PANZURA

PANZURA CLOUDFS SOLUTION BRIEF

Healthcare and Life Sciences

Leading healthcare providers and pioneering life sciences organizations rely on Panzura to securely manage and protect their mission-critical data, accelerating breakthroughs in patient care, drug discovery, and genomic research.

The relentless drive for improved patient outcomes, coupled with the exponential growth of diverse datasets – from high-resolution medical imaging and genomic sequencing to clinical trial data and real-world evidence – presents unprecedented challenges for healthcare and life sciences institutions. Ability to effectively manage and leverage this data is no longer just an operational necessity, but a critical factor in competitive advantage and, ultimately, patient well-being.

The sheer velocity and volume of data generated – including multi-terabyte medical images, massive genomic datasets, and longitudinal patient records – are overwhelming traditional storage infrastructures, hindering timely access and analysis crucial for diagnosis and treatment planning. When a radiologist needs immediate access to a high-resolution scan for a critical diagnosis, or researchers require seamless collaboration on terabytes of clinical trial data across continents, the performance and reliability of the underlying data infrastructure become paramount. The burden on IT to ensure this while maintaining stringent security and compliance is immense.

Navigating the complex landscape of regulatory compliance, including HIPAA, GDPR, and other regional mandates for Protected Health Information (PHI) and Personally Identifiable Information (PII), while simultaneously defending against increasingly sophisticated cyber threats targeting sensitive patient and research data, creates a critical need for robust data governance and security.

Whether embracing the scalability of secure public clouds, implementing private cloud solutions, or adopting a hybrid approach, a comprehensive data management strategy is essential to ensure secure access, robust protection, and seamless collaboration across the healthcare and life sciences ecosystem.

In this solution brief, we'll outline how Panzura helps healthcare and life sciences organizations address the complex and evolving challenges related to data storage, protection, access, and management. The escalating data deluge, coupled with stringent regulatory demands, persistent cybersecurity threats, the imperative for seamless data interoperability across disparate systems, and the growing reliance on advanced analytics and AI for drug discovery and personalized medicine, highlights the indispensable need for sophisticated, scalable, and secure data management solutions like Panzura CloudFS.

Consolidate and Control Distributed Data

Traditional on-premises storage architectures struggle to keep pace with the exponential growth of medical imaging archives, genomic sequencing outputs, and research datasets. The endless cycle of capacity upgrades and hardware refreshes drains budgets and IT resources that could be better allocated to innovation.

The common scenario of data silos across hospital departments, research labs, and remote clinics leads to significant data duplication – redundant copies of patient records, imaging studies, and research data consume valuable storage and create inconsistencies, hindering a unified view of information. The proliferation of machine-generated data from diagnostic equipment, laboratory instruments, and wearable devices often remains trapped in localized silos, impeding its integration into centralized data lakes essential for advanced analytics and AI-driven insights in areas like predictive diagnostics and personalized treatment.

Panzura CloudFS, a hybrid cloud file platform underpinned by a global file system, consolidates distributed data into a single, authoritative data set that is visible, and accessible, across the entire organization, facilitating collaboration among multidisciplinary teams, e.g., radiologists, oncologists, and pathologists.

Your Choice of Object Store

CloudFS is compatible with all leading public cloud stores, including AWS, Azure and Google Cloud, as well as on-premises object stores such as Cloudian and IBM, and many others. That gives you the ability to select the storage that best fits your usage, budget, and regulatory requirements now and the flexibility to make a different choice if and when your needs change.

Minimize File Duplication

CloudFS deduplicates redundant data before moving it to your chosen object store, allowing you to realize a 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. This can dramatically reduce storage needs, especially for large medical imaging files and genomic data.

Access Data in Real Time

With CloudFS, all users in your organization work from the authoritative data set stored in your cloud or object store. No changes in workflows, or user behaviors are required – users interact with files in the same way they always have, and CloudFS provides them with a local-feeling file experience. In practice, that means even massive DICOM image sets, whole slide images, or video recordings of surgical procedures open quickly for authorized clinicians anywhere, enabling timely consultations and collaborative diagnoses.

Maintain File Consistency

CloudFS makes files and file edits immediately visible everywhere, as soon as they are stored or saved. This real time file consistency, across every location in the global file network, means that users can rely on opening the authoritative patient file every time, reducing the risk of errors in diagnosis or analysis.

Seamlessly Move Critical Applications to the Cloud

With Panzura, there's no need to rewrite legacy applications to support your move to the cloud. CloudFS provides the critical translation between files and cloud or on-premises object storage, allowing you to migrate even your most critical workflows without changing applications, or the way your users work.

Finding Files At Speed

Panzura Data Services allows you to rapidly ingest and query billions of files from multiple sources, giving you a powerful search engine to find anything in just moments, regardless of where it's stored.

Make Data Resilient Against Damage

CloudFS protects against ransomware and other data damage or deletion by making data immutable so it cannot be changed. Every 60 seconds, every location syncs data into the object store simultaneously, where it is stored in a Write-Once, Read-Many (WORM) format and further protected by global, immutable snapshots so a global recovery point is never more than 60 seconds away. Files, folders, or the entire file system can be restored to a precise point in time.

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 equips you with cyberstorage, which incorporates NIST cybersecurity functions into storage, strengthening your security posture with multiple layers of defense and resilience. Using cyberstorage ensures your organization remains secure and compliant by providing advanced data protection and management throughout every phase of your projects. With built-in end-to-end encryption, immutable storage capabilities, and granular access controls, CloudFS safeguards critical patient data against unauthorized access, breaches, and cyber threats such as ransomware attacks.

FIPS 140-3 certification ensures data remains securely encrypted both in flight and at rest, making it unreadable even if intercepted. Strict access controls, audit logs, continuous monitoring, and automated compliance tracking further ensure adherence to HIPAA's stringent security and privacy requirements, reducing risks and maintaining patient trust.

Empowering High Availability

CloudFS meets strict regulatory requirements for highly resilient, highly available file services, ensuring uninterrupted access to critical patient data and research information to provide continuity of care and prevent delays in crucial workflows. Every location in a global file system always has read access to data from every other location. Data is stored securely in the centralized object store 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. Local HA uses an active/passive stand-by pair of nodes that offer rapid failover. With Global HA, in the case of a regional outage, a stand-by node will assume lock management for the failed CloudFS node. 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.

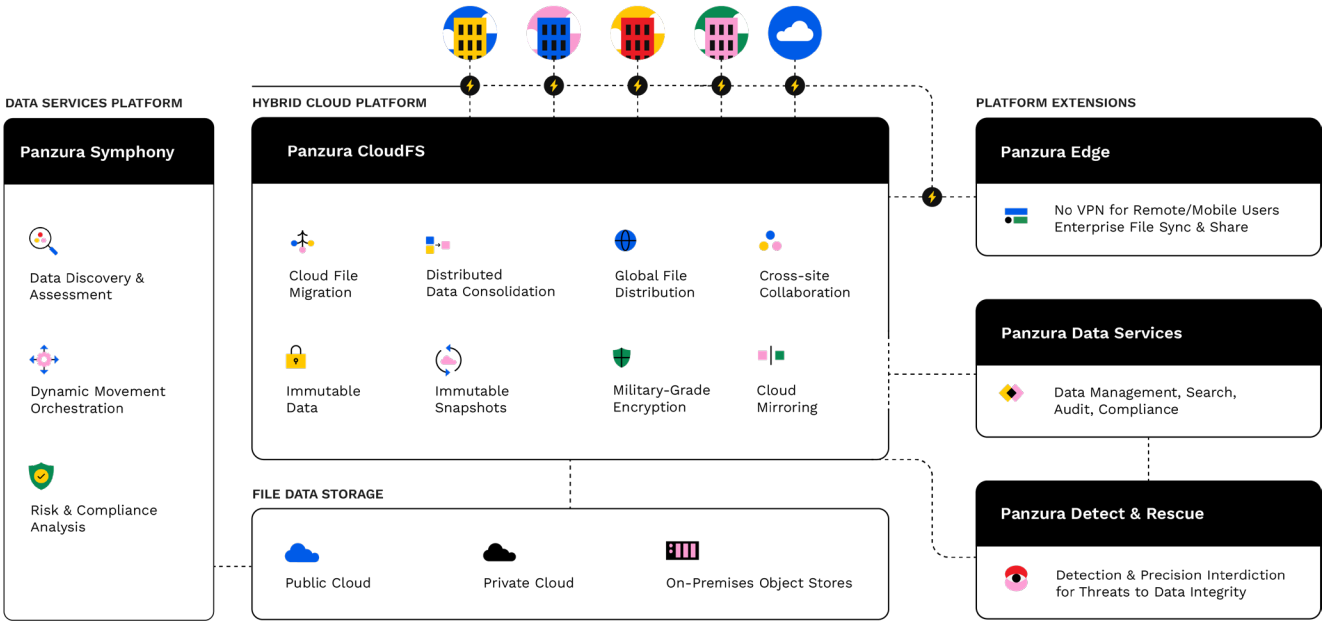
Regional Store allows globally dispersed organizations to operate up to 4 active copies of the object store in different cloud regions offered by their choice of AWS or Azure. These regional buckets are synced via the hyperscaler back-end network and allow office locations in each region to read and 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 applications like medical image analysis, drug discovery, and predictive diagnostics by strategically positioning vast unstructured datasets – including imaging, genomic sequences, and clinical notes – closer to your Large Language Models (LLMs) with CloudFS. To further enhance security and efficiency for advanced AI use cases, take a look at how Panzura Symphony functions as a Zero Trust Data Broker, streamlining secure data access for training your LLMs.

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.**