COHESITY

WHITE PAPER

Cohesity REDLab: Rigorously testing the real-world resilience of Cohesity products

Validating and advancing malware defense with real-world threats in a secure lab

TABLE OF CONTENTS

Executive Summary

COHESITY
REDLab

Malware and ransomware show no signs of slowing. Their persistent evolution presents a formidable challenge for cybersecurity and data protection professionals.

Malicious actors increasingly use the very tools and resources designed to defend against them. When successful, they can breach, threaten, and extort organizations. Staying ahead calls for a dynamic, proactive approach to data security—one that evolves as quickly as threats do.

To meet this challenge, we built the **Cohesity REDLab**—a proprietary lab where we rigorously test and validate our solutions against real-world threats. Our REDLab is an air-gapped environment designed to allow full-spectrum threat testing while protecting Cohesity infrastructure. We use deep validation insights to continually evaluate and enhance the data security capabilities of our NetBackup and DataProtect solutions, so your data, operations, and reputation remain protected.

Validating Ransomware Protection with REDLab

Ransomware protection features are critical elements of our portfolio. In our design process, we initially used publicly available research and quickly realized that we needed more specific information and firsthand insights to maximize the efficiency of our solutions. To build stronger defenses and more effective recovery capabilities, we needed to study ransomware behavior in controlled, real-time scenarios.

That's where **REDLab** comes in.

REDLab is Cohesity's proprietary lab where we rigorously test the real-world resilience of our products using live malware, advanced exploits, and modern attack techniques. It's staffed by a dedicated team of senior security engineers and researchers. The team was supported by an external consulting team with more than 100 years of combined experience to validate our initial REDLab tests.

Our first task was to verify our claims about ransomware resilience. The REDLab team performed simulated and real ransomware attacks on **Cohesity NetBackup** and **NetBackup Appliances**. These findings shaped how we assess ransomware detection capabilities and strengthen the protection of data. The tests also gave us a new perspective into the inner workings of ransomware itself.

In today's dynamic threat landscape, it's critical that we test against all possible threat vectors to confirm the resilience and stability of our products. REDLab allows us to do just that—ensuring our solutions can withstand evolving threats while allowing us to develop and deliver new capabilities efficiently. Through this initiative, we've deepened our understanding of the requirements for infrastructure, applications, ransomware identification, and debugging. It also helped us define how to simulate disaster recovery scenarios, as well as how to maintain, clean up, and quickly rebuild systems. REDLab enables us to consistently provide industry-leading ransomware protection.

From secure malware handling procedures to debugging and system rebuilds, REDLab has become a cornerstone of our product security and cyber resilience innovation. Our core work includes:

- Performing malware research and monitoring threat actors, attack trends, and new techniques.
- Collecting real malware and exploit kits from global honeypots, sandboxes, and intelligence feeds.
- Detonating malware against Cohesity products in controlled environments.
- Analyzing the malware kill chain with real malware.
- Curating, developing, and updating detection mechanisms.
- Writing a product-specific fuzzer program to expose vulnerabilities.
- Benchmarking detection accuracy and performance.
- Collaborating with engineering teams to improve security capabilities like threat detection logic and recovery capabilities.

94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack.*

* The State of Ransomware 2024, Sophos

Threat-Testing Cohesity NetBackup

At Cohesity, our development teams are dedicated to continuously improving malware detection, threat prevention, and overall data protection. To prepare for rigorous threat-testing of NetBackup in REDLab, we hardened the entire NetBackup stack, then selected several of the top 30 most disruptive malware samples seen from recent years. These were injected into multiple production-like datasets, including applications and unstructured data.

We then tested NetBackup's core capabilities for protection, detection, and recovery against these real-world threats.

Protect

Hardened NetBackup Flex

The full NetBackup Appliances stack has been hardened for security and impenetrability, including proprietary security policies that conform to security technical information guide (STIG) guidelines, mandatory access control, and intrusion detection and protection services that maintain an audit trail of important users and system actions.

Consolidated data protection

NetBackup provides a single console to protect multi-cloud, virtual, physical, and modern workloads from any place—all from one console.

Tamperproof hardware

Appliances hosting immutable storage can move into a heightened security level to protect data and infrastructure.

Zero Trust-based security controls

Granular role-based access control (RBAC) with multifactor authentication (MFA) uses a security assertion markup language (SAML) 2.0-compliant identity provider.

Secured access controls

NetBackup offers role-based access, single sign-on, and customizable authentication.

Detect

Integrated malware scanning

NetBackup provides automated and on-demand scans for protected backups.

Anomaly detection

NetBackup identifies unusual data across your entire environment and provides alerts to suspicious anomalies in near-real-time.

Threat hunting

NetBackup performs IOC-based threat hunting using a searchable index of SHA-256 hashes for unstructured file backups.

IT Analytics

Cohesity IT Analytics provides a ransomware risk assessment dashboard with predictive analytics to identify potential risks within backup environments.

Recover

Isolated Recovery Environment (IRE)

The IRE offers a secure copy of critical backup data, providing administrators with a clean set of files on demand for recovery.

Active Directory

NetBackup provides the capability to recover a lost Active Directory.

Recovery post infection

Includes a range of capabilities to recover at scale:

- NetBackup instant rollback for VMware
- VM recovery
- Instant access for MSSQL and VMware
- NetBackup Snapshot Manager
- Universal share and protection points
- Long-term retention archive
- Bare metal restore

Tiered Recovery Orchestration

NetBackup provides users a choice of data-mover technologies to rehearse or orchestrate recovery of one or more multi-tiered applications.

Detection was performed with NetBackup malware scanning, Symantec protection, and Microsoft Defender.

When well-known scanners failed to detect the malware, our NetBackup anomaly detection stepped in—providing a critical layer of defense. The REDLab team shared malicious signatures with the respective vendors to help them improve their own detection capabilities.

The testing validated the strength of NetBackup ransomware protection features. They also uncovered new ideas and identified areas for improvement that we've actively worked on to address new product features. We continue to conduct rigorous testing to harden our solutions as part of the development process.

Threat-Testing Cohesity DataProtect

A recent development in our security strategy involved expanding threat-testing and validation on more of the Cohesity Data Cloud. Specifically, we expanded the scope of REDLab to include Cohesity DataProtect. We now continuously validate DataProtect's overall security posture, including the key capabilities outlined below, and plan to expand testing to include threat detection and threat hunting—all under real-world conditions.

Protect

Zero Trust-based security controls

Granular role-based access control (RBAC) with native multifactor authentication (MFA), Quorum to prevent unilateral administrative changes without multiple levels of approval, and DataLock, a WORM time-bound feature that locks and retains files in a View for compliance and regulatory purposes.

Consolidated data protection

DataProtect protects workloads across on-premises, cloud, and SaaS with a secured unified platform.

Secure single sign-on

Simplified single sign-on (SSO) access to the Cohesity cluster with any Identity Provider (Idp) that uses SAML 2.0 based SSO.

Detect

Anomaly detection

Our platform, Cohesity Data Cloud, constantly monitors metrics such as volume of modified snapshots and change rates in the backup data continuously. If an anomaly is detected during a protection run, it triggers an alert.

Security Center

Provides visibility into the security posture of your Cohesity cluster, including unresolved software vulnerabilities, misconfigurations, anomalies detected, and sensitive data within your systems.

Recover

Instant mass restore virtual machines

Recover hundreds of VMs instantly, at scale, to any point in time.

Instant NAS volume access

Make NAS backup datasets immediately accessible to users without any data transfer for faster operational recovery.

Staying Ahead of the Curve

Cohesity solutions integrate with third-party security information and event management (SIEM) platforms. These integrations allow SIEM platforms to ingest our DataProtect and NetBackup audit events, anomaly alerts, and malware security threats, before they escalate into a business continuity event.

If a malware infection is confirmed on a protected system, NetBackup can use built-in controls to automatically pause data protection and expiration activities. Additionally, IT teams can program security orchestration, automation, and response (SOAR) platforms to launch NetBackup APIs to automate security responses.

Looking ahead, our dedicated team of security researchers and engineers will continue to exchange threat intelligence with leading organizations such as the Joint Cyber Defense Collaborative (JCDC)—a U.S. government-led consortium coordinated by the Cybersecurity and Infrastructure Security Agency (CISA)—as well as the **Cohesity Data Security Alliance** and the broader open-source community. This collaboration, combined with deep security validation insights, will further strengthen our ability to identify emerging attack patterns and enhance our product capabilities to help customers improve their cyber resilience.

Recommended Reading

We think you'll find the following white papers, guides, and blogs helpful.

- Leading the charge: First-to-market with hyper-accelerated threat scanning
- Cohesity Data Cloud: A Unified Platform for Superior Cyber Resilience and Economic Outcomes
- How to achieve cyber resilience
- How to formulate a "wartime" response strategy to destructive cyberattacks

Learn more at Cohesity

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000061-001-EN 6-2025