PANZURA

DATASHEET

Panzura Detect and Rescue

Ransomware Resilience for CloudFS Files

In a world where ransomware is a “when” not “if” risk, Panzura Detect and Rescue provides the detection, alerting, and fast path to recovery you need to protect your CloudFS files.

Panzura Detect and Rescue provides a vital layer of ransomware resilience for Panzura CloudFS data. It comprises both cloud-native software and expert assistance. Tightly integrated with other components in the Panzura Platform, the Detect application uses machine-learning detection algorithms trained on your CloudFS environment to identify and alert on suspicious patterns that may indicate a ransomware attack in your environment. If ransomware is confirmed, the Rescue facet of Detect and Rescue provides a fast path to file recovery and business resilience via Panzura’s experts.

Why Detect and Rescue Matters

With the average number of monthly ransomware attacks growing 75% between the first and second halves of 2023 in the U.S., and human error a leading cause for the delivery of ransomware payloads (phishing was the most common vector, reported in 41% of incidents), ransomware is a near and present danger for every organization.

Every minute ransomware is present in your IT systems equals time lost in neutralizing its existential threat to your organization. And even with the robust passive protections inherent in how Panzura CloudFS captures and stores snapshots and metadata, it’s a security best practice to add active layers of resilience for the files you need to stay in business.

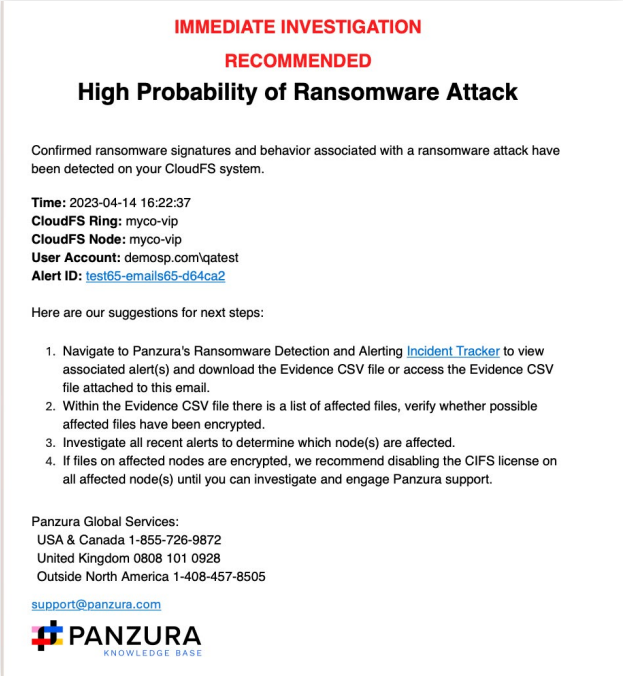
Panzura Detect and Rescue improves ransomware monitoring, speeds alerting, and (if ransomware is found) can help cut recovery time to hours or days from weeks to months.

Detect and Rescue Use Cases

Even though CloudFS file snapshots are immutable, like all stored data they present an attack surface which benefits from added layers of protection.

For those using CloudFS, there are four major use cases where Detect and Rescue provides value.

Use Case 1



IMMEDIATE INVESTIGATION RECOMMENDED

High Probability of Ransomware Attack

Confirmed ransomware signatures and behavior associated with a ransomware attack have been detected on your CloudFS system.

Time: 2023-04-14 16:22:37
CloudFS Ring: myco-vip
CloudFS Node: myco-vip
User Account: demosp.com\qatest
Alert ID: test65-emails65-d64ca2

Here are our suggestions for next steps:

1. Navigate to Panzura's Ransomware Detection and Alerting Incident Tracker to view associated alert(s) and download the Evidence CSV file or access the Evidence CSV file attached to this email.
2. Within the Evidence CSV file there is a list of affected files, verify whether possible affected files have been encrypted.
3. Investigate all recent alerts to determine which node(s) are affected.
4. If files on affected nodes are encrypted, we recommend disabling the CIFS license on all affected node(s) until you can investigate and engage Panzura support.

Panzura Global Services:
USA & Canada 1-855-726-9872
United Kingdom 0808 101 0928
Outside North America 1-408-457-8505

support@panzura.com

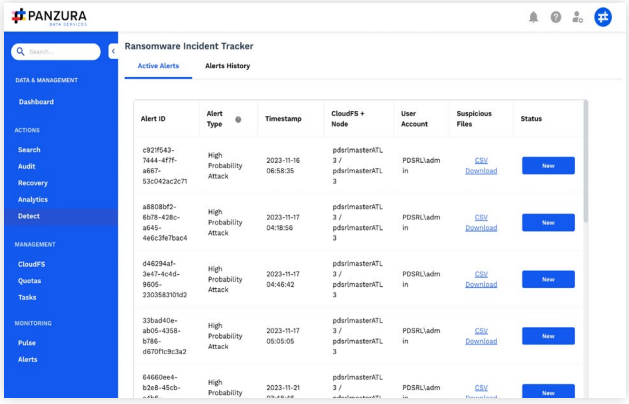
PANZURA KNOWLEDGE BASE

Enabling early ransomware detection.

Time to remediation matters. You can't remediate what you can't detect—and with Detect and Rescue, you'll have a new layer of resilience for early ransomware detection. The Detect application uses machine learning and AI-infused training on your organization's CloudFS environment to establish expected behaviors and values. After the training period, patterns that fall outside the norm are flagged by Detect for further attention, and automatic alerting can be set for near real-time awareness.

Unlike other solutions, Detect not only can identify known ransomware but also new or previously unknown ransomware. Because Detect trains on your environment, it can surface these hard-to-detect risks by identifying anomalies from expected values with accompanying actions indicating ransomware-like behaviors.

Use Case 2



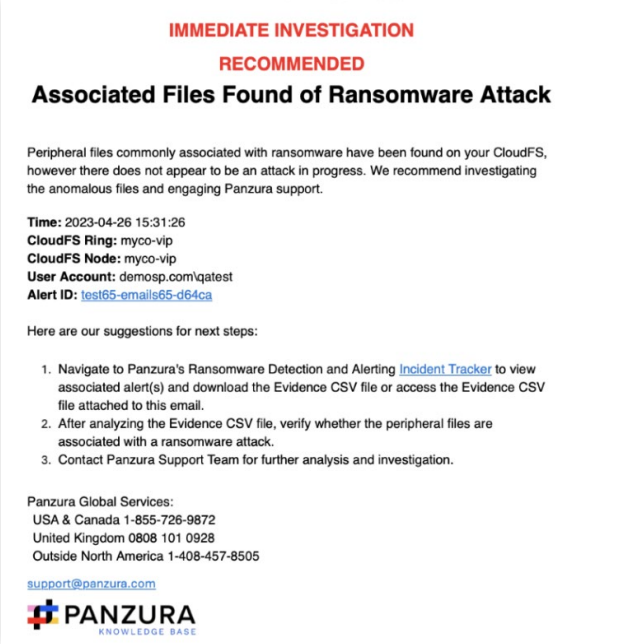
Empowering frontline IT, Storage, and Security admins.

Once Detect and Rescue is trained on your CloudFS environment, automated alerting can be enabled for frontline admins. They will receive near-real-time SMS and email alerts, allowing them to notify security teams to help stop possible ransomware attacks fast. As a best practice, anyone who will be on the recipient list for automated alert should be trained in what these alerts mean, what to do, and who else to involve. The resources noted here will provide a framework for preparing your teams to respond appropriately.

Further support for frontline admins includes:

- Suspicious user activity tracking for IT security admins via the Panzura Data Services (PDS) Incident Tracker.
- Services to enable storage admins to recover from ransomware via Data Rescue capabilities.

Use Case 3



IMMEDIATE INVESTIGATION RECOMMENDED

Associated Files Found of Ransomware Attack

Peripheral files commonly associated with ransomware have been found on your CloudFS, however there does not appear to be an attack in progress. We recommend investigating the anomalous files and engaging Panzura support.

Time: 2023-04-26 15:31:26
CloudFS Ring: myco-vip
CloudFS Node: myco-vip
User Account: demosp.com\qatest
Alert ID: test65-emails65-d64ca

Here are our suggestions for next steps:

1. Navigate to Panzura's Ransomware Detection and Alerting Incident Tracker to view associated alert(s) and download the Evidence CSV file or access the Evidence CSV file attached to this email.
2. After analyzing the Evidence CSV file, verify whether the peripheral files are associated with a ransomware attack.
3. Contact Panzura Support Team for further analysis and investigation.

Panzura Global Services:
USA & Canada 1-855-726-9872
United Kingdom 0808 101 0928
Outside North America 1-408-457-8505

support@panzura.com

PANZURA KNOWLEDGE BASE

Reducing risks from ransomware.

Ransomware can be challenging to detect, for many reasons. During that time, ransomware footprints from associated files and unusual activity can help surface "low and slow" ransomware attacks. For example, a user who has been phished may have become an unwitting vector for ransomware. If an anomaly with fingerprints suggestive of ransomware is delivered into a CloudFS environment, not only will Detect flag the suspicious event, an audit trail can help identify the malicious user actions associated with the attack. Detect has been architected with layered algorithms sensitive to timescales and sequences, making it possible to uncover ransomware lurking in your environment.

Use Case 4

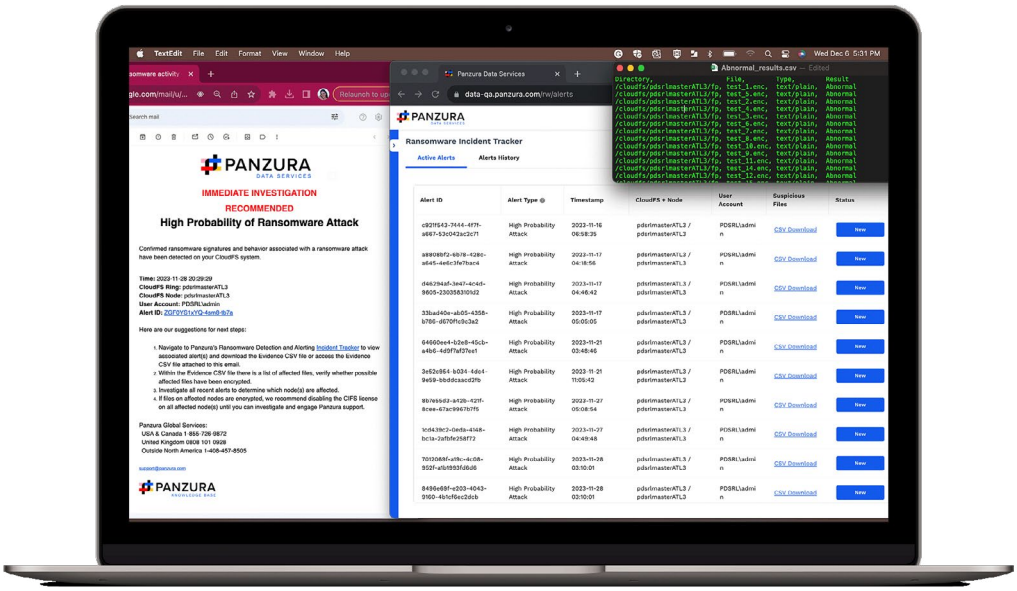
Speeding the return to the last-known-good state.

Detect and Rescue provides a comprehensive layer of resilience for CloudFS ransomware risks, including expert recovery assistance. The Rescue facet of Detect and Rescue provides your IT and Storage teams guidance and assistance from Panzura experts on quickly returning to the last-known-good state. When anomalies that resemble ransomware are detected, an alert is sent to the Detect and Rescue administrator. Here are the next steps they should take:

1. Download evidence files from the Panzura Data Services incident tracker.
2. Review those files potentially affected by ransomware to verify whether they have been encrypted.
3. If files are found to be encrypted, and this step is not yet automated, manually disable the system license for the impacted node and disable access for everyone continuing to write to that node.
4. Contact Panzura at support@panzura.com for recommendations on how to clean out the payload.
5. Once your organization has validated that the payload has been cleaned out, engage Panzura for for recovery assistance.

Detect and Rescue Capabilities

These major features of Detect and Rescue provide the capabilities you need to add layers of ransomware resilience to your CloudFS files.



Admin-friendly reporting and management.

Detect and Rescue uses a table generated by Panzura Data Services that is derived from a proprietary algorithm running atop the Data Services audit stream. This table makes it easy for frontline IT admins to manage, monitor, and share updates on suspicious activity. It also enables faster verification and recovery by listing potentially affected files.

Algorithmic detection.

The machine-learning detection algorithm, once trained on your CloudFS environment, detects suspicious behavior patterns across the entire file system for footprints that are reminiscent of a ransomware attack.

Save processing resources while managing and monitoring.

Monitoring activity is “bucketed,” meaning Panzura doesn’t constantly scan the node, resulting in greater efficiency and lower processing costs.

SMS and email notification automation.

Detect and Rescue provides SMS and / or email notifications within minutes, automatically, to your choice of recipients, for rapid alerting on potentially suspicious activity.

Alerting history repository.

The full history of alerts is preserved and stored to provide a reference for security and audit teams.

Expert-assisted rapid response.

Panzura experts have experience in assisting customers with recovery to the last-known good point before loss, and are ready to make ransomware or other catastrophic file loss a non-issue for your organization.

Additional capabilities

Roles and access levels
- Detect and Rescue Administrator
- Data Services Administrator
- Read-Only User

Administrator efficiency and empowerment
- Automated user interdiction
- Alerting controls and configuration
- Evidence downloads
- Alert investigation status setting

Lightweight attack verification process on affected systems, including:
- Compromised user identification and audit drill-down including timestamps
- Peripheral file type scans for items associated with ransomware attacks
- Detection of known ransomware families, as well as new and unknown ransomware detection through the Detect verification process

Detect and Rescue Requirements and Compatibilities

Detect and Rescue is part of the Panzura Platform, and requirements and compatibilities for Detect and Rescue are:

- Panzura CloudFS 8.2 or later versions.
- Panzura Data Services Audit licensing, to provide the user action stream needed for the Detect algorithm to function.
- Panzura Data Services Search and Recovery licensing, to enable self-service recovery through access to the metadata already local to CloudFS nodes.
- Panzura Data Services Ransomware Detect licensing, to monitor the entire CloudFS file system and enable use of machine learning detection techniques on suspicious behavior.
- One or more cloud object stores for CloudFS, which is compatible with almost all cloud object storage, including Amazon Web Services S3, Azure Blob Storage, Google Cloud Storage, IBM Cloud Object Storage, Dell EMC ECS, Wasabi, Cloudian, and others.

Learn more about Detect and Rescue today

See the technical documentation for Panzura Detect and Rescue here.

Request a demo:

- Visit panzura.com to schedule your demo, OR
- Complete this form for demo request.