help bring greater transparency and control to organizational IT. Additionally, deploying Artificial Intelligence with comprehensive privacy guardrails enables organizations to leverage LLMs fully without concerns about data leakage.

Compliance and governance: Demand for regulatory compliance is on the rise, with regulations such as Sarbanes-Oxley (SOX), HIPAA, and GDPR forcing companies to carefully monitor their data usage and processing. A GFS should support detailed logging and monitoring of file-related operations, allowing companies to meet the most stringent auditing requirements. Options must also be available to enable data immutability and offer secure deletion.

Protocol compatibility: Migrating from a local to a global file system should not disrupt existing workflows. Traditional protocols (e.g., SMB/CIFS, NFS, S3) used for accessing files on file servers and NAS should continue to operate seamlessly with a GFS in place. Additionally, access policies (e.g., ACL) previously assigned to files should remain intact.

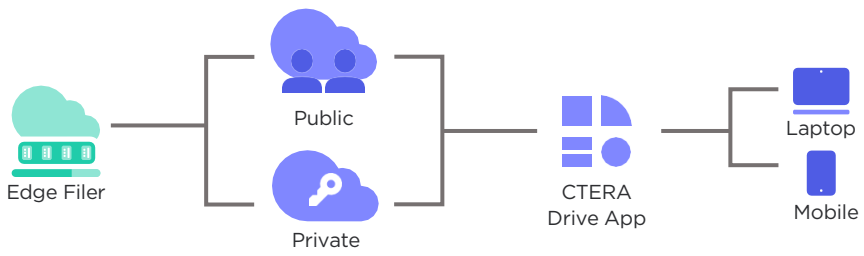
The CTERA Global File System

CTERA Enterprise Data Services are delivered through an innovative Intelligent Data Platform that is built on a hybrid cloud architecture. The innovative hub and spoke data delivery model offers a fully integrated, cloud-native GFS solution designed to meet the needs of the modern enterprise.

CTERA Intelligent Data Platform includes the following components:

- **CTERA Portal:** Facilitates access to cloud storage services; handles data protection and file sync & share services; used for provisioning and monitoring global file services.
- **CTERA Edge Filers:** Virtual appliances that function as “cloud storage gateways” to streamline cloud storage access for remote sites.
- **CTERA Drive:** Endpoint clients that support consistent remote file access and sharing for user workstations as well as mobile apps (smartphones, tablets).

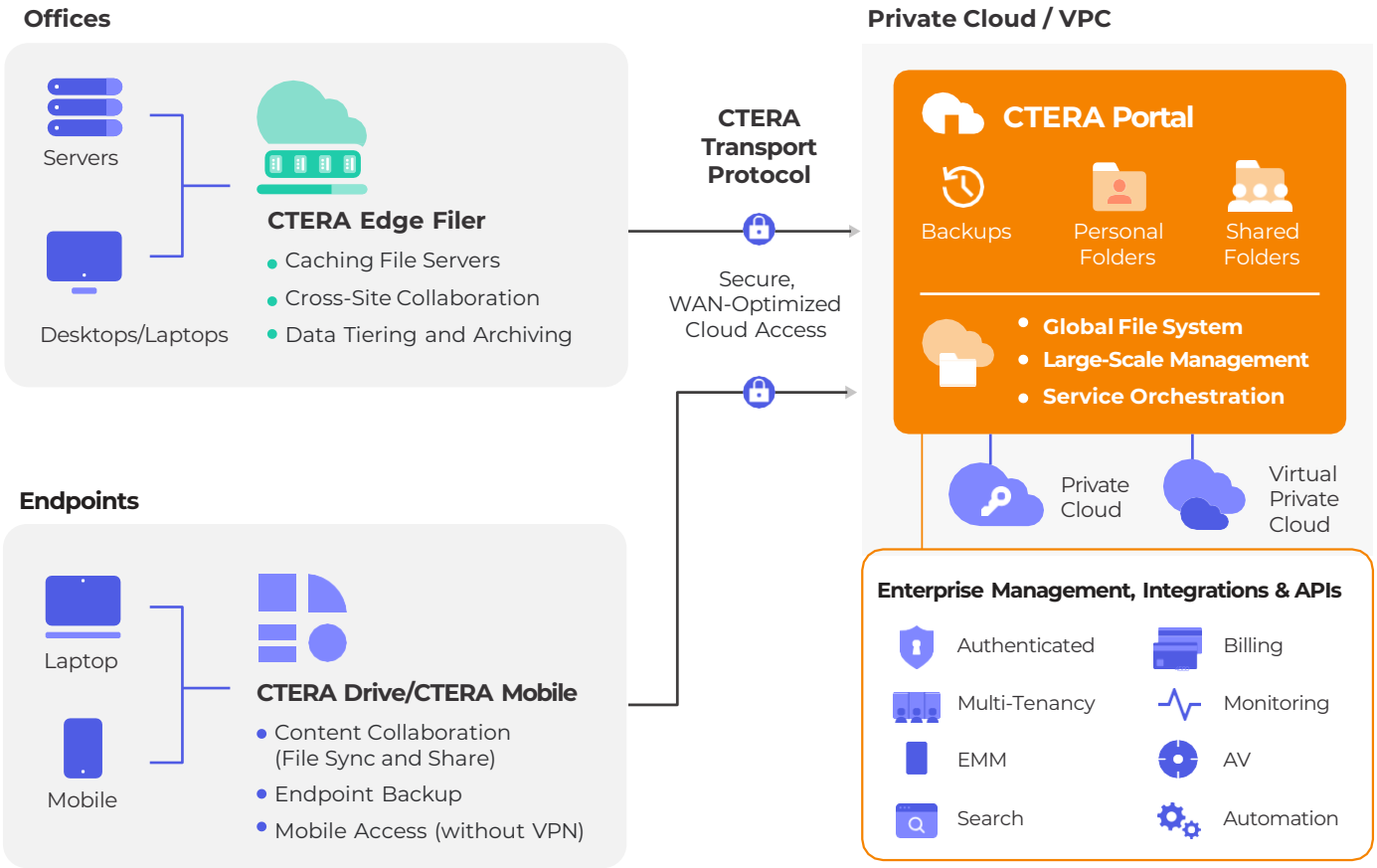
CTERA Global File System & Central Management



Together, these components allow CTERA to offer true enterprise global file services: files are centrally stored and protected while users can easily access them everywhere; CTERA Edge Filers and CTERA Drive clients guarantee fast and secure file access for remote sites and mobile users; and modern content collaboration services allow users to freely sync and share files. These services are offered with total security, featuring military-grade encryption and full control over data residency.

Solution Architecture

Below is the underlying architecture for the CTERA Intelligent Data Platform:



The CTERA Portal is a software service deployed as a virtual appliance. It can run in an enterprise data center (i.e., private cloud) or on IaaS (infrastructure as a service) cloud providers. When using a public cloud service, the CTERA Portal can run in a virtual private cloud (VPC), leaving control over security in customers' hands. CTERA supports a wide range of on-premises and cloud storage infrastructure providers, including Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, HPE, Hitachi Vantara, and others. Customers are free to select their cloud services of choice.

The CTERA Portal software has two main roles: a) it offers a broad range of data management services, such as file storage/retrieval, data protection, sharing, etc., and b) it handles service orchestration tasks, such as assigning storage quotas, configuring remote devices/agents, monitoring, etc. The CTERA Portal comes with built-in integrations with a wide range of third-party services, including Active Directory, various mobile device management (MDM), and antivirus (AV).

CTERA Edge Filers enable sites with bandwidth and/or latency limitations to accelerate and secure remote access to cloud storage. CTERA Edge Filers utilize caching and optimization techniques to deliver the best user experience. They act like a local NAS, supporting traditional file protocols while serving as a "gateway" to cloud storage. CTERA Edge Filers eliminate the need to deploy, configure and manage a local file server. Each filer synchronizes its file content to the cloud, adding the benefit of offsite cloud storage. AI-based ransomware detection and mitigation shut down attacks. The result is a perfect solution for remote site data protection and disaster recovery, all while greatly reducing the costs associated with keeping up with local storage needs.

CTERA Drive is installed on user workstations, enabling file sync and share (FSS). When installed on mobile devices (iOS, Android), they offer simple access to centrally managed files and FSS services. The built-in integration with Microsoft Office Online Server (OOS) allows users to create a file on their desktop, modify it using their smartphone, and then access it via a browser. This enables true access anytime, anywhere, for any device workflow. With CTERA Drive Connect, both Mac and Windows users can take advantage of dynamic caching while full ACL support ensures consistency between SMB and remote desktop users.

CTERA DevOps SDK provides a powerful toolset to automate CTERA Portal and CTERA Edge Filer deployments and tasks, greatly reducing administrative overhead and repetitive tasks while ensuring consistency of configurations across the organization.

Aside from offering "all-in-one" Enterprise Data Services, the CTERA Intelligent Data Platform has several unique attributes:

Military-grade security: A private and secure architecture powered by end-to-end encryption, zero-trust authentication, antivirus, and fully private or air-gapped deployment.

AI ransomware and exfiltration detection & mitigation: Shut down attacks before they impact your organization, ensuring your data and reputation remain protected.

Global deduplication: Most modern storage solutions apply deduplication only to centrally stored files. CTERA has taken this concept to the next level by implementing deduplication at both the cloud and edge. Not only does the CTERA Portal support global deduplication, but CTERA Edge Filers and CTERA Drive also provide clients with source-based deduplication, greatly reducing the size of files sent to the cloud and substantially lowering storage costs.

WAN optimization: To overcome bandwidth and latency limitations, a slew of optimization techniques are used to reduce file sizes and transfer times to/from any access point. High resiliency to latency allows synchronization to function effectively, even in remote or challenging edge sites.

Intelligent caching: Every CTERA Edge Filer and CTERA Drive application includes a built-in file cache. Caching accelerates remote access while enabling access points to "view" the entire file storage space, allowing on-demand access to all available files.

Cloud neutrality: The CTERA platform is cloud-agnostic. It works with multiple cloud providers, empowering customers to select any cloud service, combine multiple services, or migrate between them. The platform offers full flexibility with no vendor lock-in.

Cloud control: With CTERA Zones, edge devices are only aware of specified data, enhancing governance and keeping synchronization efficient. Meanwhile, CTERA Storage Routing lets you store blocks strategically to fully leverage multi-cloud flexibility and vendor agnosticism.

Built-in discovery and migration toolsets: With CTERA Migrate, the CTERA Edge Filer becomes an adept data migration device with advanced reporting and informative graphical metrics for effortless understanding of datasets. Bringing your data into a modern enterprise data services platform has never been easier.

Global File Locking: Many workflows demand reliable and scalable file locking, while others may be impeded by it. With CTERA, Global File Locking can be enabled not only for specific folders, but also for specific file types, offering the ultimate control all within a 100% private deployment.

Central monitoring: The CTERA Portal features activity dashboards and analytics, allowing administrators to observe, monitor and troubleshoot every aspect of their GFS. With CTERA Insight, these metrics become exponentially more powerful for the visualization of both macro- and micro-level operations and trends.

Multi-tenancy: File services can be easily partitioned into multiple tenants – each with dedicated storage and service settings. Service providers with multiple external customers, or IT organizations serving different departments (each viewed as an internal customer), can provision and manage file services per "customer."

Horizontal scalability: The CTERA platform effortlessly scales from one to tens of thousands of users and sites. It is actively used in massive 50PB+ deployments. CTERA Edge Filers are highly efficient in CPU, RAM, and storage utilization, boasting excellent resource/user ratios.

IT-as-a-Service: CTERA supports financial procedures with capabilities such as user quotas, chargebacks, and billing APIs, which are all ideal for both service providers and enterprises implementing cross-departmental IT charges.

Automation and orchestration: Managing a large global file system with thousands of access points and tens of thousands of users can be challenging. To simplify this process and support scalability, the CTERA Portal includes advanced management tools, including template-based automation and a powerful DevOps SDK.

A "Security First" Foundation

Files may contain sensitive data, such as intellectual property, know-how, or customer information. As such, they must be protected from global theft, leakage and loss. Founded by security veterans, CTERA has adopted a "security-first" approach for its GFS platform.

Key highlights:

- **100% private installation option:** The CTERA Portal, the heart of its GFS, can be installed either on-premises or at a virtual private cloud (VPC), allowing customers to maintain full control over all data, security, and access rights.
- **Source-based encryption:** Files are encrypted by the CTERA GFS right at their source. Every file is fully encrypted – at rest – wherever it is stored (AES 256), or when transmitted – in transit – across the network (TLS/ SSL).
- **Private key management:** Encryption keys are created and managed by customers and never leave their control. Strong authentication: CTERA supports the most advanced user authentication and authorization schemes, including Active Directory (AD), two-factor authentication, and smartcards/ military common access cards (CAC).
- **Full ACL support:** File access rights have been traditionally enforced by access control lists (ACL). CTERA handles the migration and support of previously defined Windows NT ACLs, and continues to enforce them at both the filer, client, and browser levels.
- **File-sharing policies:** CTERA supports fine-grained policies for file sharing, based on file names, users or user groups. Native integrations: Platforms like Splunk and Varonis are supported to help enable powerful auditing in compliance with industry requirements.
- **Centralized antivirus (AV):** The CTERA Portal can be configured to work with third-party antivirus utilities, allowing easy quarantining of infected files. Bitdefender AV protection at the edge quarantines infected files before they reach your GFS.
- **AI ransomware protection, and exfiltration prevention at the edge:** CTERA Edge Filers stop attacks before they spread and notifies your security team of the event.
- **Remote wipe:** The platform supports global file access, including via mobile devices. CTERA Drive can be instructed to delete file content in the event of a user losing their phone or laptop.
- **Compliance:** The CTERA Intelligent Data Platform is designed to meet the requirements of a broad range of data privacy and data security regulations (e.g., FIPS 140-2, HIPAA, GDPR and more).

“Caching Everywhere”

CTERA has fully embraced caching technology and applies it throughout its GFS architecture. Both the CTERA Edge Filers and CTERA Drive applications have built-in caching technology. Whether you work at a remote site, use your laptop on the go, or access content via your smartphone, caching ensures efficient file access.

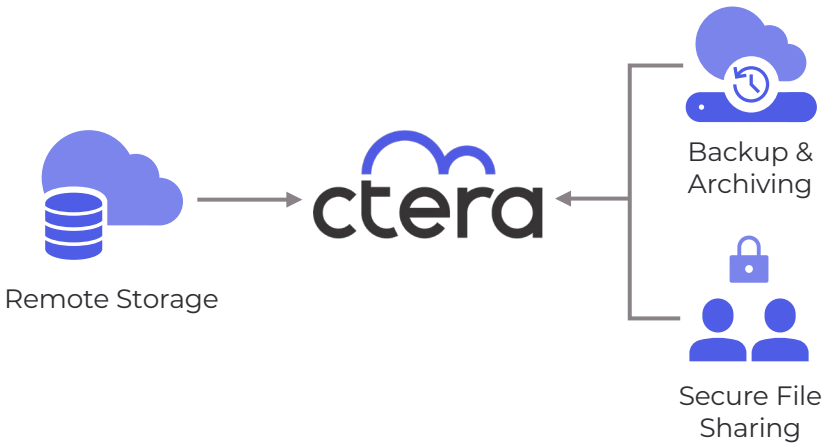
The first obvious benefit of caching is reduced response time. Retrieving a file from the cloud often involves pulling its content over a long network link. Bandwidth and latency limitations may cause lengthy “read” operations. Keeping a “local copy” of frequently accessed files eliminates the need to retrieve the same data repeatedly, thus accelerating “read” operations. Caching also streamlines “write” operations; clients can quickly update the local cache while letting the system handle in the background the lengthier process of uploading the new data to the cloud.

CTERA effectively handles file consistency: it ensures that whenever a file is read by a client, its latest version is indeed served. And when a client updates a file locally, its cloud source is quickly updated. Global File Locking can be enabled to prevent simultaneous updates by multiple clients, or the CTERA Portal will automatically create file versions, eliminating any risk of data loss.

Caching has another important benefit: it allows clients to access a virtually unlimited file storage space. CTERA Edge Filers and CTERA Drive applications provide full access to directory and file attributes information (aka “metadata”). Metadata represents a fraction of the size of the dataset, even for extremely large file repositories. Metadata enables users to easily retrieve any file visible to them – based on permissions. The local cache stores only the most frequently accessed files, or files “pinned” by users, thus enabling access to extremely large file repositories while requiring a modest amount of local storage.

This capability relieves administrators from the need to regularly upgrade storage capacity at remote sites or on users’ workstations. The cloud repository size may grow exponentially over time, but the amount of storage used by the CTERA cache remains fairly constant.

Suppose you invested in deploying a GFS. How would your life and your users’ lives change? To answer this question, let’s examine a few use cases for the CTERA platform:



Remote-Office filers: In a globally distributed enterprise, many users work at remote offices. Traditionally, addressing their file storage needs meant deploying a file server or a NAS at each office. Those devices had to be continuously maintained and regularly upgraded. To further complicate matters, all the data stored on them had to be backed up and transferred offsite.

With the CTERA solution, simply deploy a CTERA Edge Filer at a remote site. Users will have access to a familiar-looking NAS, but all data will be automatically synched to the cloud. No need to worry about complicated backup processes or specialized DR plans. At remote locations with challenging connectivity, like construction or mining sites, WAN optimization and the CTTP protocol offer a resilient solution that synchronizes reliably despite latency constraints.

Cross-site collaboration: Sharing files between users has traditionally been a complex/inefficient process, a security challenge, or both. Setting up a file server with ever-changing access rights is a pain. As exchanging files through emails is inefficient and leakage prone, using external file-sharing services comes with significant security risks.

CTERA offers an intuitive and secure file sync & share (FSS) service. The service is built into its CTERA Drive apps and CTERA Edge Filers. It is therefore available to any user, at any site, using any device. Simple, fine-grained sharing controls guarantee information security without sacrificing ease of use.

Home folders: CTERA lets users maintain their personal home folders from anywhere while automatically protecting them in the cloud. Users can seamlessly access their files via a CTERA Drive app installed on their workstation or mobile device, or via their office CTERA Edge Filer. The FSS service offers access to personal files anywhere and the ability to share them with others when needed. Gone are all the complexities associated with protecting and managing users' home folders!

File data tiering and archiving: Leverage a CTERA Edge Filer or CTERA Drive to ingest local file data and tier it to lower-cost object or cloud storage. The platform also supports file data archiving, providing a local view of cloud archival data (via stubbing) that can be accessed whenever needed. With CTERA storage routing, file blocks can be written to specific buckets based on need.

Content distribution: Enterprises often need to make file-based content available to users globally. Examples include project documents, enterprise information broadcasting, marketing materials, etc. Replicating this content to every remote site is a time- and resource-consuming process.

With the CTERA GFS, all that's needed is to place the desired content in a shared folder. Users throughout the distributed enterprise immediately "see" the new content via their CTERA Drive app or CTERA Edge Filer. There's no need to "push" the content to remote locations ahead of time. The built-in syncing and caching mechanism can easily handle on-demand access to new content.

Services Excellence

Incredible technologies are nothing without service and support levels to match. CTERA Global Services is built on a foundation of customer empowerment and trust building. Deployments see white-glove installations, data transfers and cutovers, greatly reducing project complexity and removing impediments to file services modernization.

CTERA Global Support teams span every time zone as a team of highly skilled and experienced engineers ensure that customer business objectives remain our highest priority.

Summary

Modern enterprises can't afford storage architectures built for a bygone era. Data must move at the speed of business — securely, intelligently, globally.

CTERA's Global File System delivers the foundation for resilient, high-performance, future-ready operations. It consolidates silos, enables seamless collaboration, safeguards data, and positions enterprises to unlock value from their unstructured data through secure AI readiness.

Ready to transform your enterprise data strategy?

Speak to a CTERA expert today.

Speak to an Expert

Calculate the infrastructure cost savings offered by CTERA in comparison to other file storage alternatives.

Calculate TCO

Request a Demo

www.ctera.com info@ctera.com USA: (917) 768-7193 Intl.: +972-3-679-9000