Panzura Detect and Rescue™

Stop ransomware in its tracks.

Detect ransomware attacks as they happen, before they have a chance to do significant data damage that needs extensive time to be assessed and then reversed.

Shut attacks off in near real time with automated user interdiction that disables affected user accounts without disrupting the rest of the business.

Get detailed alerts with affected user accounts, altered files and folders, and ransomware variant detected, for a clear view of what needs to be restored and cleaned.

Detect and Rescue extends and bolsters the data resilience capabilities of the CloudFS hybrid cloud file platform by providing active storage protection to minimize disruption and maximize business continuity. Detect and Rescue works hand-in-glove with Panzura Data Services audit capabilities to parse and assess file operations within CloudFS in near real time, looking for anomalies.

File data in CloudFS is already highly resilient. The platform makes data immutable so it cannot be damaged and further protects it with immutable global snapshots taken every 60 seconds. This passive resistence delivers a global recovery point objective of 60 seconds or less. Additionally, recovering pristine data with CloudFS involves restoring lightweight metadata-based snapshots, so takes a fraction of the time of traditional data restoration methods.

This positions organizations to achieve the near impossible; swift data recovery without losing recent file changes or facing extensive disruption and downtime.

However, ransomware attacks seldom run in a straight line, which can leave IT admins faced with bulk restoration that inadvertently damages clean data by rolling back recent edits, or a lengthy investigation process.

How it Works: Beyond Scanning to Proactive Monitoring

Traditional methods of scanning and monitoring data struggle to get clear on what normal looks like.

Third-party applications that scan active file systems tend to flag a high number of false positives because differentiating between normal operations that might look suspicious on the surface and genuine cyber threats is difficult when training on multiple types of file systems and vendors.

Solutions scanning inert data in backups can have a much higher degree of accuracy, but require significant processing power, which affects file operations and run far more slowly than an active file system can afford.

Detect and Rescue compares files and file changes to expected behavior patterns in real time and watches for anomalies. When it detects something unexpected, it acts fast. If a pattern starts to emerge where files deviate from what is considered normal behavior, Detect and Rescue immediately takes action.

The Power of Prevention: Immediate Response

When a significant deviation is detected — whether it's an unfamiliar file type, changes in file extensions, or unexpected behavior — Detect and Rescue doesn't just alert you; it takes action.

For instance, if suspicious activity is detected across multiple files in a short period, the system will interdict it by automatically shutting off write access for the affected user or users. This prevents further damage or data modification while the security team investigates the issue.

Interdiction is immediately followed up by notifications to administrators containing all the information they need to investigate further, giving them a fast path to data restoration using clean snapshots.

Email, SMS or SIEM-integrated alerts are detailed within the Panzura Data Services ransomware tracker. This contains detail of files and folders affected, the ransomware variant detected and the user accounts involved.

Not only does Detect and Rescue provide a fast path to data recovery, it gives operational teams a head start on what is set to become a larger issue. Often, the first place an attack is detectable is within files, so catching it at this point can help to prevent other systems being affected.

Learn More

Read the Data Services technical whitepaper.

Read the CloudFS technical whitepaper.

Talk to our sales team.