COHESITY

RESILIENCE EVERYWHERE

CYBER RESILIENCE IN THE RANSOMWARE ERA

How Cohesity helps organizations withstand and recover from cyberattacks while aligning with the NIST Cybersecurity Framework 2.0.

CONTENTS

FROM DATA RESILIENCE TO CYBER RESILIENCE

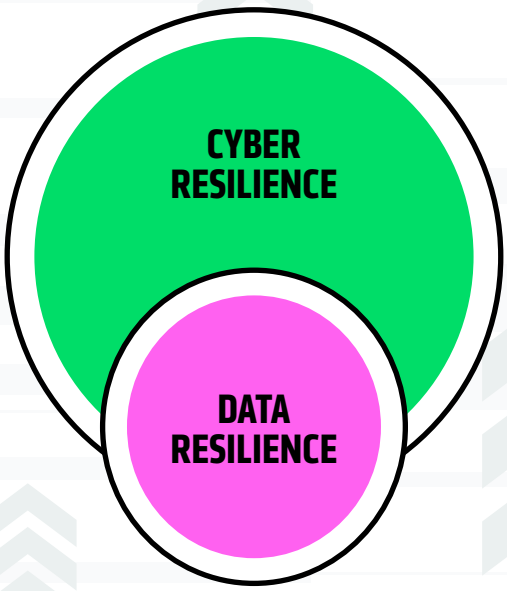
Natural disasters pose a huge threat to business operations. A lightning strike, hurricane, tornado, or flood can cause serious damage and bring business to a halt. In these situations, data resilience strategies ensure that data remains intact and accessible even in the event of hardware failures, accidental deletions, or natural disasters.

But these events aren't actively targeting your business with ongoing, intentional attacks.

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, responding to cyber threats requires investigation to discover these causes and drive remediations to prevent their recurrence.

Plus, 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 includes elements like cybersecurity preparedness, incident response plans, employee training, and threat intelligence.



Today's cyber threats need modern solutions that promote global visibility into protected data assets and streamline collaboration between IT and security practitioners.

At Cohesity, our modern, AI-powered data security solutions empower organizations to strengthen cyber readiness, accelerate incident response, and achieve fast, secure recovery.

WITH COHESITY YOU CAN:

- Protect all your data
- Ensure your data is always recoverable
- Gain visibility into vulnerabilities and threats in your backup data
- Respond quickly and effectively to attacks and hunt for threats that evade traditional defenses
- Recover systems and data quickly and securely

The result is a more resilient business better able to prepare for, withstand, respond to, and recover from cyberattacks.

A CONFIDENCE-CAPABILITY PARADOX

78% of organizations have confidence in their company's cyber resilience strategy[1]. This is generally a good sign, so long as this confidence is backed by concrete capabilities. But data shows a disconnect between strategic intent and actual capabilities.

98% aim to recover data and restore business processes after an attack within one day[2].

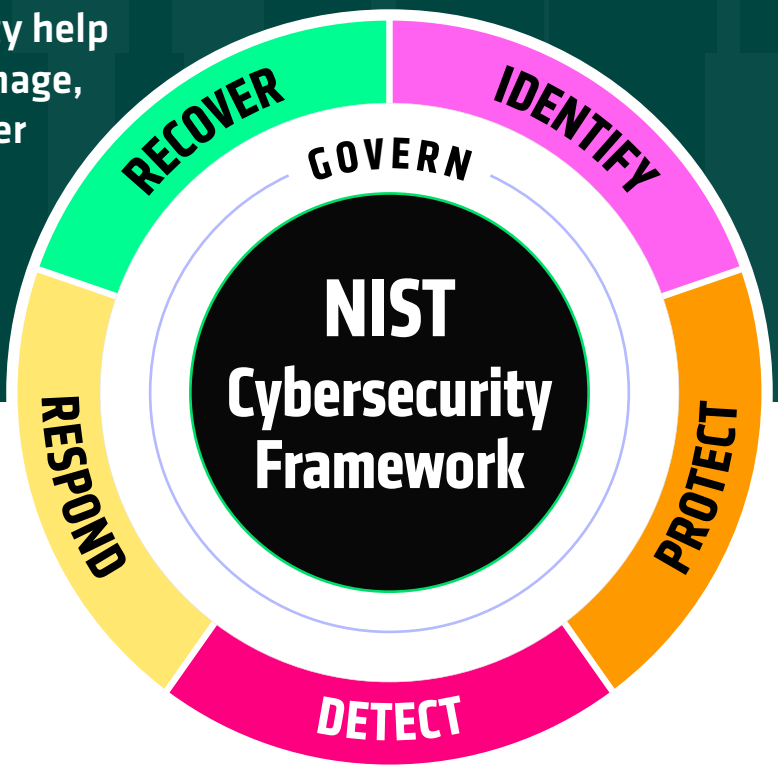
But only **2%** could achieve this[3].

Fortunately, Cohesity provides a proven playbook with processes and tools to help customers around the globe resume operations quickly and mitigate the impacts of an attack.

[1-3] Cohesity global cyber resilience report 2024

6 KEYS TO CREATING A CYBER RESILIENT BUSINESS

Our data security solutions at Cohesity help organizations better understand, manage, and reduce risks—and strengthen cyber resilience in alignment with the key functions of the NIST Cybersecurity Framework: Govern, Identify, Protect, Detect, Respond, and Recover.



GOVERN

- Classify backup data to understand regulatory requirements
- Support compliance with cyber insurance frameworks and other contractual obligations related to third-party data

IDENTIFY

- Scan fragile systems for vulnerabilities without impact
- Identify critical systems that aren't backed up
- Improve future incident response and BC/DR activities
- Identify areas for improvement in organizations' cyber resilience programs

PROTECT

- Protect enterprise data at scale
- Protect backups from attacks
- Test backups and restores

DETECT

- Detect ransomware encryption, wiper attacks, and malicious insiders
- Proactively hunt for indicators of compromise so you're immune to evasion techniques
- Send security detections to SOC tools for correlation
- Capture more forensic artifacts and trigger incremental snapshots based on EDR/XDR signals
- Identify malware in NAS servers

RESPOND

- Engage Cohesity CERT (Cyber Event Response Team) to speed response and secure recovery
- Restore response tooling and AD to a trusted state and provide rapid access
- Rapidly establish a clean room for response and recovery
- Passively hunt for artifacts to identify additional impacted systems
- Forensically examine historical filesystems
- Understand the historical vulnerabilities that were exploited in the attack
- Assist in complying with regulatory and compliance obligations to notify regulators, partners, and impacted data subjects

RECOVER

- Ensure recovery of systems and data allows for mitigation of threats

1.

Govern backup data to understand regulatory requirements and address risk

Today's data landscape is sprawling—like an overstuffed garage—making it increasingly difficult to locate sensitive data and ensure that it's properly protected. This lack of visibility heightens the risk of data exposure and regulatory noncompliance.

To manage this risk, organizations must not only meet legal and regulatory requirements (such as HIPAA, CCPA, and GDPR) but also demonstrate strong internal controls through effective cybersecurity governance. Increasingly, these controls aren't just about compliance—they're becoming essential to obtaining cybersecurity insurance.

With the frequency and severity of cyberattacks on the rise, cyber insurance has become a critical risk-transfer strategy. It helps cover financial losses such as data recovery, legal fees, and other fallout following an incident. But insurers are demanding more from customers, requiring proof of robust data protection and security controls before issuing or renewing policies.

To get ahead of these requirements, we help organizations:

Discover and classify sensitive data. Use our unlimited, immutable backup snapshots to discover and categorize sensitive data across your environment. Our built-in data classification engine uses hundreds of classifiers and AI-driven algorithms to identify and label regulated and high-risk information, helping you inventory digital assets and apply appropriate security policies.

Support compliance with cyber insurance requirements and other contractual obligations related to third-party data. Our platform helps meet the rising expectations of insurers and regulators by implementing best-practice controls:

- Isolated backup environments separate from the production network
- Dedicated cloud backup services
- Encryption at rest and in transit
- Immutable backup snapshots
- Role-based access with separate credentials
- MFA enforcement for both internal and external access
- Backup integrity testing before restoration to ensure they're free of malware

2.

Identify cyber resilience risks

Effectively managing cybersecurity risk requires a clear understanding of vulnerabilities across your IT environment—including backup systems. It also entails prioritizing the protection of data assets according to their classification and continuously improving through security testing, drills, and lessons learned from past incident response and recovery efforts.

CyberScan
Powered by tenable

Scan fragile systems for vulnerabilities without impact.

Use Cohesity CyberScan, powered by Tenable, to perform vulnerability scans on backup snapshots, and avoid impact on production systems.

Identify critical systems that aren't backed up.

Integrating Cohesity with your preferred Data Security Posture Management (DSPM) vendor is a powerful way to uncover hidden cyber resilience risks. DSPM solutions provide visibility into both known and forgotten data repositories across various cloud platforms, classify the data to identify sensitive information, and determine the risk of exposure.

While much of your sensitive data may already be protected by the Cohesity Data Cloud and existing backup policies, significant gaps often remain. That's where the integration with DSPM comes in.

By combining insights from DSPM with Cohesity, you can identify critical systems and data that aren't backed up and quickly extend backup policies to cover them—enhancing security and reducing risk.

Other key operational benefits include:

- Optimized frequency of backups and retentions based on the criticality of data within datastores backed up by Cohesity
- Prioritized restoration of data based on business criticality of data
- Streamlined incident response through "just-in-time" analysis of affected data (explored further in the Response function)

Together, DSPM and the Cohesity AI-powered data security platform help improve your security posture across multicloud environments.

2.

Identify cyber resilience risks

Identify improvements for future incident response and BC/DR activities.

Evaluate your organization's current response and recovery capabilities and chart a path toward industry best practices with the **Destructive Cyberattack Resilience Maturity Model (DCARMM).**

Developed by Cohesity, this model aligns with leading frameworks such as the SANS 6-Step Incident Response Process, RE&CT, MITRE D3FEND, and NIST SP 800-61, enabling organizations to:

- Assess preparedness for destructive cyberattacks
- Benchmark resilience maturity against industry peers or regional standards
- Identify gaps and build a roadmap for continuous improvement

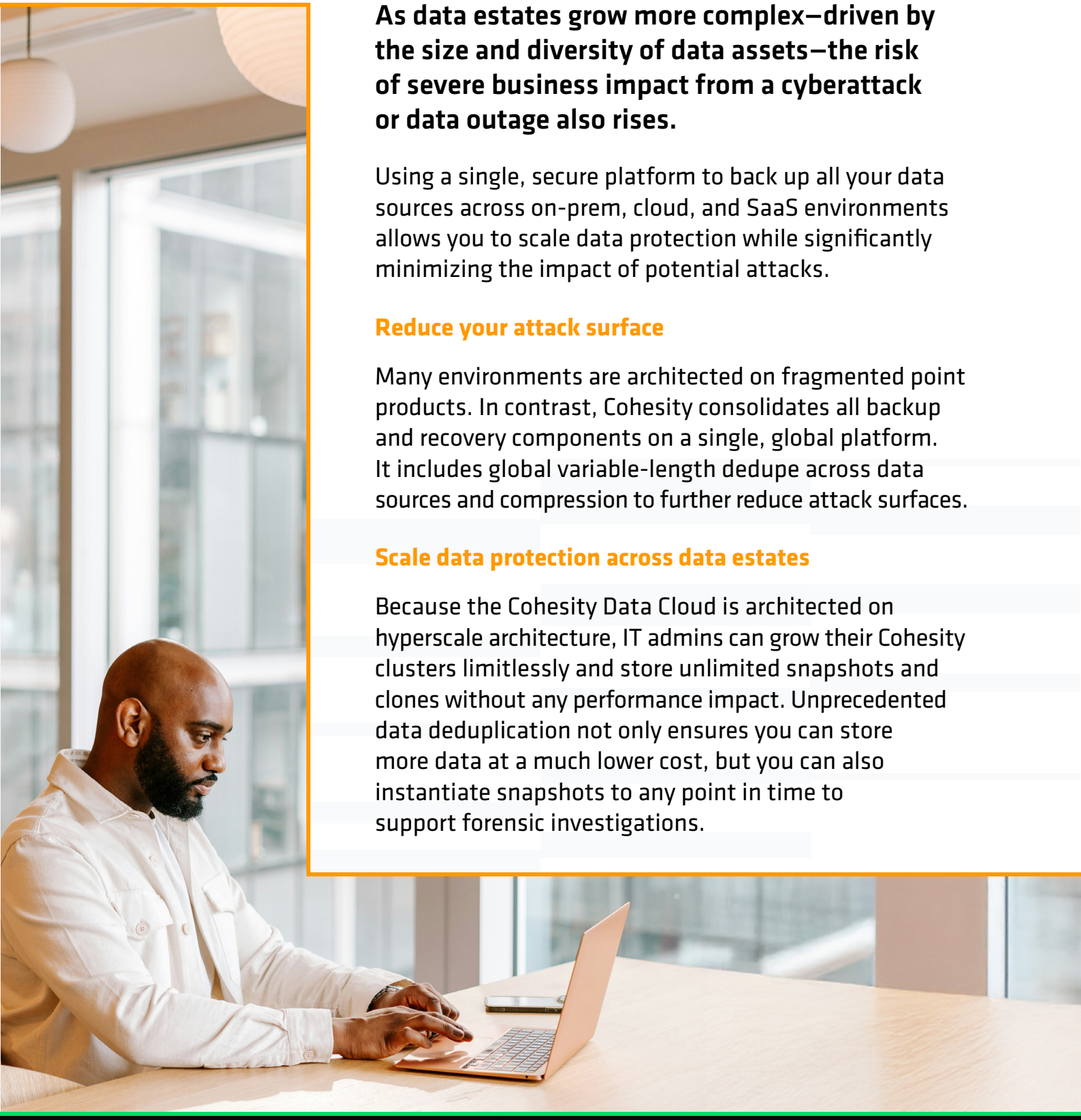
Your organization can use it as a strategic tool to strengthen your cyber resilience posture and guide investment in people, processes, and technology.

Identify areas that need improvement in your cyber resilience program by investing in third-party assessments.

Cohesity CERT (Cyber Event Response Team) cyber resilience consulting services offer proactive, expert-led engagements designed to strengthen your cyber resilience before the next incident strikes. From in-depth resilience assessments based on the DCARMM to tailored action plans, CERT helps you identify gaps, reduce risk, and build lasting defenses.

3.

Protect enterprise data at scale



As data estates grow more complex—driven by the size and diversity of data assets—the risk of severe business impact from a cyberattack or data outage also rises.

Using a single, secure platform to back up all your data sources across on-prem, cloud, and SaaS environments allows you to scale data protection while significantly minimizing the impact of potential attacks.

Reduce your attack surface

Many environments are architected on fragmented point products. In contrast, Cohesity consolidates all backup and recovery components on a single, global platform. It includes global variable-length dedupe across data sources and compression to further reduce attack surfaces.

Scale data protection across data estates

Because the Cohesity Data Cloud is architected on hyperscale architecture, IT admins can 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, but you can also instantiate snapshots to any point in time to support forensic investigations.

3.

Protect enterprise data at scale

Protect backups from attacks

Using Zero Trust principles, Cohesity has adopted a multilayered security approach that minimizes the risk of ransomware targeting backups—and the risk of inadvertent or malicious deletion of data.

- **Immutable read-only state snapshots** The Cohesity Data Cloud is purpose-built to thwart cyberattacks by storing backup snapshots in an immutable state. Snapshots aren't mounted for external applications, and modifications or deletions of immutable backup snapshots are disabled without approval.
- **DataLock policies** – Our 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. We support 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 two or more people to protect data from insider threats and stolen credentials.

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.

Test backups and restores

Using **cyber recovery orchestration**, you can generate customizable blueprints that automate recovery workflows and enable rigorous testing in non-production environments. This way, your organization can better prepare for cyber incidents and streamline recovery to reduce downtime and data loss.

4.

Detect potential cyberattacks and compromises

Cybercriminals will stop at nothing to find and exploit any vulnerability in your data environment. Early detection of abnormal changes in backup data or user behavior is essential to minimize the impact of an attack.

This is where AI plays a critical role—identifying subtle data activity patterns that may go unnoticed by humans. And by automatically capturing backup snapshots of critical data at the onset of a ransomware attack—detected by EDR/XDR tools—you can reduce data loss and accelerate recovery.

Detect ransomware encryption, wiper attacks, and malicious insiders.

Proactively monitor, model, and optimize operations using predictive analytics to assess trends. Our AI-based algorithm establishes patterns and continuously scans for anomalies in the data across snapshots over time.

Anomaly detection expedites remediation by sending a notification to your IT administrators as well as to the Cohesity support team.

This provides security teams with insights into behavior that could indicate a ransomware or wiper attack—or even the presence of a malicious insider.

These alerts can also be shared with your Security Operations Center using their event correlation tools (e.g. SIEM).

Proactively hunt for threats in backup data.

Ransomware and other attacks use deceptive tactics to cloak malware. Cohesity threat hunting helps you find elusive threats using AI-driven threat detection that identifies the latest variants of ransomware and other cyberattacks.

Our extensive library of behavioral patterns is updated frequently with the latest threats.

We also support commercial threat intelligence feeds, such as CrowdStrike Falcon Adversary Intelligence, and ingest any IOCs in YARA format from other third-party sources.

4.

Detect potential cyberattacks and compromises

Send security detections to SOC tools for correlation.

Push critical security detections—such as IOCs, anomalies in changes in backup data, and sensitive data alerts—into your SOC tools (e.g., SIEM, SOAR) to support rapid threat detection and response.

Cohesity integrates with leading platforms like CrowdStrike, Splunk, and Microsoft to seamlessly share telemetry, so your SOC can aggregate, analyze, and correlate Cohesity insights with high-volume log data from across your infrastructure.

The result: a unified, real-time view that enhances visibility and accelerates detection of potential ransomware or other cyber threats.

Capture more forensic artifacts and trigger incremental snapshots based on EDR/XDR signal.

The integration between the Cohesity Data Cloud and Cisco XDR allow you to automate backing up of critical data the moment Cisco XDR detects a ransomware attack—reducing recovery point objectives (RPO) and minimizing business disruption.

These backup snapshots also provide incident responders with a more granular context of file system changes, making forensic investigations faster and more effective.

Identify malware in NAS servers.

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.

"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

5.

Respond quickly to cyber incidents

Once a cyber incident is detected, the organization must act swiftly to contain the incident, investigate its scope, and mitigate risks to enable a secure recovery.

High-impact incidents—such as ransomware and wiper attacks—can disrupt the systems needed to deliver products and services to customers, and the internal IT systems critical to managing them. These scenarios require a different, more structured workflow that goes beyond standard data breach protocols.

Rushing to recover without investigating and mitigating the threat can leave underlying vulnerabilities in place—risking reinfection and extended downtime.

Secure recovery from such attacks requires understanding how the incident occurred and how to remediate its root causes. This disciplined approach is the essence of every best-practice cybersecurity incident response framework.

1. **Engage Cohesity CERT** early in the incident response process for fast, expert assistance. Our team helps contain the threat, minimize downtime, assist with forensic analysis of backup infrastructure, support regulatory compliance and breach notification requirements, and facilitate secure recovery to production.

2. **Restore response tooling to a trusted state and provide rapid access.** When a cyberattack hits—and your business is down—there's no time to waste. Rapid response is critical, and a **digital jump bag**™ helps you act immediately.

   Ideally prepared in advance of an incident, the digital jump bag is a protected and trusted repository that provides rapid access to the tools, software, configuration files, and documentation needed to launch an effective response. Stored in a vaulted immutable location beyond the reach of adversaries, it's the foundation for the entire Cohesity Clean Room solution, supporting the critical stages of incident response and allowing for a secure, confident recovery.

3. **Restore clean Active Directory (AD) infrastructure.** Few systems are more business-critical—or more heavily targeted—than AD. At the start of incident response, it's imperative to thoroughly investigate and clean your AD environment before bringing other response tooling back online and certainly before restoring AD to production. Skipping this step leaves the door wide open for attackers to re-enter, undermining recovery efforts and prolonging business disruption.

   With **Cohesity Identity Resilience powered by Semperis**, you can restore AD to a trusted state up to 90% faster.

5.

Respond quickly to cyber incidents

4. **Rapidly establish a clean room for response and recovery.** A clean room should be implemented as a trusted environment where analysts and investigators conduct forensic investigations, understand vulnerabilities exploited in the attack, and ensure infected data isn't reintroduced into production environments.

5. **Passively hunt for artifacts to identify additional impacted systems.** Our threat hunting capability detects IOCs across your organization's infrastructure—even when systems are isolated for containment. This capability is resilient to the common defense evasion techniques that can blind or delay detection by traditional endpoint security tools.

> *"During the tense days following the attack it was reassuring to have CERT's expertise. Having been through this before, they knew just what to do, starting with locking down the Cohesity backups so that files wouldn't be deleted at the end of their retention period–just in case we hadn't restored them yet. CERT also walked me through changing Cohesity settings to pause memory recycling, aka garbage collecting, which can better preserve our forensic options. Our experience with CERT was excellent in all respects."*
>
> ***Florida County IT Executive***

6. **Forensically examine historical filesystems.** Our data protection allows access to a full-time series of immutable snapshots via UI and API, so responders can conduct detailed, file-level forensic investigations across retained backup data.

7. **Understand the historical vulnerabilities that were exploited in the attack.** With the Cohesity CyberScan solution, you can scan backup snapshots for known vulnerabilities. This allows security teams to identify vulnerabilities during an attack, even if a system is unreachable due to containment, has been wiped, or was patched by an adversary after an intrusion.

8. **Assist in complying with regulatory and compliance obligations to notify regulators, partners, and impacted data subjects.** Our AI-driven data classification scans backups to identify sensitive and regulated data, helping organizations meet regulatory requirements, even in destructive cyberattacks where critical data stores are encrypted or wiped. We also help restore communication capabilities needed for incident management as part of the Cohesity Clean Room solution. Communication templates to notify stakeholders can be held in the digital jump bag for quick access.

6.

Recover systems and data securely

The recovery phase of incident response must support the thorough eradication of threats—preventing reinfection and reducing the likelihood of similar future attacks.

The Cohesity Clean Room solution gives you the flexibility to choose your preferred recovery strategy—whether recovering and cleaning existing systems or rebuilding from the ground up.

It supports rapid volume recovery, allowing an entire file system to be recovered before applying mitigations to eradicate threats. It also enables fast rebuilds from trusted software images and known-good configurations.

"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.

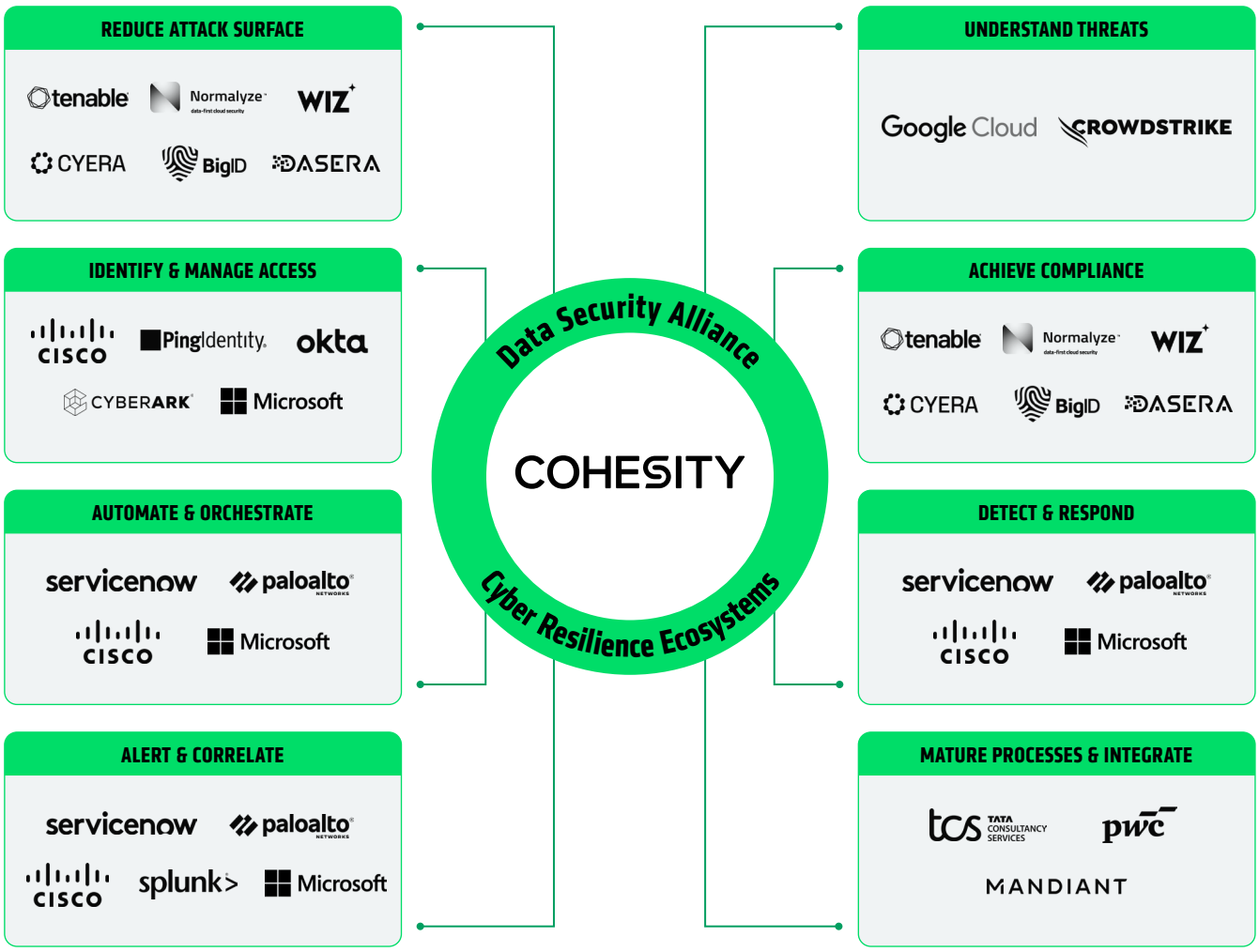
Cohesity has literally saved us hundreds of hours of work, and I'd say it prevented us from having to actually pay the ransom note. We all still have jobs and the community has a functional hospital because we have had so much success with Cohesity.

Sam Stewart
Sky Lakes Medical Center
Network Systems Analyst

STRENGTHENING CYBER RESILIENCE THROUGH PARTNERSHIPS

Cyber resilience is a team sport. No single vendor's solution can investigate and remediate an incident in its entirety.

That's why we established the Data Security Alliance, an ecosystem of leading security and cyber recovery companies that helps you reduce cyber recovery risks, boost the efficiency of your Security Operations Center, and protect more of your data estate using tools you already have.



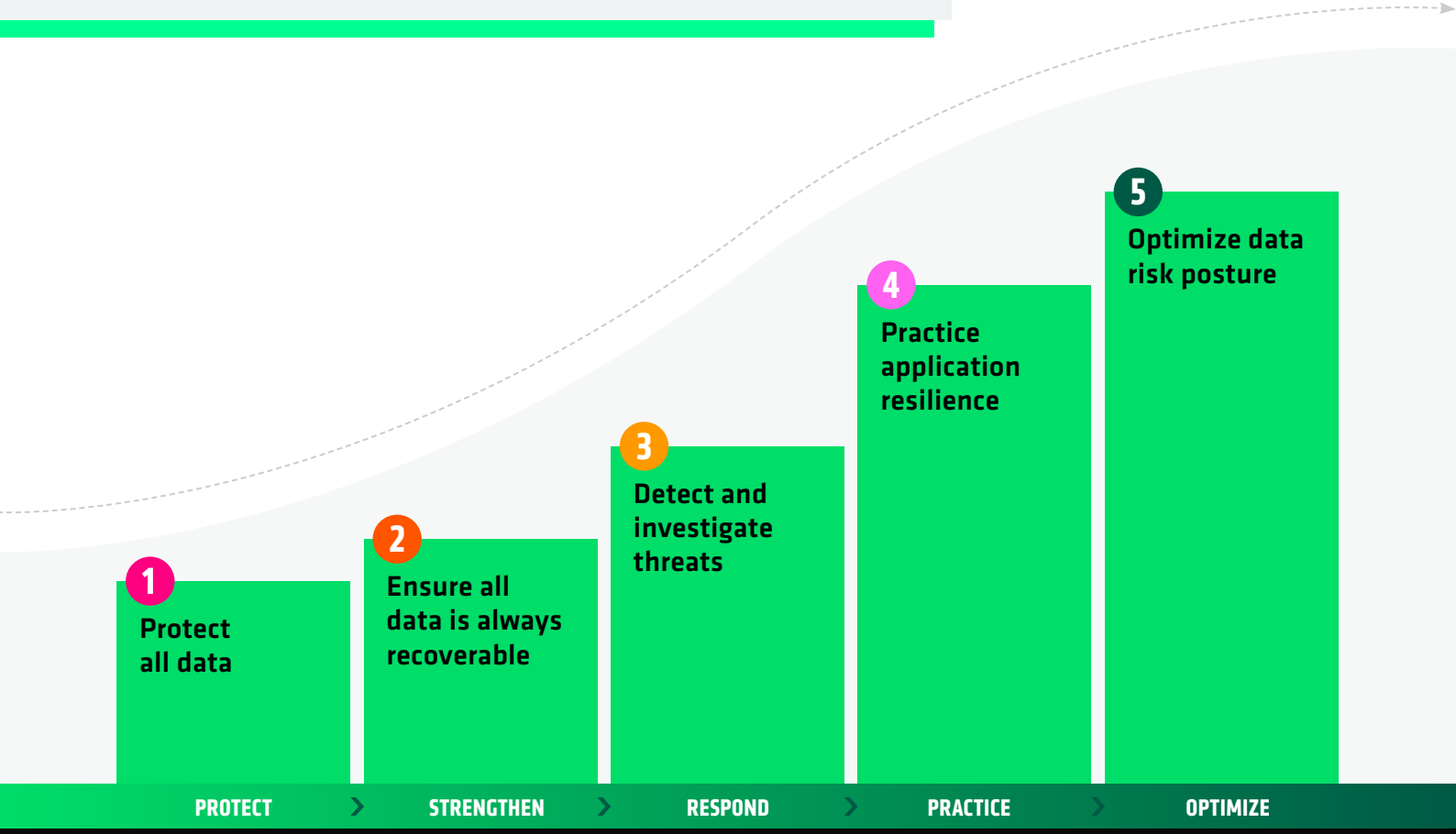
WHAT'S NEXT

FOR YOUR ORGANIZATION...

The Cohesity 5 steps to cyber resilience

You've explored the six keys to building a cyber resilient business and how we support each stage of the NIST Cybersecurity Framework (CSF). Now it's time to put those insights into action.

To help you get started, we've developed a **five-step cyber resilience playbook** aligned with industry best practices for cyber response and recovery. It's a practical guide that shows you how to implement concrete, repeatable actions using the Cohesity Data Cloud and services. Each step helps you achieve the outcomes of the NIST core functions.



The Cohesity ***5 steps*** to cyber resilience

1. PROTECT ALL DATA

NIST CSF Alignment: ***Protect***

Build resilience by protecting data everywhere it lives—at enterprise scale. The Cohesity Data Cloud supports **1,000+ data sources**, including VMs, SaaS apps, databases, and NAS environments, while reducing cost and risk through global deduplication and compression.

This approach lowers storage costs for IT and reduces the attack surface for security teams—two critical factors for a stronger Protect function.

2. ENSURE DATA IS RECOVERABLE

NIST CSF Alignment: ***Protect and Recover***

Protection is only as strong as your ability to recover.

- **Harden your platform:** Enable defenses like MFA, role-based access control, and Quorum to enforce separation of duties and minimize insider risk.
- **Isolate critical data:** Create secure, recoverable copies with Cohesity's cyber vault – available as a Cohesity-managed cloud vault or a self-managed solution.

These steps ensure you can restore trusted copies when it matters most.

3. DETECT AND INVESTIGATE THREATS

NIST CSF Alignment: ***Identify and Detect***

Resilience depends on early detection. With Cohesity, you can:

- **Identify vulnerabilities**, including gaps in data protection.
- **Continuously scan backups** for ransomware and malware indicators.
- **Hunt for specific threats** in backup data so you're immune to evasion techniques.
- **Send findings** to your SIEM/SOAR tools for rapid SOC correlation and response.

The result: Threats are caught sooner and response teams act faster.

4. PRACTICE APPLICATION RESILIENCE

NIST CSF Alignment: ***Respond and Recover***

Discover the final step >

Don't wait for an attack to test your recovery plan.

- **Rehearse regularly:** Practice your recovery plans as if you're under attack to validate your recovery processes and readiness.
- **Automate recovery:** Use our platform's recovery orchestration to streamline workflows and accelerate system restoration after an incident.

This step transforms recovery from a manual, stressful process into a repeatable, well-practiced playbook

The Cohesity ***5 steps*** to cyber resilience

5. OPTIMIZE DATA RISK POSTURE

NIST CSF Alignment: *Govern, Identify, and Respond*

- **Strengthen data security governance:** Use your Cohesity data and our data classification capabilities to understand what data you have, assess its risk level, and apply the right security controls.
- **Identify critical systems that aren't backed up:** Identify sensitive data across your entire estate—including backups—and ensure it's adequately protected. You can streamline this process by combining the capabilities of your preferred Data Security Posture Management (DSPM) tool and our platform.
- **Assess incident impact:** If a breach occurs, and especially if your critical data stores are encrypted or wiped, you can use your backups to quickly assess what sensitive and regulated data may have been exposed, so you can meet regulatory and compliance obligations to notify regulators, partners, and impacted data subjects.

See cyber resilience in action

Discover how 7 organizations across industries recovered quickly and securely from ransomware attacks.

GET THE EBOOK

PUTTING IT ALL TOGETHER

Together, our five-step cyber resilience playbook gives you a clear, actionable path to operationalizing the NIST CSF.

With Cohesity's modern data security platform, you can not only protect and recover but also continuously optimize your cyber resilience posture.

LEARN MORE ABOUT OUR CYBER RESILIENCE SOLUTIONS

COHESITY
RESILIENCE EVERYWHERE

6100008-006-EN 11-2025