Panzura CloudFS vs. Egnyte

CloudFS Offers True Data Ownership and Control, Real-Time Collaboration, Enterprise-grade Security, and Lower Overall TCO.

Panzura CloudFS is built from the ground up on a true global file system architecture, which is a key differentiator from Egnyte's sync-based model. The following comparison tables highlight that CloudFS provides a single authoritative data source, real-time global and byte-range locking, and zero version conflicts by design. This contrasts with Egnyte, which lacks these capabilities and may lead to manual conflict resolution. Furthermore, CloudFS enables a unified global namespace and is designed for the hybrid and multi-cloud era, ensuring immediate data consistency and the ability to prevent data corruption from sync conflicts, which are not features of Egnyte's sync-based approach.

In terms of cost, resilience, and data control, CloudFS offers distinct advantages. The comparison tables show that CloudFS provides global variable-block deduplication and cross-site data redundancy elimination, leading to significant storage volume and WAN bandwidth reductions. For data resilience, CloudFS offers immutable snapshots every 60 seconds with a near-zero RPO, and it includes automated AI-powered threat interdiction. This is a stark contrast to Egnyte's standard reliance on 4-hour snapshot intervals and the potential need for manual recovery. Moreover, CloudFS provides superior data sovereignty by allowing customers to own and manage their encryption keys and choose their data storage location, eliminating vendor lock-in and allowing for true multi-cloud arbitrage.

Learn More

Go deeper by downloading the full Panzura CloudFS vs. Egnyte whitepaper.

Looking to take control of your file data? Contact a Panzura expert for a non-obligation demo.

Already a Panzura customer? Talk to your Customer Success Manager about how you can get even more out of your CloudFS investment.

panzura.com

File Locking and Conflict Resolution Comparison

Egnyte	Panzura CloudFS
While Egnyte provides file sharing capabilities, its sync-based architecture can create situations where multiple users work on local cached versions. When changes are synchronized back to the cloud, conflicts may require manual resolution.	Real-time global file and byte-range locking ensures that when a civil engineer in Chicago opens a CAD file, colleagues in other offices see that sections are locked for editing. This prevents the frustrating scenario where two team members modify the same component, requiring manual conflict resolution later.

Architectural Comparison

Underlying Design	CloudFS	Egnyte
Single source of truth architecture	✓	No
Real-time global file locking	✓	No
Byte-range locking for simultaneous editing	✓	No
Zero version conflicts by design	✓	No
Immediate data consistency	✓	No
Direct peer-to-peer data exchange	✓	No
Eliminates manual conflict resolution	✓	No
Unified global namespace	✓	No
Cloud-native file system architecture	✓	No
Prevents data corruption from sync conflicts	✓	No
Multi-site file sync and share	✓	✓
Local caching for performance	✓	✓
Cloud storage integration	✓	✓
Simultaneous file and object access via S3 interface	✓	No
VPN-less access	✓	✓

Cost Optimization Comparison

Capability	CloudFS	Egnyte
Global variable-block deduplication	✓	No
Cross-site data redundancy elimination	✓	No
WAN bandwidth reduction (35-85%)	✓	No
Eliminates full file re-transfers for minor changes	✓	No
Single-instance storage across all locations	✓	No
Storage volume reduction (70-80%)	✓	No
Immediate write-time deduplication	✓	No
Zero egress costs for in-region AI/ML	✓	No
Dynamic block-level caching	✓	No
Local storage footprint reduction (35-85%)	✓	No
Intelligent data transfer optimization	✓	No
Chunky deduplication	Admin Defined	✓
Smart caching for frequently accessed files	✓	✓
Cloud storage integration	✓	✓

PANZURA

Data Resilience Comparison

Capability	CloudFS	Egnyte
Snapshot Protection		
60-second Immutable Snapshots	✓	No
Truly Immutable (Ransomware-proof)	✓	No
4-hour Vulnerability Windows	No	✓
Recovery Performance		
Near-zero RPO (60 seconds max data loss)	✓	No
Automated threat interdiction	✓	No
Manual recovery intervention required	No	✓
Hours-long restoration processes	No	✓
Business Continuity Architecture		
Built-in BC/DR (no separate solution)	✓	No
Every node is active DR site	✓	No
Sub-5-minute automated failover	✓	No
Requires separate BC/DR solutions	No	✓
Multi-data center dependency	No	✓
Advanced Capabilities		
Immutable snapshots across entire global system	No	✓
Automated threat interdiction	No	✓
Single integrated platform	No	✓
Eliminates traditional backup dependency	No	✓
Instant clean data restoration	No	✓
Behavioral fingerprinting and workflow awareness	No	✓

Competitive Intelligence and Multi-Cloud Strategy Comparison

Capability	CloudFS	Egnyte
Data Control & Ownership		
Customer always owns and manages encryption keys	✓	No
Customer chooses data storage location	✓	Limited
Data remains truly portable	✓	No
No vendor permission required for data movement	✓	No
Regulatory Compliance		
Granular control over data placement by jurisdiction	✓	Limited
Unified global file system with localized data	✓	No
Rapid response to evolving regulations	✓	No
Avoids costly compliance migrations	✓	No
Cloud Strategy & Economics		
True cloud agnosticism	✓	No
Multi-cloud arbitrage capabilities	✓	No
Direct hyperscaler negotiations	✓	No
Security Architecture		
Zero-trust data architecture alignment	✓	No
Customer-controlled cryptographic security	✓	No
Eliminates trust amplification risk	✓	No
Reduced supply chain attack surface	✓	No
Operational Independence		
Avoids sovereignty debt accumulation	✓	No
No vendor lock-in for data access	✓	No
Freedom to bring data back on-premises	✓	No

PANZURA

AI-Ready Feature Comparison

Feature	CloudFS	Egnyte
Data Architecture for AI		
Cloud object storage in native format for AI	✓	Limited
Direct S3 access for AI services	✓	No
Customer controls underlying storage for AI	✓	No
Cost & Performance		
Potential for reduced egress fees	✓	Limited
Multi-cloud flexibility for AI services	✓	No
Global deduplication reduces dataset sizes	✓	No
Enterprise-class Control		
Customer-managed encryption keys	✓	Limited
Direct cloud provider relationships	✓	No
No vendor mediation for AI data access	✓	No