PANZURA

SOLUTION BRIEF

Streamlining SOX Compliance with Data Management

Panzura's modern approach to data management is optimized for security and performance. It streamlines the organization's ability to implement the security controls for financial data mandated by the Sarbanes-Oxley Act as well as protecting both regulated and unregulated data.

This document should be read in conjunction with the technical whitepapers for both Panzura CloudFS and Data Services, for a full understanding of their capabilities. These can be found at panzura.com/resources.

The Need for Data Consolidation

Core to any organization's ability to manage and protect data is to know exactly where that data resides. For organizations operating localized data storage across multiple locations, simply finding all copies of relevant data is complex and time-consuming. Multiple similar – if not identical – copies of files sit in data silos across the organization. Exponentially more copies are made using traditional backup processes, plus offsite replication for redundancy.

This legacy approach to backup, at each location, makes yet another copy, which is retained per the organization's data retention policy. The result is multiple copies of individual files across the organization.

This immeasurably complicates any requirement to identify, supply, secure access to, or prove compliance for any piece of data.

CloudFS consolidates data into a single, authoritative data source that is de-duplicated, compressed and encrypted, and stored using the public or private cloud object storage of the organization's choice. Metadata file pointers record which data blocks comprise a file at any given time. This simplifies data management, minimizes the storage footprint and ensures data integrity for the organization by removing redundant data.

CloudFS then allows secure, performant

PANZURA

access to this authoritative data set to authorized users, from any location in the organization's network.

Data Access and Authentication

CloudFS integrates with existing Microsoft Active Directory services to allow only authorized users to access the file system, according to the file and directory permissions they have been granted.

Data Encryption and Privacy

To guard against data breaches, military-grade AES-256-CBC encryption is used to encrypt data stored at the edge and in the cloud.

Transport layer security (TLS/SSL) encryption technology securely transmits data over the network between local nodes and the cloud.

Panzura CloudFS uses the following standards-based encryption:

- AES-256-CBC data encryption technology
- RSA data encryption certificates
- X.509 certificates for HTTPS/TLS/SSL authentication

Encryption Certificates and Keys

Panzura supports Key Management Interoperability Protocol (KMIP) servers for managing encryption certificates. This approach allows organizations to create encryption certificates that align with their specific security policies. Encryption keys are managed by the organization. These are never stored in the cloud, leaving cloud providers unable to read data in CloudFS.

Data Auditability and Record Keeping

CloudFS logs each and every action taken on every file within the file system.

These logs can be used in conjunction with Panzura's own data intelligence layer Panzura Data Services, as well as third-party data intelligence options such as Varonis or Splunk to track and alert on unauthorized user access, or data movement.

Just as importantly for SOX compliance, file actions such as create, write, and remove are captured, as are setting or removing file and directory permissions.

Using Data Services for example, an organization can quickly and easily demonstrate all actions taken on files within relevant directories, along with the time stamp and user responsible.

Data Protection and Durability

To ensure organizations remain compliant by retaining financial data as mandated, keeping it protected and available, CloudFS defends data against threats and protects it from damage.

For early threat detection and defense, CloudFS integrates with Varonis as well as supported ICAP anti-virus and malware scanning providers.

Moreover, CloudFS guards against any data loss, damage or destruction by storing it in an immutable form (Write Once, Read Many) and further protecting

it with read-only snapshots. With CloudFS, once data is in the 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, CloudFS 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.

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

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.