PANZURA

PANZURA CLOUDFS SOLUTION BRIEF

Media and Entertainment

With the relentless increase in resolution and complexity of media assets – from raw camera footage and intricate VFX renders to high-fidelity audio masters – editing, real-time collaboration across distributed teams, and rapid file transfers between studios and remote artists have become bottlenecks, leading to project delays and escalating costs, all while raising critical security concerns.

The iterative nature of media and entertainment (M&E) content creation can generate millions of files within a single project. The common practice of replicating these massive datasets across geographically dispersed post-production houses, VFX studios, and broadcast facilities often consumes vast amounts of valuable storage.

These fragmented on-premises storage silos severely restrict collaborative workflows, forcing remote editors, animators, and VFX artists to contend with slow access times, hindering their productivity. Consequently, the exponential growth of media data has compelled technology teams to explore the seemingly limitless scalability of the public cloud to augment or replace their existing infrastructure. While the public cloud offers vast storage capacity, it often introduces new challenges for high-performance access to multi-gigabyte and terabyte-sized media files. Remote editing suites, animation studios, and sound design teams frequently experience sluggish file access and operational delays, directly impacting project timelines and potentially jeopardizing release schedules for films, episodic content, and games.

In an industry where the seamless collaboration of distributed creative teams on shared media assets is paramount for meeting demanding production schedules, overcoming the performance bottlenecks associated with cloud storage is not just desirable – it's a critical necessity. The inability for geographically separated artists and technicians to collaborate efficiently on massive media files, coupled with slow transfer times, directly limits the utilization of your talent pool, stifles creative iteration, and increases the risk of missing crucial delivery deadlines.

Beyond the sheer scale of data management, the escalating threat of piracy, pre-release leaks, and ransomware attacks targeting high-value media assets and intellectual property has become a top priority for M&E technology teams. Ensuring robust resilience against these sophisticated threats adds significant complexity for organizations seeking a comprehensive data protection strategy.

While the initial allure of cloud migration for resolving storage silos and capacity limitations seems appealing, many M&E companies find that it introduces new challenges, notably performance bottlenecks for demanding workflows and unpredictable, often exorbitant, cloud egress fees associated with frequent data access. In an industry where every minute of production time translates directly

to revenue, the speed and responsiveness of the underlying file system to keep pace with intensive content creation demands are absolutely critical.

IThis solution brief details how Panzura empowers media and entertainment organizations to overcome the intricate and rapidly evolving challenges of managing their digital content. We will explore how our platform addresses the explosive growth of high-resolution media files, enforces stringent content security protocols, safeguards valuable intellectual property, ensures seamless interoperability across a diverse ecosystem of production tools and platforms.

Consolidating Distributed Mega-Sized Media Files

The ever-increasing size of the files you work with means there's a constant need for more capacity. Traditionally, on-premises media storage was deployed and dedicated as a repository for specific applications such editing, compositing, graphic creation, playout and so on. As applications and users multiplied, storage silos proliferated as well.

Although each site would function individually, data efficiencies were not addressed at the global level, meaning duplicated files could reside at each site and – depending on the type of deduplication process in use – within each storage volume. All solutions do not deduplicate data in the same way. This really matters, as the outcomes of the different approaches are completely different. Using volume deduplication for example, duplications will be identified and removed within each volume.

However, that still means a storage repository with 100 volumes can have the same single "deduped" file in each one of those volumes. This can consume an enormous amount of unnecessary storage space. For example, if a 10GB file exists in each of the 100 volumes, that single file occupies 1TB of total capacity. By contrast, global deduplication looks across an entire file system, removing redundant copies and leaving just one authoritative copy of that file. With global deduplication, that same 10GB file will occupy just 10GB of storage. Panzura CloudFS consolidates distributed multi-media data into a single, authoritative data set that is visible and accessible across the organization.

Minimizing Duplication

CloudFS deduplicates redundant data before moving it to your chosen cloud or object store, using global deduplication. Panzura doesn't simply deduplicate files though. Instead, CloudFS looks at the data blocks that comprise files, and deduplicates at the block level. That means that files that contain identical elements, e.g. logos, watermarks, and other re-used assets also benefit from deduplication, even though the files themselves are not identical. This can allow you to realize a very significant reduction in your overall data footprint. CloudFS maintains this globally deduplicated data set at all times, checking for redundancies every time it moves data into your cloud storage.

Accessing Data in Real Time

With CloudFS, your creative teams, regardless of location, access a single, authoritative source of your valuable media assets residing in your chosen cloud or object storage. This seamless integration requires no disruption to existing workflows or changes in user habits. Artists interact with their video, audio, and graphics files with the same responsiveness they experienced with local storage. This means that opening and saving even massive project files occurs with the speed and efficiency they expect.

Maintaining Immediate File Consistency

CloudFS stands as the industry's fastest global file system, ensuring that edits to even the largest media files are instantly visible to all authorized users, no matter the number of studios, broadcast centers, or remote teams involved, or the geographical distances separating them. Forget about

cumbersome scheduled file replications between sites. Panzura's real-time file consistency guarantees that every user always works on the most up-to-date, authoritative version of any asset, complete with the latest modifications.

Empowering Collaboration

CloudFS revolutionizes how geographically dispersed teams collaborate on media projects. For compatible creative applications, Panzura automatically locks a file the moment it's opened for editing, preventing simultaneous, conflicting writes. Furthermore, for applications supporting byte-range locking (common in many media tools), Panzura enforces this granular control. This allows multiple artists to work concurrently within the same complex file, while securely locking the specific elements they are actively modifying. This fosters a real-time, co-located editing experience, even when team members are located across continents.

Transferring Large Files, Fast

CloudFS ensures rapid availability of even the most substantial video and high-resolution media files across all connected locations. Panzura's intelligent compression techniques minimize the volume of data that needs to be transferred at any given time, all without any degradation in the original media quality. This accelerates content sharing for reviews, approvals, and distribution workflows.

Keeping Data Protected

CloudFS provides inherent protection against accidental file deletion or corruption stemming from malware or ransomware attacks through its resilient data architecture. All data managed by CloudFS is stored in an immutable – Write Once, Read Many (WORM) – format. Once an asset is committed to your object storage, it cannot be altered or overwritten.

Every new edit or newly created file is stored as distinct data blocks. Consequently, in the event of a malware or ransomware incident, the existing, pristine media assets remain untouched and recoverable, as the malicious software cannot modify the immutable data.

Catch and Stop Ransomware

An extended capability of the CloudFS hybrid cloud platform, Panzura Detect and Rescue identifies ransomware in real time and stops it automatically by switching off the affected users, followed by a comprehensive ransomware tracker to help administrators rapidly identify and recover damaged files. Meanwhile, CloudFS's data insights and intelligence layer — Panzura Data Services — enables configurable alerting on suspicious user behavior, e.g. multiple file copy or move actions that may indicate data exfiltration.

Restore Damaged or Lost Data

In the event of any file damage – whether caused accidentally or as part of a wider encryption attack such as a ransomware event – individual files, folders, or the entire file system can be restored to a pristine state with no data loss, and minimal disruption.

Read-only system snapshots are taken on a scheduled basis, and record the file system at that point in time. Additionally, snapshots are taken at every site location in the CloudFS every 60 seconds. This provides the ability to restore any file to any point in time as required.

Ensure Data Compliance

CloudFS provides your organization with Cyberstorage, seamlessly integrating NIST Cybersecurity Framework functions directly into your storage infrastructure. This strengthens your overall security

posture with a multi-layered defense, purpose-built for protecting high-value media assets. By leveraging Cyberstorage, you can ensure your organization remains secure and compliant with evolving industry standards and client expectations throughout the entire lifecycle of your creative projects.

With built-in, end-to-end encryption, immutable storage capabilities, and granular access controls, CloudFS rigorously safeguards your critical media assets—including high-resolution video, master audio files, intricate visual effects projects, and sensitive intellectual property like pre-release content and proprietary workflows—against unauthorized access, data breaches, leaks, and sophisticated cyber threats such as ransomware.

FIPS 140-3 certification ensures that your valuable content remains securely encrypted both during transfer and when stored, rendering it unreadable even if intercepted. Strict, role-based access controls, comprehensive audit logs tracking all data access and modifications, continuous monitoring for suspicious activity, and automated compliance tracking further ensure adherence to stringent content protection requirements, contractual obligations, and industry best practices. This proactive approach significantly reduces risks, safeguards your creative investments, and preserves the trust of your clients, distributors, and stakeholders.

Empowering High Availability

CloudFS meets strict requirements for highly resilient, highly available file services. Every location in a global file system always has read access to data from every other location. Data is stored securely in the cloud and each location can read that data. In the event of a disaster in one location, every other location already has access to the data for immediate recovery.

Three options for CloudFS virtual nodes offer high availability to suit your requirements and budget.

1. Local high availability uses an active/passive stand-by pair of nodes that offer rapid failover.
2. With global high availability, in the case of a regional outage, a stand-by node will assume lock management for the failed CloudFS node.
3. Instant Node offers a sub-5 minute recovery, inclusive of boot time, with no dedicated stand-by node required. Instead, Instant Node utilizes available virtual machine CPU and memory.

Cloud Mirroring provides high availability for your object store by enabling a passive, identical copy of your data in a secondary hyperscaler or low cost object store provider such as Wasabi, Backblaze or Seagate Lyve Cloud. In the event of a primary object store outage, all CloudFS nodes will fail-over to the secondary store for read and write operations, with no disruption to users.

Regional Store allows globally dispersed organizations to operate up to 4 active copies of the object store in different cloud regions offered by their choice of AWS or Azure. These regional buckets are synced via the hyperscaler back-end network and allow office locations in each region to read and write data over the shortest possible distance to maximize performance. Should a single object store become unavailable, the CloudFS nodes will fail over to an object store in the next closest region.

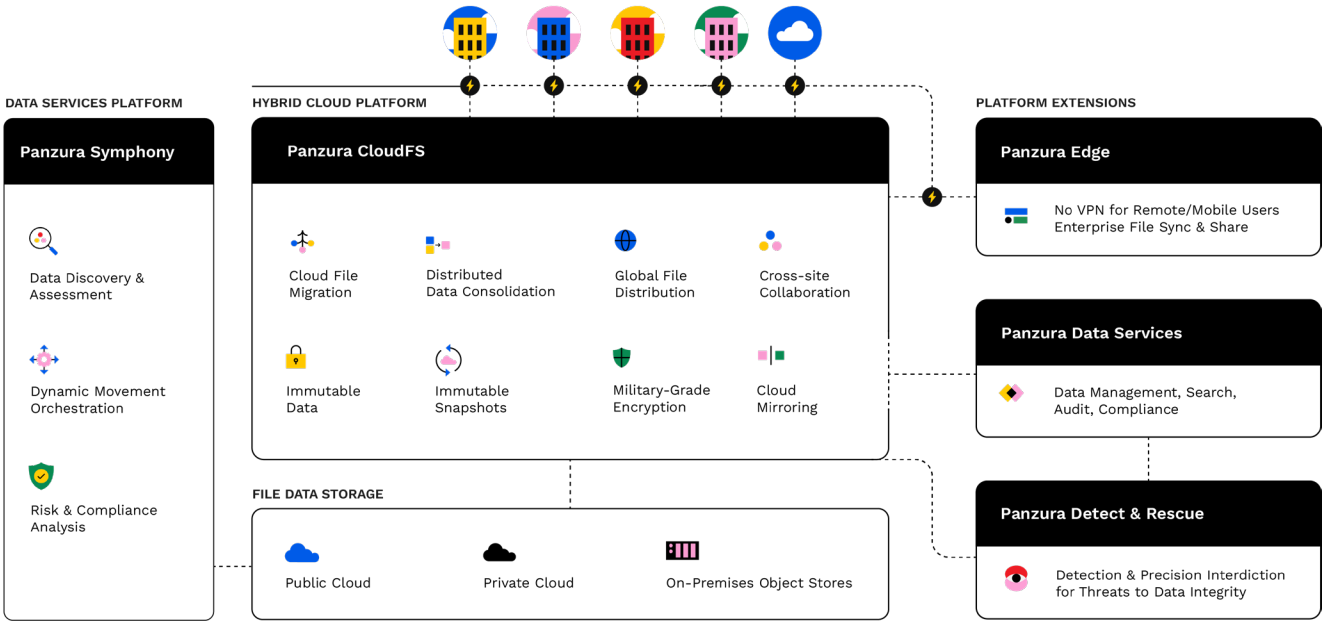
Ready for AI

Accelerate the training of AI models for innovative media applications—such as intelligent content tagging, automated video analysis, personalized content recommendations, and efficient media asset management—by strategically positioning your vast unstructured media datasets closer to your AI and Machine Learning platforms with CloudFS. This includes massive video archives, high-resolution image libraries, extensive audio collections, and complex project files.

To further enhance security and efficiency for advanced AI-driven media workflows, explore how Panzura Symphony functions as a Zero Trust Data Broker, streamlining secure and compliant data access for training your AI models on sensitive content. This ensures your valuable media assets are utilized effectively while maintaining stringent security protocols.

Work with your data, the way that works for you

Every part of Panzura's data management solution has been specifically and intentionally designed to let you put data at the fingertips of the people who need it, the moment they need it, while keeping it secure, protected against threats, and compliant with external regulations as well as internal mandates.



Panzura empowers today's digital-first organizations to do impossible things with file data, making them more agile, efficient, and productive. They trust Panzura to help them consolidate dispersed data, see and manage data in and out of the cloud, make it more cyber-resilient and AI-ready, and ensure it is available to people and processes where and when it's needed.

Discover how Panzura can fuel your success at **panzura.com.**