PANZURA

WHITEPAPER

Choosing the Right File Data Solution for AEC: Panzura CloudFS vs. The Competition

The Evolving AEC Landscape for File and Project Data Management Demands a Shift from Analog to Architecture

September 2025

INTRODUCTION

The Foundational Choice for the AEC Digital Future

The Architecture, Engineering, and Construction (AEC) industry faces rising project complexity and tightening profit margins. With the global AEC market projected to scale from $10.05 billion in 2023 to $24.36 billion by 2032, firms are under immense pressure to digitally transform. This is not a simple matter of adopting new software tools, but rather a fundamental re-architecting of how firms manage, collaborate on, and protect their critical project and file data.

Yet despite this massive growth opportunity, a staggering 72% of AEC firms still describe their digital maturity as “moderate” or “low,” ranking the industry just above agriculture in tech adoption. The persistent reliance on outdated, fragmented workflows has led to a pervasive data crisis, costing the global industry an estimated $1.8 trillion annually in inefficiencies and rework.

The urgency has never been greater. While 98% of megaprojects overshoot their budgets by nearly a third, early digital adopters are realizing transformative gains. According to Autodesk, operationalizing digital processes provides a solution to construction’s productivity problem. In fact, there is evidence that digital transformation can result in productivity gains of 14–15% and cost reductions of 4–6%.

This report provides a comprehensive, expert-level analysis of four different file data management solutions—Panzura CloudFS, Egnyte, Nasuni, and CTERA—specifically for the unique demands of the AEC sector. The analysis demonstrates that while a Common Data Environment (CDE) is widely recognized as a necessity for modern collaboration, a deep architectural divide exists among these solutions that dictates everything from performance and cost to security and control.

Panzura CloudFS is a strategic platform built on a superior architecture that directly addresses and solves the industry’s most critical data challenges.

Core Advantages of CloudFS

1. **Architectural Superiority:** CloudFS’s mesh architecture provides immediate, near real-time data consistency and eliminates the inherent latency of sync-based and hub-and-spoke models.
2. **TCO & Efficiency:** CloudFS’s inline global deduplication ensures redundant data is never written or stored in the first place, delivering unparalleled Total Cost of Ownership (TCO) savings.
3. **AI-Ready Foundation:** CloudFS removes data silos and access bottlenecks. Its native cloud object format and direct S3 access create a unified platform for both

file and cloud native workflows. This simplifies data collection and preparation, enabling artificial intelligence (AI) and analytics initiatives without complex data migration.

4. **Threat Control:** CloudFS provides enterprise-grade protection specifically designed for the AEC industry's high-risk profile. Its Threat Control feature uses AI to create a unique behavioral profile for each user. This allows it to proactively detect and stop anomalies like mass deletions, data exfiltration, or unusual file activity.
5. **Defense in Depth:** Intelligent detection is combined with CloudFS's core capabilities: 60-second immutable snapshots that ensure rapid recovery to a clean state, and automated disaster recovery, providing a layered defense against ransomware and data loss.

These architectural advantages translate directly into measurable business outcomes that cannot be replicated by some alternative solutions. For AEC firms, this means the elimination of version conflicts and a reduction in large-file save-times from eight minutes to 30 seconds. This translates to a quantifiable improvement in project completion, often 15–20% faster.

Most critically for today's threat landscape, CloudFS provides comprehensive ransomware protection that can save firms from the previously cited multi-million-dollar average recovery costs. In an environment where construction firms face daily cyber threats, this protection alone justifies the investment.

It also means up to 70–80% reduction in storage costs and a 35–85% typical reduction in WAN bandwidth consumption, delivering significant compounding savings. Moreover, CloudFS offers a near-zero Recovery Point Objective (RPO) with immutable, 60-second snapshots, creating a defense-in-depth architecture that is fundamentally resilient against cyber-attacks like ransomware and other forms of deliberate or accidental data loss. It provides built-in, sub-five-minute automated disaster recovery.

The decision between these solutions comes down to a strategic investment that will define an AEC firm's ability to compete, grow, and innovate in the digital era. The evidence establishes that Panzura CloudFS is not just a better choice. It's the definitive solution for achieving real and lasting competitive advantage.

THE STATE OF THE AEC INDUSTRY

Digital Imperative, Data Crisis

As project complexity continues to rise and client expectations evolve, the AEC industry is under immense pressure to deliver faster, more efficiently, and with greater transparency. Recent data reveals the scale of this transformation as firms worldwide plan to increase digital tool investment, while technology adoption among these businesses has accelerated to an average of 6.2 technologies per firm, which is up 20% from 5.3 in the previous year.

Fully 79% of AEC executives now affirm their firm's future depends on digital technologies, yet transformation has been hindered by reliance on outdated workflows and deep-seated inefficiencies stemming from fragmented and siloed data.

The competitive gap is widening rapidly. More than half of AEC firms now use AI in business development, proposal writing, and project analytics. This is a sharp rise linked to higher win rates. Median proposal win rates climbed to 50% in 2025 for firms integrating AI, while proposal submissions fell 38% as firms focus on higher-value pursuits, resulting in a 52% increase in total awarded work value according to Deltek.

The consequences of this pervasive data problem are staggering. According to multiple studies, poor-quality data is a strategic risk with huge financial implications. A landmark study by Autodesk and FMI attributed 14% of all avoidable rework to bad data, an annual cost of $88 billion.

Furthermore, McKinsey found that poor-quality data can lead to a 20% decrease in productivity, highlighting how data inaccuracies can directly undermine operational efficiency and profitability. Additional research confirms that data management issues contribute to 98% of megaprojects overshooting budgets by nearly a third, creating an estimated $1 trillion in lost value annually across the global industry. These financial losses are compounded by other negative outcomes, including project delays, misallocated resources, and missed opportunities for innovation.

The Ransomware Crisis: A Multi-Million-Dollar Problem

The AEC industry's data fragmentation has created a perfect storm for cybercriminals with a 41% increase in organizations appearing on data-leak sites. The industrial sector, which includes AEC, experienced the costliest increase of any industry, rising by $830,000 per breach over the previous year. With 96% of construction attacks also targeting backup systems and 61% succeeding in compromising them, traditional data protection strategies have proven inadequate.

The root cause lies in architectural vulnerability. Traditional file servers and sync-based systems create multiple data copies across locations, each representing a potential

attack vector. When ransomware strikes, these systems often lack the immutable backup capabilities needed for rapid recovery, forcing companies to choose between paying ransoms or facing prolonged downtime that destroys project schedules and client relationships.

To address these challenges, the industry has embraced the concept of a CDE. A CDE serves as a centralized digital hub that acts as a single, authoritative source of information for all project stakeholders, ensuring that everyone is working from the most reliable, up-to-date data. This approach is designed to reduce confusion, minimize costly errors, and improve collaboration.

However, not all file data management solutions are architecturally capable of serving as a true CDE. Many solutions, while offering cloud storage and basic collaboration tools, are built on an architectural model that conflicts with the principles of a CDE. An organization may invest in a seemingly modern tool, only to find it is still battling the same underlying data integrity and consistency challenges that a traditional file server presented.

The accumulation of this technological debt is a direct consequence of a historical “capital light” approach to foundational infrastructure. While avoiding upfront capital expenditures may have seemed prudent, the resulting reliance on a patchwork of disconnected systems has created significant long-term risk and financial exposure.

In fact, the AEC industry’s high-value intellectual property and schedule-driven nature make it a prime target for sophisticated cyber threats, including ransomware. With phishing attacks topping the list of initial access techniques and the sector’s reliance on third parties and contractors creating additional vulnerabilities, the core problems of costly rework, project delays, and crippling security risks are the direct, quantifiable result of fragmented and outdated data architecture.

To achieve true digital transformation and secure a competitive advantage, these firms must move beyond treating collaboration as a feature and instead adopt a file data platform designed to serve as a single source of truth.

A Tale of Three Architectures: The Definitive Divide

At the heart of the debate between Panzura CloudFS and its competitors lies a core architectural divergence that dictates everything from collaboration performance to TCO. While all of these solutions operate in the hybrid cloud, they do so with fundamentally different approaches to data management that create vastly different security, performance, and cost outcomes.

The first architectural model, exemplified by Egnyte, is the sync-based collaboration system. This approach replicates files to local caches and individual machines, creating multiple, distributed copies of the same data across different locations. A synchronization process then attempts to manage consistency between these multiple file copies. While this model can be helpful for simple reading of cached files, it may introduce inherent

complexities related to version control and conflict resolution, particularly for the large, collaborative workflows that are the norm in AEC.

From a cybersecurity perspective, we believe sync-based architectures are particularly vulnerable because they create multiple attack surfaces. Each synchronized copy represents a potential entry point for ransomware, and the distributed nature can make comprehensive backup and recovery significantly more complex. When security incidents occur, administrators may need to identify and remediate threats across multiple data repositories while attackers continue to propagate through the network.

Customers have reported that this often creates a "sync trap" where multiple users inadvertently work on different, local versions of the same file. When changes are synchronized back to the cloud, conflicts may arise, which could require expensive and time-consuming manual resolution by IT administrators. This is a potentially significant source of "collaboration friction" and lost productivity.

FOCUS IN CONTEXT

For example, a small engineering firm experiences over 15 file conflicts weekly, each requiring approximately 45 minutes of expensive engineering time to resolve, directly impacting project schedules and profitability. The sync-based architecture, in essence, could perpetuate the very fragmentation and versioning issues that a true CDE is designed to solve.

Modern AEC workflows compound these challenges. BIM models routinely exceed 500GB, with design teams working on hundreds of linked files simultaneously. Traditional sync-based systems may struggle with these file sizes, often requiring overnight synchronization windows and creating productivity "dead zones" where teams potentially cannot access updated files. Every minute of waiting translates to billable time lost.

In contrast to the sync-based model, CloudFS operates as a cloud-native unified global file system with a single, authoritative "golden copy" of all file data, which resides in the customer's chosen cloud object storage. This architecture eliminates the version proliferation and synchronization complexity that plagues sync-based systems, transforming distributed collaboration from a constant battle against file conflicts into a seamless experience. The central, authoritative data source ensures that all users, regardless of their location, work directly on the same dataset.

Hub-and-Spoke vs. The Clear Advantage of Mesh

While Panzura CloudFS, Nasuni, and CTERA are all categorized as global file systems, a crucial architectural difference has a notable impact on real-world performance, especially for real-time collaboration. The architectures of both Nasuni and CTERA can be described as a hub-and-spoke model, which includes a serial functionality. In this design, data changes are moved from the edge locations (the spokes) to the central cloud repository (the hub) and are then distributed to all other spokes.

This hub-and-spoke model, while effective for consolidating data, may create a latency bottleneck. All data transfers must be brokered through the cloud store, which can prevent direct, real-time communication between sites. The time it takes for a change to propagate can be significant, with some sources indicating that users may have to wait up to 5 minutes—multiplied by the number of individual sites—for file changes to show up.

This delay can be a major source of collaboration friction, particularly for time-sensitive AEC workflows. Nasuni and CTERA architectures are based on this model, which creates a serial dependency for data to be updated across sites. This serial functionality can lead to collaboration delays as all sites must wait for the data to be replicated from the cloud hub.

For modern AEC practices where multiple disciplines work simultaneously on complex BIM models and design files, delays are productivity killers. When a structural engineer makes critical changes to a model in Chicago, the architect in Vancouver may not see those changes for several minutes, potentially leading to conflicting modifications and expensive rework. In fast-paced project environments where decisions cascade through multiple disciplines, even minor delays compound exponentially.

Hub-and-spoke models also create potential single points of failure for cybersecurity. If attackers compromise the central repository, they may be able to access or corrupt all organizational data. The sequential nature of hub-and-spoke propagation can delay threat detection and response across distributed locations, giving ransomware time to spread throughout the network.

The CloudFS architecture is different. It is built on a mesh architecture. While CloudFS nodes sync with the central cloud repository, they also communicate directly with each other via a proprietary peer-to-peer (P2P) data exchange.

This is a core architectural advantage that allows CloudFS to achieve immediate file consistency everywhere. Changes are processed and shared directly between local nodes in near real time, with a simultaneous bursting sync to the cloud and other nodes. This peer-to-peer data exchange is the central advantage that breaks the causal chain of latency, enabling true real-time collaboration that hub-and-spoke models simply cannot match.

CloudFS’s mesh architecture provides inherent security advantages through its distributed but unified approach, as well. This peer-to-peer communication enables immediate file locking and data consistency across all nodes, while immutable cloud storage serves as an incorruptible backup.

The Threat Control feature, powered by AI, provides an added layer of defense by detecting anomalies and potential attacks. When combined with 60-second snapshot capabilities and automated recovery, this creates a defense-in-depth architecture that can detect, isolate, and recover from attacks faster than competing solutions.

Moreover, the AEC industry now faces an unprecedented cybersecurity crisis that makes the choice of file system architecture a business survival issue. Construction was the

most targeted industry for ransomware in 2023, with a staggering 41% increase in ransomware incidents. The industry experiences 20–25 major ransomware attacks daily, with 96% of attacks on construction companies also attempting to compromise backups and 61% succeeding.

The financial impact is devastating. Average ransom payments skyrocketed from $400,000 in 2023 to $2 million in 2024, which is a 500% increase. With global cybercrime costs projected to reach $10.5 trillion by 2025, and construction bearing disproportionate impact, secure data architecture has transformed from a nice-to-have into a business continuity imperative.

The following table provides a concise overview of the core architectural differences and their functional implications for AEC organizations and their workflows.

Architectural Comparison for AEC Workflows

Underlying Design	Egnyte	Nasuni	CTERA	Panzura CloudFS
Single Source of Truth Architecture	No	✓	✓	✓
Data Consistency	Eventual Consistency	Centralized Consistency	Centralized Consistency	Near Real-time, Centralized Consistency
Data Exchange Model	Sync	Hub-and-Spoke (Cloud-Only Brokerage)	Hub-and-Spoke (Cloud-Only Brokerage)	Full Mesh Topology
Global File Locking	No	✓	✓	✓
Byte-Range Locking for Simultaneous Editing	No	No	No	✓
Eliminates Manual Conflict Resolution	No	✓	✓	✓
Unified Global Namespace	No	✓	✓	✓
Prevents Data Corruption from Sync Conflicts	No	✓	✓	✓
Ransomware Multiple Attack Surface Vectors	Multiple Vectors	Moderate Risk	Moderate Risk	Minimal Risk
AI-Powered Threat Control	✓	✓	✓	✓

DIMENSIONS OF SUPERIORITY

Definitive Analysis of Panzura CloudFS

The architectural distinction between Panzura CloudFS and its competitors translates into tangible, quantifiable advantages across five critical dimensions for AEC firms—productivity, TCO, cybersecurity resilience, regulatory compliance, and strategic independence.

For AEC professionals, performance is not measured in abstract metrics. Instead, it's measured in the time it takes to open, save, and collaborate on multi-gigabyte files. Applications such as Revit, Civil 3D, and MicroStation are notoriously sensitive to the high latency of WAN connections, where the "chattiness" of conventional file protocols can create significant bottlenecks and user frustration.

The performance challenge has intensified dramatically. Modern BIM models routinely exceed 500GB, with design teams working on hundreds of linked files simultaneously. According to the AIA Firm Survey Report 2024, BIM is now standard practice for 95% of large firms and 88% of mid-size firms, making high-performance file collaboration a competitive necessity rather than a luxury.

Panzura CloudFS, Nasuni, and CTERA all aim to solve this problem by providing file locking, which ensures that when a user opens a file, it is locked for editing, and colleagues in other locations are immediately aware. However, CloudFS goes a step further with byte-range locking, as supported by applications, which is a game-changer for industries that require true co-authoring.

This capability allows multiple users to work on separate, distinct parts of the same file simultaneously without conflict. Nasuni generally lacks this critical feature, and we consider CTERA's implementation to be limited, which can prevent true, real-time co-authoring workflows on complex BIM and CAD models. The most significant performance difference, however, lies in peer-to-peer data exchange with CloudFS, which is enabled by its full mesh architecture.

FOCUS IN CONTEXT

A mid-sized structural engineering firm with eight global offices was able to reduce large file save wait times from eight minutes to just 30 seconds after implementing Panzura CloudFS. This dramatic reduction in collaboration friction, combined with the elimination of all version conflicts, enabled the organization to complete 15% more projects annually. The firm calculated that time savings alone generated an additional $1.83 million in billable revenue per year, while simultaneously improving client satisfaction through faster project delivery.

Furthermore, CloudFS delivers intelligent, block-level transfers and WAN optimization that reduces bandwidth usage by 35–85% by transmitting only unique data blocks across the network. For a large CAD assembly, a minor change of a few kilobytes might require a traditional sync solution like Egnyte to re-transfer hundreds of megabytes. CloudFS, however, only transmits the changed blocks, eliminating unnecessary network traffic and delivering LAN-like performance over any connection.

A financial evaluation of a file system architecture must extend far beyond a simple comparison of software licensing fees. Egnyte's per-user pricing model, for instance, potentially conceals a range of hidden and compounding costs related to data duplication, bandwidth consumption, and operational overhead. When factoring in cloud egress fees, which can reach $0.09 per GB for data retrieval, sync-based systems can generate thousands of dollars in unexpected monthly charges for active AEC workflows. The true economic implications are directly tied to underlying architecture.

This is where the advantage of CloudFS again becomes evident in terms of inline, global deduplication. While Nasuni and CTERA also leverage deduplication for cost savings, the CloudFS method is fundamentally more efficient. CloudFS performs deduplication as data is being written and changed, preventing redundant data from ever being stored in the first place.

Core Technical Benefit Comparison

Capability	Egnyte	Nasuni	CTERA	Panzura CloudFS
Global fixed-block deduplication	No	✓	✓	✓
Inline, write-time deduplication	No	No	No	✓
Cross-site data redundancy elimination	No	✓	✓	✓
Storage volume reduction	No	~60%	✓	Up to 70–80%
WAN bandwidth reduction	No	✓	✓	Typically 35–85%
Single-instance storage across all locations	No	✓	✓	✓
Eliminates full file re-transfers	No	✓	✓	✓
Cloud egress cost optimization	Minimal	Moderate	Moderate	High

This is a critical distinction from a post-process deduplication model, which allows redundant data to be written to storage before it is identified and removed. Metadata, which tracks unique data blocks, is shared almost instantly among all CloudFS nodes, ensuring every location receives immediate benefits from data deduplicated by any other node in the network, and that only unique data ever makes it to the object store.

The financial advantages of the CloudFS architecture are substantial and quantifiable, stemming from its ability to eliminate redundant data, caching at the edge, and a fully resilient architecture from cloud to edge. Unlike a siloed environment which requires replication targets and a separate backup solution, CloudFS employs global deduplication and single-instance storage. This results in storage volume reductions in some cases as high as 70–80% across all sites and in the cloud object store.

Beyond direct storage costs, the CloudFS architecture eliminates the need for any backup solutions and hardware, as the global file system itself serves as a continuous data protection platform through frequent, immutable snapshots.

Cybersecurity: Defense Architected for Continuity

The risk of a cyberattack is not a theoretical threat for AEC firms—it's the critical business risk of our time. This heightened risk is why a file data solution's architectural approach to resilience is paramount. Egnyte, for example, relies on a defensive model that includes snapshots with a standard interval of every four hours. This may create a vulnerability window that modern threat actors can possibly exploit, as they often remain in a network for weeks, identifying and compromising backup data before deploying their payloads.

Modern ransomware follows a sophisticated multi-stage approach: initial infiltration through phishing (the top attack vector), lateral movement, data exfiltration, and finally encryption. The average dwell time between initial compromise and ransomware deployment is 21 days, giving attackers ample time to identify and corrupt backup systems with longer snapshot intervals.

Panzura CloudFS, in contrast, integrates data protection directly into its core architecture. It creates immutable snapshots of the entire file system every 60 seconds. These snapshots cannot be deleted or compromised by ransomware or other threats. This creates a near-zero Recovery Point Objective (RPO)—the fastest in the industry according to Frost & Sullivan—which ensures that in the event of an attack, a firm risks losing no more than one minute of data.

Advanced AI-Powered Threat Detection

CloudFS goes beyond passive protection with AI-powered Threat Control capabilities that monitor for rapid file encryption, unusual access patterns, and other indicators of compromise in real time. The system automatically triggers protective measures before damage can spread, providing proactive defense rather than reactive recovery. This contrasts sharply with traditional solutions that rely on external security tools and manual intervention.

While Nasuni offers an RPO of “up to 5 minutes old, per volume,” and CTERA claims RPOs measured in 5 minutes, CloudFS’s more granular, default 60-second RPO across the entire global file system is a significant advantage. The CloudFS architecture also shifts the model from reactive restoration to proactive continuity. Because every node is a part of the unified global file system, every site becomes an active disaster recovery site. This provides built-in disaster recovery capability with sub-five-minute automated failover, reducing TCO by eliminating the need for a separate BC/DR solution.

This stands in contrast to traditional models, where a slow restore from a snapshot may take a significant amount of time (possibly days or weeks) for larger datasets. Industry case studies show that conventional recovery processes for large AEC datasets can require 5–10 days for complete restoration, during which projects remain stalled and billable work is essentially impossible. CloudFS, in this context, ensures business continuity is not a contingency plan but a built-in feature of the platform itself.

Moreover, the AEC industry faces increasing regulatory complexity that varies significantly by project location and client requirements. European GDPR regulations, U.S. state privacy laws, and international data sovereignty requirements create a compliance landscape that can determine eligibility for major projects. Many AEC firms now work on projects subject to International Traffic in Arms Regulations (ITAR), critical infrastructure regulations, or government contracts requiring specific data handling protocols.

In several U.S. states, national, and supra-national jurisdictions, carbon disclosure requirements for public projects have been implemented, adding another layer of data management complexity. The ability to control data location, encryption keys, and access patterns has become essential for winning large-scale public and private projects.

Strategic Independence and AI-Readiness

In an increasingly complex regulatory landscape, data governance and strategic independence have become a business imperative for AEC firms. This is a dimension where Panzura CloudFS holds a decisive advantage.

CloudFS operates on a-bring-your-own-key (BYOK) model, which allows customers to use their chosen cloud provider’s Key Management Service (KMS) to manage their own encryption keys. It’s a vital feature that ensures the organization retains true cryptographic control and ownership of its data. This level of control, combined with CloudFS’s cloud agnostic model, provides AEC firms with strategic independence and frees them from vendor lock in, a potential risk with SaaS-based alternatives like Egnyte.

The ultimate advantage in this dimension, however, is the architectural readiness for the AI revolution with CloudFS. The future of the AEC industry is increasingly data-driven, with 78% of organizations now using AI in at least one business function, which up from 55% just a year earlier. The biggest barrier to AI adoption is the data transformation bottleneck, which can consume 60–80% of AI project timelines as firms struggle to clean, prepare, and migrate unstructured file data into a format that AI services can understand.

The economic impact of this barrier is substantial. Organizations often spend significant AI initiative budgets on data preparation alone, before any value can be extracted. For AEC firms pursuing multiple AI use cases—from automated clash detection to generative design—these costs multiply fast, creating a drag for firms with file data architectures that require data transformation.

Architectual Comparison for AEC Workflows

Capability & Outcome	Egnyte	Nasuni	CTERA	Panzura CloudFS
Productivity & Performance				
Real-time Global Locking	No	✓	✓	✓
Byte-Range Locking	No	No	Limited	✓
P2P Data Exchange	No	No	No	✓
WAN Optimization	No	✓	✓	35–85%
File Save Time Reduction	8+ mins	5+ mins	3–5 mins	30 secs
Total Cost of Ownership (TCO)				
Global Deduplication	No	✓	✓	✓
Inline Deduplication	No	No	No	✓
Storage Volume Reduction	No	~60%	✓	Up to 70–80%
Cloud Egress Cost Management	High	Moderate	Moderate	Minimal
Annual TCO Savings	Baseline	30–40%	35–45%	Up to 50–70%
Data Resilience & Security				
Ransomware Vulnerability Window	Standard 4+ hours Window	Standard 5 mins	Standard 5 mins	60 secs
Immutable Snapshots	✓	✓	✓	✓
Built-in DR/BC	No	No	✓	✓
Automated Failover	No	No	Available	<5 mins

Capability & Outcome	Egnyte	Nasuni	CTERA	Panzura CloudFS
Strategic Independence & AI				
S3 Object Store Agnostic	No	✓	✓	✓
BYOK Model	No	✓	✓	✓
AI-Ready Data Foundation	No	✓	✓	✓
Direct S3 Access for AI	No	No	✓	✓
Data Transformation Required	Required	Required	Required	Eliminated for AI
AI Initiative Prep Costs	✓	✓	✓	Zero

Panzura CloudFS is architecturally ready for this transformation because it stores all file data as native objects in the customer's chosen S3-compatible object storage. CloudFS supports on premises, public and private cloud-based object storage providers (AWS, Azure, GCP, Wasabi, etc.). This is the preferred format for cloud native AI services, meaning a firm's data is already in the right format for analysis from day one. CloudFS provides direct access to this data via an S3 front-end interface, eliminating the need for complex and costly extraction or data movement processes.

While Nasuni and CTERA are also developing AI capabilities, their approaches may still require data movement or API integration for custom workflows. For example, one source notes that with Nasuni, data may need to be transitioned to Azure Blob Storage using AzCopy before it becomes accessible for certain AI services, potentially adding complexity and cost to every AI initiative.

The direct S3 access model of CloudFS eliminates these complex and costly steps, often with zero egress costs when AI processing occurs in the same cloud region as the data. This can prevent significant vendor margin stacking and provide firms with the data agility needed to capitalize on the next wave of industry transformation.

THE VERDICT

Your Strategic Choice for AEC Transformation

The analysis of Panzura CloudFS, Egnyte, Nasuni, and CTERA reveals that while all four serve a purpose in the file management ecosystem, they are built on fundamentally different architectures that lead to vastly different outcomes for AEC firms. In an industry facing unprecedented digital transformation pressure, cybersecurity threats, and AI adoption challenges, the choice of file system architecture will determine survival.

Recent industry data paints a picture. With 77% of established AEC firms planning to increase investment in AI and emerging technologies, and proposal win rates climbing to 50% for AI-integrating firms while falling for traditional approaches, the competitive gap is widening rapidly. Early digital adopters report 30% productivity gains, 25% reduction in rework, and 20% faster project delivery, while laggards face increasing pressure from digitally advanced competitors.

Egnyte's sync-based model, while providing basic file sharing, is a legacy approach that potentially perpetuates the very data fragmentation and versioning issues that are costing the industry billions of dollars in lost productivity and rework. We believe its architectural model is fundamentally misaligned with the demands of modern AEC collaboration, particularly given the industry's status as the top ransomware target.

Architectual Comparison for AEC Workflows

Metric	Competitor Average	Panzura CloudFS
File Conflict Incidents	15+ weekly	Zero
Large File Save Times	8 minutes	30 seconds
Annual Savings	Baseline	Significant
Storage Reduction	60% average	Up to 70–80%
WAN Reduction	Varies	Typically 35–85%
Recovery Point Objective (RPO)	Hours	Standard 60 seconds
Project Completion	Baseline	15–20% faster
Ransomware Protection	Vulnerable Windows	Immutable Architecture
AI Initiative Savings	Negligible	Significant

Quite simply, as we see it, in an environment where AEC firms reportedly face major attacks daily and average recovery costs exceed $2 million, sync-based architectures with multiple attack vectors and manual conflict resolution are not just inefficient—they're possibly dangerous.

While Nasuni and CTERA offer global file system capabilities, they operate on hub-and-spoke architectures that potentially introduce latency bottlenecks and single points of failure that could compromise both performance and security. Many users report that their sequential data propagation models, while functional for basic file sharing, may not match the immediate consistency and peer-to-peer performance that global design teams require. In the current threat landscape, hub-and-spoke models may create vulnerable central points that sophisticated attackers can exploit. The sequential nature of data propagation delays threat detection and response, potentially giving ransomware time to spread throughout distributed networks.

Panzura CloudFS, by contrast, is a solution built on a unified global file system with a full mesh architecture. This design is uniquely capable of solving the most critical challenges facing distributed AEC teams, from optimizing WAN latency to delivering comprehensive TCO savings and unbreakable resilience.

The evidence presented throughout this report makes the case for Panzura CloudFS's superiority irrefutable. The platform delivers core advantages that its competitors cannot match.

The choice between these platforms transcends technology selection. It's a strategic decision. With global cybercrime costs projected to reach $10.5 trillion by 2025 and AEC firms bearing disproportionate impact, the security advantages of CloudFS alone justify the investment. The ability to maintain operations during and after cyberattacks—while competitors possibly face weeks of downtime—creates substantial advantages that extend far beyond technology.

FOCUS IN CONTEXT

Consider the cumulative impact where a firm choosing CloudFS not only gains 15–20% faster project completion and 70–80% storage cost reduction but also eliminates the risk of $2+ million ransomware losses, saves hundreds of thousands per AI initiative, and positions itself for immediate adoption of next-generation technologies. Meanwhile, firms selecting legacy architectures face mounting costs, increasing vulnerability, and growing technological debt that becomes harder to overcome with each passing quarter.

Panzura CloudFS is the superior technical solution, and a definitive file data platform for thriving in the digital-first future for AEC. The question is not whether to modernize your file data architecture, but whether you'll choose the platform that positions your firm as a leader capable of capitalizing on this transformation while remaining secure from cyber-attack and data loss, or one that perpetuates the inefficiencies and vulnerabilities that are competitive dampers.

In an industry where early adopters gain compounding advantages and laggards face marginalization, the choice of CloudFS represents an investment. The time for incremental improvements is over. The future belongs to organizations with the vision to adopt transformative file data architectures that solve real and ongoing challenges head on.

For AEC companies that require high-performance, real-time collaboration on large files and demand a resilient, cost-effective, and future-ready platform, Panzura CloudFS is the right solution. The evidence is clear and compelling.

We invite you to compare Panzura CloudFS with the alternatives. We are certain you will find CloudFS to be the superior option for your AEC applications and workflows. Schedule a no-commitment demo and complimentary TOC evaluation now with an AEC expert.

This analysis is based on publicly available information, vendor documentation, industry research, and independent technical evaluations. Organizations should conduct their own assessments based on specific requirements and environments. All product and company names are trademarks or registered® trademarks of their respective holders. Use of those names does not imply any affiliation with or endorsement by their owners. The opinions expressed above are solely those of Panzura LLC as of September 25, 2025, and Panzura LLC makes no commitment to update these opinions after such date.