panzura

Enterprise Cloud Data Protection and Compliance

Panzura Freedom™ helps organizations manage the explosive growth of unstructured data by transforming the complex and costly traditional storage model to the cloud. Because Panzura Freedom is underpinned by Panzura CloudFS™, it delivers maximum data protection for organizations that need to meet the strictest data protection, retention, and security regulations. Panzura CloudFS is the first enterprise file system purpose built for the cloud.

Panzura CloudFS provides complete cloud data protection and high-availability with no single point of failure. Enterprises can eliminate cumbersome backup and DR processes with dedicated and global HA options, immediate data consistency, granular snapshot restoration, and a near-zero RPO. CloudFS incorporates military grade encryption, secure erase, and other important security features.

Panzura CloudFS protects data with FIPS 140-2 compliant encryption. Data at rest is protected with AES-256 bit encryption, while TLS 1.2 encryption secures data in flight. Since data is deduplicated and compressed before it is sent over the wire, it would not be intelligible even if it were intercepted.

Regulatory Compliance

The US Department of Commerce National Institute for Standards and Technology (NIST) has confirmed that the Panzura CloudFS is compliant with the Federal Information Processing Standards (FIPS) 140-2 validation criteria.

Panzura is certified compliant with the US Health Insurance Portability and Accountability Act (HIPAA). Organizations subject to HIPAA regulations are assured that the Freedom Family complies with the regulations and security needs of electronic Protected Health Information (ePHI) data.

Panzura CloudFS cloud data protection and compliance benefits:

- Encryption in flight and at rest
- Meet FIPS 140-2, HIPAA, HITECH, USGCB, and other regulatory security compliance requirements
- Strong, standards-based authentication methods for file access
- Secure erase

Panzura CloudFS is also compliant with the US Government Configuration Baseline (USGCB) for IT products. The USGCB sets security configuration baselines for IT products, such as Panzura, that can be deployed across federal agencies.

Encryption Technology

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 filers and the cloud. Panzura keeps storage costs low by ensuring that the footprint used for encryption is small and efficient. CloudFS avoids data bloat and makes data stored in the cloud confidential and completely unreadable.

Panzura uses the following standards-based encryption:

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

KMIP

Panzura supports Key Management Interoperability Protocol (KMIP) servers for managing encryption certificates. Panzura allows you to create encryption certificates that align with your security policy.

Data Masking and Obfuscation

Data masking, or obfuscation, makes data unreadable by replacing randomly chosen characters with randomly chosen data – effectively securing it. Panzura uses encryption technology to mask data stored in CloudFS, which includes directory names, file names, and file data. In addition to encryption, Panzura chunks files, deduplicates them, and compresses the results before sending the data to the cloud.

The combination of all of these technologies effectively masks the data. Even if someone were able to access production data in the cloud they would only be able to view completely incoherent strings of characters.

Secure Erase

For IT environments that require the ability to securely remove all traces of highly sensitive files, CloudFS secure erase makes it possible to delete a file or folder so that the contents cannot be restored, even using the most advanced technology available. CloudFS secure erase is the highest purge level that can be attained without physically destroying the disk drives. It removes all versions of specified files and folders from the Panzura Freedom Filer and the associated objects stored in the cloud. All data is securely erased and replaced with zeros. Secure erase can be used with any supported cloud provider.

Secure erase operations conform to the latest recommendations by the National Institute of Standards and Technology, Computer Security Division; Special Publication 800-88 dated September 2012.

The combination of public cloud provider data availability and durability, combined with the enterprise grade data protection technologies inherent in Panzura CloudFS are unsurpassed. This makes the Panzura Freedom Family™ of products the ideal choice to be part of any solution that needs to meet HIPAA, HITECH, the Data Protection Act or other data protection, security, or privacy regulation.

Panzura, Inc. | 695 Campbell Technology Pkwy #225, Campbell, CA, USA | 855-PANZURA | www.panzura.com