

# **Cohesity Data Cloud: Eine einheitliche Plattform für überlegene Cyber-Resilienz und wirtschaftliche Ergebnisse**

Ein Überblick für Führungskräfte

## INHALTSVERZEICHNIS

Zusammenfassung	3	Die überlegene Wirtschaftlichkeit der Cohesity Data Cloud	10
Einleitung	4	Der Weg nach vorn	11
Gewünschte Ergebnisse	5	Architektonische Entwicklung	11
Die Anatomie der Cohesity Data Cloud: Heute und Morgen	6	Schwerpunkte der Entwicklung	12
Ein Blick in die Zukunft	8	Fazit	14
Datenschutzanwendungen	8	Über die Autoren	14
Erweiterte Datensicherheit	9		
KI und Analysen	9		

# Zusammenfassung

Die moderne Ära der Datensicherung und -sicherheit – definiert durch Cyber-Resilienz und KI – verlangt nach einer modernen Plattform. Die ideale moderne Plattform wird nach Maß gefertigt und berücksichtigt dabei die gängigen Unternehmensanforderungen. Dazu gehören die Geschwindigkeit der Cyber-Wiederherstellung, die Skalierbarkeit zur Unterstützung hunderter Datenquellen in hybriden und mehreren Clouds, die Einhaltung von Zero Trust Security und anderer Prinzipien, Benutzerfreundlichkeit und native Funktionen, die die Wiederverwendung von Unternehmensdaten für KI-Szenarien fördern. Alle diese Anforderungen sollten Teil einer Plattform sein, die die Investitionsausgaben und die laufenden Betriebskosten minimiert.

Die Cohesity Data Cloud erfüllt heute alle diese Anforderungen. Darüber hinaus verspricht ihre kurzfristige Weiterentwicklung ein noch überzeugenderes Wertversprechen, da NetBackup und dessen Unterstützung für über 1.000 Workloads in die branchenführende hyperkonvergente Plattform von Cohesity integriert werden.

Dieses Whitepaper beschreibt die Weiterentwicklung der Cohesity Data Cloud, insbesondere in Hinblick auf die Integration von NetBackup. Wir erläutern auch, wie das Portfolio Unternehmen unvergleichlichen Datenschutz, fortschrittliche Cyber-Resilienz und bahnbrechende KI-basierte Analysen bietet – und das alles im Exabyte-Maßstab.

**Wir haben eine echte „Summe der Teile“-Lösung geschaffen. NetBackup-Kunden behalten alles, was sie an dieser Anwendung lieben, und profitieren gleichzeitig von den einzigartigen Funktionen der Cohesity Data Cloud.**

Die Geschichte kennt Beispiele für entscheidende Momente, in denen innovative Elemente kombiniert wurden, um eine weltweit führende Plattform zu schaffen. Die P-51 Mustang, wohl das beste kolbengetriebene Jagdflugzeug aller Zeiten, war eine Kombination aus der P-51-Zelle (mit ihrer laminaren Tragfläche und dem Meredith-Effekt-Kühler) und dem Rolls-Royce-Merlin-Motor (mit der besten Leistung/Performance ihrer Klasse). Wie Sie in diesem Whitepaper sehen werden, verwenden wir das Dateisystem der Cohesity Data Cloud als sprichwörtlichen Merlin-Motor der weiterentwickelten Plattform. Es wird erstklassige Funktionen bieten, die wir im Detail beschreiben werden.

# Einleitung



**„Cohesity setzt sich dafür ein, die Investitionen unserer Kunden zukunftssicher zu machen . . . dies bedeutet kontinuierliche Unterstützung für Veritas NetBackup, NetBackup Appliances und Alta Data Protection ... über viele Jahre hinweg.“**

Sanjay Poonen, Cohesity CEO

Die Datenschutzbranche hat sich von ihren Wurzeln in Compliance und Auditing hin zur Unterstützung von Disaster Recovery und Business Continuity entwickelt. Inzwischen sind die Marktanforderungen weiter gereift. Wir befinden uns in einer neuen Ära, die von zwei Themen geprägt ist: Cyber-Resilienz und KI.

In diesem Whitepaper beschreiben wir, wie Cohesity – der Pionier im Bereich des hyperkonvergenten Datenschutzes und jetzt führend in der KI-gestützten Datensicherheit – weiterhin Innovationen vorantreibt, um Unternehmen dabei zu helfen, der Situation gerecht zu werden.

Wir werden die anhaltenden architektonischen Vorteile der Cohesity Data Cloud, unserer führenden Datenplattform, detailliert darstellen. Heute bietet diese Plattform erstklassige Cyber-Resilienz für die größten Marken, darunter 85 % der FORTUNE 100. Wir werden auch untersuchen, was die Zukunft für die IT-Leiter von Unternehmen bereithält, während die NetBackup-Anwendung immer stärker in die Cohesity Data Cloud integriert wird. Schließlich werden wir uns die Plattformattribute zur Ermöglichung von erweiterten KI-Szenarien ansehen, indem hochwertige Enterprise-Backup-Daten, die auf der Plattform gespeichert sind, wiederverwendet werden.

# Gewünschte Ergebnisse

Was veranlasst IT-Führungskräfte dazu, eine hyperkonvergente Plattform wie die Cohesity Data Cloud zu übernehmen? Ein Schlüsselfaktor ist die Besorgnis und Angst vor den Risiken und Kosten, die mit ihrem Status quo verbunden sind. Eine fragmentierte, siloartige Datenlandschaft ist im täglichen Betrieb kostspielig zu verwalten und angesichts sich verändernder Cyberbedrohungen notorisch schwer zu schützen und zu sichern.

Unternehmen, die auf die Cohesity Data Cloud umsteigen, erzielen häufig bessere Ergebnisse in fünf Schlüsselbereichen, die wir die 5 S nennen:

- **Speed** (Geschwindigkeit) – Sie können sich von Cyberangriffen viel schneller erholen als mit ihren vorherigen Systemen.
- **Security** (Sicherheit) – Sie verbessern ihre Sicherheitslage, erkennen Bedrohungen, schützen Daten und erholen sich schnell von Cyberangriffen.
- **Scale** (Skalierung) – Sie können ihren gesamten Datenbestand auf einer einzigen Plattform sichern und schützen, selbst im Petabyte-Maßstab.
- **Simplicity** (Einfachheit) – Sie können ihren Datenbestand verwalten und Datensicherungs- und Wiederherstellungsworkflows von einer einheitlichen Kontrollebene und einem Satz von APIs aus durchführen.
- **Smarts** (Intelligenz) – Sie gewinnen Geschäfts- und Betriebseinblicke aus ihren Daten mit erweiterten KI-Fähigkeiten.

# Die Anatomie der Cohesity Data Cloud: Heute und Morgen

Diese oben genannten Geschäftsergebnisse zu unterstützen, war das Ziel der Gründungsingenieure von Cohesity, als sie die branchenweit erste hyperkonvergente Web-Scale-Plattform entwickelten.

Die Cohesity Data Cloud ist so ausgelegt, dass sie alle unstrukturierten Daten einschließlich Backups, Dateien, Objekte, Test-/Entwicklungs- und Analysedaten auf einer einzigen Web-Scale-Plattform konsolidiert und verwaltet, die sich von der Edge bis zur Cloud erstreckt.

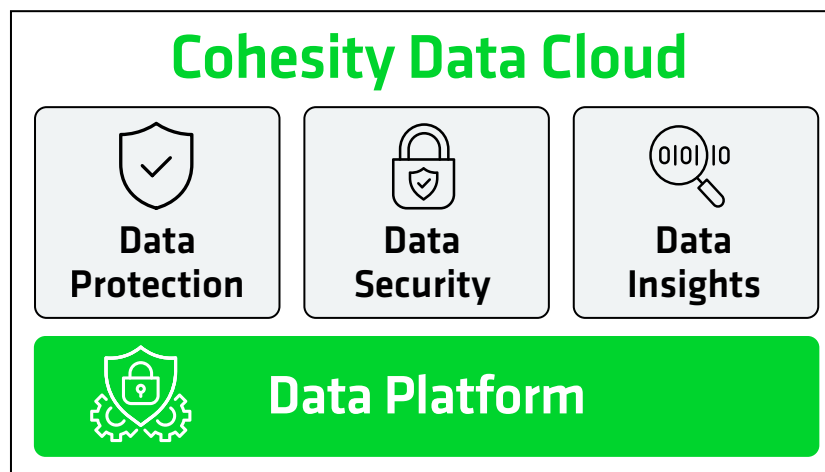
Der bemerkenswerteste Aspekt dieser neuen Plattform ist ihr Dateisystem: [SpanFS](#)<sup>®</sup>

Wie der Name schon sagt, ist SpanFS dafür ausgelegt, alles zu umfassen:

- **Skalierung:** SpanFS bietet unbegrenzte Skalierung über mehrere Knoten hinweg. SpanFS ist vollständig verteilt und hat keinen Single Point of Failure. Die Skalierung erfolgt linear, und beim Entfernen oder Hinzufügen von Knoten werden die Daten dynamisch wieder ins Gleichgewicht gebracht. SpanFS bietet ständige Verfügbarkeit, störungsfreie Upgrades und ein Pay-As-You-Grow-Verbrauchsmodell.
- **Geschwindigkeit der Cyber-Wiederherstellung:** SpanFS hilft bei der schnellen Wiederherstellung nach Cyberangriffen, und ist bis zu zehnmal schneller als andere Lösungen. Die Cohesity Data Cloud speichert immer eine unbegrenzte Anzahl vollständig hydratisierter Backup-Snapshots, die sofort gemountet

werden können, sodass Ihre Daten (über Direct Mount) bei Bedarf sofort verfügbar sind, während im Hintergrund Daten an Produktionsstandorten wiederhergestellt werden. Diese nahezu sofortige Datenwiederherstellung stellt sicher, dass die Geschäftstätigkeit schnell wiederhergestellt wird, nachdem erfolgreich auf einen Cyberangriff reagiert wurde.

- **Private und Public Cloud:** SpanFS verwaltet Daten in privaten Rechenzentren und Public-Cloud-Standorten. Der Web-Scale-Ansatz ermöglicht die Bereitstellung in der Public Cloud, die für Archivierung, Tiering oder Replikation verwendet werden kann. Für die Replikation wird SpanFS im Rechenzentrum oder in der Public Cloud bereitgestellt, um Daten zur Unterstützung mehrerer Anwendungsfälle zu verwalten.
- **Speicherung:** SpanFS unterstützt Datenschutz, Dateien, Objekte, Test-/Entwicklungskopien und Analysedaten. Es unterstützt alle wichtigen Funktionen, die für diese Anwendungsfälle erforderlich sind, unter anderem die global verteilte NFS-, SMB- und S3-Speicherung, die unbegrenzte Anzahl an Snapshots, globale Deduplizierung, Verschlüsselung, Replikation, globale Indexierung und Suche, und gute Leistung bei sequenziell und zufällig erzeugten Abläufen.
- **Mandanten:** SpanFS unterstützt mehrere Mandanten mit leistungsfähigen QoS-Funktionen, Datenisolation unter Mandanten, getrennten Verschlüsselungsschlüsseln und einer rollenbasierten Zugriffskontrolle.



- **Medienstufen:** SpanFS erstreckt sich über SSD- und HDD-Medienstufen und verwendet basierend auf I/O-Profilen die am besten geeignete Stufe.

Unsere Engineering-Teams fügen SpanFS eine OST-Schnittstelle hinzu, um diese Funktionen zu ergänzen. OST (Open Storage Technology) ist ein Protokoll innerhalb von NetBackup, das die breiteste Palette von Speicheroptionen in der Branche auf native Weise ohne spezielle Datenverarbeitung öffnet. Diese OST-Schnittstelle zu SpanFS wird dessen Integration in NetBackup unterstützen.

Das SpanFS-System umfasst auch mehrere integrierte Sicherheitsfunktionen, darunter:

## Verschlüsselung von Daten im Ruhezustand und bei der Übertragung

Cohesity Data Cloud verschlüsselt alle Daten im Ruhezustand und alle Datenflüsse innerhalb der Plattform. Verschlüsselung verhindert, dass nicht autorisierte Benutzer Daten außerhalb der Plattform einsehen können. Die auf der Plattform gespeicherten Daten sind unverständlich, es sei denn, sie werden von einem autorisierten Benutzer oder Prozess aufgerufen und entschlüsselt.

## Unveränderliche Datenspeicherung

Daten, die von der Cohesity Data Cloud gesichert werden, ändern niemals ihren gespeicherten Zustand. Unser zugrunde liegendes Dateisystem bietet unveränderliche Backup-Snapshots, um Änderungen und die vorzeitige oder versehentliche Löschung von Daten zu verhindern. Basierend auf einer Hyperscale-Architektur speichert Cohesity gesicherte Daten in unserem gesicherten Dateisystem, das von außerhalb eines Cohesity-Clusters nicht zugänglich ist. Die Backup-Snapshots werden in einem schreibgeschützten Zustand gespeichert. Externe Anwendungen oder nicht autorisierte Benutzer können den Snapshot nicht ändern.

## Zugriffskontrolle: Basierend auf Zero-Trust-Prinzipien

Gemäß des National Institute of Standards and Technology (NIST) ist Zero Trust wie folgt definiert: „Zero Trust ist der Begriff für eine sich entwickelnde Reihe von Cybersicherheitsparadigmen, die die Verteidigung von statischen, netzwerkbasierten Perimetern verlagern, um sich auf Benutzer, Vermögenswerte und Ressourcen zu konzentrieren.“ Zero-Trust-Prinzipien im Kontext der Cohesity Data Cloud konzentrieren sich auf die Validierung der Authentizität und Autorisierung von Benutzern für jeden Zugriff oder jede Änderung an der Plattform.

## Multifaktor-Authentifizierung (MFA)

MFA bietet eine starke Authentifizierung von Benutzern, um unbefugte Änderungen an den Plattformeinstellungen oder Daten zu verhindern. MFA verbessert die Plattformsicherheit, indem Benutzer aufgefordert werden, sich durch mehr als nur einen Benutzernamen und ein Passwort zu identifizieren. Passwörter und Benutzernamen sind anfällig für Brute-Force-Angriffe und können gestohlen werden. MFA erfordert, dass der Benutzer Login-Anfragen mit einer Antwort authentifiziert, die nur er selbst geben kann (z. B. eine Handy-Challenge), oder mit einem zeitbasierten Einmalkennwort (TOTP). Cohesity unterstützt native MFA oder MFA-Drittanbieter wie Ping, Duo, Okta und mehr

## Rollenbasierte Zugriffskontrolle (RBAC)

Die granulare rollenbasierte Zugriffskontrolle in der Cohesity Data Cloud ermöglicht es einem Unternehmen, Benutzern die geringsten Berechtigungen zu gewähren, die erforderlich sind, um ihre Arbeitsanforderungen auszuführen, Risiken zu minimieren und Bereiche außerhalb ihrer Verantwortlichkeiten unerreichbar zu halten. Unternehmen können Cohesity-Benutzerrollen auf bestimmte Anwendungen, Funktionen oder Arbeitsabläufe in der Plattform beschränken und dadurch die Aktivitäten eines Benutzers basierend auf seiner Rolle und seinen Verantwortlichkeiten einschränken. Beispielsweise können Unternehmen bestimmte Benutzer darauf beschränken, nur Datensicherungen oder Datenermittlungen durchzuführen.

## Quorum

Die Cohesity Data Cloud verwendet Quorum-Funktionen, um einseitige Änderungen an der Plattform innerhalb von Administratorkonten zu verhindern. Diese entscheidende Kontrolle schützt vor unbeabsichtigten Benutzerfehlern, böswilligen Administratoren oder kompromittierten Konten. Mit Quorum erfordern Benutzeranfragen zum Ändern von Einstellungen oder Verwaltungsfunktionen mehrere Genehmigungen.

## Prüfung

Die Cohesity Data Cloud verfügt über einen Prüfpfad für alle Aktionen, die auf dem Cohesity-Cluster durchgeführt werden. Diese Aufzeichnungen belegen die Einhaltung von Vorschriften und Betriebsintegrität. Prüfpfade können auch Bereiche der Nichteinhaltung identifizieren, indem sie Informationen für Audit-Untersuchungen bereitstellen. Prüfprotokolle erfassen Benutzeraktivitäten für Anmeldung/Abmeldung, Änderungen an Daten oder Dateneigenschaften und Auftragsplanung. Die Plattform organisiert Protokolle nach Kategorien, wie z. B. Active Directory oder Cluster, für eine schnelle Analyse.

# Ein Blick in die Zukunft

Mit Blick auf die Geschäftsergebnisse sowie das Dateisystem und die grundlegenden Sicherheitsfunktionen lohnt es sich, das Aussehen der Cohesity Data Cloud zu enthüllen, wenn NetBackup vollständig in ihre Infrastruktur und ihre gemeinsamen Dienste integriert ist.

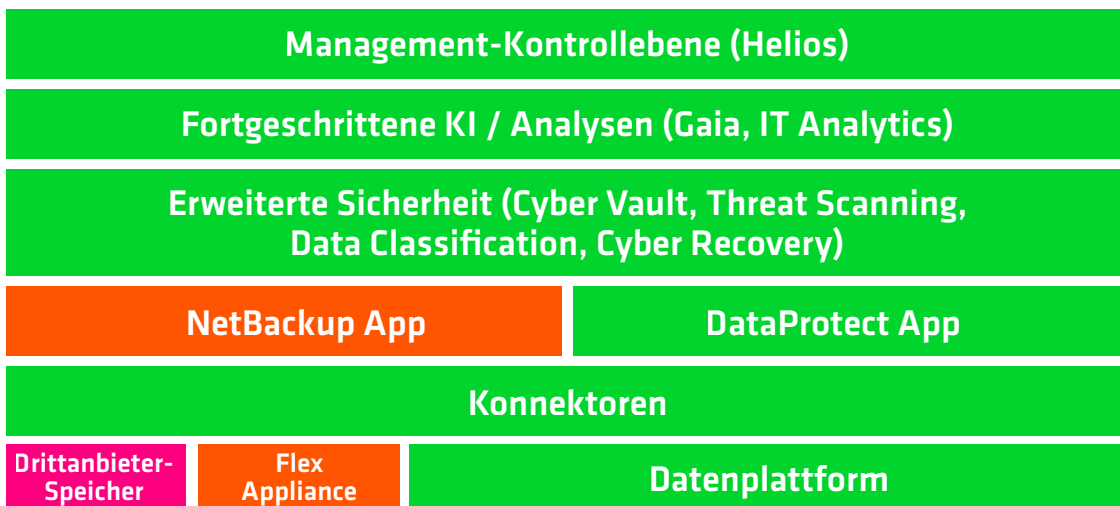
## Datenschutzanwendungen

NetBackup war die bahnbrechende Anwendung für Datensicherung und -wiederherstellung, die im Jahr 1987 auf den Markt gebracht wurde. Seitdem hat das Produkt Tausende von Kunden begeistert und 19-mal den „Leadership“-Status im Gartner Magic Quadrant erhalten. Die Anwendung unterstützt über 1.000 Datenquellen und kann auf mehr als 1.000 zusätzliche Ziele schreiben. Tatsächlich ist es die einzige Anwendung, die viele entscheidende Datenquellen in den größten Marken der Welt unterstützt.

In der Zwischenzeit hat Cohesity mit seinem erstklassigen Dateisystem die hyperkonvergente Web-Scale-Datenschutzbranche geschaffen. Das DataProtect-Produkt bietet unübertroffene Geschwindigkeit bei der Cyber-Wiederherstellung und Leistung im Petabyte-Maßstab. Das ist ein Grund, warum der hyperkonvergente Ansatz von so vielen der FORTUNE-500-Unternehmen verwendet wird.

„Veritas hat eine erstklassige Backup-Anwendung entwickelt, während Cohesity eine erstklassige Plattform um sein einzigartiges Dateisystem herum aufgebaut hat, das auch Datensicherung und -wiederherstellung durchführt. Dies gab uns die Möglichkeit, sie zu kombinieren, wobei Cohesity als zugrunde liegendes Speichersystem für die NetBackup-Anwendung verwendet wurde.“

## Cohesity Data Cloud



Die Management-Kontrollebene (Helios) steuert sowohl NetBackup als auch DataProtect. Darüber hinaus können Sie sehen, dass die Datenanalysemodule auf Daten zugreifen können, die an beiden Orten gespeichert sind. Schließlich können erweiterte Sicherheitsfunktionen mit den Datenschutzanwendungen verwendet werden, um eine robuste Strategie für die Cyber-Resilienz bereitzustellen.

Auf der Ebene des Datenschutzes werden Sie feststellen, dass NetBackup-Kunden mehrere Optionen haben. Zunächst kann NetBackup weiterhin auf disaggregierte Speichergeräte wie Data Domain schreiben. Darüber hinaus investiert Cohesity weiterhin in Flex-Appliances, sodass bestehende Kundeninvestitionen geschützt sind. Schließlich kann NetBackup mit der bevorstehenden OST-Integration auf SpanFS schreiben und alle Vorteile der Cohesity Data Cloud nutzen.

Beachten Sie das Feld „API External Integration“ auf der linken Seite. Die Cohesity Data Cloud verfolgt einen API-First-Ansatz, um Kunden bei der Integration ihrer Cohesity-Bereitstellung in andere Unternehmenssysteme zu unterstützen, wie z. B. vorgelagerte Anwendungen (Bereitstellung, Infrastructure-as-Code-Tools, CDM) und nachgelagerte Anwendungen wie ITSM, SIEM/SOAR und Abrechnung.

## Erweiterte Datensicherheit

Die grundlegenden Funktionen zum Datenschutz waren für Compliance- und Auditierungsszenarien ausreichend. Sie waren weiterhin wertvoll für Szenarien der Notfallwiederherstellung und der Geschäftskontinuität. Aber im Zeitalter zerstörerischer Cyberangriffe benötigen Unternehmen mehr als nur die Grundlagen – sie benötigen umfassende Funktionen zur Reaktion und Wiederherstellung bei Cyberangriffen. Cohesity und das neu hinzugekommene Veritas-Team haben hier eine starke Erfolgsbilanz in Sachen Innovation. Unsere Arbeit konzentriert sich darauf, sicherzustellen, dass Sicherheits-Workflows sowohl auf DataProtect- als auch auf NetBackup-Anwendungen angewendet werden können.

Es gibt so viel zu sagen über unsere kombinierten Sicherheitsfunktionen, dass wir ein Whitepaper und Präsentationen zur Weiterentwicklung erstellen werden, die sich ausschließlich damit befassen. Cohesity und Veritas bieten eine komplementäre Reihe von Sicherheitsfunktionen. Wir planen, sie in eine einzige Reihe von Standard-Sicherheitsfunktionen für DataProtect und NetBackup zu integrieren, während die kombinierte Plattform weiterentwickelt wird.

Sowohl DataProtect- als auch NetBackup-Kunden werden von einem branchenführenden Portfolio an Sicherheitsanwendungen profitieren, das das gesamte Spektrum der erforderlichen Funktionen abdeckt. Dazu gehören Plattformsicherheit, Datentresore, proaktives („Friedenszeit“) und reaktives („Kriegszeit“) Bedrohungsscanning, Reinraum, Orchestrierung, Datenklassifizierung und Data Security Posture Management (DSPM). Durch die Umstellung auf ein gemeinsames Dateisystem und eine gemeinsame Datenstruktur können wir diese Sicherheitsfunktionen auf einer einzigen Codebasis bereitstellen. Unser Ansatz für ein gemeinsames Dateisystem ist ein Schlüsselement unseres Sicherheitsansatzes.

## KI und Analysen

Cohesity verwaltet jetzt über 100 Exabyte an Daten – weit mehr als alle anderen Hersteller in dieser Kategorie zusammen. In dieser Ära der KI sind all diese Daten bei den Entwicklungsteams von Unternehmen sehr gefragt. Wie hilft Cohesity also?

Die Cohesity Data Cloud ist eine moderne Plattform, die für das KI-Zeitalter bereit ist. Ihre hochwertigen Datensicherungen werden in einem leistungsstarken Dateisystem indiziert und gespeichert, das speziell für die KI-Dienste entwickelt wurde, die die Welt im Sturm erobern. Cohesity Gaia, unser KI-Produkt, das auf unserer Plattform aufbaut, ist ein RAG-Dienst (Retrieval Augmented Generation), der es Ihnen ermöglicht, mit Ihren Daten zu sprechen.

Zusätzlich zu diesen Dateneinblicken bietet die Cohesity Data Cloud „KI-gestützte betriebliche Einblicke“. Hier nutzt die Plattform eingebettete KI, um die Leistung und Effizienz kontinuierlich zu verbessern. Ihre Infrastruktur- und InfoSec-Teams können diese Funktionen nutzen, um Ihr Datenvermögen intelligenter zu verwalten und KI zur schnelleren Untersuchung und Beseitigung potenzieller Bedrohungen einzusetzen.

Schließlich bietet IT Analytics Beobachtbarkeit mit tiefgreifenden Einblicken über eine einzige Konsole, um Daten in Ihren Multicloud-Umgebungen zu lokalisieren, zu analysieren und zu korrelieren. Verwenden Sie dieses Berichtsmodul, um Kosten zu optimieren, den Zustand Ihrer Speicherumgebungen mit Überwachung und Warnmeldungen im Auge zu behalten und Ihr Risiko durch die Identifizierung ungeschützter Daten zu verringern.

# Die überlegene Wirtschaftlichkeit der Cohesity Data Cloud

Die Cohesity Data Cloud bietet im Vergleich zu allen anderen Alternativen niedrigere Gesamtbetriebskosten (TCO). Die Integration von NetBackup in die Plattform verstärkt die wirtschaftlichen Vorteile. Zu den wichtigsten Vorteilen, die Sie genießen werden, gehören:

- Größere betriebliche Effizienz, da Sie dank der Skalierung und Leistung von Cohesity mehr Petabytes an Daten pro Bediener schützen und sichern können;
- Niedrigere Rechenzentrumsaufwendungen in Bezug auf Platz, Kosten und Strom aufgrund der hocheffizienten hyperkonvergenten Hardware von Cohesity;
- Außerbetriebnahme überflüssiger Add-on-Point-Produkte dank der in der Plattform integrierten Sicherheitsfunktionen;
- Optimierung Ihrer Speicherkosten mit der branchenweit besten Datenduplizierung und -kompression der Plattform;
- Laufend niedrigere Betriebskosten mit flexiblen Bereitstellungsmodellen, die Ihren Geschäftsanforderungen entsprechen.

Eine kürzlich durchgeführte IDC-Studie ergab, dass eine Gruppe von Cohesity-Kunden diese Kennzahlen für den Geschäftswert erreicht hat:

- Drei-Jahres-ROI von 233 %
- 6-monatige Amortisationszeit
- 52 % Reduzierung der toolbezogenen Kosten
- 39 % effizientere IT-Infrastrukturteams
- 36 % effizientere Sicherheits- und Backup-Teams
- 6 % produktivere Compliance-Teams

# Der Weg nach vorn

## Architektonische Entwicklung

Bislang haben wir das resultierende Wertversprechen der einheitlichen Plattform beschrieben. Die nächste logische Frage lautet: „Wie kommen wir dorthin?“

Wir beabsichtigen, diese Entwicklung mit minimalen Störungen durchzuführen, damit sie für Sie nahezu unsichtbar ist. Schließlich müssen Sie immer noch einen Datenbestand schützen und Ihr Unternehmen weiterhin mit Datensicherungs- und Wiederherstellungsvorgängen unterstützen.

Um dies anzugehen, haben wir unterschiedliche durchdachte Ansätze entwickelt, um Ihnen einen nahtlosen Weg zur einheitlichen Plattform zu bieten. Wir nennen diese Ansätze **Evolution** und **Revolution**. Mehrere Prinzipien leiten unsere Bemühungen dabei an, Ihnen das überzeugendste Ergebnis zu liefern.

Lassen Sie uns diese nacheinander durchgehen.

**Prinzip 1: Dauerhafter Hardware-Support:** Durch diese Evolution werden keine Hardware-Systeme für Datensicherung und -wiederherstellung „auf der Strecke bleiben“ oder „verwaist“ sein. Jedes Stück Hardware, das Sie gekauft haben oder kaufen werden, wird bis zum Ende der Lebensdauer der Hardware für NetBackup, DataProtect oder die einheitliche Plattform verwendbar sein. Dies gilt für Legacy-Veritas-Hardware (Appliances und OST-Partnerhardware), Cohesity-Whitelabel-Produkte und Partner-Hardware für Datenknoten.

**Prinzip 2: Bereitstellung Ihrer Wahl:** Wenn Ihnen Ihr Bereitstellungsmodell gefällt, können Sie es beibehalten. Viele Kunden haben die Einfachheit von Appliances zu schätzen gelernt. Einige bevorzugen den „Build-your-own“-Ansatz, während andere sich für den hyperkonvergenten Bereitstellungsansatz entscheiden. Wir bieten weiterhin verschiedene Bereitstellungsoptionen an, um den Anforderungen jedes Rechenzentrums – ob lokal oder in der Cloud – in einem kostengünstigen und flexiblen Modell gerecht zu werden. **Wir weisen jedoch darauf hin, dass die Speicheroptionen, die auf SpanFS basieren, Kunden erweiterte Funktionen bieten werden, die ohne SpanFS nicht verfügbar sind.**

**Prinzip 3: Sorgenfreie Weiterentwicklung:** Sowohl die Anforderungen an Rechenzentren als auch an die Cloud entwickeln sich im Laufe der Zeit weiter, und wir entwickeln uns mit ihnen weiter. Wir möchten Sie mitnehmen, anstatt unseren Kunden Veränderungen nach einem bestimmten Zeitplan aufzuzwingen. Ein NetBackup-Kunde möchte beispielsweise eine YARA-basierte Überprüfung einführen oder vielleicht einen **Digital Jump Bag™** in einem Datentresor bereitstellen. Er möchte vielleicht auch mit hyperkonvergenten Architekturen experimentieren, die knotenbasierte Cluster verwenden, im Gegensatz zu herkömmlichen Veritas-Geräten oder verteilten topologischen Ansätzen. Für diese Kunden werden wir einen schrittweisen Evolutionsplan mit maßvollen und durchdachten Migrationsschritten veröffentlichen. Wir werden dies mit operativer Unterstützung und Serviceleistungen kombinieren und mit Ihnen Schritt für Schritt zusammenarbeiten, um sicherzustellen, dass diese Evolution den anspruchsvollen SLAs entspricht, die mit Ihren Bereitstellungen verbunden sind.

Ein Nebeneffekt des evolutionären Ansatzes ist, dass wir eine einzige operative Schnittstelle, Analysewerkzeuge und Datensicherheitsfunktionen bereitstellen werden, die auf beiden Produktplattformen verfügbar sein werden. Mit der Zeit werden wir die Daten- und schließlich die Steuerungsebenen für diese separaten Plattformen zusammenführen, und sie werden eine einzige Bereitstellung der kombinierten Plattform darstellen.

**Prinzip 4: Revolutionäre Beschleunigung:** Andere Kunden sind vom hyperkonvergenten Ansatz von Cohesity fasziniert und möchten ihn gerne ausprobieren. Mit dieser Architektur können sie ihre TCO senken, eine größere Skalierung erreichen und ein reibungsloseres Wachstum sowie effizientere Upgrades erleben. Für diese Kunden werden wir eine Reihe von Tools und Dienstleistungen anbieten, um einen revolutionären Bereitstellungsansatz zu unterstützen. Wir werden es diesen Kunden ermöglichen, neue Workloads auf DataProtect bereitzustellen und/oder bestehende Workloads und Daten auf DataProtect zu migrieren.

# Schwerpunkte der Entwicklung

Diese Vereinheitlichung wird in fünf architektonischen Schwerpunktbereichen erfolgen, von denen die meisten aktiv parallel stattfinden. Kunden werden die Vorteile frühzeitig erkennen. Während des gesamten Prozesses wird Cohesity Sie weiterhin unterstützen und Ihnen helfen, Ihre SLAs gegenüber Ihren Stakeholdern einzuhalten. Obwohl die Arbeit parallel abläuft, haben uns unsere Kunden gebeten, eine Phasenbeschreibung zu erstellen, damit sie verstehen können, welche größeren Änderungen in welcher Reihenfolge erfolgen. Wir stellen diese hier vor, mit dem Hinweis, dass diese „Phasen“ stark ineinander übergehen werden. Unter Berücksichtigung dessen finden Sie hier die Elemente des **fünfphasigen Evolutionsplans von Cohesity**:

## 1. Einheitliche Managementebene

Der erste Schritt ist der am deutlichsten sichtbare – die Bereitstellung einer zentralen Verwaltungsschnittstelle. DataProtect-Administratoren kennen und schätzen bereits die vertraute Cohesity-UX („Helios“). In dieser Phase integrieren wir NetBackup-Funktionen in Helios. Nach Abschluss dieser Phase können Sie eine zentrale Verwaltungskonsole sowohl für NetBackup- als auch für DataProtect-Bereitstellungen nutzen.

## 2. Einheitliche Daten-/Speicher-Ebene

Die Integration von SpanFS ist der Schlüssel zur Nutzung der Stärken von NetBackup mit der Web-Scale-Architektur von SpanFS. Alle oben beschriebenen Funktionen können die Skalierung und Resilienz von SpanFS nutzen. Im Gegensatz zum InfoScale-Speichermanagement bietet SpanFS zusätzliche betriebliche Vorteile. Die Datenvirtualisierung in SpanFS („Views“) ist der Architektur inhärent. Dies wird die Skalierung des Betriebs (wie sofortiger Zugriff und universelle Freigaben) erheblich verbessern, indem die Kosten für diese Funktionen intelligent auf einen gesamten SpanFS-Cluster verteilt werden. Außerdem werden die gleichzeitigen Vorgänge in großem Maßstab erhöht. Darüber hinaus wird NetBackup sowohl NetBackup-Ansichten als auch [SmartFiles](#)-Ansichten derselben Sicherungssätze auflisten. (SmartFiles ist ein eigenständiger Mechanismus zur Interaktion mit SpanFS.) Auf diese Weise kann die Lösung NetBackup-Daten mit den Sicherheitsanalysefunktionen von DataProtect verarbeiten.

Die Integration des SpanFS-Speichers in NetBackup OST bietet im Vergleich zu herkömmlichen Integrationen in Drittanbieter-Systeme einzigartige Möglichkeiten. Um dies zu beschreiben,

werden wir die wichtigsten Funktionen von OST hervorheben, gefolgt von einer Beschreibung der differenzierten Attribute der Integration.

NetBackup Open Storage Technology (OST) ist der Industriestandard für das Schreiben von deduplizierten Backup-Daten und das Durchführen optimierter Kopieroperationen auf Speicherarrays von Drittanbietern. Ohne OST können diese Arrays nur Daten zwischen Arrays replizieren (FIFO). OST bietet die nötige Granularität zum Einsatz nativer Datentransfer-Tools mit Deduplizierung, um Backup-Kopien effizient zu erstellen und die Aufbewahrungsfristen unabhängig voneinander zu verwalten. Allein dieser Kopierservice senkt die Kosten für die Datensicherung. (Sekundärkopien werden oft länger aufbewahrt als die Primärkopie. Solche Anforderungen können mit Volumenreplikationsrichtlinien nicht erfüllt werden.)

Neben der Optimierung der Kopierservices bietet OST:

- Accelerator – Patentierter Deduplizierungs-Vorverarbeitungsprozessor, der verhindert, dass Backup-Auswahldaten, die sich seit der letzten Verarbeitung nicht geändert haben, dedupliziert werden.
- Accelerator für VMware – Patentierter Deduplizierungs-Vorverarbeitungsprozessor, der auf VMDK-Snapshot-Daten arbeitet.
- Optimierter synthetischer Schutz – Nutzt das Wissen des Deduplizierungsspeichers, um Backup-Abbildungen aus vorhandenen gespeicherten Deduplizierungsdaten ohne Datenverschiebung aufzulisten. Der optimierte synthetische Schutz verwendet eine vollständige Auswahl aus der geschützten Quelle und erstellt eine Backup-Abbildung, indem nur deduplizierte Daten im Backup-Speicher verwendet werden, ohne Lese- oder Schreibkosten für Backup-Daten.
- Sofortige Wiederherstellung für VMware – stellt eine VMDK zum Start bereit oder stellt eine VMDK inkrementell auf einen früheren Zeitpunkt wieder her.
- SDK – ermöglicht es Drittanbietern, OST-„Plugins“ zu schreiben, um ihren Wert durch NetBackup-Funktionen zu erhöhen.
- Zusätzlich zur OST-Funktionalität wird die SpanFS-OST-Implementierung diese exklusiven Funktionen bieten:
- Client Direct-Deduplizierung überall dort, wo NetBackup-Agents vorhanden sind. Hier stellt Client Direct eine Verbindung vom Agenten direkt zum Speicherserver her. Dies minimiert den Bedarf an Media-Server-Ressourcen zur Verarbeitung von Backup-Daten und senkt dadurch die Kosten.

- Intelligente Stream-Handhabung für wiederholbare Effizienz bei der Deduplizierungsvorverarbeitung. Dies gilt für alle Typen von Workload- und Backup-Streams, einschließlich VMware, Hyper-V, AHV, NDMP, nicht verschlüsselte und verschlüsselte Datenbanken sowie verschiedene Dateisystemtypen. Intelligente Stream-Handler analysieren einen Datenstrom und bestimmen die für den Stream einzigartigen Grenzen. Dies stellt sicher, dass die Deduplizierungs-Engine jedes Mal effizient und konsistent arbeitet, wenn der gleiche Datentyp verarbeitet wird.
- Instant Access nutzt SmartFiles-Ansichten von Backup-Abbildungen über Dateisystem-NAS-Freigaben. Instant Access bietet eine direkte Möglichkeit, geschützte Daten in einer Backup-Abbildung zu durchsuchen, ohne die Daten über eine NAS-Freigabe des Inhalts wiederherzustellen.
- Universal Shares verwenden „Thin Provisioned“ SmartFiles-Scale-out-NAS-Freigaben für Anwendungs-Dump- und Sweep-Operationen. Anwendungsbesitzer verwenden diesen Mechanismus, um ihre Schutzanforderungen zu steuern, zu schützen, wiederherzustellen und zu validieren, ohne Kenntnisse über die Backup-Anwendung zu haben. Dies wiederum senkt die NAS-Kosten.

Die Integration in SpanFS wird 100 % OST-konform sein und MSDP einen einzigartigen Mehrwert und Funktionen hinzufügen.

**Dies ist eine übergeordnete Lösung für OST, die jeder anderen OST-konformen Deduplizierungslösung von Drittanbietern überlegen ist.**

Die kombinierten Fähigkeiten von NetBackup Data Reduction Intelligence und die Virtualisierungs- und Skalierungsfähigkeiten von SpanFS werden eine noch stärkere Lösung für Kunden bieten, die sowohl Data Protect- als auch NetBackup-Workloads auf derselben Datenspeicher-Ebene hosten können.

### 3. Einheitlicher Sicherheitsschutz

Hier werden Sie von zu 100 % einheitlichen Sicherheitsfunktionen profitieren, die sowohl in NetBackup- als auch in DataProtect-Bereitstellungen zum Einsatz kommen. Lassen Sie uns einige Anwendungsfälle detailliert beschreiben, die in dieser Phase umgesetzt werden. Sie suchen nach Indicators of Compromise (IoCs) mit einem Satz von YARA-Regeln in beiden Anwendungen. Sie können Entwicklungs-/Testfunktionen für beide Produkte auf ähnliche Weise orchestrieren. Schließlich können Sie Warnmeldungen aus beiden Anwendungen an Ihre nachgelagerten SIEM/SOAR-Systeme weiterleiten, um Ihre Bedrohungserkennungsfähigkeiten zu erweitern. All dies wird im Rahmen von Phase 3 bereitgestellt.

### 4. Funktionskonvergenz – Grundlagen

In dieser Phase konvergieren wir die Funktionen von DataProtect und NetBackup auf der kombinierten Endplattform. Dies wird für viele unserer Kunden größtenteils unsichtbar sein, da sie bereits beide Anwendungen, NetBackup und DataProtect, über eine zentrale Bedienoberfläche verwenden. Dennoch ist dies ein wichtiger Schritt, um alle wichtigen Assets aus beiden Produktportfolios zusammenzuführen.

Dies ist der erste Punkt, an dem ein Kunde sowohl NetBackup- als auch DataProtect-Anwendungen auf einem zentralen Zielspeicher betreiben kann, wenn das Ziel SpanFS unterstützt.

### 5. Funktionskonvergenz – Erweitert

In dieser Phase bringen wir die verbleibenden NetBackup-Mikroservices auf die integrierte Plattform und ermöglichen es Ihnen, eine zentrale, einheitliche Plattform für alle Ihre Bereitstellungen zu betreiben. Es gibt architektonische Überlegungen, die wir für diese Phase noch klären müssen. Unsere Engineering-Teams entwickeln beispielsweise noch die Möglichkeit zur Archivierung und Wiederherstellung von NetBackup von Band. Dies ist für Unternehmen, die über jahrzehntelange Bandspeicherbestände verfügen, von entscheidender Bedeutung. Wir müssen ihnen eine Möglichkeit bieten, von der kombinierten Plattform aus auf diese Bänder zuzugreifen.

# Fazit

Die Welt der Daten wächst auseinander und nicht zusammen. Die Komplexität wird aus mehreren vertrauten Gründen weiter zunehmen: ein explodierendes Datenvolumen in Rechenzentren, Clouds und Edge-Standorten; es gibt mehr Datenquellen als je zuvor; die regulatorische Landschaft bringt weiterhin mehr Anforderungen mit sich; und die Bedrohungslandschaft zerstörerischer Cyberangriffe verändert sich weiterhin auf unvorhersehbare Weise.

Cohesity Data Cloud ist eine beliebte Unternehmensplattform, die trotz dieser Komplexität überlegene Ergebnisse liefert. Das Wertversprechen der Plattform wird in den kommenden Monaten

mit der Hinzufügung von NetBackup noch überzeugender: höhere Geschwindigkeit bei der Cyber-Wiederherstellung, mehr Skalierung und Leistung für die meisten Datenquellen, erweiterte Sicherheitsfunktionen, die von Grund auf integriert sind, branchenführende Einfachheit und Benutzerfreundlichkeit sowie eingebettete KI-Funktionen zur Rationalisierung von Abläufen und Beschleunigung von Szenarien zur Wiederverwendung von Daten in Ihrem Unternehmen.

## Ein Hinweis zu zukunftsgerichteten Aussagen

Dieses Dokument enthält zukunftsgerichtete Aussagen, die Risiken, Unsicherheiten und Annahmen unterliegen. Sie sollten sich nicht auf zukunftsgerichtete Aussagen als Vorhersagen zukünftiger Ereignisse verlassen. Alle Aussagen, die keine historischen Tatsachen darstellen, können als zukunftsgerichtet angesehen werden. Zukunftsgerichtete Aussagen umfassen Aussagen über neue oder geplante Produkte und Funktionen bzw. die Verfügbarkeit von Diensten sowie technologische Entwicklungen.

Obwohl wir der Ansicht sind, dass die in den zukunftsgerichteten Aussagen zum Ausdruck gebrachten Erwartungen angemessen sind, können wir nicht garantieren, dass die in den zukunftsgerichteten Aussagen zum Ausdruck gebrachten zukünftigen Ergebnisse, Leistungen oder Ereignisse erreicht werden.

Alle in diesem Dokument erwähnten nicht veröffentlichten Dienste oder Funktionen sind derzeit nicht verfügbar und werden möglicherweise nicht rechtzeitig oder überhaupt nicht allgemein verfügbar gemacht, wie es nach unserem alleinigen Ermessen bestimmt wird. Jegliche auf diese Weise genannten Dienste oder Funktionen stellen keine Lieferzusagen, Verpflichtungen oder Pflichten von Cohesity, Inc. dar und dürfen nicht in einen Vertrag aufgenommen werden. Kunden sollten ihre Kaufentscheidungen auf der Grundlage von Diensten und Funktionen treffen, die derzeit allgemein verfügbar sind.

## Über die Autoren

### Tim Burlowski

#### VP of Product Management

Tim Burlowski ist Vice President of Product Management bei Cohesity und verantwortlich für Datenschutz und -resilienz, einschließlich Roadmap & Strategie für NetBackup. Tim kam 1998 zu Veritas und hat den größten Teil seiner Karriere darauf verwendet, die weltweiten Daten zu schützen, indem er die Produktqualität verbesserte, das Kundenerlebnis vereinfachte und die Skalierung und Resilienz für NetBackup- und NetBackup-Appliance-Kunden erhöhte.

### Jim Tavares

#### Senior Director, Security Solutions

Jim Tavares leitet das Security Center of Excellence bei Cohesity – ein erstklassiges Team mit vielfältigen Erfahrungen in den Bereichen Sicherheit, Backup/Wiederherstellung und IT. Zuvor arbeitete er für VMware, wo er öffentliche und private cloudbasierte 5G-Netzwerke in den USA, Europa und Asien bereitstellte. Davor war er ein langjähriger Cisco-Veteran, wo er Führungsaufgaben in den Bereichen Produktmanagement, Lösungsentwicklung, Services, Strategie und Channel-Management innehatte. Jim hat einen Bachelor- und einen Master-Abschluss in Ingenieurwissenschaften von der University of Pennsylvania und einen MBA von der Rutgers University.

## Erfahren Sie mehr bei [Cohesity](#)

© 2025 Cohesity, Inc. Alle Rechte vorbehalten.  
Cohesity, das Cohesity-Logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios und andere Cohesity-Marken sind Warenzeichen oder eingetragene Warenzeichen von Cohesity, Inc. in den USA und/oder international. Andere Unternehmens- oder Produktnamen können Warenzeichen der jeweiligen Unternehmen sein, mit denen sie verbunden sind. Dieses Material (a) soll Ihnen Informationen über Cohesity und unser Geschäft und unsere Produkte liefern, (b) wurde zum Zeitpunkt der Erstellung für wahrheitsgemäß und korrekt gehalten, unterliegt aber Änderungen ohne vorherige Ankündigung und (c) wird ohne Gewähr zur Verfügung gestellt. Cohesity lehnt alle ausdrücklichen oder impliziten Bedingungen, Zusagen und Gewährleistungen jeglicher Art ab.

# COHESITY

[cohesity.com/de-de](https://cohesity.com/de-de)

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

2000060-001-DE 5-2025