PANZURA

SOLUTION BRIEF

Panzura Edge

Secure, Performant File Access and Sharing to the Edge

In today's interconnected digital environment, data needs to be securely available anywhere, on any device, to any user you authorize. That includes your teams and it may also include your trusted partners and clients, for selected projects.

There are numerous legitimate needs to share files between trusted organizations. As companies form relationships with vendors, clients or partners, projects frequently require secure, restricted digital deal rooms or project spaces in which project teams can share, access and edit project or deal-specific files.

Additionally, widely distributed workforces have a constant need to be able to access company files from any device, including mobile phones, and work with them as easily and seamlessly as if they were in the office.

Anything less risks putting a significant dent in your productivity.

All too often though, that need for sharing and collaboration drives people to move files outside of your organization's file system — and therefore outside of IT control — simply because the file system isn't up to the task. Either it lacks a secure, governed way to provide limited-time access to those outside your organization, or remote access is so slow and awkward on mobile devices that users resort to making file copies.

OneDrive, Dropbox, Box, Google Drive and even iCloud have become popular options for business file-sharing, in addition to dedicated enterprise file sync and share options, which can be deployed either on-premises or in the cloud. Each of them is yet another tool for already-overloaded IT teams to manage.

Worse, it's easy for well-meaning individuals to create accounts with these and other file-sharing tools, and use them to store and share your company's sensitive documents.

This kind of shadow IT presents extraordinary challenges to the infrastructure and operations teams tasked with keeping track of your organization's sensitive information.

Now, your IT team has lost visibility into where files are and who is viewing and editing them, so you risk being out of compliance. They've lost or reduced their ability to keep files safe from damage or unauthorized access at the very time when those files are most valuable, and most vulnerable.

These security risks are not trivial. Even when IT teams have carefully assessed third-party file sharing solutions and approved them for company use, they present a particularly tempting target for hackers and ransomware gangs, as their data-rich environment carries a valuable payload. Repeated attacks on Dropbox from 2012 through to the present, and the continued impact of these attacks over time, are just one such case in point.

Under the best of circumstances, you no longer hold the encryption keys to your own data, which leaves your security in someone else's hands. In the worst of circumstances, some of your company's most sensitive data may be held hostage, or exposed.

Bulletproof, performant file access from edge to core

Beyond the risks, few conventional file sync and share tools can meet the challenges posed by real-time workloads, large file sizes and geographic distribution.

The expectations of end-users are high. In the digital age, we expect our files and software applications to respond in real time, regardless of the device we're using to access them. For organizations whose users are already accustomed to globally available, local-feeling file performance on their desktop or laptops regardless of their location, nothing less than extending that same performant file access to users at the edge can ever be acceptable.

There are three key considerations for IT leaders:

01 **Real-time, local-feeling performance** when opening and editing files. Unnecessary delays of even a few seconds at a time have a significant impact on productivity and the organization's bottom line when multiplied by many users across many workdays.

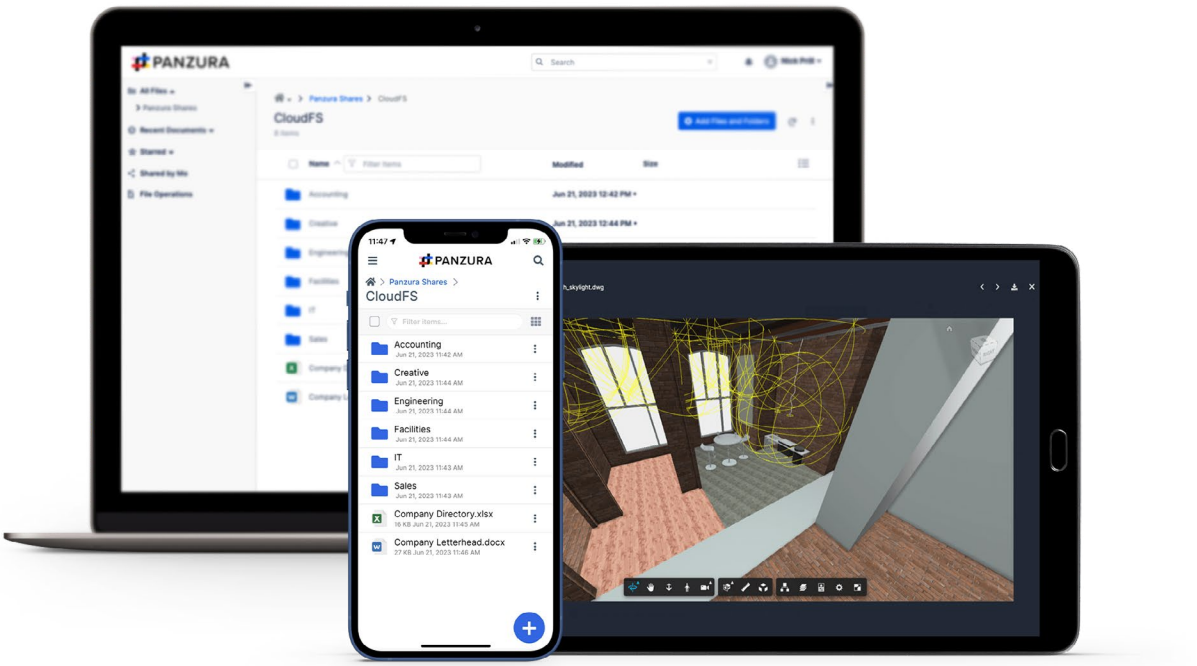
02 **Ransomware resilience.** When file data is protected by an immutable global file system with a near-zero global recovery point objective (RPO), moving it out of the file system exposes it to serious risk.

03 **Consolidation of data silos.** Keeping unstructured (file) data visible, auditable and compliant is already extraordinarily complex for IT teams. Replicating files to extend access creates yet another data silo to monitor and manage.

While there are numerous options for getting files to your distributed workforce and to trusted partners, they also present a wide range of capabilities when it comes to performance, ransomware resilience, and data consolidation. From cloud-based storage and file sharing linked to software applications such as those offered by Adobe and Autodesk, to storage-agnostic file sync and share options, the options offer a wide range of potential performance, security and data management outcomes.

Panzura Edge seamlessly extends secure, performant file access to your users at the edge, and beyond the confines of your organization

Using Panzura Edge, your remote workers and offices have anytime, anywhere, hyper-secure, and low-overhead access to Panzura CloudFS file data. Edge allows you to sidestep expensive and slow VPN use without compromising on security or visibility. And, it provides easy, visible collaboration with third parties without duplicating data.

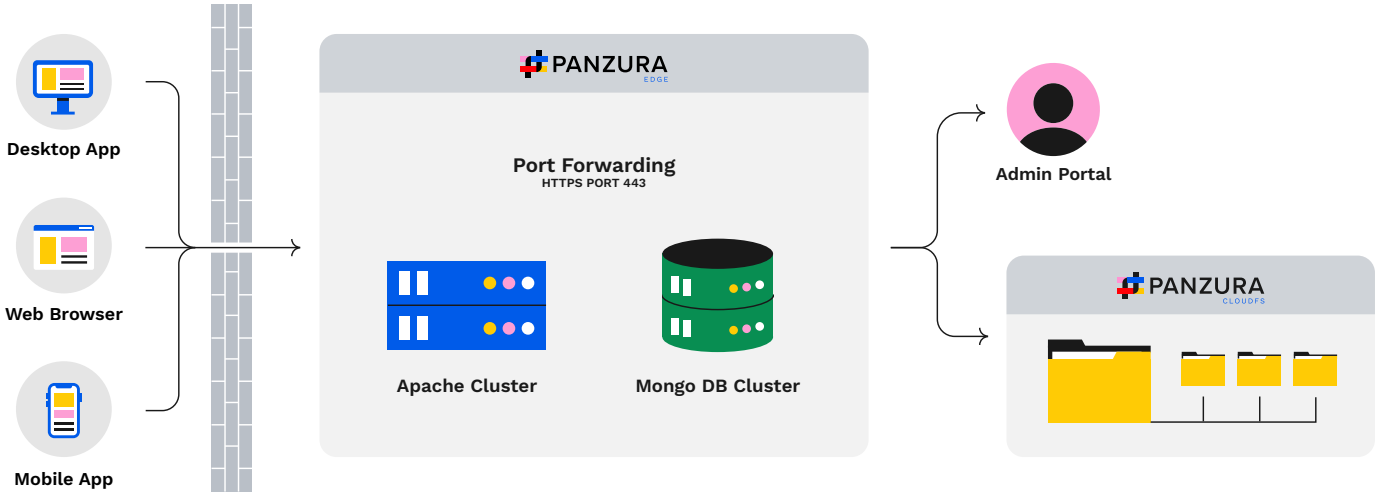


Secure, Simple, Remote File Server Access

Panzura Edge provides fast, secure, intuitive access to files from any location or device — phones, tablets and laptops — without the need for a VPN. Edge honors your existing file network permissions, reducing configuration and management overhead, and providing far easier and faster deployment than other remote-access and file-sharing services. Edge supports direct file sharing using configurable passwords, expiring links, download prevention, and other security methods that users can set when sharing their data.

How it Works

Panzura Edge works with CloudFS, and is self-hosted, deployable either on-premises or through IaaS in the cloud of your choice. It installs on a Windows server; a web-based Admin Portal is available to configure and manage the system.



Through layered security protocols, Edge enables secure file access while being deployed within your firewall. Edge is ideal for inhospitable conditions, massive files, tough security requirements, and viewing complex files.

Reduced File Duplication

With other remote-access and file-sharing solutions that stand outside of your corporate domain, you risk unsecured data duplication. Panzura Edge reduces duplicate data—saving you the significant costs of time, energy, inaccuracy, revenue, and excess storage—because all workers access the same, synchronized, highly secure CloudFS data store. By avoiding employees' need for online, third-party storage, you also reduce or eliminate the costs and risks that result from shadow IT.

Streamlined Collaboration

Panzura Edge also answers the challenge of collaborating with third parties—your partners, customers, and other organizations. Edge lets you establish secure locations for partners to access and upload data without needing to access your corporate network or VPN, allowing for streamlined yet highly secure collaboration. With built-in options such as an AutoCAD viewer and Teams integration, even the most widely distributed work teams can access, view, and collaborate on the most complex files.

Granular Control

File sync and share doesn't mean losing control or visibility of your file data.

- Control of encryption keys. With Edge, you own the keys, not a SaaS provider.
- A single, highly-secure data set. Internal and external access are controlled.
- Control over data residency. Get data mobility without compromising compliance.
- Fine-grained control over file views. Set file viewer permissions, scope, time limits, and more.
- Limit the number of downloads for a shared file.
- Automatically expire a share.
- Prevent downloads.
- Watermark sensitive data in preview.
- Allow anonymous file uploads.
- Secure password-protected file sharing.
- Two-factor authentication (2FA).

Enterprise-Grade Security

Edge supports the most sensitive and secretive of workloads—even those requiring dark sites.

- Data is protected at rest by AES 256-bit encryption, which is so secure it's approved for federal use.
- Data in flight is encrypted using SSL/TLS secure tunnel, allowing for secure file sharing.
- Data within the object store is made immutable by CloudFS, with global read-only snapshots providing a sub-60 second RPO for the entire file system.
- Data is immune to ransomware and other file damage, including accidental deletion, as soon as it is synced to the object store.
- File locking prevents accidental overwrites.

Digital Rights Management

- Digital Rights-Managed (DRM) web viewer enables even the least technical team members to prevent risky sharing.
- No access to the full document. With Edge, collaborators only can view the file, and re-distribution is impossible.
- No risk from screenshots. Users can share files with limited visibility, allowing recipients to use their cursor to roll over sections of the document to read, while the rest of the file is obscured.

Next Steps

Take the next step in supporting secure file access for your mobile and remote teams and partners. Extend CloudFS with Panzura Edge—email sales@panzura.com and let's talk.