

WHITE PAPER

The future of NetBackup

The critical role of NetBackup in the
Cohesity Data Cloud



TABLE OF CONTENTS

Executive summary	3	A phased, risk-managed approach to the Cohesity Data Cloud	7
The Cohesity Data Cloud vision: A shared, secure foundation	4	Phase 1: Unified management via the Helios control plane	7
Architectural principles of the Cohesity Data Cloud	4	Phase 2: DirectIO and SpanFS integration	7
Unified control plane and user experience	4	Security and innovation without architectural change	7
Shared security services across NetBackup and DataProtect	5	Evidence of continued NetBackup investment	8
AI and analytics as platform services	5	Supporting governance, compliance, and long term planning	9
Common data platform and storage services	5	Call to action: Define a secure three year path forward	10
Architecture built for coexistence, not forced convergence	6	Conclusion	10
NetBackup's role in the Cohesity Data Cloud	6		

Executive summary

NetBackup has long been trusted by enterprises to protect mission critical data across regulated, complex, and highly distributed environments. That assurance is well founded.

Cohesity NetBackup continues to innovate to solve for backup, recovery, risk, and compliance.

NetBackup has a healthy and strategic future as part of Cohesity, with ongoing investment, active engineering development, and a carefully defined modernization path that prioritizes **stability, security, and customer choice**.

Rather than forcing architectural disruption or accelerated migrations, Cohesity has adopted a **phased, low risk approach** that allows organizations to modernize on their own terms.

This paper outlines that approach, highlights delivered capabilities, summarizes continued NetBackup investment, and explains how customers can plan a secure, compliant, multiyear path forward.

The Cohesity Data Cloud vision: A shared, secure foundation

At the core of Cohesity's strategy is the Cohesity Data Cloud, a modern, distributed data management and security architecture designed to support multiple data protection products while enforcing consistent security, governance, and operational controls.

Both NetBackup and DataProtect participate in this architecture. While they remain distinct products with different operational models and use cases, they are increasingly integrated through shared, cloud native control planes and platform services. This architectural approach allows customers to benefit from innovation across the portfolio without requiring wholesale change.

Architectural principles of the Cohesity Data Cloud

The Cohesity Data Cloud is built around several key principles that are especially important for regulated and risk sensitive environments:

- Separation of control plane and data plane, enabling centralized governance without disrupting local data operations
- Policy driven security and compliance, applied consistently across products
- Shared platform services, reducing operational complexity and risk
- Modularity and extensibility, allowing customers to adopt capabilities incrementally

This design ensures that customers can modernize management, security, and analytics independently of how data is protected at the workload layer.



Data Insights



Data Security



Data Protection

Data Platform

Unified control plane and user experience

A defining characteristic of the Cohesity Data Cloud is the Helios control plane, which provides centralized management, monitoring, and visibility across Cohesity products. The user-centric Helios control plane has long been the enabling technology for the simple unified user experience across the Cohesity portfolio. As an important proof point of the inclusion of NetBackup as part of the Cohesity Data Cloud, the ability to manage NetBackup from within Helios was made available in August 2025, just eight months after the Veritas acquisition.

Through Helios, customers gain:

- A consistent administrative experience across the Cohesity portfolio
- Centralized visibility across environments and products
- Shared reporting, alerting, and insights
- Reduced operational risk through standardization

This unified experience is especially valuable for enterprises managing mixed environments or planning gradual evolution.

Shared security services across NetBackup and DataProtect

Security is not confined to individual products within the Cohesity Data Cloud. Instead, security services are architected as shared capabilities that can be applied consistently across the portfolio.

Examples include:

- Cyber resilience and recovery services, designed to strengthen response to ransomware and destructive events
- Immutability and isolation, enforced at the platform level
- Threat detection and analytics, informed by cross platform telemetry
- Secure access controls and auditing, aligned with enterprise governance frameworks

For NetBackup customers, this means security advancements increasingly arrive as additive services, rather than disruptive product changes. Customers can enhance protection posture without modifying their NetBackup workflows or architectures.

AI and analytics as platform services

Within the Cohesity Data Cloud, AI driven analytics and intelligence are delivered as platform level services, not tightly coupled to any single backup product.

This architectural decision is deliberate, as it allows analytics to improve without forcing application changes. It also supports consistent insight across heterogeneous environments.

As a result, both NetBackup and DataProtect can benefit from AI assisted operational insights, anomaly detection, and behavioral analysis. Additionally, capacity and utilization intelligence and cross environment visibility become possible through a single management interface.

Common data platform and storage services

The Cohesity Data Cloud includes a modern, scale out data platform, built on the SpanFS file system, which serves as a common storage and services foundation.

From an architectural perspective:

- DataProtect is built natively on this platform
- NetBackup can integrate through controlled interfaces such as DirectIO
- Storage services are designed to be policy driven, resilient, and auditable

This shared platform enables:

- Consistent security controls at the data layer
- Improved scalability and resilience
- Support for advanced services without re architecting applications
- Incremental storage modernization aligned with customer tolerance for change

The result is a single architectural foundation capable of supporting multiple operational models.

Architecture built for coexistence, not forced convergence

A critical attribute of the Cohesity Data Cloud is that it is explicitly designed for coexistence.

NetBackup and DataProtect:

- Share control planes, security services, and analytics
- Operate independently where required
- Can be deployed, scaled, and evolved on different timelines
- Remain compatible with customer defined architectures

This model ensures customers are never forced into premature convergence, while still benefiting from innovation at the platform level.

The Cohesity Data Cloud is not a single product. It's an architecture designed to unify security, governance, intelligence, and experience across multiple data protection platforms, without sacrificing stability or control. For NetBackup customers, this architecture provides assurance of long term viability, access to innovation without disruption, and a safe, supported path forward.

NetBackup's role in the Cohesity Data Cloud

Cohesity recognizes that NetBackup environments often operate under strict regulatory, operational, and business constraints. These environments protect data that is subject to compliance frameworks, internal governance standards, and rigorous audit requirements.

NetBackup is therefore treated as a core, strategic platform within Cohesity, not a transitional product.

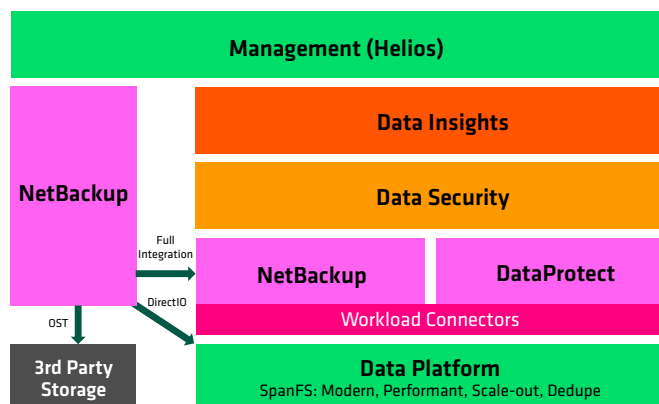
At Cohesity, our commitments include:

- Continued NetBackup product development and releases
- Full enterprise grade support and lifecycle management
- Compatibility with regulated and compliance driven environments
- A modernization roadmap that reduces risk rather than introduces it

The guiding principle is continuity with optionality: modernization without forced change.

A phased, risk-managed approach to the Cohesity Data Cloud

Cohesity has integrated NetBackup into the Cohesity Data Cloud in deliberate phases that emphasize **operational safety, architectural compatibility, and regulatory alignment**.



Phase 1: Unified management via the Helios control plane

The first phase focuses on **visibility, consistency, and governance**—without changing NetBackup's protection model.

NetBackup can now be managed through the **Helios control plane**, providing:

- A unified management and monitoring experience
- Centralized visibility across Cohesity products
- Consistent policy awareness and operational insight
- Reduced administrative risk through standardized interfaces

Critically, this phase **doesn't require changes** to existing NetBackup architectures, policies, or operational practices. Instead, it enhances oversight while preserving established controls.

Phase 2: DirectIO and SpanFS integration

The second phase introduced **DirectIO**, a tightly controlled integration point between NetBackup and the Cohesity data platform.

DirectIO enables NetBackup to **write directly to the Cohesity SpanFS scale out storage architecture**, allowing customers to modernize storage while:

- Retaining NetBackup as the backup and recovery system of record
- Avoiding data migration risks
- Maintaining existing operational workflows
- Introducing modern, resilient storage incrementally

From a risk perspective, DirectIO acts as an **architectural bridge**, not a forced transition—supporting gradual adoption while preserving auditability and operational continuity.

Security and innovation without architectural change

Importantly, many of the most impactful capabilities available to NetBackup customers are delivered outside the NetBackup core itself, through enhancements to the broader Cohesity portfolio that integrate seamlessly.

In the future, this will include:

- **Security capabilities**, such as cyber resilience services, vaulting, and recovery enhancements that strengthen posture without modifying NetBackup workflows
- **AI assisted insights and analytics**, surfaced through shared control planes and services rather than requiring NetBackup re architecture
- **Platform level innovation**, where advancements in storage, recovery services, and analytics enhance outcomes without altering deployment models

This approach is designed to ensure that customers don't need to trade **operational stability for innovation**.

Evidence of continued NetBackup investment

Our continued commitment to NetBackup is demonstrated through the continuation of our twice yearly major release cadence. Some key capabilities that have been released since the Veritas acquisition include:

- **Security enhancements** aligned with evolving ransomware and cyber recovery requirements, including Post Quantum Cryptography for data in flight, Freeze and Maintenance mode, Yara threat detection, Sophos malware scanning, new capabilities for adaptive risk engine, and expanded malware scanning and entropy detection to new workloads. FortKnox for NetBackup (previously called Alta Recovery Vault) added support for GCP, making it the first vaulting platform in the industry with this capability.
- **Unified user experience** by adding NetBackup management support to the Helios control plane.
- **Expanded workload and platform support**, ensuring relevance across hybrid architectures, including Oracle Private Cloud Appliance, incremental support for AWS DynamoDB, AWS RDS for SQL Server, AWS Aurora PostgreSQL, Azure PostgreSQL, Snapshot Manager enhancements, 7 new PaaS workloads.
- **Management and usability improvements**, particularly when paired with Helios.
- **Integration of NetBackup with SpanFS delivered as NetBackup DirectIO**, enabling NetBackup customers to gain the benefits of the modern scale-out SpanFS without disruption to their NetBackup deployment.

- **Enhancements to the Flex appliance platform** including upgrade simplification to meet the downtime window as well as support for large VLANs for multi-tenant environments.

These releases reflect sustained engineering investment and reinforce NetBackup's role as a supported, evolving enterprise platform. Additionally, some of the capabilities from the NetBackup portfolio have been incorporated into the Cohesity Data Cloud to enable DataProtect users to benefit from these innovations:

Cohesity RecoveryAgent provides orchestrated recovery at any scale to help organizations recover from conventional disasters as well as cyberattacks.

Signature-based threat hunting helps identify threats by scanning backup data for known malicious patterns (signatures), such as file hashes, YARA rules, or other indicators of compromise (IOCs), to detect previously known threats inside backup images.

The NetBackup center of excellence for workload integration accelerates the expansion of workload connectivity.

Supporting governance, compliance, and long term planning

Effective data protection must go beyond backup and recovery to address cyber resilience, regulatory compliance, and enterprise risk management. NetBackup's role within the Cohesity Data Cloud is anchored in a structured and defensible approach to these priorities.

The Cohesity 5 Steps of Cyber Resilience[®] framework provides a clear, best practice model for strengthening organizational readiness. This framework focuses on protecting all data, ensuring recoverability, detecting and investigating threats, validating application resilience, and continuously optimizing risk posture. Taken together, these capabilities support a shift from reactive recovery planning to proactive resilience engineering, aligning data protection strategies with broader governance and compliance requirements.

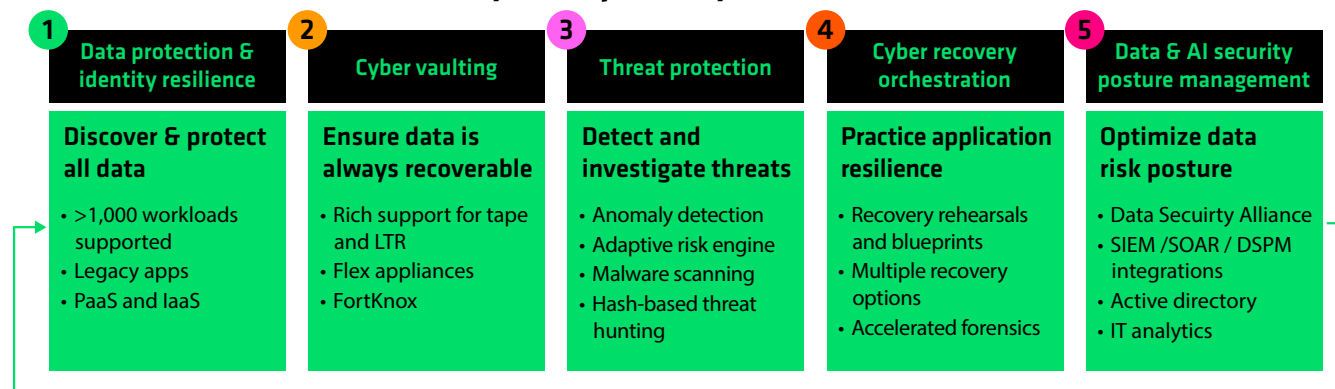
This model is reinforced by our scale of innovation. With approximately twice the research and development investment of comparable competitors, Cohesity continues

to advance key areas such as cyber resilient recovery, AI driven threat detection, and data risk analytics. For NetBackup customers, this means continuous access to new capabilities without requiring disruptive platform changes.

This approach is designed for hybrid environments. NetBackup remains a trusted system of record for data protection, while Cohesity platform services extend security, analytics, and governance capabilities across the broader environment. This enables organizations to strengthen their risk posture while preserving operational stability and aligning with internal change control and audit processes.

The result is a risk managed, compliance ready foundation that supports both current operational requirements and long term strategic planning—ensuring that NetBackup continues to play a central role in enterprise data protection within the Cohesity Data Cloud.

Cohesity 5 steps of cyber resilience[®]



Call to action: Define a secure three year path forward

NetBackup customers are encouraged to engage with their **Cohesity account team** to:

- Request a briefing on the **future of NetBackup**
- Review current and upcoming integration phases
- Upgrade to the latest release to see all the innovation you already own
- Assess security, compliance, and operational priorities
- Define a **3 year project plan** that aligns Cohesity capabilities to your specific risk and business requirements

These engagements are designed to support informed decision making, not to impose timelines or force transitions.

Conclusion

Modern enterprises cannot afford fragmented resilience strategies, stalled AI programs, or uncontrolled infrastructure growth. They need a platform that brings protection, intelligence, and efficiency together by design.

Cohesity delivers that foundation—unifying cyber resilience, AI-ready data activation, and cost optimization in a purpose-built platform engineered for hybrid and multicloud environments.

With Cohesity Data Cloud, organizations:

- **Recover with confidence** from ransomware and destructive attacks
- **Activate governed intelligence** from the complete, time-series history of enterprise data
- **Streamline operations** through unified management across all workloads and environments
- **Control costs** as they scale, with proven reductions in storage, tooling, and operational overhead

The outcome is clear: a resilient enterprise, an intelligent data strategy, a streamlined operating model, and an efficient foundation that turns every backup into measurable business value.

For more information, visit [Cohesity.com](https://cohesity.com)

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000096-001-EN 7-2026