PANZURA

SOLUTION BRIEF

Ransomware Protection and Rapid Recovery with Immutable Data

The persistence, pervasiveness, and documented success of ransomware attacks would suggest it may not be possible to mount a complete first-line defense, even within well-resourced organizations. That makes it essential that critical business data is as close to invulnerable as it can possibly be. That is, if your environment is attacked, and even accessed, the data itself will not fall.

Understanding Ransomware

Ransomware is software designed to carry out a digital kidnap of a firm or organization's data, by taking it hostage and demanding payment of a ransom for its safe return.

It aims to achieve this by encrypting data so effectively that you come to believe you cannot regain access to your files without them being unlocked for you.

Or, that restoring access to clean files is going to be so slow, so disruptive and so fraught with data loss that you may believe you have no other options.

Your ability to avoid paying a ransom depends on being able to restore access to your data, without relying on your attacker to decrypt it. As a result, attackers often target backups, and snapshots first, to limit your options.

Relying on older, perhaps incomplete backups can result in an enormous amount of data loss, and is such a slow process that restoration may take weeks or even months.

It's When. Not If.

Attacks are so frequent, that you should assume that your organization will be hit, at some point.

Data Defense

Ransomware defense is reactive by its very nature, and while defensive software does an excellent job of fending off multiple attacks, the number of possible entry points to an organization's network makes it all but impossible to prevent every attempt.

Regardless of how quickly defensive solutions react to a known ransomware variant, substantial damage can still be done before an attack can be brought under control.

That means defense alone is not a complete solution, although, it remains an essential part of your security strategy.

Data Protection

Assuming that it's not completely possible to keep ransomware out, mitigating a ransomware attack depends on protecting data. That means the data needs to be structured in such a way that—even if it is compromised—it cannot fail.

By virtue of storing data that needs to be editable, legacy file systems are inherently vulnerable to ransomware. When attacked, they do exactly what they are designed to do, and allow files to be changed.

Immutable data architecture changes your posture against ransomware and malware because it's fundamentally resistant to attack. Rather than simply being a solution to help either defend or protect, it reduces the impact an attack on your organization by being unaffected.

Panzura CloudFS makes cloud object storage immutable, and thus, impervious to ransomware.

To a user, CloudFS looks and feels like any other file system. Files can be opened, edited and saved, copied or deleted—by any authorized user, at any location—in real time.

Maintaining a Pristine Data Set

Behind the scenes is a radically different, much simpler, and infinitely more robust storage structure.

CloudFS is a global cloud file system that stores file data as blocks in cloud object storage, as a single authoritative data set that every user in the organization works from.

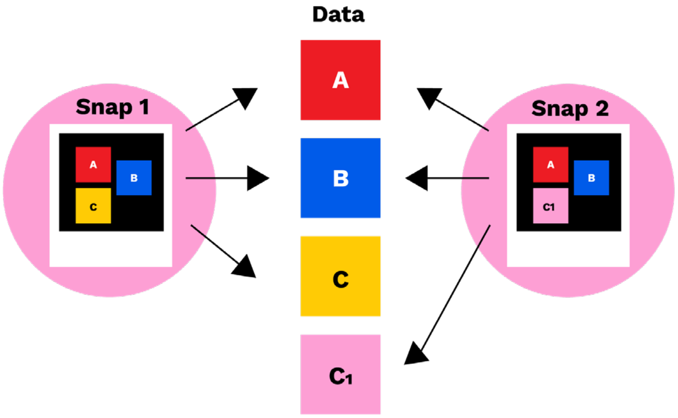
Those data blocks are immutable—stored in a Write Once, Read Many form so that once stored, they cannot be changed, edited, or overwritten. Consequently, they are unaffected by malware.

Metadata pointers are used to record which blocks comprise a file at any given time, and CloudFS uses these metadata pointers to know which blocks to assemble in order to open the current version of a file.

As users create or edit files, changed data is moved to object storage every 60 seconds, stored as new data blocks and leaving existing blocks untouched.
At the same time, the metadata pointers are updated to reflect any new blocks that form the file.

For example, a Microsoft Word document fileone.docx is comprised of blocks A, B and C. Some edits are made to the content of the document that sits in block C.

Block C is immutable, so the edits are captured in a new block – C1, and the file's metadata pointers show that fileone.docx is now made up of blocks A, B and C1.



These immutable data blocks are further protected by file system-wide read-only snapshots that are taken at configurable intervals, with the default being 60 minutes.

Additionally, read-only snapshots are taken at the local node level every 60 seconds, and these are used to transfer new and changed data to the object store.

Whenever snapshots are taken, they capture the metadata pointers that have recorded which data blocks make up files at that specific point in time.

Being read-only, these snapshots are also impervious to ransomware, and they effectively provide a granular – and very fast – way to restore data back to any previous version.

Immutable Data and Ransomware Attacks

In the event of a ransomware attack, malicious code is inserted into your files, changing them.

A legacy storage system allows a file to be edited as this code is inserted, changing the file itself. By contrast, when a file is attacked by ransomware on CloudFS, it is now comprised of completely new blocks of data.

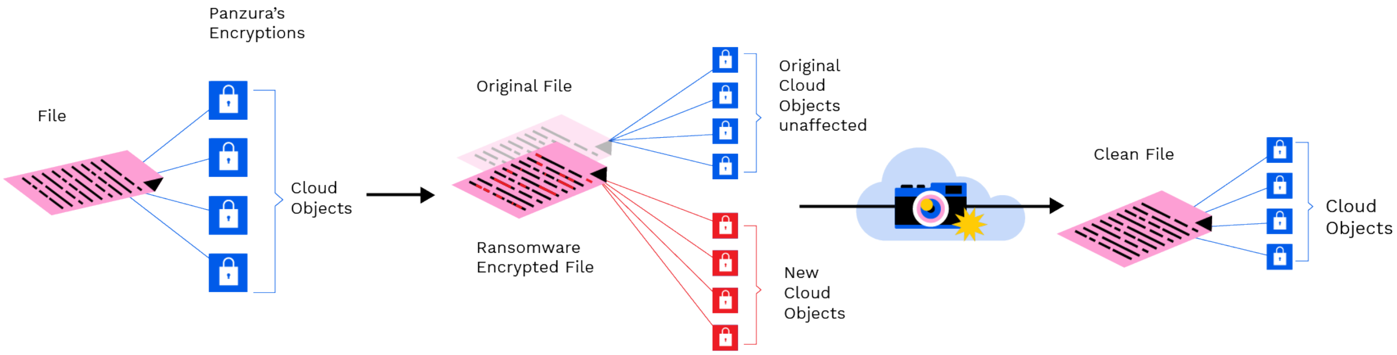
Panzura recognizes the encryption as changed file data, and the resulting encrypted files are written to the object store as new data blocks.

In this example, fileone.docx is substantially changed and is now comprised of blocks D, E and F. This point in time is also captured by a snapshot.

Since CloudFS preserves existing data as original objects in the object store, any file encrypted by the ransomware code can be immediately reverted back to its state prior to infection, using snapshots.

This can be easily done for a single file, entire directories, or even the entire global file system.

With Panzura's immutable data, your files aren't encrypted at all. Instead, file pointers are now pointing to data blocks containing encryption. Reverting to the snapshot prior to the attack points back to clean data blocks... and your clean files are restored. Unlike restoring from a backup, this approach allows granular restoration of files, with a near-zero recovery point objective, to minimize any data loss.



Rapid Detection and Restoration

Panzura's powerful SaaS data management solution Data Services offers a single, unified view and management of your data. Data Services assists rapid recovery from ransomware by enabling administrators to find affected data fast.

Alerts on unexpectedly high CPU load, memory load, or cache misses—indicating an unusually high number of seldom-used files are being accessed—give administrators early warning that an attack may be underway. Reports such as most active users, and most accessed directories can help to pinpoint the nucleus of the attack.

Audit is a flexible, accelerated search that operates based on the similarities between the search queries and the indexed data. Using audit actions such as writing to files, renaming or setting file attributes can narrow a search to find damaged files, as well as the compromised user account. Search results also offer one-click access to a complete audit trail, to allow identification of data-damaging actions and their timeline.

Search allows files in CloudFS, and other connected NFS and SMB file shares, to be found in seconds. Once the suspect files or data blocks are located, mitigation actions can begin.

Recovery allows swift reversion of any infected individual file to a previous "clean" version, rendering the ransomware attack harmless.

Analytics provides insight into file systems changes, including file size deltas, hot, warm, and cold data that has been accessed or modified, and daily changes of stored data.

Mass File Restoration

Panzura CloudFS provides IT administrators with the ability to restore entire directories, and all associated content, to a point in time captured by snapshot prior to the attack. Whereas restoring from backups involves moving data and can consequently take a significant amount of time to complete, using snapshots to restore files to a previous state simply involves moving metadata.

Metadata is a fraction of the size of the files it represents, so it takes a fraction of the time to move. As a result, restoring even a large volume of sizeable files takes just moments.

Panzura Global Services

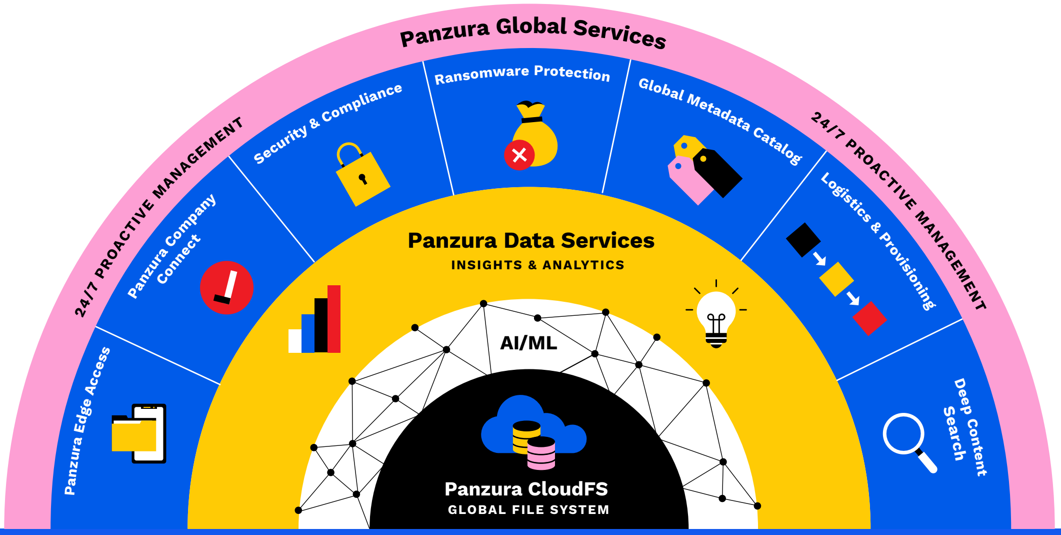
The Panzura services team provides assisted ransomware recovery as part of our premier services package. They work closely with IT teams to help them to know when they're bringing attacks under control by stopping the spread of affected files, as well as helping to restore clean file copies quickly, and without losing any data.

Protection Beyond the File System

While a file system does not store structured (database) data, storing database backups in CloudFS gives you an immutable backup to restore from. Additionally, backup data from other, less resilient, file systems can be given resilience to ransomware by being stored immutably in CloudFS.

About Panzura

Panzura makes hybrid multi-cloud data management seem easy. Panzura's multi-cloud data management platform is a single, unified data engine designed to securely power the most rigorous, large-scale multi-site enterprise data workflows across the globe. Intelligent edge technologies enable LAN performance with cloud economics together with simplified data management, advanced analytics, reduced operational complexity, and improved security.


Panzura Global Services
24/7 PROACTIVE MANAGEMENT
Panzura Edge Access
Panzura Company Connect
Security & Compliance
Ransomware Protection
Global Metadata Catalog
Logistics & Provisioning
24/7 PROACTIVE MANAGEMENT
Deep Content Search
Panzura Data Services
INSIGHTS & ANALYTICS
AI/ML
Panzura CloudFS
GLOBAL FILE SYSTEM