COHESITY

WHITE PAPER

April 2023

Amplify Your Ransomware Defenses: Protect, Detect and Recover

Withstand and Recover from Ransomware and Cyber Threats

Table of Contents

Cohesity for Cyber Resilience

The Cohesity platform provides exceptional value for organizations to protect and manage vast enterprise data stores. But cyber criminals target data stores for various nefarious activities, most notably ransomware and data theft. Ransomware continues as the leading threat as it provides easy monetization, and therefore cyber criminals work non-stop to compromise organizations.

And ransomware attacks show no signs of waning. In 2021, an estimated 714 million attacks occurred1 with a new organization becoming a victim every 11 seconds2. Cybercriminals are highly organized and have created tools and services for various stages of a ransomware attack. With one errant user click, a simple system misconfiguration, and the infiltration of new undetectable malware, organizations can face disastrous results. Ransomware attacks can result in customer distrust, revenue loss, and the disruption of current and future operations.

Along with ransomware, global conflict has raised the risk of nation state sponsored attacks. As noted in the US CISA 'Shields Up' alert and warnings from other nations, all organizations must take exceptional care to ensure their information systems can resist sophisticated and persistent attacks.

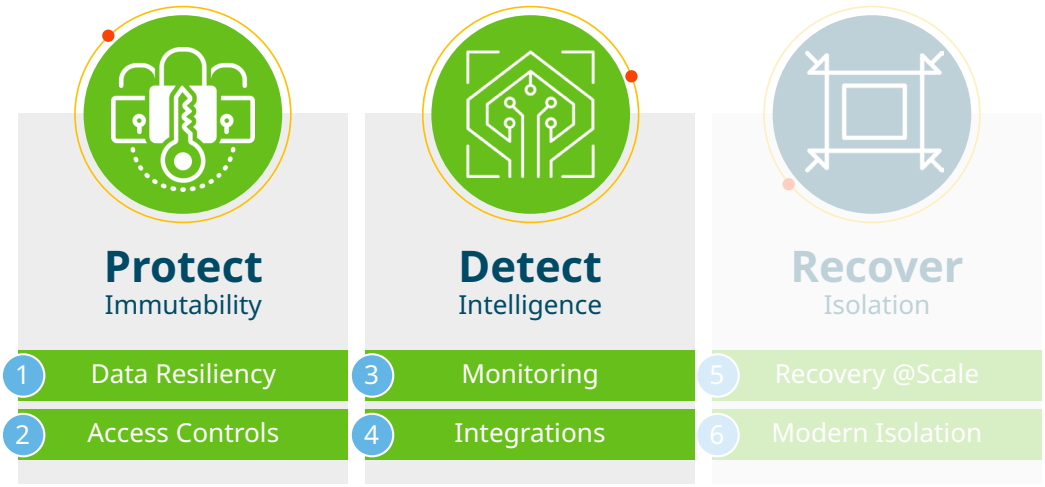
These challenges and the need for 24x7x365 operations create a mandate for strong security for data management, where the data management platform can resist and actively defend against data centric threats and most importantly, recover at scale. Core security capabilities ensure that data can not be corrupted or deleted by ransomware attacks, stolen by data thieves or malicious insiders and that organizations can detect ongoing attacks are more important than ever.

The First and Last Line of Defense Against Ransomware

Before attacks occur, organizations need to **protect** the recovery data and platform; during an attack, **detect** threats in data and users; and after an attack, **recover** data and processes @scale. Protecting, detecting and recovering from ransomware, data breaches or insider threats requires several key capabilities and functions.

For protection and detection, the protect and detect capabilities provide data resiliency for preventing the intentional or accidental destruction of data. The safeguards include strong access controls to protect settings from unauthorized access or changes and to secure and ensure the confidentiality of the data. Cohesity leverages AI/ML for the detection of threats and vulnerabilities, monitoring of data and user to identify attacks and data exfiltration, and classification to assess attack impact. Supporting these capabilities are integrations with leading security applications to automate incident response as well as to leverage existing enterprise security services such as key management, identity and access management, multi factor authentication, and threat and vulnerability scanning. These capabilities work in concert to provide a hardened data management platform that will prevent the ability of an attack to tamper with or destroy data and to help organizations better detect attacks in progress.

For recovery, Cohesity provides unparalleled recovery at scale and modern isolation. Recovery at scale allows organizations to identify their best recovery point, detect vulnerabilities and threats in their backup data, understand the status of specific data, immediately provide access to files and objects and restore thousands of VMs in minutes. Modern isolation provides trusted recovery for worst case scenarios, where the organization's primary location has been disabled and is not available or suitable for recovery.



Lock the Data and Platform, Monitor for Threats and Vulnerabilities

Data resiliency consists of three essential functions. First, data must be immutable and have configurable persistence; the data can not be changed once written and specific copies will be kept until they expire as defined by the organization's policy. Next, data stored and transmitted by an organization's data management platform must utilize strong encryption to prevent the unauthorized viewing of data. Privacy and industry regulations such as GDPR, PCI and HIPAA require organizations to encrypt personal identifiable information (PII), payment card industry (PCI) data and protected health information (PHI); and this represents a small subset of global laws and regulations mandating this safeguard. These capabilities protect the data from malicious actions spawned by ransomware and ensure that data retains confidentiality and integrity. Finally, to ensure the platform is available for backup schedules as defined by the organization's recovery point objectives, the data management platform requires fault tolerance with redundancy to ensure no single point of failure.

Access controls enable organizations to precisely control who can access and modify the data management platform, adhering to Zero Trust principles. With multi-factor authentication (MFA), only verified users may login to the platform. This is critical to prevent administrative account takeover and unauthorized changes to data and settings. Coupled with granular role-based access controls (RBAC), organizations can tightly control what capabilities users may access to support the principle of least privilege. Further controlling changes to platform settings, quorum prevents unauthorized updates by requiring two or more approvals to change configurations or settings.

Monitoring provides capabilities to analyze and monitor platform data for indications of attacks in progress, compromised workloads, and intelligence about the data. Detection and analysis capabilities include monitoring the data for unusual changes that may indicate the presence of ransomware or other malicious activity, as well as scanning backup data for indicators of compromise (IOCs). By using threat protection to scan backup data for IOCs, organizations can ensure that their recovery is reliable and will not reintroduce malware that could create reinfection.

A critical component to understanding the potential impact of a ransomware attack is data classification. Data classification helps organizations determine what private or sensitive information may have been exposed. To support rapid response and recovery, ransomware detection alerts can be routed to both IT and security operation teams for coordinated incident response.

Security Integrations to existing security infrastructure provides a force multiplier for securing and protecting the data management platform. Integration with vulnerability management and threat detection solutions help identify risks and threats whilst identity and access management integrations enable organizations to leverage existing access controls. SIEM and SOAR integrations facilitate incident response and ticketing, providing the environmental support needed to secure the platform and enable seamless collaboration of security and IT operations.

The Cohesity platform uses Zero Trust architecture, analytics, and platform safeguards to secure and harden the data management platform. This provides several essential benefits for reducing risk and improving cyber resiliency. These benefits include the security and resilience of data against ransomware attacks and data breaches, data protection for operational failures and natural disasters, the security of archived data, and data intelligence to support data governance and compliance.

Drilling Down

The following provides a detailed review of the capabilities and functions that power the Cohesity platform. Each major component of the architecture is reviewed by category, which consists of:

Data Resiliency: Encryption of Data at Rest and in Motion, Fault Tolerance, and Immutable Data Storage

Access Controls: Multi-Factor Authentication (MFA), Role-Based Access Controls (RBAC), Quorum, Auditing, and Continuous Monitoring

Detection and Analytics: Anomaly Detection, Vulnerability and Threat Detection, Data Classification, Behavior Monitoring

Security Integrations: Security Information and Event Management (SIEM), Security Orchestration and Automate Response (SOAR), Identity Management, Threat Detection Solutions, Vulnerability Management, and Application Programming Interface (API)

Data Resiliency: Ensure the Integrity and Availability of Platform Data

Encryption of Data at Rest and in Motion

Cohesity encrypts all data and data flows within the platform. Encryption prevents unauthorized usersfrom viewing data outside of the platform; data stored in the platform is unintelligible unless accessed and decrypted by an authorized user. Most privacy and industry regulations, notably GDPR, CCPA, PCI and HIPAA require organizations to protect PII, PCI and PHI with encryption. Platform data is encrypted at rest using AES 256 encryption. The platform has multiple options for securely managing encryption keys—either Cohesity's managed Key Management Service (KMS) or organizations have the flexibility to manage keys via Amazon WebServices KMS or other third-party vendors such as Thales, Fortanix and Entrust.

For data in flight, the Cohesity data management platform uses the TLS standard. TLS encrypts data to ensure that eavesdroppers and hackers are unable to see data flowing to and from the platform. This is critical to protect private and sensitive data for security and compliance. Cohesity utilizes the TLS 1.2 and mTLS protocols for transport layer security with only FIPS-approved cipher suites with Perfect Forward Secrecy (PFS) protection.

Fault Tolerance

The Cohesity data management platform provides tolerance for multiple system faults to provide high availability of the platform. This prevents outages from a single point of failure to support SLA and business continuity requirements. Clusters can continue operation with multiple failures of HDDs and SDDs and nodes, chassis and racks. Additionally, the clusters can sustain faults to power supplies, fans, and networks.

Immutable Data

Data that is backed up by Cohesity will never change from its saved state, until the data expires. Cohesity's SpanFS™ provides an immutable backup snapshot to prevent modification or deletion of data. Based on hyperscale architecture, Cohesity SpanFS can store backed-up data in its secured file system in immutable snapshots that cannot be directly accessed or mounted from outside of a Cohesity cluster. The backup snapshots are stored in a read-only state; no external application or unauthorized user can modify the snapshot.

Any attempts to write to an immutable backup snapshot are written on (zero-cost) clones, which are also marked read-only upon completion of each Protection Run. For any mount-based restores used during Cohesity's instant mass restore process, the internal view is first cloned and then exposed to the external environment, always keeping the internal view inaccessible externally. Writes to internal views during backup are only allowed via trusted internal services and authenticated APIs. For additional security, DataLock, Cohesity's Write Once Read Many (WORM) features can be applied to Cohesity snapshots. If DataLock is enabled, the backup snapshot cannot be deleted by anyone, including administrators, until the DataLock expires.

Access Control: Zero-Trust Architecture

As defined by the National Institute of Standards and Technology (NIST), zero trust is as follows: "Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources." Zero trust focuses on validating the authenticity and authorization of users for any access or changes to the platform.

Multi-Factor Authentication (MFA)

Multi-factor Authentication (MFA) provides strong authentication of users to thwart unauthorized changes to the platform setting or data. MFA improves platform security by requiring users to identify themselves by more than a username and password. Passwords and usernames are susceptible to brute force attacks and can be stolen. MFA requires the user to authenticate login requests with a response only they can provide (such as a mobile phone challenge), or Time-based One-time Password (TOTP). Cohesity supports native MFA or third party MFA providers such as Ping, Duo, Okta, and more.

Role-Based Access Controls (RBAC)

Granular Role-based Access Control enables an organization to grant the least privilege required for users to execute their job requirements, minimizing risk, and keeping areas outside their responsibilities unreachable. Organizations can restrict Cohesity user roles to specific applications, capabilities, or workflows in the platform, thereby limiting what a user does based on their role and responsibilities. For example, organizations can restrict specific users to only performing backups or executing data discovery.

Quorum

Cohesity leverages quorum to empower organizations to prevent unilateral changes to the platform within administrative accounts—a crucial control to protect against unintentional user error, rogue admins, or compromised accounts. With quorum, user requests to change settings or administrative functions require multiple approvals to authorize the request.

Auditing

The Cohesity platform maintains a user audit trail for all actions performed on the Cohesity cluster. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non compliance by providing information for audit investigations. Audit logs capture user activity for login/logout, changes to data or the data's properties and job scheduling. The platform organizes logs by categories, such as Active Directory or Cluster, for rapid analysis.

Security Posture Monitoring

The Cohesity platform provides environment monitoring to help reduce the risk of human errors and misconfigurations. Monitoring scans the Cohesity environment, including an array of security configurations, and considers a host of factors such as access control, audit logs, and encryption framework that are critical to protecting the security posture of the data cluster.

Monitoring: AI and ML to Detect Malicious Activity

Data Anomaly Detection

The Cohesity platform immediately analyzes data ingested from production environments on each and every backup for telltale signs of unusual activity or data changes. This activity may indicate a ransomware attack. A central dashboard alerts on anomalies based on how the timing and frequency of data reads and writes, the randomness of data and how files change, including files added, deleted and modified. Using the Cohesity anomaly detection feature, organizations can set alerts for conditions that could indicate ransomware or other malicious activity.

User Behavior Anomalies

Anomalous user behavior and inappropriate data setting can increase the risk of data leakage. With DataHawk, organizations can review data access and logs in SmartFiles for unusual data activity and use that could indicate malicious actions. Administrators can easily search audit logs to determine who is creating, modifying, accessing, or deleting files in a manner that does not support typical operations. This provides security teams insights into behavior that could indicate a ransomware attack or other malicious activity.

Vulnerability and Threat Detection

Vulnerabilities in organizations' landscapes can be exploited by threat actors to gain access to systems and launch attacks. With the Tenable vulnerability solution, Cohesity helps organizations identify, investigate, and prioritize vulnerabilities. The solution analyzes backup VMs and will identify over 76,000 vulnerabilities and helps organizations prioritize the vulnerabilities for remediation.

Threat detection helps identify malicious software that could be used by attackers to launch ransomware, or cyber-attacks, steal data or gain control of an organization's systems. Cohesity leverages threat detection to scan the platform to detect threats and malware. Threat detection is driven by threat intelligence from Qualsys to help the organization identify indicators of compromise (IOCs) that could indicate an emerging attack. Cohesity has native support for malware detection via its ClamAV solution. These solutions help organizations ensure their recovery data does not have threats and malware prior to restore.

Data Classification

Data proliferation defines the growing locations, volume, and diversity of data across organizations also referred to as 'mass data fragmentation.' With proliferation, organizations need automation to track the growing sources of critical and sensitive data.

With the new DataHawk solution that leverages BigID's proven data classification engine, Cohesity provides automated data classification so organizations can discover and classify information to identify potential sensitive data exposure from attacks. AI-based classification illuminates s sensitive data location and classification.

These predefined policies help organizations meet their global and regional requirements for GDPR, CCPA, HIPAA and other regulations. And organizations can leverage 100+ predefined patterns to create policies tuned for their specific challenges and needs.

Security Integrations: Leverage Existing Tools for Detection, Response, and Remediation

It takes a village to keep the bad actors at bay. Virtually all organizations have tool sets for detecting malware, viruses and vulnerabilities and have created extensive practices and policies for validating that information resources are safe for use. Therefore, the Cohesity platform is designed to integrate into an organization's existing security strategy, e.g. to ensure consistent implementation of user authentication and data encryption, complement existing solutions and processes for incident response and management,

and leverage threat and vulnerability detection solutions already in place. This allows the Cohesity data management platform to support and amplify the organization's security policies and processes. Integrations encompass several security categories, including SIEM and SOAR, identity management, vulnerability management, and threat detection as follows:

Security Information and Event Management (SIEM)

Organizations utilize SIEM to gain real-time analysis of security alerts generated by applications and network hardware. The Cohesity data management platform generates alerts that indicate ransomware attacks or other malicious activity. With Cohesity and Splunk, Microsoft Sentinel, or Cisco SecureX integration, organizations can automate their response to these alerts. This enables organizations to accelerate ransomware threat investigations and response by aggregating and correlating insights into compromised data with other global intelligence and contextual information into a single platform.

Security Orchestration and Automate Response (SOAR) and IT Service Management (ITSM)

SOAR and ITSM helps organizations with the security management, security operations automation, and security incident responses. They enable organizations to rapidly and effectively respond to incidents, such as suspected ransomware by the Cohesity data management platform. Cohesity has integrations with Palo Alto Networks Cortex XSOAR solution and ServiceNOW ITSM. These integrations help security and IT teams manage and recover from ransomware attacks. Data anomalies are detected by the Cohesity data management platform and routed to XSOAR or ITSM which provides automated incident processing and management coupled with threat intelligence and malware detection.

Identity Management Solutions

Many organizations use identity management solutions for a common, highly secure method to authenticate users. The Cohesity data management platform supports native MFA or third-party MFA providers such as Ping, Duo, Okta, and more.

Vulnerability Management

Vulnerability management provides insight into potential risks posed by vulnerabilities in the backup VMs. The solutions categorize and prioritize these vulnerabilities to help organizations reduce the risk of data breaches and malware such as ransomware. Organizations can leverage the Tenable vulnerability management technology, with over 76,000 documented vulnerabilities, to help identify vulnerabilities of the VMs managed by the Cohesity Data Management Platform. With Cohesity CyberScan, powered by Tenable, a detailed dashboard gives a global view of all cyber exposures within your production VM environment to help reduce risk. By understanding blind spots in the infrastructure, organizations can address critical cyber exposures and vulnerabilities before they are exploited.

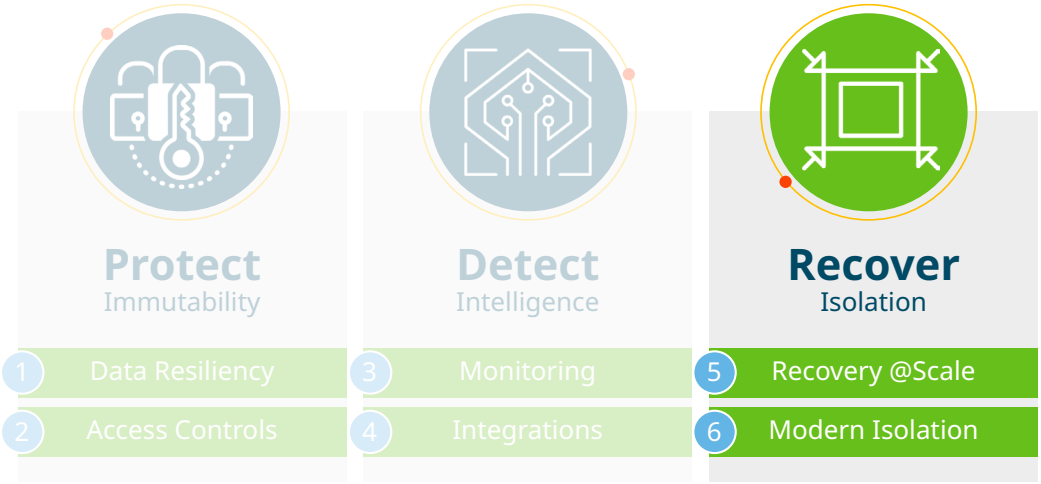
Privileged Access Management

Privileged access management enables organizations to strengthen the security of administrative access to enterprise resources. With backup and recovery solutions such as Cohesity DataProtect, administrators may need administrative access to hundreds if not thousands of data clusters for management and administrative purposes. CyberArk Central Policy Manager (CPM), integrated with the Cohesity data security and data management platform, eliminates the need for time-intensive manual processes for credential management while simultaneously securing user identities from cyberattacks. Administrators can also gain secure and controlled access to Cohesity cluster and IPMI interfaces through CyberArk Privileged Session Manager (PSM), eliminating the risk from internal and external threats looking to compromise user identities and data.

Application Programming Interface (API)

Beyond the pre-built integrations called out in the above, the Cohesity data management platform can integrate with any security solution with a secure, yet open API. Alerts, status information and other intelligence from the Cohesity platform can be leveraged by third-party security applications to meet the specific needs and operating challenges of organizations. So, expect to see the list of out-of-the-box integrations evolve over time based upon customer demand, but now it's possible to create bespoke integrations today to suit your needs.

Recover: Instantly Recover Critical Business Processes and Files



Recovery at Scale: Accelerate Recovery, Support 24x7 Operations and Hit SLAs

Recovery at scale provides organizations immediate access to critical business processes and data to meet their demanding recovery time objectives (RTOs). First, based on the ML-models, the platform provides organizations the last known good recovery point and powerful search so that organizations can ascertain the

status of specific data instances. Next, with fully hydrated snapshots, organizations can recover hundreds of VMs, files or any size database instantly. This process allows IT staff to meet business SLAs while saving time and resources.

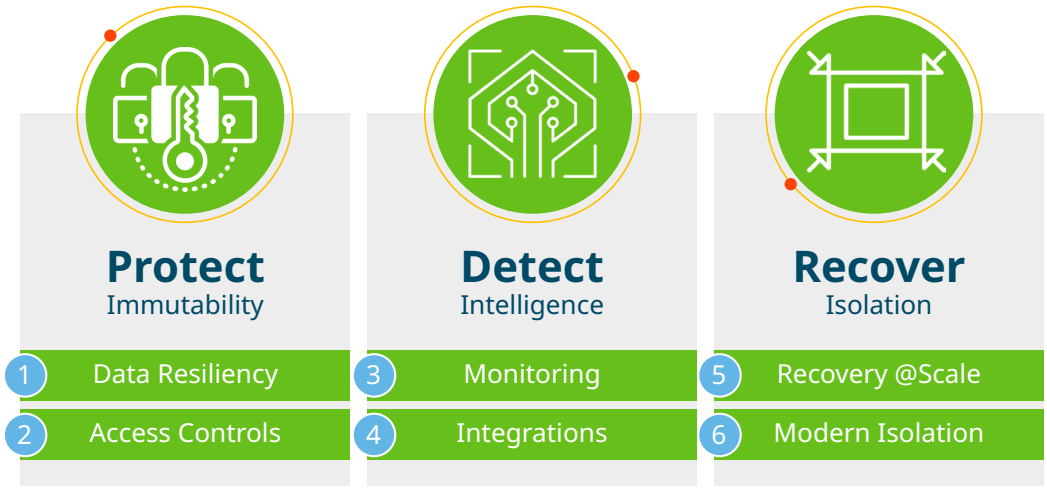
And organizations can have immediate access to files and objects. Organizations can rapidly access file and objects with Cohesity Smartfiles. They can instantly clone the last good backup of its NAS shares and serve those files directly from the Cohesity cluster—recovering the service to users without the need to move data. Organizations can also recover critical data from ActiveDirectory if access control lists have been affected.

Modern Isolation: In Case of Catastrophic Loss of Local Backup Data

As recommended by 'Shields Up', organizations should implement the 3-2-1 rule for backup data: 3 total backup data copies, 2 local and 1 isolated. The isolated copy provides another offsite copy of backup data in case of a catastrophic event that disables the local copies of data.

Isolation can be done in various ways, with isolation to tape, customer managed isolation to cloud or SaaS provided isolation. For demanding RTO and RPO requirements, most organizations would utilize isolation in the cloud or via SaaS. These options provide the best balance of recovery and isolation. But the choice of isolation is not an either or decision, multiple options can be selected to support various data types, such as transaction data or primarily static intellectual property, source code or trade secrets.

Conclusion: It's Not an Option



Cohesity's capabilities to protect, detect and recover for ransomware defense is a layered approach to securing and increasing the resilience of data and providing rapid recovery. Protection leverages encryption, immutability, and WORM capabilities to protect backup data from unauthorized changes and Zero Trust principles to control and manage platform user access with granular RBAC, MFA, and bank grade security with Quorum. Detection provides actionable insight with analytics for data anomalies and user behavior, and near real-time threat detection, and is integrated into existing controls to amplify existing ransomware defenses. The final phase, recovery, uses powerful instant mass recovery and file access to get critical business processes and data back online.

And to keep pace with the continually changing threat landscape, the platform is driven by AI and ML that provide critical capabilities to stay ahead of emerging security threats that can't be done with manual processes.

Ransomware and other threats have elevated data management to the forefront of security and cyber resiliency. Without a hardened, intelligent, and integrated data management platform to resist, thwart and recover from cyber attacks, organizations will risk catastrophic data loss and business interruptions.

Sources:

1 https://blog.sonicwall.com/en-us/2021/10/cyber-threat-alert-ransomware-breaks-another-record/

2 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

About Cohesity

Cohesity is a leader in data security and management. We make it easy to secure, protect, manage, and derive value from data—across the data center, edge and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, data security, disaster recovery, file and object services, dev/test, and analytics—reducing complexity and eliminating mass data fragmentation.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.

2000044-004-EN 4-2023