

An abstract graphic in the top right corner of the slide. It features a dark grey, isometric-style building with several rectangular cutouts. To the left of the building, there are several concentric, glowing green lines that curve around the building's corner, suggesting a signal or data flow. The background is a solid dark blue-grey.

Cyber resilience in the ransomware era

Five keys to withstanding and
recovering from cyberattacks

COHESITY

From Data Resilience to Cyber Resilience

Natural disasters are a huge threat to business operations. A lightning strike, hurricane, tornado, or flood can cause great damage and bring business to a halt. That said, they're not actively trying to victimize your business through ongoing attacks. In these instances, data resilience strategies ensure that data remains intact and accessible even in the event of hardware failures, accidental deletions, or natural disasters.

Compare that to a cyber threat. Threat actors never stop working and employing new tools to hold your data hostage and take your business down. Attack vectors are often multifaceted and evasive. And the risk of reinjecting vulnerabilities, compromised accounts, and other attack artifacts back into your environment is a pervasive threat. Compared with traditional business continuity and disaster recovery scenarios where the root cause is usually obvious, facing cyber adversaries requires investigation to discover these causes and drive remediations to prevent their recurrence.

In addition, in a ransomware attack, the security infrastructure and key evidence may have been impacted by the incident, and impact the ability to deliver products and services.

When developing a cyber resilient business, IT and security leaders need more robust, dynamic, and collaborative processes compared with processes used when responding to a standard outage caused by natural disasters or technical outages. Cyber resilience builds on data resilience practices and encompasses elements like cybersecurity preparedness, incident response plans, employee training, and threat intelligence.



From Data Resilience to Cyber Resilience

Today's cyber threats need modern solutions that promote global visibility into protected data assets and streamline collaboration between IT and security practitioners. Cohesity's modern, AI-powered data security and management solutions offer capabilities to strengthen cyber resilience, and protect the business at large.

The result is a more resilient business better able to withstand the threat of cyberattacks.

With Cohesity you can:



Understand your data and risks



Respond efficiently and effectively to attacks



Ensure your data is safe and available



Recover clean data at scale



Automate security operations

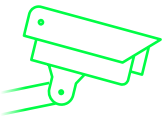


Not If, But When...

Ransomware attacks have recently been growing in complexity and frequency. In fact, 90% of organizations believe the threat of ransomware attacks has increased in 2023¹. And yet, 80% fear their cyber resilience strategies aren't enough². This increased risk is top of mind for security and IT leaders, CEOs, and board members, who seek assurances that when—not if—an attack occurs, they'll be able to respond quickly and safely to them.

In the event of an attack, streamlining detection to minimize the threat is a primary challenge. Organizations need centralized visibility across all data estates, with automated detection for anomalies and cyber threats so they can assess the risk before introducing contaminated data back into production.

A lack of interoperability between legacy systems and new and existing data security technologies (e.g., vulnerability management), and urgent needs to build for scale (e.g., cloud hosting), further compound this risk.



80%

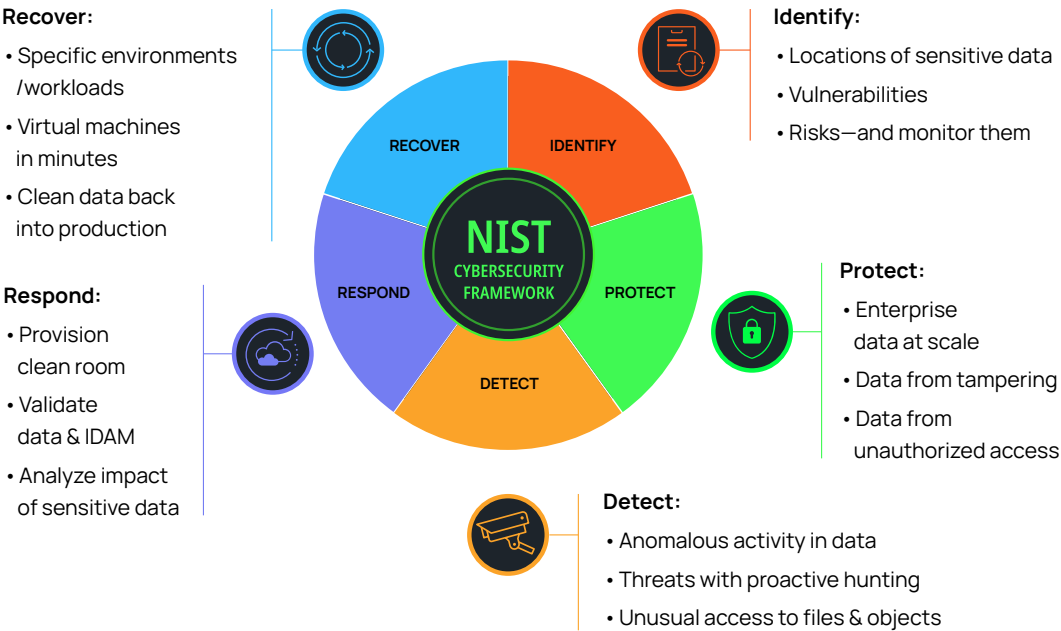
of organizations fear their cyber resilience strategies aren't enough.



^{1,2} The State of Data Security and Management Report, 2023

5 Keys to Creating a Cyber Resilient Business

Cohesity's data security and management solutions align to the key functions of the NIST cybersecurity framework: identify, protect, detect, respond, recover.



Before an Attack		During an Attack		After an Attack
Identify	Protect	Detect	Respond	Recover
Identify critical and sensitive data with AI-powered data classification and continuously scan for anomalies.	Protect and isolate on-prem, cloud-native, and SaaS data with immutable snapshots and multilayered security controls.	Detect attacks using AI-powered threat intelligence to identify the latest ransomware and other cyberattacks and minimize impact.	Rapidly establish cyber clean rooms to support triage, investigation, and remediation tasks to prevent future attacks.	Recover quickly and safely from cyberattacks with targeted restore of data at any scale to any point in time.

Let's now look at the key capabilities across each function that improve cyber resilience strategies against today's threat actors.

1: Identify

critical business data and anomalies

Being cyber resilient begins with modern backup and recovery. With unlimited, immutable snapshots, you can use backup data within Cohesity to understand risk exposure and minimize the impact of attacks. Start by locating your organization's most sensitive data. Then use AI-driven data classification to tag sensitive data—streamlining risk management, optimizing resource allocation, and strengthening overall resilience against cyber threats.

- **Discover and identify sensitive data** – Data classification allows organizations to discover and categorize sensitive data and digital assets based on their importance and sensitivity. Customers can save time chasing false positives and reach resolution faster with more than 200 built-in classifiers and AI-driven algorithms to analyze, tag, categorize, label, and classify data sets. Data classification also helps identify the extent of the breach to guide triage and response prioritization, and regulator notification workflows, to minimize regulatory risk. Classifications can also be integrated with governance, risk, and compliance tooling to further enhance response times.

- **Automatically monitor backup data for anomalies** – Monitor and detect anomalies that can signal ransomware attacks, malicious insiders, and even wiper attacks. Share these alerts with leading SIEM/SOAR solutions to unite operational teams. In the fight against ransomware, Cohesity's AI-driven learning gives you an advantage by offering insights people may miss by automatically and continuously monitoring the data ingested from primary sources.
- **Gain global visibility into data and security posture** – The Cohesity Security Center centralizes the management and response to ransomware and other threats that pose a risk to your data and your organization's reputation. Thanks to its powerful dashboard and drill-down capabilities, you can leverage security posture monitoring, anomaly and threat detection, data classification, user activity tracking, and cyber vaulting—helping protect your organization's data, detect an attack, and recover quickly without paying a ransom.

1: Identify

critical business
data and anomalies

“We needed a next-gen data management platform, and Cohesity stood apart because of its ease of use, rapid recovery at large scale, and strong cyber protections.”

Nationwide

2: Protect

enterprise data at scale

As data estates grow in complexity due to the heterogeneity and size of data assets, so does the likelihood the business will be severely impacted if a cyberattack or data outage occurs. Scale data protection with a single management plane across workloads (on-prem, cloud, and SaaS) and significantly mitigate an attack's impact.

- **Isolate critical business data** – You can automatically replicate data to another immutable Cohesity cluster on-prem or in the public cloud to ensure an additional immutable copy of the data is always available.
- **Reduce your attack surface** – Many environments are architected on fragmented point products. In contrast, Cohesity consolidates all backup and disaster recovery components on a single, global platform. It includes global variable-length dedupe across data sources and compression to further reduce attack surfaces. Using Cohesity CyberScan, customers with a Tenable license can even perform vulnerability scans on backup snapshots, avoiding impact on production environments.
- **Scale data protection across data estates** – Because Cohesity is architected on hyperscale architecture, it allows IT admins to grow their Cohesity clusters limitlessly and store unlimited snapshots and clones without any performance impact. Unprecedented data deduplication not only ensures you can store more data at a much lower cost, it also means you can instantiate snapshots to any point in time to improve forensic investigations.



2: Protect

enterprise data at scale

- **Protect backup data at scale with multilayered security architecture** – Using Zero Trust principles, Cohesity has adopted a multilayered security approach that minimizes the risk of backups becoming a ransomware target—and the risk of inadvertent or malicious deletion of data.
 - Immutable read-only state snapshots – Cohesity's platform is purpose-built to thwart cyberattacks by protecting and storing backup snapshots in an immutable state. Snapshots are not mounted for external applications, and the ability to modify or delete the immutable backup snapshot without approval is disabled.
 - DataLock policies – Cohesity's write-once-read-many (WORM) capabilities for backup allow certain roles to set unchangeable DataLock policies on selected jobs.
 - Multifactor authentication (MFA) – Any person accessing a Cohesity backup must authenticate using two forms of verification. Cohesity supports multiple authentication providers so your organization can maintain strong authentication even if the primary server is impacted by a cyber incident.
 - Data encryption – Cohesity features software-based FIPS-validated, AES-256 standard encryption for data in flight and at rest.
 - Role-based access control and least privilege – Cohesity reduces the risk of unauthorized access by enabling IT staff to grant each person a minimum level of access to data needed to do a particular job.
 - Separation of duties – With Cohesity quorum, any root-level or critical system change must be authorized by one or more persons to protect data from insider threats and stolen credentials.

3: Detect threats

Cybercriminals will stop at nothing to find and exploit any vulnerability in your data environment. Proactive threat hunting, continuous monitoring of data changes and user behavior, and detecting anomalies are critical for minimizing the impact of an attack. This is where AI can play a critical role in getting ahead of cybercriminals by detecting data activity imperceptible to humans.

- **Proactively scan for threats** – Systematically identify and assess vulnerabilities and potential security risks within your organization's digital infrastructure. Cohesity incorporates a deep AI learning-based ransomware detection engine and provides intelligent threat protection with rapid scanning for anomalies, potential threats, and other indicators of a ransomware attack. The solution integrates a set of highly curated and managed IOC (Indicators of Compromise) threat feeds that are updated daily. Leverage over 100K built-in threat rules, or bring your own Yara rules, to ensure elusive malware is identified. By regularly scanning networks, systems, and applications, you can easily pinpoint which backups have indicators of malware and which don't.

- **Recognize patterns, data changes, and user behavior anomalies** – Proactively monitor, model, and optimize operations using predictive analytics to assess trends. Cohesity's AI-based algorithm establishes patterns and continuously scans for data changes in Cohesity. Cohesity anomaly detection expedites remediation by sending a notification to your IT and security administrators as well as to Cohesity's support team. Incident Responders can easily search audit logs to determine who is creating, modifying, accessing, or deleting files. This provides security teams insights into behavior that could indicate a ransomware or wiper attack or even a malicious insider.
- **Quickly take action** – Once notified, your IT and security administrators as well as Cohesity's support team can work together to determine next steps. In addition to monitoring backup data change rates to detect potential ransomware attacks, Cohesity uniquely detects and alerts for file-level anomalies within unstructured files and object data.

3: Detect

threats

“Though we hadn’t experienced a major cyberattack, we liked knowing that Cohesity’s backups can’t be altered by attackers, and that data is continually scanned to detect suspicious changes from one backup to the next.”

Chris Dove, Enterprise Architect, California Department of Finance

4: Respond

quickly to threats

In the event a threat actor has evaded defenses and encrypted data in a ransomware attack, before you consider recovery, it's critical to invest time in response to lower the likelihood of reattack. In the event of a ransomware attack, every second means products and services cannot be provided to consumers. Fortunately, up-front response preparedness will streamline recovery efforts.

- **Global actionable search** – Allows you to globally search data and metadata across all workloads to take appropriate actions such as rapid instantiation of systems at any point in time during the incident or recovery from a ransomware attack, from a single UI.
- **Establish a cyber clean room to assess the impact** – Data needs to be isolated and protected from bad actors so when it's time to recover, your backup copies will be available and clean to safely restore your data, apps, and systems. By isolating data through a virtual air gap, you can establish a clean room to perform forensics, understand vulnerabilities exploited in the attack, and ensure that infected data is not reintroduced back into production.



4: Respond

quickly to threats

“Without our Cohesity views, we would not have been as equipped to rapidly investigate and perform the needed forensic activities.”

David Bannister, Vice President of Technology Services,
SiteOne Landscape Supply

- **Scan for sensitive data exposure and regulatory compliance**
– Use ML/NLP to determine if sensitive data has been exposed and ensure appropriate remediation and compliance processes. Cohesity supports over 200+ prepackaged and customizable patterns to understand regulatory obligations (e.g., GDPR, HIPAA), automatically or proactively discover and classify personal, health, and financial data when a breach occurs, and determine whether sensitive data was exposed during the attack. Data anomalies detected by Cohesity can be routed to SOAR or ITSM systems to automate incident processing and management and streamline engagement with regulators.
- **Develop incident timeline** – Cohesity offers unlimited, immutable snapshots that can be instantiated within the clean room to any point in time. From there, you can more easily compare deltas across data and systems (e.g., Active Directory) to develop an incident timeline and allow incident responders to perform granular forensics leading up to an attack.
- **Remediate vulnerabilities and remove persistent mechanisms** – Use the knowledge gained during clean room forensic investigation to patch vulnerabilities, bolster controls, develop and deploy missing preventative and detection rules, and remove attack artifacts.

5: Recover

data safely

Should the worst case happen and attackers request ransom, the main goal is to recover data and minimize losses. This is because data losses not only lead to noncompliance but also pose a risk of losing crucial business transactions. The currency of data protection is reflected in recovery points, emphasizing the importance of having frequent backup snapshots of business data.

- **Deep visibility for a clean recovery you can trust**
– Mitigate risk by ensuring you don't reinject a cyber vulnerability into your production environment during data restore. With vulnerability scanning and a detailed dashboard to show your team the health status and cyber vulnerability index of your backup snapshot, you can recover to a clean point in time and meet your business SLAs.
- **Targeted workload recovery** – While Cohesity supports the ability to instantly recover hundreds of VMs to any point in time, this capability is better suited to a disaster recovery scenario than to most cyberattacks. Cohesity offers you the flexibility to selectively recover clean data and systems with ease.



5: Recover

data safely

“Our organization suffered a critical ransomware attack, effectively crippling our entire infrastructure. With Cohesity, we’ve been able to recover machines and file shares, verify they’re clean, and bring the applications back online. Cohesity has literally saved us hundreds of hours of work and I’d say it prevented us from having to actually pay the ransom note. We all still have jobs and the community has a functional hospital because we have had so much success with Cohesity.”



















Sam Stewart, Sky Lakes Network Systems Analyst

Sky Lakes Medical

Partnering to Improve Cyber Resilience

From network security to data protection, encryption, threat detection, incident response, and compliance—no single individual or vendor can do it all. A team with diverse talents and companies that work together is essential to combating cyber threats, which is why we created the Data Security Alliance.

With our leading industry partners, including Cisco, BigID, Palo Alto Networks, Tenable, Microsoft, CrowdStrike, and Qualys, among others, we collectively deliver critical technical integrations, best practices, and thought leadership to improve cyber resiliency for the world's largest organizations.

Vulnerability Scanning	Automated Ransomware Response	Threat Scanning	Sensitive Data Loss Prevention	Intelligent Data Protection
<p>Understand risk exposure using backup data to prevent attacks and communicate risk.</p> <p>Cohesity CyberScan, powered by Tenable, enables you to run vulnerability scans on backups and snapshots.</p> <ul style="list-style-type: none"> - Discover blind spots without impacting prod systems - Prevent attacks with actionable remediation recommendations - Avoid reinjection of vulnerabilities during recovery through backup snapshot health 	<p>Respond and recover from a ransomware attack.</p> <p>Cohesity shares incident alerts and relevant metadata with SOC's to initiate recovery and response workflows.</p> <ul style="list-style-type: none"> - Enrich SOC visibility into active ransomware threats with insights from Cohesity - Correlate, triage, investigate and respond to ransomware incidents in one location 	<p>Prevent malware reinfection by scanning backups.</p> <p>Cohesity consumes threat feeds to identify markers of known malware and remediate at risk files and data.</p> <ul style="list-style-type: none"> - Pinpoint which backups have indicators of malware and those that do not - Restore your environment quickly with confidence 	<p>Prevent unintended exposure of sensitive and confidential data or deliberate data exfiltration.</p> <p>Cohesity classifies sensitive data, sharing that information with our partners to fingerprint and monitor internet traffic to prevent data loss.</p> <ul style="list-style-type: none"> - Combines data-at-rest protection from Cohesity with data-in-motion protection from our partners - Classification on backup data is far less complex, prevents impact on prod systems, and requires no additional infrastructure 	<p>Provide visibility into the data they should be protecting.</p> <p>Cross-partner data discovery, classification, and posture across clouds with augmented insights from Cohesity on what data is protected or unprotected.</p> <ul style="list-style-type: none"> - Backup administration informed by deep understanding of underlying data type - Consolidated view of data risk - Proactively protect data from malicious attacks
	     	   	 	    

To learn more about how the Data Security Alliance partners to improve cyber resilience, [read our white paper](#).

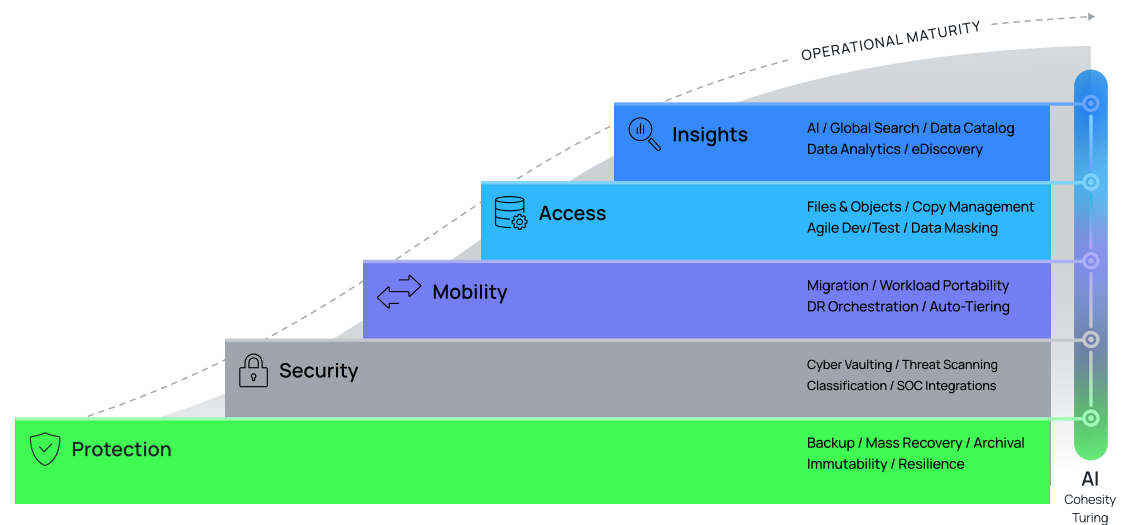
Getting Started with Modern Cyber Resilience

In the age of multicloud, hybrid environments, and the growing threat of ransomware attacks, today's enterprises need modern solutions that promote global visibility into protected data assets and streamline collaboration between IT and security teams.

The foundational layer of cyber resilience is data protection. Robust backup and recovery capabilities will give you confidence in your organization's ability to gracefully recover from unplanned disruptions.

From there, organizations should progress to data security. In this stage, organizations integrate data resiliency systems with additional cyber resiliency capabilities and other existing security investments to further reduce risk from cyberattacks and other threats.

For organizations looking for a blueprint to implement modern data security and management at scale, check out our resources and read our white paper:



An executive's guide to modern data security and management

Get the white paper



Ready to mature your cyber resilience strategy?

Discover our data security solutions

COHESITY

www.cohesity.com