PANZURA

PANZURA CLOUDFS SOLUTION BRIEF

Government and Public Sector

The IT landscape for public sector and government organizations has never been more complex. Faced with exponentially increasing volumes of data, often siloed across various departments and agencies, a comprehensive data management approach is no longer optional – it's essential for effective governance and service delivery.

The sheer scale of data being generated daily strains already tight resources. The common practice of creating multiple copies for essential functions like backup, disaster recovery, and compliance with mandates such as the Federal Records Act, HIPAA (where applicable), and state- or region-level data retention policies can lead to a fivefold increase in storage, placing immense pressure on IT budgets and personnel tasked with managing these vast, security-sensitive datasets.

Furthermore, maintaining strict regulatory compliance and safeguarding sensitive data against increasingly sophisticated cyber threats pose significant risks and add layers of complexity to IT operations. Government agencies are particularly vulnerable to attacks targeting citizen data, critical infrastructure, financial, and national security information.

Whether your agency is leveraging approved cloud services (FedRAMP-certified) or establishing a secure private cloud with on-premises object storage, a robust data management strategy is paramount for securing, protecting, and efficiently distributing information to the personnel who need it.

This solution brief outlines how Panzura CloudFS helps public sector and government organizations address the intricate and evolving challenges of data storage and management. The rapid growth of sensitive citizen information, stringent compliance with regulations like the Federal Records Act and state-level data protection laws, the constant threat of cyberattacks, the critical need for interoperability across diverse governmental platforms and agencies, and the increasing adoption of analytics and AI for improved public services underscore the indispensable need for advanced, scalable, and highly secure data solutions tailored specifically to the unique demands of public sector and government organizations.

Consolidate File Shares

Data distributed across multiple storage devices, and often across multiple locations, is prone to a significant amount of duplication as multiple copies of similar and identical files occupy storage space. While cloud storage presents with a cost-effective pricing structure, simply lifting and shifting that data

into the cloud replaces one set of data islands with another. Performance problems working with cloud-stored data, coupled with storage inefficiencies and lack of visibility can quickly render a cloud move ineffective. Panzura CloudFS consolidates distributed data into a single, authoritative data set that is visible, and accessible, across the organization.

Reduce Storage and Restrict Data Growth

CloudFS translates files to objects and deduplicates redundant data blocks at the most granular possible level — blocks of just 128kb in size — before moving them to your chosen cloud or object store. Its global deduplication method runs advanced, inline block-level deduplication on any data in the object store, checking for redundancies every 60 seconds, before it moves data into your object storage. On average, CloudFS customers reduce their overall data volume by 35%, ranging up to 80%.

Maintain File Consistency

CloudFS makes file edits immediately visible everywhere, as soon as they are saved. This real time file consistency, across every location in the global file network, means that users can rely on opening the authoritative file, complete with any changes, at all times.

Empower Collaboration

For workloads that require people to work together on the same files, without running over the top of each other, CloudFS empowers cross-site collaboration to meet security compliance in a way nobody else can. Instantaneous, automatic file locking locks down a file for editing the moment it's opened. When using applications that support element or byte-range locking, such as Microsoft Excel, CloudFS allows multiple users to work within the same file, without overwriting each other. It's the same file experience users have when they're sitting in the same office location, even if they're thousands of miles apart.

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 a data block is committed to your object storage, it cannot be altered or overwritten.

Every new edit or newly created file is stored as new data blocks, which never overwrite existing blocks. Consequently, in the event of a malware or ransomware incident, the existing, pristine data remains 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 global 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, with a global recovery point that is never more than 60 seconds.

Ensure Data Security and Regulatory Compliance

Using cyberstorage ensures your organization remains secure and compliant by delivering robust data protection and secure management at every stage. With built-in end-to-end encryption, immutable storage capabilities, and granular access controls, CloudFS safeguards critical government data—including citizen records, classified information, operational documents, and sensitive communications—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. Continuous monitoring and automated compliance tracking further ensure adherence to stringent governmental regulations and security standards, reducing risks, protecting public trust, and enhancing operational integrity.

Secure Erasure

Secure and complete document erasure is made possible through CloudFS Secure Erase and is the highest purge level that can be attained without physically destroying the disk. Secure Erase is able to delete all traces of legal records stored in the cloud and follows the guidelines for media sanitization as set out in the Special Publication 800-88 of the National Institute of Standards and Technology (NIST).

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

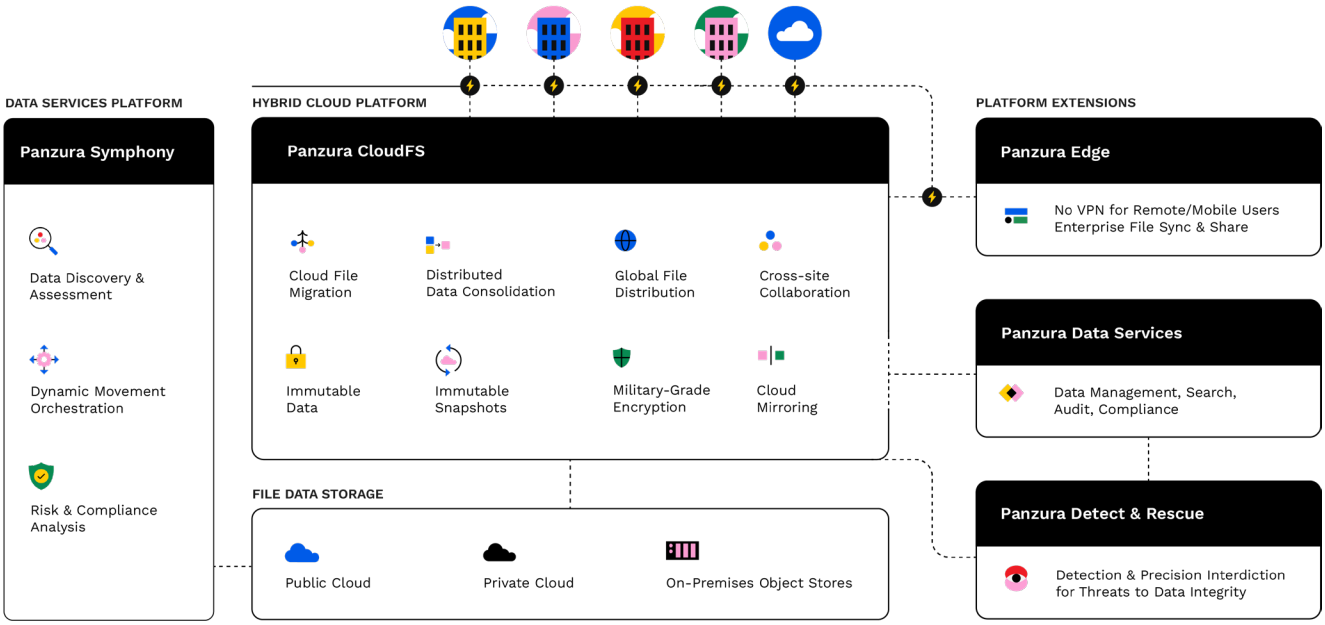
Accelerate AI training on unstructured data by strategically positioning your data closer to your Large Language Models (LLMs) with CloudFS. If you're using a cloud-based AI solution hosted by the same provider as your object storage, simply deploy a CloudFS node within the same cloud region. This setup

allows you to leverage CloudFS's S3 interface to efficiently scan your file system without incurring egress fees.

For on-premises LLM deployments with cloud-based object storage, be aware of potential egress fees, or opt for an object store provider that offers zero egress charges. To further enhance security and efficiency for advanced AI use cases, refer to Panzura's solution brief onhow Panzura Symphony functions as a Zero Trust Data Broker, streamlining secure and compliant data access for training your AI models on sensitive content.

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.**