COHESITY

e-Book

Defend Your Data from a Ransomware Attack

3 Ways Cohesity Next-Gen Data Management Improves Cyber Resilience

The Big Question

Ransomware is the fastest growing type of cybercrime. Analysts predict **ransomware will attack a business every 2 seconds** by the end of 2031.[1] And every time a cybercriminal succeeds, the organization attacked is damaged—financially and often reputationally.

More than 180 zettabytes of global data is expected to be created, captured, copied, and consumed by 2025, according to Statista[2]. As data continues to grow at an unprecedented rate, how will your legacy backup and data management product keep up?

Your backup is supposed to help protect your data from ransomware, yet its capabilities likely fall short of Cohesity's next-gen data management solution. Your product itself can be a prime attack target because 85% of systems targeted most by ransomware are Windows.[3] It might back up your data but it is not immune to sophisticated ransomware attacks. Additionally, without ML/AI-aided early anomaly detection, it likely can't proactively detect and rapidly recover from ransomware—Cohesity can.

Doesn't your organization deserve better? What would you do if you knew a comprehensive backup and data management solution purpose-built to protect, detect, and rapidly recover from ransomware was available today? Would you switch, simplify, save, and solidify your data defense?

$265 BILLION

Predicted global ransomware damage costs by 2031.[4]

[1,4] Cybersecurity Ventures. "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," June 3, 2021.

[2] Statista. "Volume of Data Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025," May 23, 2022.

[3] SafetyDetectives. "Ransomware Facts, Trends, & Statistics for 2022."

Not If, But When...

Despite the best efforts to thwart ransomware attacks, cyber criminals are innovative, and they continue to create new malware. This means more sophisticated and targeted ransomware attacks all the time—with the same goal: Disrupt business operations in the hopes victims will pay to restore order.

No industry is immune. And because enterprises are now even more attractive targets than consumers, your organization must proactively prepare for when, not if, cyber criminals come for your data.

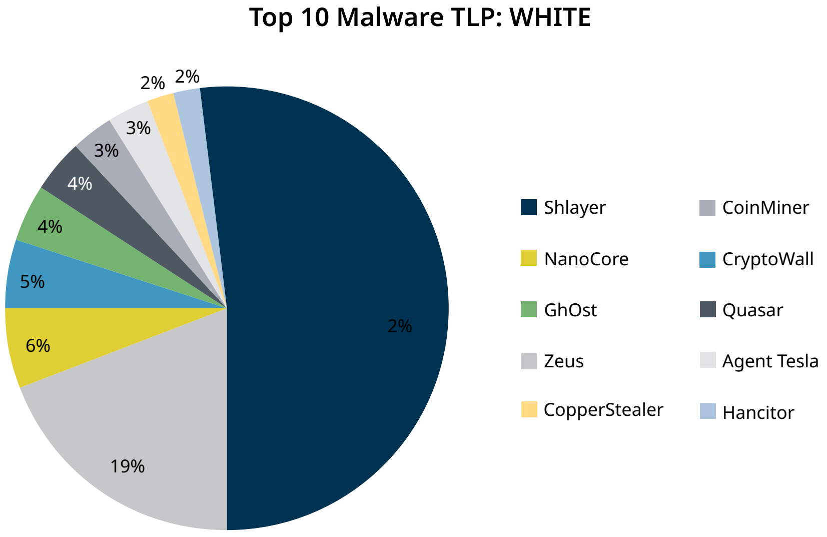


Figure 1: Top 10 Malware-Breakdown Source: Center for Internet Security, May 2021

Expanding Targets to Your Biggest Asset: Your Data

Success in today's digital economy means maximizing use of your organization's data for competitive advantage. Dev/test, insights, and analytics are a few ways to put your data to work—especially backup and other unstructured data, which represents 80% of all enterprise data.

Yet explosive data growth and the value of that data are attractive to ransomware hackers. These cyber criminals have begun targeting your backups more aggressively to gain full control of what has long been considered your insurance policy to business continuity.

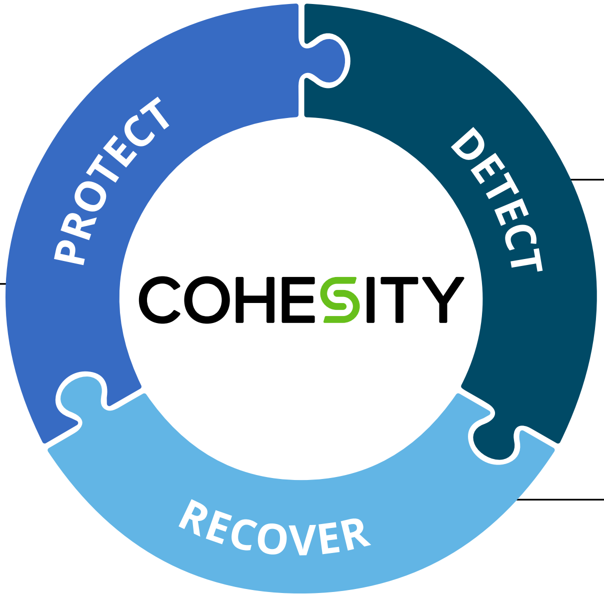
79%

Organizations surveyed report having experienced a ransomware attack within the last year.[5]

[5] Enterprise Strategy Group. "The Long Road Ahead to Ransomware Preparedness," March 2022.

3 Keys to Defending Your Backed Up Data

Lightning-fast changes in how and where malware appears now make it impossible for your enterprise to combat each potential new attack. Cohesity is a comprehensive next-gen data management solution to defend your backup data against ransomware.



- Immutable backup
- WORM (DataLock)
- RBAC
- MFA
- Encryption framework
- Quorum

- ML/AI-aided early anomaly detection
- Daily change rate on logical data
- Daily change rate on stored data
- Pattern based on historical data ingest

- Machine learning-based recommendation
- Discover vulnerabilities for clean recovery
- Restore at scale
- Data isolation

Taking a multi-layered approach to data protection is the best way to safeguard your backup data against ransomware attacks. It comes down to three important concepts that Cohesity has built in:

Protect	Detect	Recover
Reduce your attack surface and prevent your backups from becoming a ransomware attack target with immutable backup snapshots, WORM and more protection capabilities.	Utilize machine learning to discover ransomware attacks by providing visibility into anomalies by monitoring data during ingestion in the backup process.	Gain deep visibility and ensure clean data recovery before instantly bringing back all of your data in one mass restore across locations and environments.

1. Protect Backup from Becoming a Ransomware Target

Malware target backups, infecting the very infrastructure you thought would be your greatest insurance policy. Compromised backup infrastructure becomes a payload for cyber criminals and time is on their side: On average, it takes organizations 212 days to identify a data breach.[6] And survey respondents believe remote work increases this time.[7] Successful ransomware attacks are often devastating: the average cost of a data breach is $4.24 million—healthcare at $9.23 million—with IT and end-user productivity loss, systems downtime, and theft of information assets representing nearly 80% of the financial impact.[8]

The Cohesity next-gen data platform protects your backup from becoming an attack target better than Veritas by:

- **Reducing 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. Beyond that, Cohesity includes global variable-length dedupe across data sources and compression to further reduce surfaces available to attack.
- **Strengthening Your Defense with Hyperscale Architecture –** Built before cloud environments were popular, legacy environments lack capabilities to defend against today's cyber criminals:
  - **Immutable read-only state snapshots –** Cohesity's platform is purpose built to thwart cyber attackers. Cohesity protects backups snapshots and stores backup data in an immutable state. That snapshot is never accessible—nor mounted for external applications. External applications can only access the backup data on Cohesity through a zero-cost clone of the original snapshot in read-write mode. Because of this unique design, ransomware cannot modify or delete the immutable backup snapshot.
  - **DataLock policies –** Cohesity's write-once-read-many (WORM) capabilities for backup allow certain roles to set unchangeable DataLock policies on selected jobs. For example, a security officer can now store backups in WORM format with a time-bound setting, enforcing data protection that cannot be deleted even by an administrator or that same security officer.
  - **Multifactor authentication (MFA) –** Any person accessing a Cohesity backup must authenticate using two forms of verification.
  - **Data encryption –** Cohesity features software-based FIPS-validated, AES-256 standard encryption for data in flight and at rest. It's the cryptographic module validated by the United States National Institute of Standards and Technology (NIST) at the Federal Information Processing Standards (FIPS) 140-2 Level 1 standard.
  - **Role-based access control –** 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.
  - **Quorum –** With Cohesity, any root-level or critical system change must be authorized by more than one person to protect data from insider threats and stolen credentials.

[6-8] Ponemon Institute and IBM. "2021 Cost of Data Breach Report," June 2021

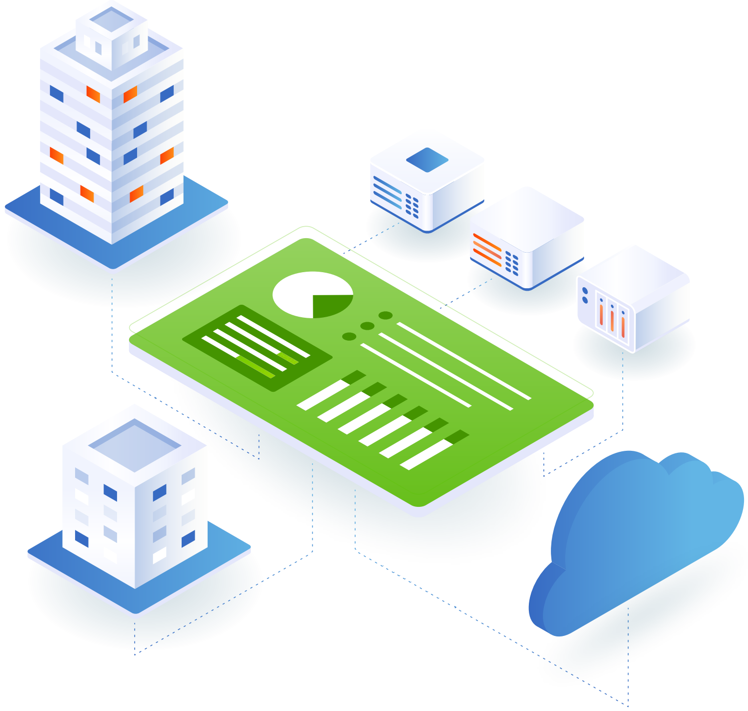
2. Detect Ransomware Attacks

Ransomware attacks are evolving fast. And they're looking to exploit your data and applications, whether they reside on-premises or in the public cloud. While legacy products lack capabilities to help you detect attacks, Cohesity detection features keep your team one step ahead.

Only Cohesity features a single, global SaaS-based user interface and security dashboard that enables your team to automate monitoring, quickly recognize change, and take action fast on your data and applications, regardless of whether they reside in self-managed or Cohesity-managed environments:

- **Automatic monitoring –** In the fight against ransomware, Cohesity's machine-driven learning gives you an advantage. Cohesity offers insights people may miss by automatically and continuously monitoring the data ingested from primary sources.
- **Recognize patterns and changes –** Cohesity's machine learning-based algorithm establishes patterns and automatically scans for data ingest/change rate anomalies to flag a potential ransomware attack in the IT production environment. If the data change rate of your primary files is out of the normal pattern range—based on daily change rates per logical data, stored data after global deduplication, or historical data ingest—Cohesity anomaly detection expedites remediation by sending a notification to your IT administrators as well as to Cohesity's support team.
- **Quickly take action –** Once notified, your IT 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. For example, with Cohesity Spotlight—a Cohesity Marketplace application that runs directly on the Cohesity platform—your team can easily search audit logs to determine anomalous file-access patterns. This includes analyzing the frequency of files accessed, number of files being modified, files added or deleted by a specific user or an application, and more. These capabilities help ensure a ransomware attack is detected fast.



3. Rapidly Recover Without Paying Ransom

Should the worst case happen and attackers request ransom, ensure your business and users enjoy the fastest recovery possible—at scale.

Cohesity has these capabilities that other products don't to get your team back to work fast:

- **Data isolation –** IT staff can automatically replicate data to another immutable Cohesity cluster on-premises or in the public cloud to ensure an additional immutable copy of the data is always available.
- **Deep visibility for a clean recovery you can trust** – Cohesity mitigates risk by ensuring you don't re-inject a cyber vulnerability into your production environment during data restore. A detailed dashboard shows your team the health status and cyber vulnerability index of your backup snapshot. Recover to a clean point in time and meet your business SLAs.
- **Unlimited scalability –** Because Cohesity is architected on hyperscale architecture, it allows IT admins to grow their Cohesity clusters limitlessly and store unlimited snaps and clones without any performance impact. And your data is close which makes for faster recovery versus pulling data back from off-prem.
- **Global actionable search –** Cohesity's unique, global search capability allows you and your teams to quickly locate data and specified infected files and take appropriate corrective actions. This includes finding a malicious file across all workloads, and taking necessary action to contain it. Cohesity search can also provide a cleanest point in time to recover recommendation.
- **Instant mass restore –** Ransomware seldom strikes just one or two VMs or files. It's a disaster recovery scenario that requires a robust, modern solution that can instantly recover hundreds of VMs, including bare metal, instantly—at scale, to any point in time. Unlike other solutions that can take days, if not weeks to recover a large number of VMs, Cohesity's instant mass restore is proven, world-class efficiency.

"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

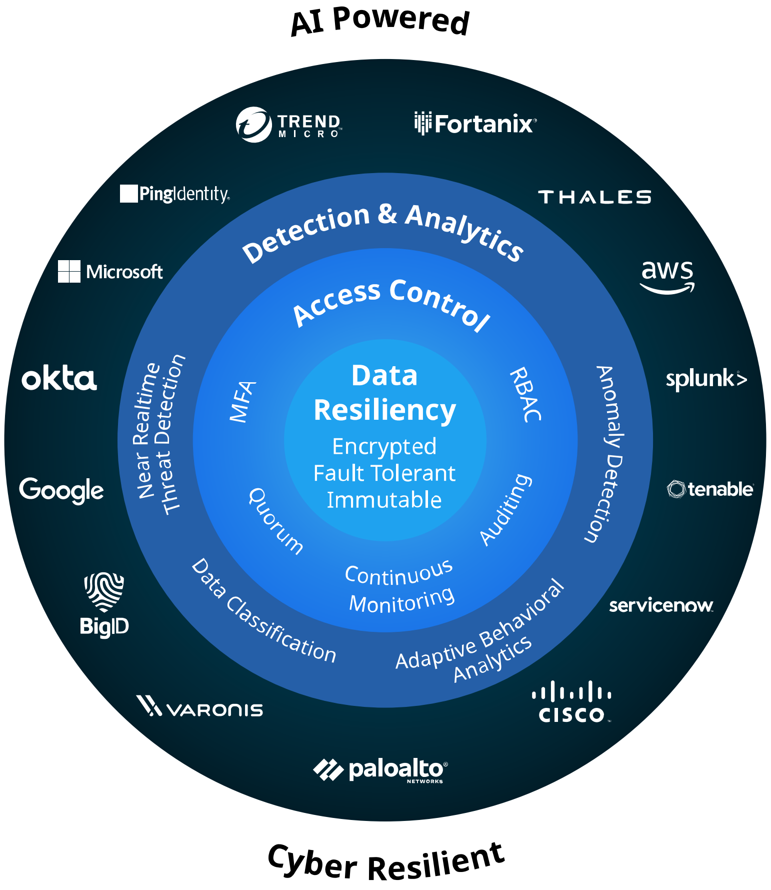
Improve Your Cyber Resilience with Cohesity Threat Defense

Beyond bolstering your backup, the Cohesity Threat Defense architecture helps you keep your data secure as part of an overall security architecture and defense-in-depth strategy.

- Thwart bad actors with advanced access controls.
- Detect threats early by identifying anomalies and attacks in near real time.
- Strengthen your security posture with tightly integrated security solutions from third parties.

Download the Amplify Your Ransomware Defenses: Protect, Detect, and Recover white paper for technical details.

Learn More at www.cohesity.com/ransomware


AI Powered
TREND MICRO
Fortanix
PingIdentity
THALES
Microsoft
aws
okta
splunk>
Google
tenable
BigID
servicenow
VARONIS
CISCO
paloalto NETWORKS
Detection & Analytics
Access Control
Data Resiliency
Encrypted
Fault Tolerant
Immutable
MFA
RBAC
Quorum
Auditing
Continuous Monitoring
Near Realtime Threat Detection
Anomaly Detection
Data Classification
Adaptive Behavioral Analytics
Cyber Resilient