PANZURA

VARONIS

SOLUTION BRIEF

Making Enterprise Data Accessible, Durable, and Secure

Data is created, stored, accessed and shared faster than security can keep up. Meanwhile, threats continue to escalate as new and inventive ways to access and compromise data emerge.

Together, Panzura CloudFS and the Varonis Security Platform can help organizations modernize, manage, protect, and defend their file and storage infrastructure.

Panzura provides a hybrid-cloud global file system extensible across hundreds of locations. Overcoming latency to deliver a local-feeling file performance, Panzura allows enterprises to consolidate data and replace legacy NAS, using public, private, or dark cloud S3 object storage as a globally available data center.

Storing data in an immutable form with read-only snapshots, Panzura CloudFS makes data impervious to ransomware. Changed data is stored as new data blocks, which do not overwrite existing data blocks.

Varonis secures unstructured data from unauthorized access and cyberthreats by automatically finding and monitoring sensitive data across on-premises and cloud data stores. Varonis detects suspicious behavior by putting data activity into context with authentication events and perimeter telemetry to quickly spot abnormal activity.

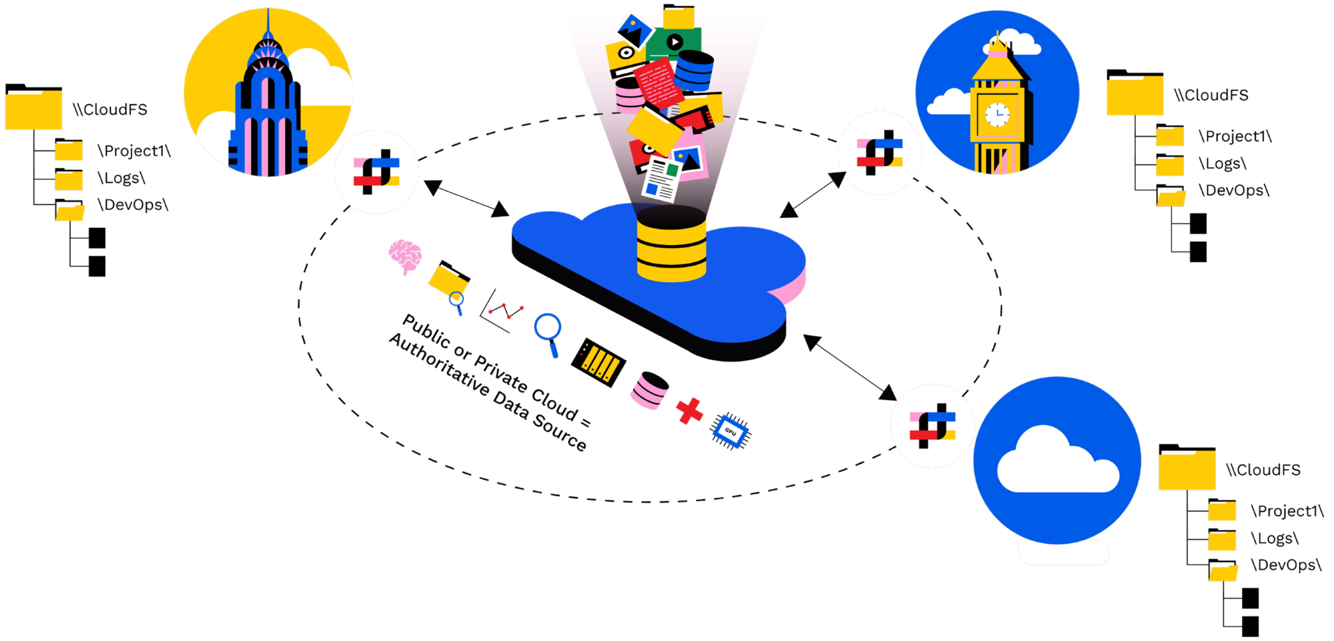
Varonis can also help mitigate the impact of breaches by restricting access to sensitive data at scale.

The joint solution optimizes the organization unstructured data footprint, protects it from cyberthreats, and scales as required. The result is one highly secure authoritative data source for multiple locations, in a resilient file system, without replicating data.

PANZURA VARONIS

Collaborate Remotely and Securely in Real Time

Allow multiple locations to operate as if everyone works under the same roof with Panzura, using one authoritative set of data. Enjoy local-feeling file performance, automatic global file locking, and immediate global data consistency.



Gain Visibility into your Entire File System

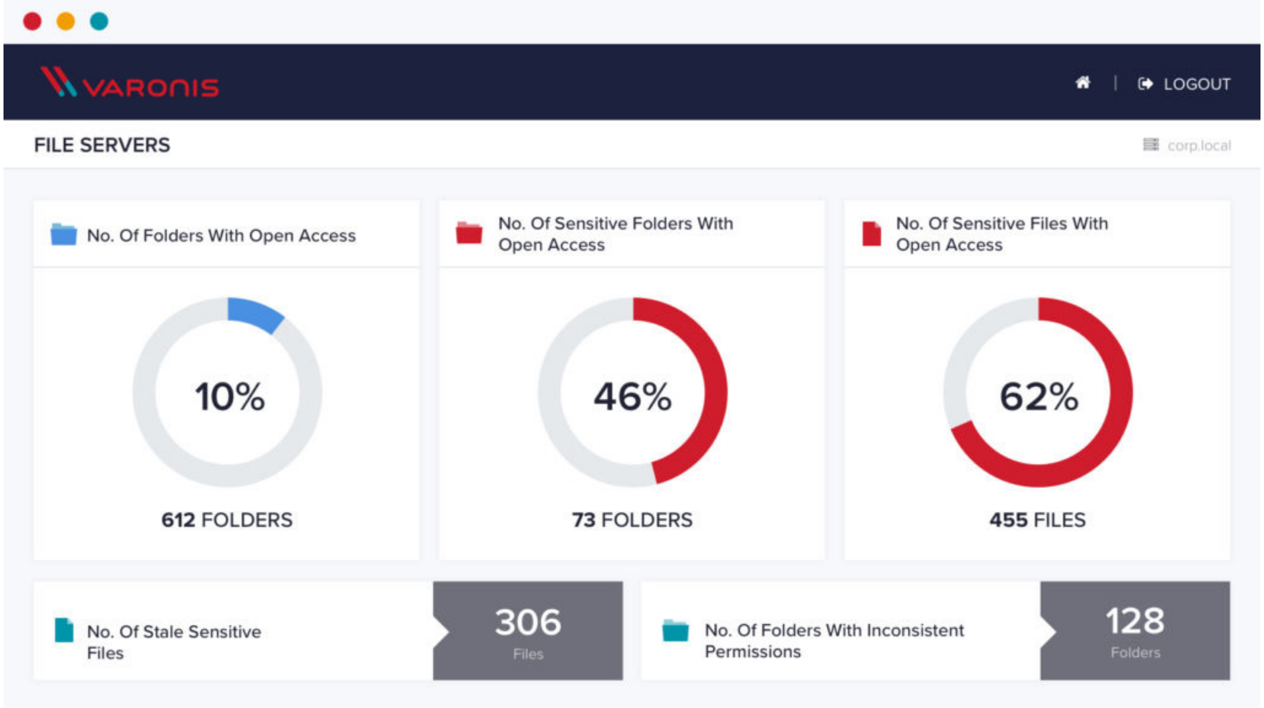
Ingest unstructured data from Panzura's global file system to monitor file system activity from one central, easy-to-read dashboard.

Visualize where sensitive data is stored, over-exposed, and at risk of compromise to malicious actors like insider threats, malware, or ransomware. Quickly pinpoint exposed folders, stale data, or inactive accounts that are still enabled.

Automatically map out your environment's permission structure with Varonis, allowing admins to easily view who has access, where data is stored, and who uses it.

Control data access at a granular level and safely automate permission changes, ensuring users only have access to the data they need, reducing overexposure and other potential risks.

With additional context like classification, geolocation information, and device pairing from Varonis, administrators and security analysts can easily understand how data is accessed and used.



FILE SERVERS

No. Of Folders With Open Access
10%
612 FOLDERS

No. Of Sensitive Folders With Open Access
46%
73 FOLDERS

No. Of Sensitive Files With Open Access
62%
455 FILES

No. Of Stale Sensitive Files
306
Files

No. Of Folders With Inconsistent Permissions
128
Folders

Rapidly Detect, Respond to, and Recover From Threats

Behavioral profiles created by Varonis' machine learning algorithms can automatically detect abnormal user behaviors like suspicious data access, lateral movement, and privilege escalation. Shut down user sessions and change passwords using Varonis' automated responses to stop attacks in their tracks and limit any damage. Recover from ransomware and other encryption by restoring files and folders from Panzura's read-only snapshots.

How can we help? Let's talk about what's right for you! You'll get answers at info@panzura.com or visit panzura.com and have a chat with us.