PANZURA Applied Software®

SOLUTION BRIEF

Ransomware Protection 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.

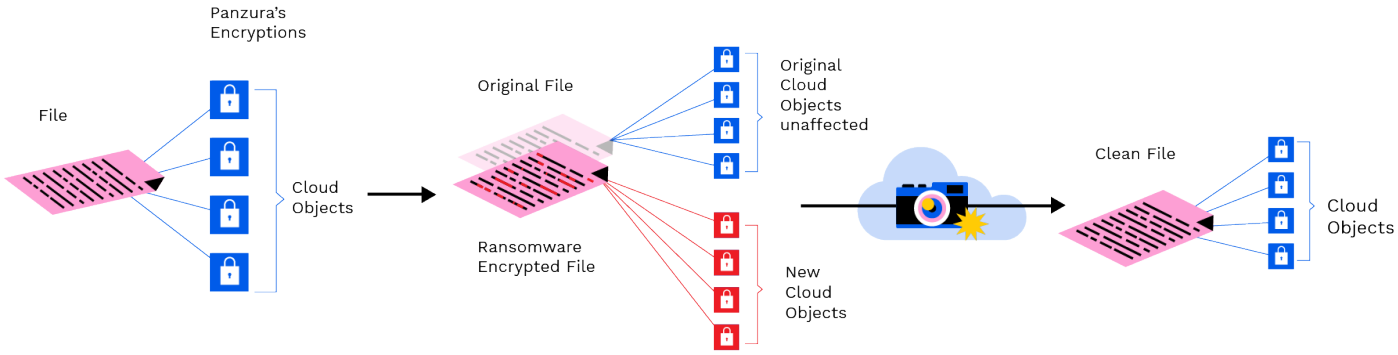
At the heart of every ransomware attack is the ability to encrypt files such that they cannot be accessed or recovered without paying a ransom to the attackers, in return for the ability to decrypt them.

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.

Panzura makes data impervious to ransomware by storing it in an immutable form (Write Once, Read Many) and further protecting it with read-only snapshots.

With Panzura's global file system CloudFS, once data is in the cloud object store, it cannot be changed, overwritten, or damaged in any way. File changes are written as new data blocks, which have no effect on existing data. As new data is saved, Panzura's global file system updates file pointers to record which data blocks comprise a file at any given time.

Panzura's lightweight, read-only snapshots then provide a granular, point-in-time ability to recover any data, by restoring from the applicable snapshot. Individual files, folders, or even the entire file system can be restored in this way.



Because both the snapshots and the data itself are immutable, ransomware attacks do not damage files in the Panzura global file system. Instead, attacks are shrugged off by quickly reverting back to previous data blocks, to make up uninfected files.

To negate the threat of data being publicly exposed, Panzura applies AES-256-CBC encryption for all data at rest in the object store. In addition, all data transmitted to or from the cloud is encrypted with TLS v1.2 while in flight, to prevent access via interception.

Encryption keys are managed by the organization, never stored in the cloud. The solution is FIPS 140-2 certified.

Rapid Detection and Granular File Restoration

Panzura's powerful SaaS data management solution Data Services offers a single, unified view and management of your data, whether it's stored in the cloud, on premises, or at the edge. 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 seldomused 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.

File 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.

Global 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.

Clone and Replace allows swift reversion of the infected files to a previous “clean” version, rendering the ransomware attack harmless.

File 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.

Panzura Support Services

The Panzura support team plays an important role in swift and granular recovery from attack, supporting you with mass restoration of files to the most recent “clean” snapshot, where required. They also work closely with IT teams to help them to know when they’re bringing attacks under control by stopping the spread of affected files.

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.

For more information on Panzura and ransomware protection see:

- panzura.com/products/data-services/
- panzura.com/solutions/ransomware/
- panzura.com/blog/ransomware-attacks-immutable-data-architecture/