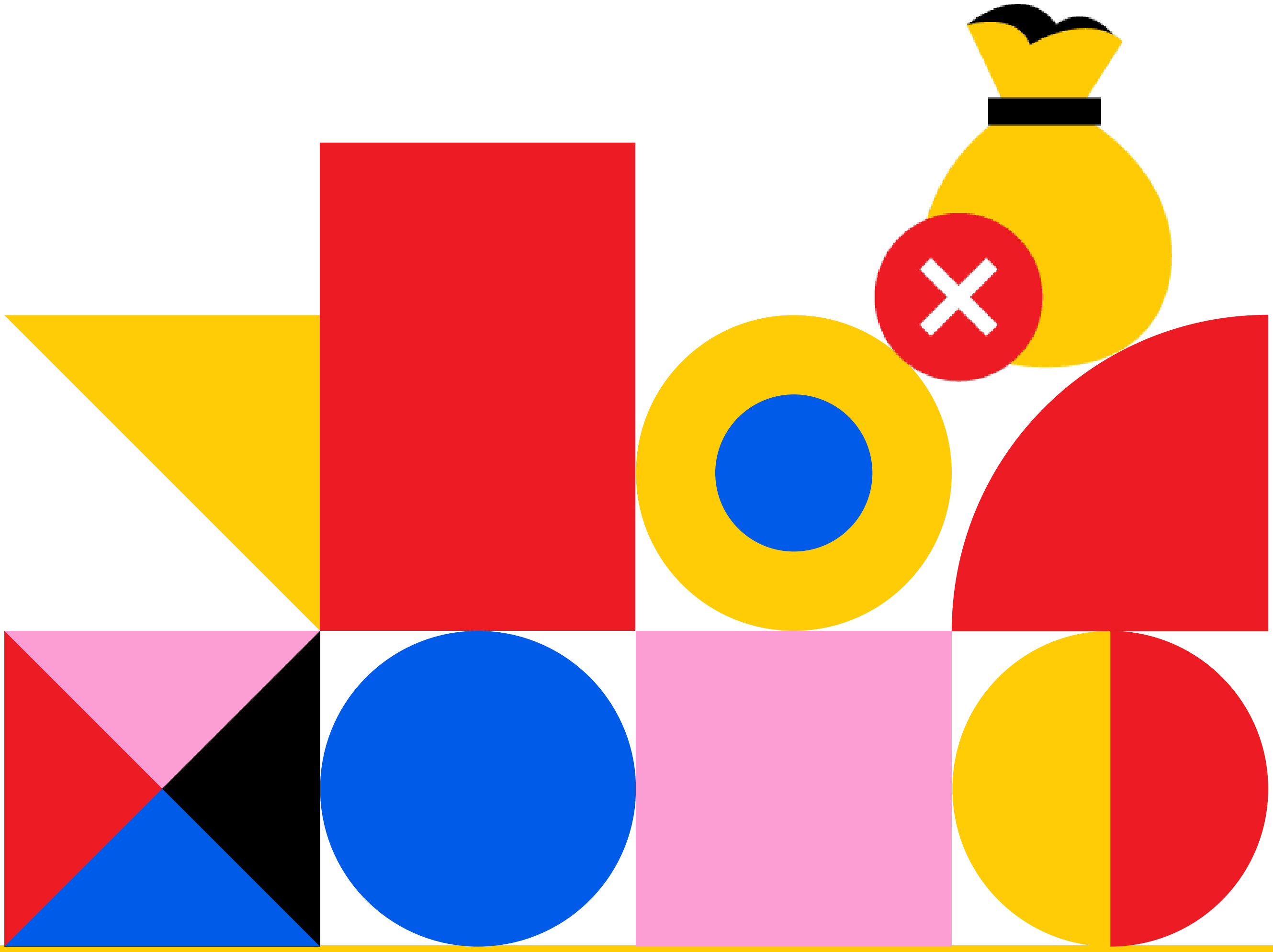
PANZURA VARONIS

Stop Ransomware Cold With Panzura and Varonis

An overview of how the enterprise can shift the balance of power in the fight against ransomware with an architecture for data resilience.



IN THIS WHITE PAPER

Ransomware attacks increasingly target data environments such as backup and storage systems. Cybercriminals see this threat vector as both exceptionally profitable and vulnerable, and there is enormous pressure to return to normal as quickly as possible when data has been locked.

Varonis and Panzura provide a ransomware defense that goes to the heart of the data environment itself.

The Panzura global file system offers protection and recovery by way of its underlying immutability, derived from methods for writing to object stores, meant to speed up access to files. This makes data impervious to encryption and prevents ransomware from impacting any of the data held in the system.

Catching ransomware that perimeter security alone does not detect, Varonis can identify and lock down access controls, as well as overexposed sensitive data that attackers could exploit. This impedes ransomware inside the Panzura global file system, as well as with other servers, NAS, and core IT resources.

This white paper examines how Panzura and Varonis have teamed up to deliver a more resilient data protection and recovery architecture. The authors discuss how the technology shields data, applications and workloads in the cloud, augmented by built-in AI-driven data analytics. They also review vulnerabilities that could lead to an attack, and countermeasures to stop ransomware cold.

CONTENTS

INTRODUCTION

Information security has always been a delicate balancing act. Organizations struggle to achieve a careful equilibrium between ease-of-use, data access, and governance—ensuring that the right people have access to the right data at the right time.

While risk can never be fully eliminated, implementation of data security controls for both protection and recovery, as well as perimeter and endpoint defenses, are vital to securing an organization's information assets, as well as its reputation and legal exposure.

Putting out a proverbial "welcome mat" by exposing access credentials, deliberately or accidentally, poses an inside threat commensurate with malicious outsiders. The enterprise faces an ongoing dilemma from accidental breach by users with poor password hygiene, as much as it does from organized cybercriminals and state actors intent on hit-and-run data theft, and sophisticated extortion schemes such as ransomware.

Disconnecting a network from the internet, while it may seem like a prudent measure, is as shortsighted as expecting everyone in an organization to follow responsible data access, management and usage procedures. Quite simply, it is a flawed business decision that turns companies, workflows and employees into an operational island surrounded by a web of competition It also renders digital transformation—leveraging the full potential of data, especially vast repositories of unstructured data which represent more than 80% of information held by large companies—impossible.

Nonetheless, more and more companies are actually considering cutting off their data infrastructure from the fast lane to competitive advantage in response to the real and growing attack surface. It's an unacceptable tradeoff. Consider that a recent report from Philips and CyberMDX indicates nearly half of U.S. hospitals have disconnected their networks in the past six months due to ransomware.

Research from Gartner reveals that by 2025, three-quarters of IT organizations will be hit by one or more attacks, which is a massive sevenfold uptick from 2020 figures. More concerning from the vantage point of CISOs, and the c-suite in general, is that these attacks increasingly target backup data and administrator functions, which are typically considered the last line of defense.

However, immutable data protection has emerged as a powerful remedy. The Panzura global file system is recognized as a definitional solution in this regard, having been engineered from the start with data resiliency in mind.

While this has always been a foundational element of the Panzura global file system, meant to protect data from inadvertent overwriting or deletion, it is now being adopted at pace by enterprise companies and large organizations looking to ensure data cannot be compromised or encrypted by malicious payloads.

In the case of attack, for instance, data held in the Panzura system can be reverted in a matter of mere minutes all the way to the level of individual files, complete directories, or the entire file system itself—with no data loss whatsoever.

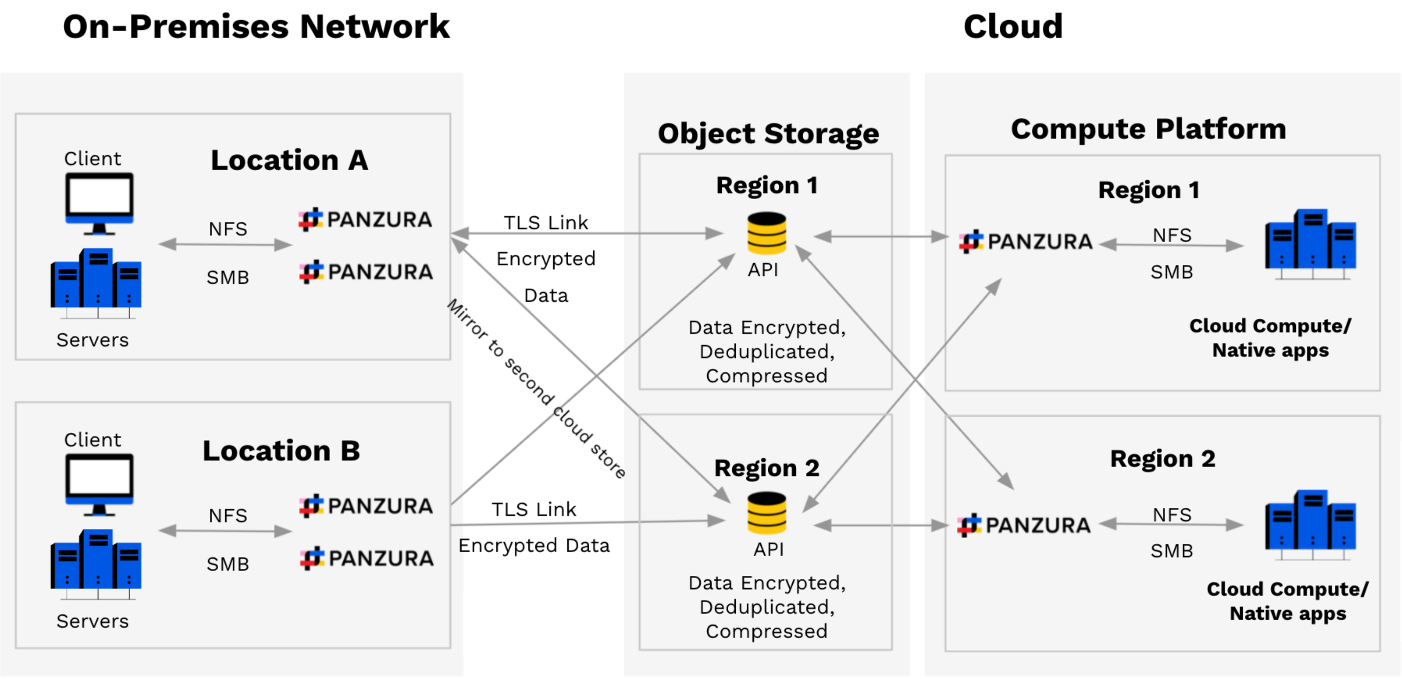
The agility and total security of the Panzura global file system has been well-publicized and verified. When a regional hospital in Illinois was hit by a ransomware attack, their entire IT infrastructure went down. The healthcare facility used automated data protection, backup, and disaster recovery capabilities in the Panzura global file system to quickly restore files to a pre-attack state and undo unauthorized data encryption. Data was restored to previous, clean versions in less than 15 minutes.

In another documented incident, Applied Software, a managed service provider of Autodesk programs and other applications primarily focused on the architecture, engineering and construction industries, saw parts of its own network attacked by a Thor ransomware injected via a rogue PDF file. Panzura allowed the IT team to quarantine infected files and recover them near instantaneously to the version auto-saved a few minutes before the incursion.

While most organizations are understandably reluctant to divulge that they have been subject to an attack, they are universally exposed to the ever-multiplying potential points of entry of the attack surface. Moreover, and perhaps more importantly, they must take into account all of the data and systems that may be affected, and the full amount of damage that a single compromised user can cause, as the full potential "blast radius".

The Attack Surface.

Illustration 1. offers a bird's eye view of a hybrid multi-cloud global file system architecture which, when deployed as shown, protects network environments from ransomware. It also provides the inherent capability of making file access seamless to users meaning the "welcome mat" is eliminated without cutting off the enterprise from the outside world.



CLIENTS

How Varonis helps

Varonis does not install or run anything on a client to monitor for ransomware activity. Rather, it analyzes data, email, and Active Directory behavior in context with perimeter activity from VPN, DNS, and web proxies as means of detecting signs of compromise throughout an attack.

Often, early indications of command and control, reconnaissance, and lateral movement are precursors to unusual data access, exfiltration, and encryption (which Varonis picks up on the servers themselves).

Varonis can automatically identify privileged accounts like service accounts, admins, or executives, and monitor for suspicious activity like privilege escalation. Varonis puts activity from both on-premises and cloud data repositories in a single interface, helping to speed up investigations.

How Panzura helps

Varonis integrates with Panzura to provide contextual performance-based alerts on anomalous user activity in the Panzura global file system. As previously discussed, this makes it possible to augment Varonis with a unified view and dashboard management of the global file system, both on-premises and at the cloud edge.

Initial access to data typically occurs at the client-user level, either through email phishing or any numerous other ways to steal credentials or inject unauthorized code into a network.

When an alert is delivered by Varonis, users can use Panzura Data Services ("Data Services") to search that user's activity throughout the global file system—such as details on individual files, specific directories, or permission touchpoints—and pull all of this information up almost immediately.

Recently, by way of anecdote, one Data Services wildcard search served 800,000 results in a matter of seconds. This type of powerful, advanced search and analysis can be applied to the entire cloud network.

SERVERS

How Varonis helps

Varonis monitors all file system activity on file servers and storage appliances, analyzes permissions, classifies data, and employs behavior-based threat models to detect and provide alerts on any meaningful deviation that may indicate compromise by ransomware.

Varonis proactively reduces the blast radius for any potentially compromised system or user by automatically remediating overly permissive access controls and enforcing a zero-trust model. When users and systems have access to only what they need, it makes it harder for an attacker to access sensitive data without detection as they escalate privileges and move laterally.

When anomalous or suspicious behavior is detected, such as accessing an unusual amount of sensitive data or modifying files in a way that resembles encryption, Varonis can automatically terminate a user session to stop the suspected attackers in their tracks.

In the event of ransomware infection, Varonis logs a full audit trail of the data that the compromised account has accessed or modified, in context with the user's role and working profile, data sensitivity, authentication and internet activity, thus allowing for quick assessment of the damage and reduced recovery time.

How Panzura helps

Working in parallel with Varonis, Panzura Data Services provides an ML- and AI-driven data analytics layer that is fully integrated with the Panzura global file system. This built-in SaaS-based logic platform is unavailable with any competitive solution, and allows organizations to apply advanced cloud-based AI and ML analysis, using intelligent and elastic search, audit and file network logic, over an entire cloud file-storage infrastructure.

Data Services is the engine behind Panzura's ability to deliver sophisticated security, performance and activity alerts, along with tools for IT admins to fully diagnose and troubleshoot their environment. It can track and audit which files and directories have been accessed, opened, changed or even deleted.

Additionally, Data Services will track if a threat-actor changes or deletes file permissions. For example, one tactic employed by adversaries is to attempt to execute malicious code by interacting with or creating system services on servers. If a non-admin user's activity is connected to any global file system processes, Data Services can rapidly pull up all of the activity in the global file system for that specific user, allowing administrators to mitigate potential system compromise by restricting file and directory permissions in real time.

The Data Services layer provided by Panzura also makes it possible to search for activity according to an individual user, or for a specific file type according to a file size range, as well as within a specific date range. Options to customize searches in multiple ways make it easier to produce fast results and insights so mitigation strategies can be applied quickly and at scale.

Panzura CloudFS

The Panzura global file system is deployed on-premises via a CloudFS virtual machine inside of VMware or HyperV. These are merely a virtualization or emulation of a computer system running software applications, and may be susceptible to ransomware attacks themselves. As a result, the virtual machine may be locked to users or encrypted at the hypervisor level, or even individually at the CloudFS level.

Either way, any CloudFS location—servers at the edge that integrate primary storage, cloud storage, back-up, versioning, and WAN acceleration—could consequently be knocked out. However, even in these cases, the file system itself has yet to be impacted, and while a particular location may be down for the count, there are several countermeasures which Panzura employs to ensure that an on-premises implementation remains unaffected.

Local HA

As Illustration 1 shows, there are two CloudFS instances in each location. Should one go down, get encrypted, catch fire or otherwise become incapacitated, the other location, assuming the CloudFS instance was not also on the affected machine, will quickly take over.

In fact, a downed virtual machine has no impact on the global file system itself, as Panzura keeps all data and metadata on the backend object store. Should a location become completely corrupted, administrators can simply redeploy the Panzura template, point it to the object store, and the system will upload the original state once again.

While these examples represent on-premises implementations, cloud implementations are not remarkably different. Panzura supports the most pervasive hyperscalers, and directly from the marketplaces of the major cloud providers.

All that is necessary is to bring up a Panzura instance, as well as a high-availability (HA) instance. Should one become unavailable, the other will take its place. There is, therefore, significantly less probability of an outage. This is because Panzura offers true cloud redundancy via its powerful cloud-mirroring capabilities, while users of competitive unified NAS providers are crippled when primary cloud storage goes offline.

Global HA

Should a data center become completely corrupted within a region, and time is expended rebuilding an environment, it is crucial to know what happens to the files for which locks were "owned" by the CloudFS instances that went down.

Panzura has no single point-of- failure with file locking that ensures always-on data consistency. When central file locking fails, which often happens with inferior unified NAS solutions, the entire Panzura system reverts to read-only.

This is achieved through Panzura's unique concept of a global HA node. This type of backup can be located anywhere, and can take the place of a virtual machine in a region that is no longer reachable.

When necessary, it takes ownership of the cohort's lock management, so that those files may be accessed, and global file system usage everywhere else is uninterrupted.

The benefit is that, in the event of an attack at the hypervisor level, data will not be lost. Given the two types of high availability offered with Panzura, both free of charge, an organization can have confidence that a ransomware incursion will be minimally impactful, and data is fully protected from corruption, encryption or deletion.

OBJECT STORE

A cloud or on-premises object store serves as the back end for the Panzura global file system. The example in Illustration 1 is a cloud-based object store, however on-premises versions can be made just as resilient, with a few minimal architecture modifications.

There are two conceivable attacks on the object storage. Firstly, an attack can come from the front via the file system itself, or secondly, from the side via an attack directly on the object store through cloud consoles.

From the Front

In this scenario, a credentialed user with file system permissions, which has become the victim of ransomware, innocently logs into the network and sets a ransomware payload free inside network boundaries. The ransomware locates the global file system and begins to methodically encrypt its way through files and directories.

Since the back end of the Panzura global file system consists of an actual object store, the data is committed as encrypted "garbage" just as the attackers planned. However, because Panzura is built on an immutable data architecture, it commits deltas (or block changes) over the lifetime of each file.

Moreover, once a ransomware begins to access and encrypt an unusual amount of data in the file system, as previously discussed, Varonis threat models will pick up this anomalous behavior by comparing it against the compromised user's established baseline.

It then alerts admins to the attack, and through the use of PowerShell commands, automated responses can be configured in Varonis to shut down the attack as soon as it is detected, mitigating any potential damage.

Consequently, when the user of an encrypted file attempts to open it, and receives an anonymous message about paying a ransom, they can simply revert the file back to the previous version.

This is done via Microsoft VSS by right-clicking on the file in question. The next step is to go to properties, select the previous version and—Voila!—recovery is instantaneous and downtime is reduced to no more than minutes.

Once an attack has been halted, files held in the global file system have been restored, and an organization is back to work, the next step is typically to restore other general IT systems—those that did not archive data in the Panzura system—from backup tapes or other backup repositories, following the incident.

But Panzura can also make this long night of work a little easier with Panzura Data Services. Previously discussed in this white paper, Data Services can help automate recovery of affected files via an audit log, elastic search, and other technology which has been put in place to assist with such events.

Varonis can detect, mitigate, and audit impact both inside the Panzura global file system, as well as with other on premises and cloud file systems.

Recovery and clone functionality within Panzura Data Services can be used not only to restore data quickly and easily, but it is also useful should an IT department choose to recover data but do not want to restore it to its original location. After an IoC, for example, the security team may still need to run post-mortem assess ments and analysis. With recovery and clone, it is possible to restore data to a different location so quick access to the original data can be achieved while audits are conducted in the background.

Cloud mirroring provides an added layer of protection and control using write-splits to two object storage targets—a primary, and a secondary. Should the primary fail, or become the target of an attack by internal or external bad actors, then an administrator would need only to fail the environment over to the second object storage target to circumvent the exploit.

Once control over the primary environment has been regained, the Panzura files can be re-synced. Incidentally, it is fortunate that cloud vendors do not charge for ingress.

THE BLAST RADIUS

This section explores details of attacks on the client, server, cloud, and known MITRE ATT&CK mitigation strategies. Both Varonis and Panzura can help with detection and recovery, and the following discussion outlines tactics around initial access, recon and foothold, privilege escalation, and impact. Together with Varonis and Panzura, it is feasible to compare and map a threat-actor's activity with the MITRE ATT&CK framework:

- Keep a full audit trail of time-stamped file activity
- Map out what servers have been touched by the threat actor
- Identify the folder to which files have been uploaded
- Reveal who has permissions to access recently uploaded files
- Utilize deep analytics to reveal how your storage footprint is changing and who is causing it
- Run our time-stamped results against your timeline; Provide evidence as needed
- Alert on unexpectedly high CPU load, memory load, or cache misses
- Use File Audit to narrow a search to find damaged files, as well as the compromised user account

Again, this is meant to broaden understanding of what is involved in the meticulous balance of security with ease of use. Panzura and Varonis are committed to ensuring a secure and usable file system environment so people can quickly and effortlessly get back to work, no matter what threats may arise.

Tactics		
Varonis https://www.varonis.com *Built to protect the most valuable and most vulnerable data against cyberattacks.*	**Panzura CloudFS / Data Services** https://www.panzura.com *Built for the Panzura File system designed to search, audit, and provide analytics for your global file system*	**MITRE ATT&CK** **(tactics/techniques/ defense/mitigation)** https://attack.mitre.org *Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations*

Initial Access		
Varonis Alerts on abnormal behavior on the file-server: ● Unusual login times ● Abnormal or black-listed geo-location logins ● Geo-location hopping ● Brute force attack ● Password spraying ● Unusual connections ● Beaconing to C2 servers ● Web shells ● Analyzing web activity & DNS queries	**Panzura CloudFS / Data Services** PDS—Search the owners for: ● Files touched during login times ● When/Which servers the threat actor has been logging into (internet facing servers, DNS servers, etc) ● What locations are impacted ● What files have been created/changed by the threat actor ● Follow the audit trail to discover any malicious activity or information about activity that took place on your data ● Dive deep into what your hot,warm, and cold data consists of and the audit information behind each data set ● Disable SMB 1 and SMB2 ● CloudFS—Data Immutability: ○ Storing event/system logs on CloudFS instance tracks initial access of threat actor ○ Threat actor can't erase footprints	**MITRE ATT&CK** Techniques: ● T1110 (*.001,.002, .003, .004) ● T1190 Detection: ● Monitor authentication logs for login failures or abnormalities ● Failed attempts across many different account types ● Keep logs on Panzura CloudFS to prevent threat actor erasing footprints Mitigation: ● M1026 ● M1027 ● M1030 ● M1032 ● M1036 ● M1051

Reconnaissance & Establishing Foothold

Varonis	**Panzura CloudFS / Data Services**	**MITRE ATT&CK**
Tracks the associations between users and the devices and the resources they access: ● Spots unusual DNS queries ● Unusual amount of reverse IP lookups ● User enumeration activity through analysis of DNS and AD ● Alert on an unusual number of connections made by an account, or connections made to systems not normally accessed ● Detect brute-force attempts like password sprays and credential stuffing ● Detect when attackers use DNS as a covert channel to hide their commands or data transfers as queries ● Detects when attackers hide their traffic in lots of connections ("white smoke") using a domain generation algorithm (DGA) ● Alert on unusual web activity, such as the use of new or unusual user agents ○ Unusual or first-time access to the internet by an account ○ Unusual upload activity	PDS—Check what other files created/accessed/modified/deleted by the owner (threat actor) ● Who has permissions to run these files: nslookup and smbtools, etc ● Map out the times these files have been accessed ● Map out what servers have been touched by the threat actor ● Folder that files have been uploaded to ● Who has permissions to access recently uploaded files ● PDS Analytics reveal how your storage footprint is changing and WHO is causing it (user with most access files ● Run our time stamped results against your timeline / Provide evidence as needed. ● Alerts on unexpectedly high CPU load, memory load, or cache misses ● Use File Audit to narrow a search to find damaged files, as well as the compromised user account. CloudFS—Data Immutability: ● Newly created Mutated or encrypted files from ransomware doesn't overwrite original files. ● Data-in-transit is TLS 1.2 encrypted ● Data-at-rest is AES-256 bit encrypted	Techniques: ● T1590 ● T1591 ● T1592 ● T1595 ● T1596 ● T1598 Detection: ● Monitor for numerous account activity ● Monitor for abnormal file or data transfers (especially those involving unknown, or otherwise suspicious accounts) Mitigation: ● M1017 ● M1054

Privilege Escalation		
Varonis	**Panzura CloudFS / Data Services**	**MITRE ATT&CK**
● Detects when known penetration tools are saved to disk ● Detects when a user searches file shares for files with passwords or other sensitive data. ● Analyzes Active Directory activity to detect credential harvesting (e.g. Kerberoasting) and other attacks. ● Highlights potential targets (e.g. administrative accounts that are associated with a Service Principal Name (SPN)) in a dashboard ● Alert when an account is added to an administrative group ● Alert if accounts connect to the internet for the first time ● Alert if accounts connect to low-reputation domains ● Alert if an account generates unusual upload activity	PDS can search for: ● Owner (threat actor) that have abnormal access to specific Files on the server they're searching for passwords on ● Potential target activity on files, permissions ● Activity for accounts that have been recently added to admin group ● All activity of an account in the file system that Varonis generates an alert on ● Enforce data compliance and security policies. ● Know who is accessing what, when the actions took place, and what they were doing. ● File Analytics provides insight into file system changes, including file size deltas, hot, warm, and cold data that has been accessed or modified, and daily changes of stored data. CloudFS—Data Immutability: ● Files modified doesn't overwrite previous written files ● Can recover original files quickly ● Store critical logs on CloudFS	Techniques: ● T1134 ● 1543 ● T1547 ● T1548 ● T1611 Detection: ● Events Logs ● Detailed command-line logging not enabled ● Abnormal User activity Mitigation: ● M1018 ● M1026

Impact		
Varonis Provides a full audit trail of data activity, showing which files may have been compromised in an attack, which were sensitive, which devices and locations were used to access data, unusual internet or upload activity, and the accounts profile, including role, working hours, and location. Varonis correlates the compromised data with user activity to identify infection rates, credential theft and persistency related to domain changes in AD.	**Panzura CloudFS / Data Services** Inhibit System Recovery: ● Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the recovery of corrupted system to prevent recovery (like VSS) Data Manipulation: ● Adversaries may insert, delete, or manipulate data in order to manipulate external outcomes, to affect a business process, organizational understanding, or decision making Data Destruction: ● Adversaries may attempt to overwrite files and directories with randomly generated data to make it unrecoverable. ● In cloud environments, adversaries may leverage access to delete cloud storage, cloud storage accounts, machine images, and other infrastructure crucial to operations to damage an organization or their customers. Disk Wipe: ● Content Wipe—may erase contacts of the storage devices on specific systems ● Disk Structure Wipe—may corrupt orboot a system wipe the disk data structures on hard drive necessary to Panzura CloudFS provides: ● Ability to segment sensitive files from non-sensitive files by storing on separate Panzura CloudFS rings ● Data-at-Rest AES-256 Encryption ● Data-in-transit TLS 1.2 Encryption ● Panzura Cloud Mirroring in a separate region ● Separate dark site ● Ability to restrict File and directory permissions to ensure ACLs are least privileges principles ● Technical controls to prevent the disabling of services or deletion of files involved in system recovery	**MITRE ATT&CK:** Techniques: ● T1485 ● T1490 ● T1561 (.001, .002) ● T1565 (*.001, .002, .003) ● T1573 Detection: Where applicable, inspect important file hashes, locations and modifications for suspicious/unexpected value. With some critical processes involving transmission of data, manual or out-of-band integrity checking may be useful for identifying manipulated data. Mitigation: ● M1020 ● M1022 ● M1028 ● M1029 ● M1030 ● M1041 ● M1053

Endgame		
Varonis	**Panzura CloudFS / Data Services**	**MITRE ATT&CK**
Can automate responses to abnormal behavior - Disabling the account - Killing active connections - Changing passwords Offers free Incident Response services to help with investigations	CloudFS/PDS—Can stop threat actor attacks: - Disabling SMB/NFS protocols - Stop snapshots - PDS search to track user/file/directory/ server activities - PDS Analytics to reveal any file/storage anomalies - Disable threat actor access to file system CloudFS has Data Immutability: - Storing event logs on CloudFS with cheap object storage allow admins to keep a larger date/timeframe from initial Access to Indication of Compromise - Since Threat actor can't erase footprints, security vendors can quickly track all activity of threat actor footprints - Export & share global search & file audit results with management - Clone and Replace allows swift reversion of the infected files to a previous “clean” version, rendering the ransomware attack harmless. - Set up alerts and receive them in slack, microsoft teams, and/or email - Monitor your top CloudFS instance for CPU and memory usage, disk I/O, events by location, SMB user counts, cache stats, etc. - Data-in-Transit Encryption - Data-at-Rest Encryption	Mission to solve problems for a safer world—by bringing communities together to develop more effective cybersecurity.

Learn About Panzura

Panzura helps enterprise companies take advantage of the cloud's benefits regardless of where data or users are located. Panzura's cloud data management capabilities drammatically reduce hybrid-cloud complexity, and simplify data storage management, while speeding up access and analysis for applications and users.

The Panzura global file system is 70% cheaper to own and operate than legacy storage and other solutions. It provides unrivaled efficiency, stability and edge performance especially at scale. Immutable security delivers permanent, at-scale data resilience for the hybrid multi-cloud with the highest level of protection and recovery against ransomware and other threats.

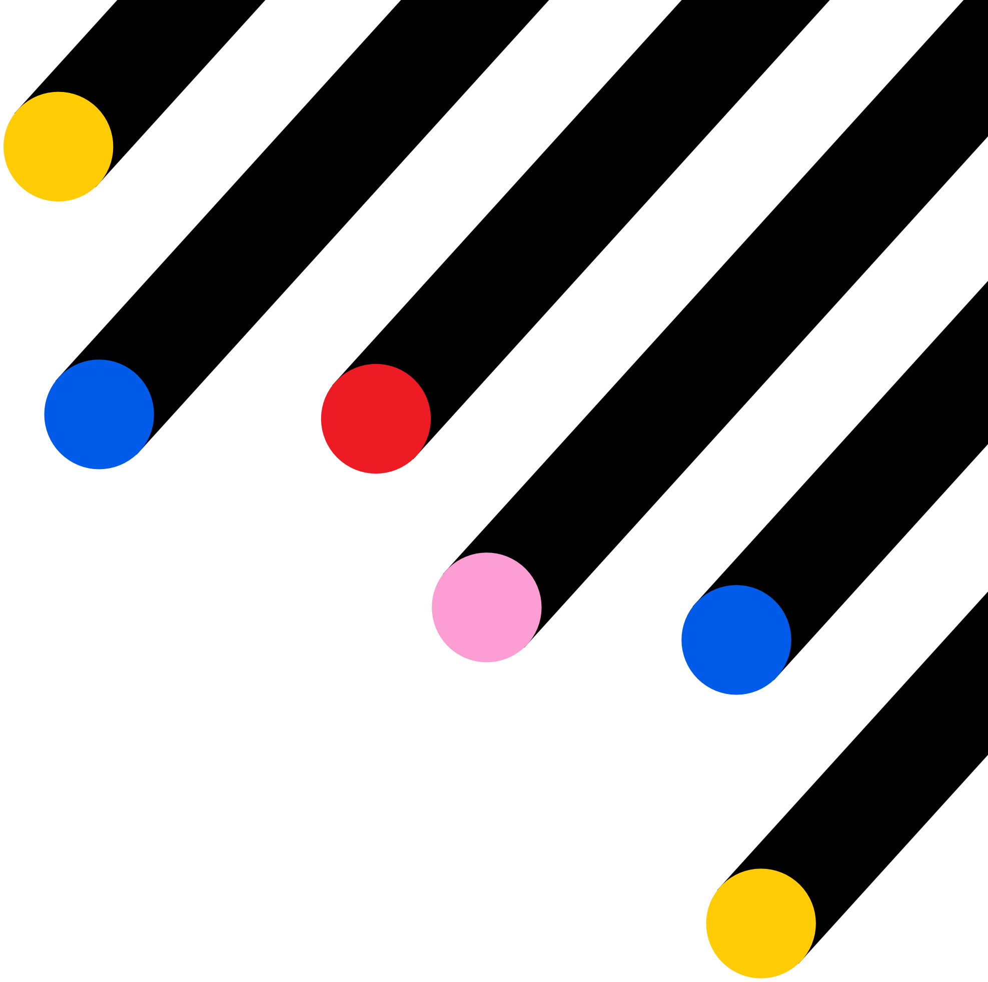
With an industry-leading Net Promoter Score of 87, Panzura provides the highest calibre customer support and services. It's an open-and-shut case when it comes to the competition because Panzura's award-winning technology outperforms at every level.

Learn About Varonis

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cyber-security companies. Varonis focuses on protecting enterprise data: sensitive files and emails;confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects cyberthreats from both internal and external actors by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation.

Varonis products address additional important use cases including data protection, data governance, zero trust, compliance, data privacy, classification and threat detection and response. Varonis started operations in 2005 and has customers spanning leading firms in the financial services, public, healthcare, industrial, insurance, energy and utilities, technology, consumer and retail, media and entertainment and education sectors.



COPYRIGHT AND DISCLAIMER

This document is copyright © 2021 Panzura LLC. No part may be reproduced by any method whatsoever without the prior consent of Panzura. Due to the nature of this material, numerous hardware and software products have been mentioned by name. It is not the intent of Panzura or Varonis to claim these names or trademarks. All trademarks or registered trademarks are property of their respective owners in the United States and/or other countries. Moreover, all company logos, graphics or illustrations are property of their respective owners and are subject to that owner's copyright.

Contact

Panzura
panzura.com
info@panzura.com