

# COHESITY

## Einkaufsführer für moderne Web-Scale-Datensicherung und -wiederherstellung

---

Eine umfassende Liste der Anforderungen zur Bewertung einer modernen Lösung



## Inhalt

Einführung: Die Datenflut ist im Gange .....	3
Zeit für Veränderung?.....	4
Bewertung: Herausforderungen im Bereich Datensicherung und -wiederherstellung für die Enterprise-IT.....	5
Evaluierungskriterien für eine moderne Lösung zur Datensicherung und -wiederherstellung.....	6
Hyperkonvergente Plattform.....	6
Zentrales, einfache Verwaltungs-Benutzeroberfläche und Dashboard.....	8
Unterstützung herkömmlicher und moderner Workloads .....	9
Schnelle und flexible Wiederherstellung.....	10
Nativ in der Cloud.....	11
Unbegrenzte horizontale Skalierung .....	12
Störungsfreie Online-Upgrades und Erweiterung .....	12
Garantierte Datenresilienz .....	13
Speicherkapazität und Effizienz maximieren .....	14
Mögliche Vorteile: Erweiterbarkeit, Sicherheit und Compliance.....	17
Wie eine moderne Datensicherung und -wiederherstellung aussieht.....	19

## Einführung: Die Datenflut ist im Gange

In dem Maße, in dem sich die Anforderungen eines Unternehmens wandeln, und Workloads stärker verteilt werden, kommt eine wichtige Erkenntnis auf: Herkömmliche Ansätze hinsichtlich Datensicherung und -wiederherstellung sind für die meisten Unternehmen nicht mehr angemessen. Unternehmen haben erkannt, dass ihre bestehenden Tools nicht mit den anderen Fortschritten in der IT-Umgebung Schritt halten, darunter bei hyperkonvergenten Systemen und software-definierter Infrastruktur, die darauf abzielen, die Komplexität im Datenzentrum reduzieren und den Anstieg der Gesamtbetriebskosten zu mindern.

Die aktuelle Umgebung im Bereich Datensicherung und -wiederherstellung weist zahlreiche Legacy-Einzelprodukte für Datensicherung, Zielspeicher und langfristige Datenretention auf. Die Verwaltung dieser Umgebung ist komplex, da jedes dieser Silos auf proprietäre Hardware- und/oder Softwarepakete ausgelegt ist, die üblicherweise eigene Management-Tools, Upgrade-Zyklen und Wartungs- und Supportverträge aufweisen.

Zugleich schaffen und verbrauchen Unternehmen mehr Daten als je zuvor, da Risse im Fundament der Datensicherung und -wiederherstellung auftreten. Daten sind die neue Währung für Unternehmen, wie oft gesagt wird, und die Datenmenge explodiert. Unternehmen weltweit sehen sich einer Datenflut gegenüber: Die Datenmenge wächst immer schneller an, da immer neue Informationstypen in bestehende Datenverwaltungssysteme aufgenommen werden.

Unternehmen speichern nicht mehr nur herkömmliche Routine-Geschäftsdaten ab. Für einige Unternehmen ist es höchst wichtig, von Menschen erzeugte Daten zu speichern. Heute absorbieren Unternehmen jedoch auch die Daten zahlreicher Sensoren und Maschinen. Und diese Geräte sind über das gesamte Unternehmen hinweg verteilt.

Eine weitere wichtige Komponente bei der Herausforderung des Datenwachstums umfasst die Unterstützung eines erheblich breiteren Anwendungsspektrums als in der Vergangenheit. Und in dem Maße, in dem die Cloud ein integrierter Bestandteil des allgemeinen IT-Ökosystems wird, werden moderne Anwendungen und deren Daten sowohl vor Ort als auch in der Cloud vorgehalten.

Es geht im Endeffekt darum, dass das Datenwachstum real ist und weitergehen wird, wie die Einführung einer stets wachsenden Anzahl von Anwendungen demonstriert. Um ein altes Klischee etwas abzuwandeln: Mit großer Datenmenge geht große Verantwortung einher. Unabhängig von der Quelle müssen Unternehmen mit dem Datenwachstum Schritt halten, wenn es um die Fähigkeit im Bereich Datensicherung und -wiederherstellung geht.

In der Realität verhält es sich jedoch oft so, dass Kunden oft bereits am Limit arbeiten und selbst im besten Fall Sicherungen nur einmal täglich durchführen können – und diese Aufgaben überschneiden sich oft mit dem Produktionsfenster während der normalen Arbeitszeit. Und was noch wichtiger ist: Sollte eine schnelle Wiederherstellung notwendig werden, wie z. B. nach einem Ransomware-Angriff, kann diese Wiederherstellung mehrere Stunden in Anspruch nehmen, mit den entsprechenden Auswirkungen auf das Geschäft. Dies könnte im Ernstfall zu einer IT-Katastrophe führen.

## Zeit für Veränderung?

Historisch haben Unternehmen erhebliche Teile Ihres IT-Budgets für Tools zur Datensicherung und -wiederherstellung ausgegeben, die mit der Zeit immer zahlreicher wurden. Sie schützen ihre Daten weiterhin mit Legacy-Lösungen für Datensicherung und -wiederherstellung, die für eine frühere Generation der Computertechnik entwickelt wurden.

Angesichts dessen, dass einige Produkte ihren Ursprung in jahrzehntealter Technik haben, können viele Tools einfach nicht mit den aktuellen Geschäftsanforderungen und der konstanten Weiterentwicklung Schritt halten. In dem Maße, in dem sich die Geschäftsbedürfnisse entwickeln, müssen Unternehmen der wachsenden IT-Komplexität einen Schritt voraus sein. Unternehmen benötigen eine IT-Infrastruktur einschließlich Tools zur Datensicherung und -wiederherstellung, die agil, einfach skalierbar, und einfach zu verwalten ist.

Wenn Sie ein Upgrade Ihrer bestehenden Legacy-Infrastruktur zur Datensicherung und -wiederherstellung erwägen, sind Sie in guter Gesellschaft. Gartner prognostiziert, dass „... bis 2021 im Vergleich zum Stand Anfang 2017 50 % der Unternehmen ihre aktuellen Sicherungs-Anwendungen durch neue Lösungen ergänzen oder ersetzen werden.“

Die Auswahl der richtigen modernen, Web-Scale-Lösung zur Datensicherung und -wiederherstellung in Enterprise-Qualität erfordert zunächst ein Verständnis aller potenziellen Probleme, gefolgt von einem Vergleich der Lösungen mit diesen Problemen. Dieser Leitfaden ist Ihr Handbuch zur Auswahl des Produkts, das die Anforderungen Ihres Unternehmens am besten erfüllt, heute und in Zukunft. In dem Maße, wie sich Ihr Unternehmen entwickelt, benötigen Sie eine Plattform zur Sicherung und Wiederherstellung, die sich gemeinsam mit Ihnen entwickeln kann.

**Der Hauptzweck dieses Einkaufsführers besteht darin, Ihnen bei der Ermittlung von Kriterien zu helfen, wenn Sie Ihre nächste Lösung zur Datensicherung und -wiederherstellung erwägen. Dieser Leitfaden umfasst folgendes:**

- Die grundlegenden Fragen, die Sie zu Ihrer aktuellen Umgebung stellen müssen
- Übliche Probleme im Bereich Datensicherung und -wiederherstellung, denen sich Unternehmen gegenübersehen
- Zu erwägende Aspekte Ihrer nächsten Lösung zur Datensicherung und -wiederherstellung, um die Zukunftssicherheit Ihrer Investition zu gewährleisten
- Beispiele für Angebotsanfragen, um sicherzustellen, dass Ihr Auswahlprozess alle relevanten Elemente berücksichtigt

Wie bei vielen Technologien der Fall ist, gibt es zahlreiche widersprüchliche Ansichten im Bereich Datensicherung und -wiederherstellung. Einige der Informationen, die verbreitet werden, zielen darauf ab, beim Käufer Furcht, Unsicherheit und Zweifel zu erzeugen. Dieser Leitfaden wird Ihnen dabei helfen, Unklarheiten zu beseitigen und bei der Modernisierung Ihrer Datensicherung und -wiederherstellung Anleitung und Sicherheit zu geben.

Wenn Sie die Evaluierungskriterien für eine moderne Lösung zur Datensicherung und -wiederherstellung durchgehen, beachten Sie insbesondere die empfohlenen Fragen an Anbieter. Wenn Sie persönlich mit dem Anbieter sprechen, achten Sie darauf, vollständige, klare und prägnante Antworten auf Ihre Fragen zu erhalten. Wenn Sie eine Angebotsanfrage für eine neue Lösung zur Datensicherung und -wiederherstellung vorbereiten, helfen Ihnen diese Fragen dabei, die Antworten zu erhalten, die Sie benötigen.

## Bewertung: Herausforderungen im Bereich Datensicherung und -wiederherstellung für die Enterprise-IT

Bevor Sie mit dem Auswahlprozess beginnen, müssen Sie potenzielle Mängel in Ihrer bestehenden Umgebung zur Datensicherung und -wiederherstellung verstehen. Tabelle 1 umfasst 7 häufige Herausforderungen im Bereich Datensicherung und -wiederherstellung, denen sich die IT gegenübersteht. Nehmen Sie sich einige Minuten, um Ihre Ausgangsposition zu ermitteln, damit Sie den Startpunkt Ihrer Suche optimal festlegen können.

Ausgabe	Beschreibung	In Ihrer Umgebung vorhanden?
Silo-Infrastruktur mit mehreren fragmentierter Benutzeroberflächen zur Konfiguration von Backup-Workflows	Erfordert Ihre aktuell Lösung die Nutzung von Backup-Software und separaten Medien-Servern, dedizierten Speicherzielen und mehreren Benutzeroberflächen, um Backup-Workflows zu erstellen? Müssen Sie separate Umgebungen zur Sicherung physischer Workloads und ein anderes Silo für virtuelle Server betreiben und noch ein weiteres Produkt und eine Konsole zum Schutz der Datenbanken und Anwendungen nutzen?	<input type="checkbox"/>
Separate Cloud-Gateway	Wenn Ihr aktuelles System öffentliche Clouds unterstützt, müssen Sie separate Cloud-Gateways einsetzen, die als Vermittler zwischen den Vor-Ort- und cloudbasierten Umgebungen zur Datensicherung und -wiederherstellung fungieren?	<input type="checkbox"/>
Forklift-Upgrades und disruptive Upgrades	Wenn es an der Zeit ist, die Umgebung zur Datensicherung und -wiederherstellung zu erweitern, müssen Sie Ihre bestehende Infrastruktur vollständig durch eine neue, kostspielige und komplexe Infrastruktur ersetzen? Müssen Sie Stillstandszeiten einplanen, um Software-Updates durchzuführen?	<input type="checkbox"/>
Langsame Wiederherstellungen, nur letzter Punkt	Leidet Ihre aktuelle Lösung aktuell an Leistungsproblemen bei der Wiederherstellung und somit zu potenziellem Nichterreichen des RTO? Oder ist nur eine Wiederherstellung von der letzten angefertigten Sicherungskopie möglich?	<input type="checkbox"/>
Variable und/oder feste Block-Deduplizierung mit Komprimierung	Variable und/oder feste Block-Deduplizierung mit Komprimierung Fehlen Ihrer aktuellen Lösung Daten-Deduplizierungsfunktionen? Wenn Ihr aktuelle Lösung diese Funktionen aufweist, sind die Deduplizierungs-Domänen beschränkt oder ist nur feste Block-Deduplizierung möglich?	<input type="checkbox"/>
Disruptive, im Voraus geplante Upgrades	Wird eine neue Softwareversion für Ihre aktuelle Lösung verfügbar, müssen Sie einen potenziell disruptiven Prozess durchführen, um die neue Version einzuführen? Oder erfordert das Upgrade umfangreiche Planung?	<input type="checkbox"/>
Sicherungsdaten können nicht wiederverwendet werden, Infrastruktur verbleibt in Silos	Bietet Ihre aktuelle Lösung nur Dienste zur Datensicherung und -wiederherstellung? Ermöglicht Ihnen die Lösung die Wiederverwendung von Daten für andere Anwendungsfälle wie Entwicklung/Test-Szenarien? Ermöglicht Ihnen Ihr aktuelles Produkt eine Effizienzsteigerung durch Konsolidierung anderer Workload-Speicherungsumgebungen?	<input type="checkbox"/>

Tabelle 1. Eine Checkliste zur Profilierung Ihrer aktuellen Umgebung zur Datensicherung und -wiederherstellung.

Wenn Sie eine oder mehrere Kästchen in Tabelle 1 angekreuzt haben, sollten Sie Ihre Optionen zum Austausch ihrer bestehenden Software zur Datensicherung und -wiederherstellung erwägen. Auf dem aktuellen Markt sind Optionen verfügbar, die die Datensicherung und -wiederherstellung aus moderner Web-Scale-Perspektive neu konzeptioniert haben, um alle diese Mängel elegant, einfach und kostengünstig zu beheben.

## Evaluierungskriterien für eine moderne Lösung zur Datensicherung und -wiederherstellung

Die Evaluierungskriterien, die Sie für ältere Lösungen zur Datensicherung und -wiederherstellung verwendet haben, sind nicht mehr relevant. Eine neue Denkweise ist von Nöten. Kommen Sie von der Ansicht ab, dass Datensicherung und -wiederherstellung eine teure Versicherung ist, die nach Diensten und Verantwortlichkeiten in Silos aufgeteilt werden muss. Heute müssen diese Fähigkeiten ein Kernelement Ihrer Infrastruktur darstellen, keinen Nebengedanken, der die Komplexität der Umgebung steigert.

Zudem erfordern moderne, anwendungsorientierte Workloads eine nahtlose Datenmobilität zwischen Vor-Ort-Umgebungen und der Cloud. Unternehmen benötigen Lösungen für Datensicherung und -wiederherstellung, die agil sind, unendliche Flexibilität bieten und schnell auf Änderungen der Geschäftsanforderungen reagieren können.

In den folgenden Abschnitten werden die wichtigsten Attribute einer modernen Lösung zur Datensicherung und -wiederherstellung erörtert.

## Hyperkonvergente Plattform

Die IT steht unter höherem Druck als je zuvor, und in dem Maße, in dem Unternehmen wichtige Initiativen zur digitalen Transformation umsetzen müssen, sinkt die Toleranz für komplexe Datenzentrum-Umgebungen, die nur den Routinebetrieb unterstützen. So wichtig, wie Lösungen für Datensicherung und -wiederherstellung für Ihr Unternehmen sind: Sie können sich keine Lösungen leisten, die unnötige Komplexität erzeugen.

Wie sieht eine moderne, zukunftsorientierte Architektur zur Datensicherung und -wiederherstellung aus reiner Hardware-Perspektive aus? Wenn Sie betrachten, wie Ihre Umgebung zur Datensicherung und -wiederherstellung mit Ihrer Produktionsumgebung in Zusammenhang steht, werden Sie erkennen, dass Sie eine nicht-statische Lösung zur Datensicherung und -wiederherstellung benötigen. Ihre Lösung muss mit dem Wachstum Ihrer Produktionsumgebung Schritt halten und muss die selbe Flexibilität aufweisen, die Sie von Ihrer Produktionsumgebung erwarten. Wenn Sie beispielsweise neue Anwendungen hinzufügen, darf Ihre Umgebung zur Datensicherung und -wiederherstellung keine wochenlange Planung und stundenlange Stillstandszeit zur Integration benötigen.

Wenn Sie Ihre Optionen zur Datensicherung und -wiederherstellung durchgehen, überdenken Sie, was Sie kaufen müssen. Bei einigen Lösungen müssen Sie Multiple-Point-Lösungen beschaffen, einschließlich:

- Sicherungs-Software
- Medien- und Master-Server
- Zielspeichergeräte
- Kompatible Bandgeräte zur langfristigen Archivierung
- Cloud-Gateway(s) zur Integration mit der öffentlichen Cloud

Ein Schlüsselziel im Bereich Datensicherung und -wiederherstellung sollte Einfachheit sein. Optionen für moderne Datenzentrum-Architektur, wie hyperkonvergente Infrastruktur, können Ihnen dabei helfen, Ihre Umgebung zur Datensicherung und -wiederherstellung einfacher zu gestalten. Hyperkonvergente Infrastruktur ist ein führender Kandidat für primäre Produktions-Workloads geworden. Angesichts der Prinzipien der Hyperkonvergenz eignet sich diese Infrastruktur noch besser für die Datensicherung und -wiederherstellung. Selbst wenn Sie im Tier-1-Setting (der primären Workload) keine Hyperkonvergenz nutzen, stellt sie dennoch wahrscheinlich eine ausgezeichnete Option für Ihre Datensicherung und -wiederherstellung dar.

Warum? Warum eignen sich hyperkonvergente Lösungen so gut für umfassende Anforderungen an Datensicherung und -wiederherstellung? Zum einen eliminieren sie Silos. In der IT finden sich bereits genug Silos. Sie sollten weder 1) Ihre Umgebung zur Datensicherung und -wiederherstellung in separat verwaltete Berechnungs-, Speicher- und Software-Silos aufteilen noch 2) mehrere parallele Umgebungen für mehrere Workloads betreiben müssen.

Die Möglichkeit, diese unterschiedlichen Silos in eine zentrale Lösung zu konsolidieren, die die Sicherungs-Software und den Zielspeicher in eine Lösung integriert, ermöglicht Ihnen eine schnelle und einfache Bereitstellung und Skalierung Ihrer Umgebung zur Datensicherung und -wiederherstellung nach Bedarf – überall.

Im Kontext der Datensicherung und -wiederherstellung kann Hyperkonvergenz zudem auf die Typen von Diensten, die Sie schützen können, anwendbar sein. Eine moderne Sicherungslösung muss sicherstellen, dass alle Workloads, die Sie betreiben, geschützt werden können. Daher muss Sie Ihre Bare-Metal-Server ebenso wie Ihre virtuellen Maschinen (VMs) schützen können, unabhängig vom Hypervisor, Ihre Enterprise-Anwendungen und -Datenbanken vollständig unterstützen sowie Ihre primären Speichersysteme und NAS-Geräte schützen.

Während der Evaluierung der nächsten modernen Lösung zur Datensicherung und -wiederherstellung sollte der IT-Experte ein Angebot in Betracht ziehen, das Silos eliminiert, indem Sicherungs-Software und Zielspeicher in eine einzige Lösung konsolidiert werden und der Bedarf nach unnötigen Master- und Medien-Servern entfällt. Und diese Lösung sollte nahtlos mit langfristigen Speichermedien synchronisiert werden können, ob in der öffentlichen Cloud oder auf Band.

Die Hardware- und Softwaresilos abzubauen, die bei Legacy-Lösungen für Datensicherung und -wiederherstellung inhärent sind, ist bereits ein wertvolles Ziel. Aber zudem eröffnet dies Möglichkeiten hinsichtlich dem Potenzial, mit gesicherten Daten andere Workloads zu unterstützen, darunter Analysen, Sicherheit und Compliance – sogar Anwendungsentwicklung und -Tests.

Ein Schlüsselproblem, das sich aus einem Legacy-Ansatz im Datenmanagement ergibt, besteht in der Massenfragmentierung von Daten, die sich ohne eine angemessene Infrastruktur praktisch nicht beheben lässt. Massenfragmentierung von Daten bezieht sich auf die wachsende Vermehrung von Daten über Workloads hinweg, innerhalb von Workloads (z. B. Datensicherung und -wiederherstellung) sowie funktions- und ortsübergreifend (z. B. Vor Ort und öffentliche Clouds). Diese Fragmentierung von Datenelementen in separate Silos reduziert das Potenzial, Wert aus diesen Daten zu schöpfen. Jede weitere Fragmentierung erschwert es dem Unternehmen, tatsächlich umfassend zu verstehen, welche Datenelemente vorliegen, wodurch die Analyse erschwert wird.

Zudem verfügt jedes Silo oft über eine eigene Infrastruktur, was dazu führt, dass unzählige Datenkopien sich in unterschiedlichen Systemen und an unterschiedlichen Standorten befinden. Eine derartige Fragmentierung steigert die Kosten, da zusätzliche Infrastruktur benötigt wird, und senkt das Vertrauen, dass eine bestimmte Kopie eines Datensatzes die „richtige“ Kopie zur Analyse ist.

Eine hyperkonvergente Plattform kann Ihnen das Potenzial verleihen, eine Reihe von Workloads in eine einzige, zusammenhängende Umgebung zu konsolidieren, die ein hohes Maß an Skalierbarkeit und Sichtbarkeit ermöglicht. Durch die Konsolidierung aller Datenkopien in eine Plattform reduzieren Sie Ihre gesamten Kapazitätsanforderungen signifikant und steigern zugleich Ihre Fähigkeit, aus Daten Wettbewerbsvorteile zu schöpfen, da Sie Vertrauen in die Vollständigkeit und Zuverlässigkeit der verbleibenden Datensätze haben können. Die Fähigkeit einer hyperkonvergenten Plattform, das Problem der Massenfragmentierung von Daten zu lösen, sollte ein Schlüsselaspekt für Unternehmen darstellen, die Initiativen im Bereich der digitalen Transformation angehen, für die Effizienz und Konsistenz der Unternehmensdaten erforderlich sind.

## Fragen, die Sie Anbietern zur Architektur Ihrer Lösung stellen sollten

- Bietet Ihre Lösung die Flexibilität einer softwareorientierten Lösung und zugleich eine vollständige Hardware-Software-Option?
- Können Sie detailliert erläutern, wie Ihre Lösung skalierbar ist und wie sich dies auf die Leistung auswirkt?
- Unterstützt Ihre Lösung die Wiederverwendung von Sicherungskopien für andere Workloads abgesehen von Wiederherstellung?

## Zentrales, einfache Verwaltungs-Benutzeroberfläche und Dashboard

Sobald ein neues System läuft, ist die Verwaltung das nächste potenzielle Problem. Und im Gegensatz zur Bereitstellung ist die Verwaltung eine tägliche Aufgabe – Benutzerfreundlichkeit ist kein nettes Extra, sondern absolut erforderlich.

Einfachheit in jedem Aspekt der IT-Infrastruktur ist eine immer wichtiger werdende Anforderung. Moderne Lösungen für Datensicherung und -wiederherstellung müssen jedoch über die reine Benutzerfreundlichkeit hinausgehen. Sie müssen zudem umfassende Unterstützung für alle Datenschutz-Anwendungsfälle über eine einzige Konsole bieten, darunter Notfallwiederherstellung, Archivierung/langfristige Datenaufbewahrung, Speicher-Tier und Replikation. Auf den ersten Blick kann es akzeptabel scheinen, unterschiedliche Datentypen über verschiedene Konsolen zu sichern, aber die Datensicherung und -wiederherstellung umfasst mehr als nur die Sicherung. Das wichtige ist die Wiederherstellung.

Bei der Wiederherstellung kann es um Minuten gehen. Die Situation kann unklar sein, und Antworten schwierig zu finden. Hierbei benötigen Sie nicht noch eine überkomplexe Administration, die Ihre Wiederherstellung zusätzlich erschwert.

Von Anfang bis Ende muss ein Tool zur Datensicherung und -wiederherstellung eine einfache, intuitive, zentrale Benutzeroberfläche bieten, die alle Aspekte der Umgebung verwalten kann, darunter die erste Bereitstellung der Sicherungs- und Wiederherstellungs-Hardware und -Software, die laufende Verwaltung von Sicherungskopien und schließlich die Wiederherstellung.

Natürlich geht eine vollständig konvergente Umgebung zur Datensicherung und -wiederherstellung weit über die reine Sicherung und Wiederherstellung hinaus; das bedeutet, dass das Management-Paradigma sowohl den Datenschutz als auch zahlreiche weitere Anwendungen umfassen und zugleich die Einfachheit bewahren muss. Anders ausgedrückt: Einfachheit umfasst die Annahme, dass die Infrastruktur versucht, durch Machine-Learning-basierte Personalisierung zu lernen, was Ihnen wichtig ist, und automatische Empfehlungen hinsichtlich Best Practices Ihrer Branche abzugeben. Ein ML-gestützter Ansatz bedeutet, dass Vorgänge schneller und präziser durchgeführt werden können, wodurch Ihr Unternehmen seine Ziele hinsichtlich der Service Level Agreements (SLAs) einfacher erfüllen kann.

Anders ausgedrückt: Die Verwaltungsebene sollte nicht nur als Konsole fungieren, sondern als intelligenter Assistent, der Ihnen helfen kann, Anomalien zu erkennen und entsprechende Empfehlungen zur Fehlerbehebung abgeben kann, wie beispielsweise hinsichtlich Kapazitätsplanung. Dies sollte ebenfalls im Umfang einer zentralen, globalen Verwaltungs-Benutzeroberfläche enthalten sein.

### Fragen, die Sie Anbietern zur Verwaltbarkeit ihrer Lösung stellen sollten

- Wie viele Maschinen sind erforderlich, um umfassende Unterstützung für Datensicherung und -wiederherstellung für Bare-Metal-Server, virtuelle Maschinen, herkömmliche und moderne Datenbanken, Container-Umgebung und SaaS-basierte Anwendungen zu leisten?
- Kann Ihre Lösung meine umfassende Kapazitätsplanung in meiner Umgebung unterstützen?
- Bietet Ihre Lösung Machine-Learning-Funktionen, die mir helfen, meine Zeit effizienter zu nutzen und die SLA-Einhaltung zu verbessern?



## Unterstützung herkömmlicher und moderner Workloads

Die heutige Workload-Umgebung unterscheidet sich drastisch von der Umgebung, die Administratoren vor nur wenigen Jahren unterstützten. Sie sind sich wahrscheinlich bewusst, dass die meisten Unternehmen mittlerweile eine Hybrid-Cloud-Umgebung nutzen, bei der sich viele Anwendungen vor Ort, viele weitere in der Cloud (SaaS und/oder IaaS) befinden. Wenn Sie bei diesen Bereitstellungs-Szenarien jedoch eine Ebene tiefer gehen, haben sich auch die Workloads selbst weiterentwickelt. Es handelt sich noch immer um virtuelle Maschinen, Dateiserver, Datenbankserver usw., aber diese wurden um moderne Workloads wie containerisierte Anwendungen auf Basis von Kubernetes oder Docker Swarm, verteilte NoSQL-Datenbanken und Hadoop ergänzt. Diese Anwendungstypen und Datenquellen sind recht neu, dementsprechend besteht ein neuer Bedarf, sie zu schützen und zu unterstützen.

Weitere Dienste sind ebenfalls recht neu, darunter unstrukturierte Daten-Repositories wie OneDrive, Teil des Office 365 SaaS-Angebots. In wachsendem Maße entdecken Kunden, dass die SaaS-Anwendungen, auf die sie sich verlassen, Datenverfügbarkeit, aber keine Datensicherung und -wiederherstellung in Enterprise-Qualität bieten. Betrachten wir beispielsweise Office 365. Microsoft betreibt den Dienst und hält ihn in Betrieb, bietet jedoch nur minimalen Schutz hinsichtlich einer Wiederherstellung im Fehlerfall. Die meisten Unternehmen benötigen jedoch mehr als nur dieses Minimum, wenn es um eine so wichtige Anwendung wie Office 365 geht.

Unternehmen sehen sich zunehmend in der Situation, einen besseren Schutz für SaaS-basierte Workloads wie Office 365, Salesforce und Workday finden zu müssen. Datensicherung und -wiederherstellung für SaaS-Angebote muss in der Lage sein, eine Kopie von SaaS-Anwendungsdaten zu erstellen und diese in einem Cluster vor Ort oder einem anderen cloudbasierten Ziel wie Azure oder AWS zu speichern.

Ihre modernen Lösungen für Datensicherung und -wiederherstellung müssen alle Anwendungen unterstützen, die Sie schon immer verwendet haben, aber zudem ebenfalls neue Konstrukte unterstützen, wenn diese auf den Markt kommen, darunter gebräuchliche SaaS-Tools, container-orientierte Dienste, NoSQL-Dienste und vieles weiteres. Diese Tools sind für moderne Unternehmen unverzichtbar, und sie benötigen Unterstützung derselben Qualität wie herkömmliche Workloads. Die Datensicherung und -wiederherstellung muss bei diesen modernen Workloads so nahtlos sein wie bei Legacy-Workloads.

### Fragen, die Sie Anbietern zur Workload-Unterstützung ihrer Lösung stellen sollten

- Unterstützt Ihre Lösung Workloads vor Ort, darunter Bare-Metal-Server ebenso wie virtualisierte und containerisierte Workloads?
- Unterstützt Ihre Lösung herkömmliche ebenso wie moderne Workloads, darunter NoSQL, Hadoop-Workloads und containerisierte Anwendungen?
- Unterstützt Ihre Lösung meine SaaS-basierten Anwendungen, darunter Office 365?

## Schnelle und flexible Wiederherstellung

Im Endeffekt besteht der gesamte Zweck einer Datensicherungs-Umgebung darin, Wiederherstellung zu ermöglichen. So einfach ist das. Dieser einzige Schwerpunkt bedeutet leider nicht, dass jedes Produkt auf dem Markt die Wiederherstellung einfach, flexibel und schnell durchführen kann – aber genau das wird benötigt. Ob die Wiederherstellung notwendig wird, wenn ein Benutzer eine einzige Datei verloren hat, oder ein Notfall auftritt, der eine Massenwiederherstellung erfordert – oft ist der Wiederherstellungsprozess zu stressig.

Ihr Wiederherstellungsprozess sollte das einfachste Element der Gleichung sein und keinen tagelangen Aufwand erfordern. Zudem sollte es keine Geduldsaufgabe sein, zu ermitteln, welche Daten wiederhergestellt werden müssen. Stellen Sie sich eine Sicherungslösung vor, deren Architektur auf die Wiederherstellung ausgelegt ist. Diese Lösung bietet eine umfassende globale Such- und Wiederherstellungsfunktion, die jede geschützte Datei indiziert, sodass jede benötigte Datei einfach auffindbar und schnell wiederherstellbar ist, unabhängig davon, wo in der Produktionsumgebung sie sich befindet. Diese Fähigkeit ist für moderne Unternehmen von höchster Wichtigkeit.

Die Wiederherstellung ist nicht immer die einfache Aufgabe, eine einzelne Datei oder einen Ordner wiederherzustellen. Oft müssen Sie vollständige virtuelle 3-Tier-Umgebungen wiederherstellen oder Sie müssen nach einem Ransomware-Angriff hunderte oder tausende Dateien und deren Abhängigkeiten wiederherstellen. Herkömmliche Sicherheitstools können Probleme bereiten, lange Wartezeiten erzeugen und bei Wiederherstellungen keine Hinweise bezüglich Wiederherstellbarkeit oder Schwachstellen geben – keine gute Situation in einer Welt, in der „RTO nahe Null“ das Ziel ist.

Ihre Lösungen für Datensicherung und -wiederherstellung müssen in der Lage sein, die letzte bekannte „gute“ Version Ihrer Umgebung unmittelbar und vollständig wiederherzustellen, unabhängig davon, ob es um eine einzelne große Datei, eine einzelne VM, mehrere hundert VM oder um alles geht. Die Lösung muss zudem große Dateien problemlos verarbeiten und wiederherstellen können.

In diesem Abschnitt möchten wir zudem darauf hinweisen, dass der Lösungsdienst in die Tiefe – bis auf Datei- oder VM-Ebene – ebenso wie in die Breite gehen muss. Bei der Granularität sollten Sie keine Kompromisse eingehen müssen. Die Lösung Ihrer Wahl sollte den von Ihnen gewünschten Grad an Granularität bieten, damit ein stressiger Wiederherstellungsvorgang nicht unmöglich wird.

### Fragen, die Sie Anbietern zu den Wiederherstellungsfähigkeiten Ihrer Lösung stellen sollten

- Bietet Ihre Lösung eine globale Suchfunktion für meine gesamte Sicherungsumgebung (Core-to-Edge-to-Cloud)?
- Unterstützt Ihre Lösung eine unmittelbare Massen-Wiederherstellung von Objekten, einschließlich der gesamten Anwendungsumgebung?
- Worin bestehen meine Optionen hinsichtlich der Granularität der Wiederherstellung?
- Kann Ihre Lösung Sicherungs-Verifizierungen vornehmen, um die Wiederherstellbarkeit sicherzustellen?

## Nativ in der Cloud

Die Nutzung der öffentlichen Cloud wird immer reifer, und Unternehmen verlagern herkömmliche Vor-Ort-Anwendungen zunehmend in die öffentliche Cloud. Im Ergebnis reicht die IT-Infrastruktur eines modernen Unternehmens weit über die Grenzen des lokalen Datenzentrums hinaus. Ihre Umgebung für Datensicherung und -wiederherstellung muss diese Evolution ebenfalls berücksichtigen.

Die Cloud hat sich als Schlüsselfaktor für die Datensicherung und -wiederherstellung herausgestellt. Mehr Unternehmen als je zuvor nutzen die öffentliche Cloud statt ein Vor-Ort-Datenzentrum als bevorzugtes Sicherungsziel. In vielen Fällen ist nun die Cloud das neue Magnetband. Die TCO-Cloud bietet Möglichkeiten zur Archivierung, die schwer zu übertreffen sind. Zudem ist die Einrichtung einer Cloud schneller, und sie bietet die Möglichkeit, Investitionskosten gegen Betriebskosten zu tauschen. Die Möglichkeit, die Elastizität und Wirtschaftlichkeit der öffentlichen Cloud für die Datensicherung und -wiederherstellung und andere Workloads zu nutzen, ist attraktiv und sollte eine native Fähigkeit moderner Plattformen sein.

Unabhängig von der aktuellen Annahme von öffentlichen Cloud-Technologien muss Ihr nächstes Produkt für Datensicherung und -wiederherstellung native Integration in die öffentliche Cloud bieten. Vielleicht gehen Sie davon aus, dass Ihre aktuelle Legacy-Lösung für Datensicherung und -wiederherstellung genügend Unterstützung für die öffentliche Cloud bietet. Vielleicht haben Sie eine Lizenz oder ein Gerät erworben, die das Produkt durch Cloud-Funktionen ergänzt oder eine Gateway-Anwendung, die Cloud-Unterstützung hinzufügt.

Vorsicht: Diese nachträglichen Ergänzungen sind oft unvollständig, kostspielig und steigern die Komplexität der Vorgänge in Ihrer Umgebung für Datensicherung und -wiederherstellung erheblich. Angesichts der Relevanz der Cloud, kann eine Lösung, die im Zeitalter vor der Cloud erstellt wurde, tatsächlich die sich stets ändernden Geschäftsbedürfnisse erfüllen? Im Gegensatz zu diesen Legacy-Sicherungslösungen entfällt bei einer modernen Lösung für Datensicherung und -wiederherstellung der Bedarf nach nachträglichen Cloud-Gateways, und sie unterstützt Cloud-Integration und native Datenmobilität.

Eine moderne Sicherungslösung ermöglicht es Enterprise-IT-Verantwortlichen, richtlinienbasierte Automatisierung zu nutzen, um ihre Daten nahtlos zwischen Vor-Ort-Infrastruktur und Cloud-Infrastruktur zu verschieben. Zu den Anwendungsfällen gehören nicht nur kostengünstige Speicherung: Sind die Daten angekommen, gehört es zur Mobilität, mittels Cloud-Computing die Anwendungsentwicklung (z.B. Einrichtung einer neuen Entwicklung/Test-Umgebung) und Analysen zu beschleunigen.

Die Notfallwiederherstellung ist ein weiterer attraktiver Anwendungsfall. Bei der Wiederherstellung geht es darum, Workloads nach einem Vorfall wieder in einen betriebsfähigen Zustand zu versetzen. Ein Vorfall kann im Schweregrad von einer versehentlich gelöschten Datei bis zur vollständigen Zerstörung des Datenzentrums reichen. Im ersten Fall ist die Wiederherstellung keine schwierige Aufgabe. Im zweiten Fall kann die Wiederherstellung eine praktisch unmögliche Herausforderung darstellen, wenn nicht die richtigen Tools vorhanden sind.

Hierfür sollten Sie ein Produkt zur Datensicherung und -wiederherstellung auswählen, das eine Bereitstellung von Workloads entweder im ursprünglichen Cluster oder an einem neuen Standort ermöglicht, ob in der Cloud oder einer Vor-Ort-Einrichtung in derselben Stadt. So können Sie unmittelbar nach einem Notfall Ihre Workloads wieder hochfahren und zugleich an ihren längerfristigen Maßnahmen zur Wiederherstellung arbeiten.

Wenn Sie neue Lösungen für Datensicherung und -wiederherstellung in Betracht ziehen, achten Sie darauf, die gesamte Anwendungsumgebung zu berücksichtigen, einschließlich Anwendungen in der Cloud.

### Fragen, die Sie Anbietern zu den nativen Cloud-Funktionen Ihrer Lösung stellen sollten

- Unterstützt Ihre Lösung eine einfache Daten- und Anwendungs-Mobilität in die öffentliche Cloud?
- Kann Ihre Lösung mir helfen, meine Cloud-nativen Anwendungen zu unterstützen?
- Können Sie meine SaaS-Anwendungsdaten schützen?

## Unbegrenzte horizontale Skalierung

Genau wie Ihre Produktionsumgebung ist Ihre Umgebung für Datensicherung und -wiederherstellung nicht statisch. Sie ändert sich konstant, im Rhythmus mit den Änderungen, die Sie an Ihrer Produktionsumgebung vornehmen.

Eine inflexible Lösung zur Datensicherung und -wiederherstellung führt zu gesteigerten Kosten und Verzögerungen bei der Bereitstellung neuer Produktionssysteme, da IT-Experten die Umgebung zur Datensicherung und -wiederherstellung auf die neuen Workloads anpassen müssen.

In einer Gegenwart, in der Speed-to-Market sich auf den Profit auswirkt, ist es nicht akzeptabel, wenn die Umgebung zur Datensicherung und -wiederherstellung den Rest des Geschäfts aufhält. Und überhaupt nicht akzeptabel ist eine derartige Situation angesichts der Tatsache, dass es auf dem Markt hyperkonvergente Lösungen gibt. Diese Lösungen sind speziell darauf ausgelegt, die Skalierung dieser Umgebungen zu vereinfachen.

Dieser Typ skalierbarer Architektur zur Erfüllung von Geschäftsbedürfnissen sollte sich zudem bei modernen Lösungen für Datensicherung und -wiederherstellung finden. Bei Legacy-Lösungen für Datensicherung und -wiederherstellung müssen Sie wichtige Entscheidungen zum Maßstab zu Beginn der Bereitstellung treffen. Das bedeutet, dass Sie Ihre Kapazitäten hinsichtlich Datensicherung und -wiederherstellung drei bis fünf Jahre im Voraus prognostizieren müssen. Wer kann dies mit plausibler Zuverlässigkeit tun (und dabei möglicherweise wertvolles Investitionskapital binden)?

Ähnlich wie beim Aufbau moderner primärer Umgebungen muss Ihre Datensicherung und -wiederherstellung auf Grundlage von Web-Scale-Prinzipien entwickelt werden. Am wichtigsten ist hierbei, dass Ihre Lösung die Möglichkeit bieten sollte, klein anzufangen und je nach Bedarf hoch zu skalieren. Das bedeutet, dass Sie mit jeder beliebigen Größe beginnen können sollten, statt anfangs zu viel Infrastruktur bereitzustellen.

Daraufhin wächst mit den sich wandelnden Geschäftsbedürfnissen auch Ihre Produktionsumgebung, womit ebenso ein Wachstum Ihres Bedarfs an Datensicherung und -wiederherstellung einhergeht. Stellen Sie sicher, dass Sie diese Umgebung bei Bedarf einfach und unterbrechungsfrei skalieren können, um die wachsenden Geschäftsbedürfnisse zu erfüllen, ohne Komplikationen und signifikante Kosten. Eine moderne Lösung, die unbegrenzt linear skalierbar ist, ohne Beeinträchtigung der Workload-Leistung.

### Fragen, die Sie Anbietern zur Skalierbarkeit Ihrer Lösung stellen sollten

- Nutzt das Produkt eine Scale-Up- oder Scale-Out-Expansionsmethode?
- Bis auf welche Ebene können Sie Ihre Umgebung zur Datensicherung und -wiederherstellung skalieren?
- Werden bei größerem Maßstab Auswirkungen auf die Leistung auftreten?

## Störungsfreie Online-Upgrades und Erweiterung

Fakten: Heutige Unternehmen erwarten von ihren Lösungen 24/7-Verfügbarkeit. Im Gegensatz zur Vergangenheit sind ungeplante Ausfälle nicht mehr akzeptabel, und selbst geplante Stillstandzeiten müssen wenige und selten sein, wenn überhaupt. Die alte Methode, Systeme für Patches, Upgrades oder Erweiterungen herunterzufahren, ist für viele Unternehmen keine Option mehr. Zugleich ist es wichtig, die Software stets auf dem neuesten Stand zu halten. Moderne Lösungen für Datensicherung und -wiederherstellung ermöglichen es den Sicherheits-Admins, Cluster mittels Rolling Upgrades ohne Ausfallzeiten zu upgraden. Bei einem „Rolling Upgrade“ wird jeder Knoten im Cluster einzeln geupgraded; alle Dienste werden während der Wartung auf den verbleibenden Knoten ausgeführt.

Dieses Rolling-Upgrade-Paradigma gilt ebenfalls im Rahmen der Erneuerungszyklen für den Austausch von Nodes. Das Konzept „Forklift-Upgrades“ findet in modernen Lösungen für Datensicherung und -wiederherstellung keine Anwendung mehr. Die Administratoren können Nodes nahtlos einbinden oder ausrangieren. Es sollte nie wieder notwendig sein, eine Umgebung für die Datensicherung und -wiederherstellung disruptiv auszutauschen, nur weil der Abschreibungsplan dies erfordert.

### Fragen, die Sie Anbietern zur Fähigkeit zu unterbrechungsfreien Online-Upgrades und -Erweiterungen stellen sollten

- Welche Prozesse nutzen Sie, um die Softwarekomponenten der Lösung zu patchen oder zu upgraden?
- Können Hardware- und Software-Updates Ihrer Lösung ohne Störung der Produktionsumgebung durchgeführt werden?
- Wird für meine Lebenszyklus-Hardware ein „Forklift“-Austausch erforderlich sein?

## Garantierte Datenresilienz

Unternehmen sichern ihre Daten nicht mehr nur einmal pro Tag. Moderne Anwendungen greifen ständig auf Daten zu und verändern sie, daher sichern Unternehmen ihre Daten öfter.

Wenn während einer Sicherung das Zielgerät ausfällt, sind die meisten Legacy-Sicherungslösungen intelligent genug, die Sicherung auf einem anderen Zielgerät weiterzuführen; dieser Prozess ist jedoch nicht nahtlos, wenn Sicherungs-Software von Drittanbietern verwendet wird. Betrachten wir beispielsweise Oracle RMAN. Hier muss bei dem Versagen eines Node der Administrator die gesamte Sicherung neu starten.

Daher sind längere Zeitfenster für die Sicherung erforderlich, die sich mit der Produktionszeit überlappen können, was sich wiederum aufgrund des schließlich konsistenten Datenzustands, den die Legacy-Lösung unterstützt, auf die RPOs (Recovery Point Objectives) auswirkt. Die Auswirkungen der schließlich Konsistenz können erheblich stärker sein, wenn der Node während einem Wiederherstellungsprozess ausfällt. Während die Daten wiederhergestellt werden, schreiben einige Anwendungen/Benutzer eventuell Daten auf dasselbe Datenvolumen, und ein Node-Ausfall zu diesem Zeitpunkt kann zu inkonsistenten und beschädigten Daten führen.

Um die Unternehmens-SLAs zu erfüllen, „Datei nicht gefunden“-Fehler zu vermeiden, und garantierte Datenresilienz zu erreichen, muss Ihre nächste Lösung für Datensicherung und -wiederherstellung strikt konsistent sein. In einem strikt konsistenten Modell wird die Anwendung oder der Client nur über den Schreibvorgang informiert, wenn die Daten an mehrere Nodes verteilt wurden. Wenn der empfangende Node ausfällt, erhält die Anwendung oder der Client also keine falsche Bestätigung, dass die Daten geschützt oder geschrieben sind. Dies führt dazu, dass die Daten strikt konsistent bleiben. Bestehen Sie auf einem strikt konsistenten Modell, unabhängig davon, ob Sie direkte Sicherungen durchführen, eine Drittanbieter-Anwendung wie Oracle RMAN verwenden oder einen Wiederherstellungsprozess ausführen.

### Fragen, die Sie Anbietern zur Datenresilienz Ihrer Lösung stellen sollten

- Kann Ihre Lösung einem Ausfall von zwei Nodes und zwei Festplatten widerstehen?
- Kann Ihre Lösung mir helfen, meine SLAs einzuhalten und Datenresilienz in großem Maßstab sicherstellen?
- Verbreitet Ihre Lösung nur die Daten, oder ebenfalls die Metadaten?

## Wie sich Datenresilienz garantieren lässt

Die Datenresilienz können Sie mittels mehrerer Methoden garantieren. Die erste Methode liegt auf Hardware-Ebene. Hardware kann ausfallen oder anderweitig unbrauchbar werden. Der Cluster muss mit derartigen Ausfällen umgehen können. Viele Lösungen sind darauf ausgelegt, dem Verlust eines einzelnen Nodes oder einer Festplatte eines Nodes zu widerstehen. Durch diese Beschränkung ergibt sich jedoch ein kritisches Problem: Ist ein Node oder eine Festplatte ausgefallen, führen weitere Ausfälle zu einem Datenverlust. Für echte Hochverfügbarkeit muss die Umgebung einem Ausfall mehrerer Hardware-Elemente widerstehen können.

Vielleicht denken Sie jetzt: „Bei uns fällt nichts aus, wir brauchen das nicht.“ Beachten Sie jedoch: Ihre Umgebung benötigt regelmäßige Updates und Upgrades. Für diese Updates werden Nodes heruntergefahren, wodurch Sie verwundbar sein können, bis der Prozess abgeschlossen ist. Bei Lösungen, die nur dem Ausfall eines einzelnen Node widerstehen können, unterliegen Sie hier einem Risiko.

Eine Lösung mit hoher Resilienz kann dem Ausfall oder Verlust zwei vollständiger Nodes oder zwei Festplatten in einer Speicherdomäne widerstehen. Fällt nun ein Node oder eine Festplatte aus, gewährleistet diese zusätzliche Resilienz, dass Ihre Umgebung geschützt bleibt, während Sie Maßnahmen zur Behebung des ursprünglichen Problems ergreifen.

Diese zusätzliche Resilienz können Sie mittels zweier Methoden erzielen: Erasure Coding und Replizierung. Bei Erasure Coding werden Daten in kleinere Blöcke aufgeteilt, bevor Sie in den Speicher geschrieben werden. Ein Algorithmus stattet jeden Block mit redundanten Daten anderer Blöcke aus, bevor die Daten auf diverse Speicherorte im Cluster geschrieben werden. Diese Methode ermöglicht es, den vollständigen Datensatz zu rekonstruieren, auch wenn nicht alle individuelle Blöcke wiederhergestellt werden können. Erasure Coding bietet sowohl höhere Resilienz als typische RAID-Systeme und nutzt zudem Kapazitäten effizienter, wodurch weniger Betriebskosten als bei RAID entstehen.

Die Replizierung ist die zweite Methode zur Schaffung zusätzlicher Redundanz, besonders auf Ebene des kompletten Nodes. Wenn Sie eine vollständige Datenkopie erstellen, kann ein Cluster dem Verlust einer oder mehrerer Nodes widerstehen, je nachdem, wie viele Replikate Sie erstellen lassen.

Um die für moderne Unternehmen erforderlichen Verfügbarkeitsgrade zu erzielen, ist eine Kombination dieser zwei Ansätze ideal, um bei Hardware-Ausfällen Schutz sowohl auf Node- als auch auf Cluster-Ebene zu bieten.

## Speicherkapazität und Effizienz maximieren

Datenkopien sind genau, wonach es klingt: Kopien von Daten, die in unterschiedlichen Teilen der Umgebung existieren können. Das Problem von Mehrfachkopien hat derartige Auswirkungen auf Unternehmen, dass eine vollständig neue Lösungskategorie eingeführt wurde: Datenkopieverwaltung. Wenn Sie Ihre Datensicherungs-Umgebung betrachten, realisieren Sie unter Umständen nicht, dass mehrere Dutzend Kopien Ihrer Daten vorliegen, insbesondere dann, wenn Sie ein Datensicherungsprodukt, das nur Minimalanforderungen genügt, verwenden. Und dies umfasst noch nicht die Datenkopien, die Sie für andere Zwecke wie Datenanalysen anfertigen könnten.

*Datenkopien bezieht sich in diesem Kontext auf die tatsächlichen Datenkopien, die Sie oder andere Personen in Ihrem Unternehmen anfertigen, um ihre Arbeit zu erledigen. Dies kann Sicherungskopien, Datenkopien für Analysen, Datenkopien für Archivierung und viele weitere Kopien umfassen. Dies unterscheidet sich von dem zuvor erörterten Datenreplikationsprozess. Die Datenreplikation ist ein wichtiger Teil der Datenresilienzlösung; Datenkopien führen oft zu einer ineffizienten Nutzung von Speicherkapazität.*

Ungeachtet dessen, wie viele Datenkopien verwendet werden oder sich in Ihrer Sicherungsumgebung finden, sollte der gesamte von diesen Daten genutzte Speicherplatz nicht nennenswert anwachsen. Die automatische Dateneduplizierung wird genutzt, um die Anzahl Datenkopien erheblich zu reduzieren, sodass Sie Ihren Speicherplatz besser nutzen können.

Zahlreiche Unternehmen verlassen sich auf separate Deduplizierungsvorrichtungen, die zu einem weiteren Silo führen und nicht skalieren. Die meisten dieser Lösungen ermöglichen nur eine Deduplizierung auf Node-Ebene. Dies ist nicht effizient, da derselbe Datensatz auf einem anderen Node im selben Cluster gespeichert sein könnte.

Es gibt zahlreiche Methoden, mit Dateneduplizierung die gewünschten Ergebnisse zu erzielen, aber viele Lösungen unterstützen nur eine dieser Methoden. Um die Auswirkungen der Dateneduplizierung zu maximieren, kann die Kombination unterschiedlicher Methoden eine günstige Auswirkung sowohl auf Geschwindigkeit als auch auf Kapazität haben.

Moderne Lösungen für Datensicherung helfen IT-Administratoren durch effiziente Datenreduzierungstechniken wie globaler gleitender Deduplizierung mit variabler Länge, den Platzbedarf des Datenzentrums zu reduzieren. In diesem Modell wird die Deduplizierung mittels einer Daten-Deduplizierungstechnologie mit variabler Länge durchgeführt, die den gesamten Cluster umfasst und alle Workloads dedupliziert, darunter Daten auf physischen Systemen sowie in VMs, Datenbanken und anderen Speichern. Sie nutzt zudem effiziente Protokolle, die zu erheblichen Ersparnissen hinsichtlich des Platzbedarf zur Speicherung führen.

Beginnen wir mit einem Überblick die Deduplizierung mit fester Länge gegenüber globaler Deduplizierung mit variabler Länge. Bei der Deduplizierung werden Datenblöcke analysiert, um zu ermitteln, ob sie mit anderen Datenblöcken, die bereits im System vorliegen, identisch sind. Ist dies der Fall, wird der Block nicht erneut geschrieben. Stattdessen wird ein Pointer mit einer Referenz zum bereits vorliegenden identischen Datenblock eingefügt. Wie aus dem Namen hervorgeht, teilen Deduplizierungsalgorithmen mit fester Länge Daten in Blöcke mit festgelegter Größe auf, die alle dieselbe Länge aufweisen.

Das Hauptproblem bei der Deduplizierung mit fester Länge besteht darin, was geschieht, wenn in anderweitig identischen Daten kleinere Unterschiede auftreten. In der untenstehenden Abbildung ist klar, dass viele der Daten identisch sind; der kleine Unterschied bedeutet jedoch, dass keine der Daten in diesem Beispiel vom Deduplizierungsprozess erfasst werden. Stattdessen werden sie im vorliegenden Zustand auf die Festplatte geschrieben, und Speicherplatz wird verschwendet.

Die Deduplizierung mit variabler Länge ist eine Methode, bei der die analysierte Blockgröße nicht im Algorithmus fixiert ist.

## Ursprüngliche Aussage

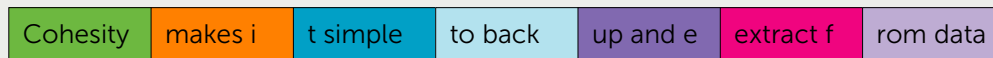
Cohesity vereinfacht die Datensicherung und -wiederherstellung

## Bearbeitete Aussage

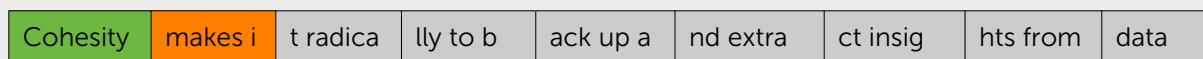
Cohesity vereinfacht die Sicherung und Extraktion von datenbasierten Erkenntnissen drastisch

## Deduplizierung mit fester Länge (8-Zeichen-Blöcke)

### Erstversion



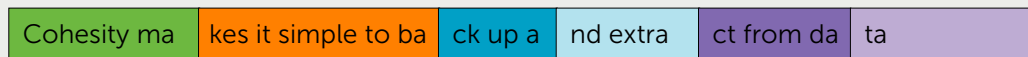
### Bearbeitet (zeigt 7 neue Datenblöcke)



gegenüber

## Deduplizierung mit variabler Länge (nach „a“)

### Erstversion



### Bearbeitet (zeigt 4 neue Datenblöcke)



\* Graue Blöcke weisen auf neue Datensätze hin

Stattdessen untersucht der Algorithmus die zugrundeliegenden Daten und nutzt eine dynamische Blockgröße auf Grundlage der analysierten Daten. So führen kleine Unterschiede im Datenstrom nicht zu einem Fehlschlag der Deduplizierung. Die tatsächlich identischen Daten werden dedupliziert, auch wenn ein Unterschied zwischen ihnen liegt. In der obenstehenden Abbildung sehen Sie die Ergebnisse einer Deduplizierung mit variabler Länge, die bei demselben Datensatz wie beim vorherigen Bild zum Einsatz kam.

Wird die Deduplizierung durch diese „gleitende“ Komponente mit variabler Länge ergänzt, bedeutet dies, dass Ihre Sicherungsdaten erheblich weniger Speicherplatz in Anspruch nehmen als bei einer Deduplizierung mit fester Länge. Noch leistungsfähiger wird dieses Konzept, wenn die Deduplizierungs-Domäne den gesamten Cluster umfasst. Bei vielen Deduplizierungs-Algorithmen ergeben sich die Speicherplatz-Einsparungen nur aus den einzelnen Nodes. Wenn sich Kopien über mehrere Nodes hinweg verteilt finden, werden diese Kopien auf Cluster-Ebene nicht reduziert. Wenn die Deduplizierung mit variabler Länge auf den gesamten Cluster erweitert wird, können sich die Speicherplatz-Ersparnisse vervielfachen.



## Fragen, die Sie Anbietern zur Speicherkapazität und Effizienz Ihrer Lösung stellen sollten

- Welche Methoden zur Datenreduzierung unterstützt Ihre Lösung?
- Was ist die durchschnittliche Reduktionsrate Ihrer Installationsbasis?
- Bietet Ihre Lösung einen konfigurierbaren Replikationsfaktor?

## Mögliche Vorteile: Erweiterbarkeit, Sicherheit und Compliance

Denken Sie bei Ihrer nächsten Lösung für Datensicherung und -wiederherstellung etwas größer. Ihre Sicherung muss keine kostspielige Versicherungspolice sein, sondern kann auch andere Geschäftsanforderungen unterstützen. Beispielsweise besteht die Möglichkeit, die gesicherten Daten und die Sicherungs-Infrastruktur zu nutzen, um eine Entwicklung/Test-Umgebung oder eine Umgebung zur Bereitstellung einer Analyse-Anwendung aufzubauen.

Ein agiler Entwickler muss so nicht mehr warten, bis ein Datenadministrator in mühsamer Kleinarbeit Daten wiederhergestellt hat, um derartige Umgebungen aufzubauen. Die Lösung kann dies unmittelbar umsetzen, die Zeit bis zur Wertschöpfung reduzieren und somit die Gesamtkosten senken. Dieselben Verbesserungen können auf Analysen angewendet werden, wodurch Sie umfassendere Einblicke in die Sicherungsdaten gewinnen können, ohne sich um den Speicherplatz zu sorgen. Wenn Sie eine neue Lösung zur Datensicherung und -wiederherstellung anstreben, erwägen Sie eine Lösung, die über die Datensicherung hinaus geht und Wertschöpfung in weitere Aspekte Ihres Betriebs einbringt.

### Sicherheit

Sicherheit umfasst mehrere Dimensionen: Zum einen die Sicherheit der gesicherten Daten; zum anderen, wie gesicherte Daten genutzt werden können, um Unternehmen bei der Verbesserung ihrer allgemeinen Sicherheit und ihrer Risikoposition zu unterstützen. Bei der Datensicherung muss das ausgewählte Produkt einen zweckmäßigen, integrierten Sicherheitsansatz nutzen, der sicherstellt, dass Ihr Unternehmen sich nicht in den Zeitungen oder im Gericht wiederfindet und seine Kunden zufriedenstellen kann.

Die Verschlüsselung ist ein Goldstandard der Sicherheit. Bei den meisten Plattformen können die Daten an mehreren Punkten verschlüsselt werden. Üblicherweise werden Daten „in Ruhe“ verschlüsselt. Das bedeutet: Daten, die gespeichert sind und nicht verwendet werden, sind vor neugierigen Blicken geschützt.

Dieser Ansatz berücksichtigt jedoch nicht, dass Daten auch genutzt werden. Schließlich wird Ihr CEO früher oder später den Finanzbericht öffnen, der im Datenzentrum gespeichert ist. Bei einigen Systemen sind Daten beim Transit im Netzwerk, nachdem sie den Speicher verlassen, nicht mehr geschützt. Ihr Ziel sollte darin bestehen, eine Umgebung zur Datensicherung und -wiederherstellung aufzubauen, die AES-256-Verschlüsselung umfasst, die stärkste übliche Verschlüsselungsmethode. Sie sollte zudem Daten sowohl in Ruhe als auch im Transit zwischen Systemen schützen.

Zudem sollten die Daten bei der Replizierung in die Cloud verschlüsselt bleiben. Es sollte für einen potenziellen Angreifer nicht möglich sein, auf einen ungesicherten Kommunikationspunkt zuzugreifen, um Ihre Daten für eine Man-in-the-Middle-Attacke zu erlangen.

Und so wichtig es ist, Daten vor Angreifern zu schützen, müssen sie natürlich für bestimmte Personen zugänglich bleiben. Sicherzustellen, dass die richtigen Personen die richtigen Zugriffsrechte auf die richtigen Daten haben, ist genau so wichtig wie der Schutz der Daten vor unbefugten Personen. Es könnte sogar noch wichtiger sein!

Heute stellen rollenbasierte Zugriffskontrollen (RBAC) und Multi-Faktor-Authentifizierung, die sich in bestehende Identitätsdienste wie Active Directory integrieren lassen, führende Methoden dar, diese Ziele zu erreichen. Ihr nächstes Produkt für die Datensicherung und -wiederherstellung muss RBAC bieten und es Ihnen ermöglichen, über unterschiedliche Parameter Zugriff auf Untermengen Ihrer Sicherungsdaten zu gewähren.

Zu guter Letzt muss bei jeder Erörterung von Datensicherung und -wiederherstellung natürlich die wachsende Bedrohung durch Cyberattacken erwähnt werden, einschließlich Ransomware und Datenpannen. Hochentwickelte Malwares wie Locky und Crypto haben es nun auf Ihre Backup-Daten abgesehen. Mit Fähigkeiten wie Unveränderbarkeit und WORM sollte Ihre nächste moderne Datensicherung diese Cyberbedrohungen aufhalten, bevor Ihre Daten zum nächsten Ziel werden. Und im Ernstfall sollte Ihre Datensicherungslösung eine flexible und schnelle Wiederherstellung in großem Maßstab ermöglichen.

Eine weitere Dimension der Sicherheit kann in der Nutzung gesicherter Daten bestehen, um Sichtbarkeit zu erzielen und potenzielle Bedrohungen zu ermitteln, wie Ransomware-Angriffe auf die primäre Umgebung, oder um Schwachstellen in der IT-Infrastruktur zu erkennen, die daraufhin proaktiv behoben werden können.

## Compliance

Sicherheit geht oft mit Compliance einher. Heute wird die Compliance bei Produkten für Datensicherung und -wiederherstellung immer wichtiger, insbesondere, wenn wir uns in einer immer stärker regulierten Welt in die Cloud begeben.

Heute müssen sich Datensicherungs-Administratoren über Themen wie Datenhoheit und die Datenschutz-Grundverordnung (DSGVO) der EU Gedanken machen. Die Datenhoheit ist eine regulatorische Anforderung für einige Datentypen; bestimmte Daten dürfen die jeweiligen Landesgrenzen nicht überschreiten. In einer Cloud-orientierten Welt ist es oft schwierig, zu ermitteln, wo sich bestimmte Daten physisch befinden. Die DSGVO ist ein Rahmen an Datenschutzerfordernungen mit dem Ziel, Bürgern die Kontrolle über personenbezogene Daten wiederzugeben. Die DSGVO ist zudem mit harschen Strafmaßnahmen für Unternehmen, die diesen Rahmen nicht befolgen, ausgestattet.

Ein allgemeineres Problem, auch in Zusammenhang mit der DSGVO, ist die Speicherung personenbezogener Daten in jeder Umgebung. Die Speicherung unnötiger oder unzureichend gesicherter personenbezogener Daten ist mittlerweile ein führender Grund für Compliance-Verstöße und Geldbußen. Jede Lösung für Datensicherung und -wiederherstellung sollte die Umgebung automatisch nach personenbezogenen Daten durchsuchen und Administratoren benachrichtigen können, wenn derartige Daten gefunden werden. Es kann legitim sein, wenn personenbezogene Daten in einem System vorliegen. Administratoren müssen jedoch klar verstehen, wo diese sich befinden, damit entsprechende Maßnahmen zur Risikominderung ergriffen werden können. Wenn Sie nicht wissen, wo die Daten sind, können Sie diese auch nicht schützen.

## Fragen, die Sie Anbietern zur Erweiterbarkeit, Sicherheit und Compliance Ihrer Lösung stellen sollten

- Wie schützt Ihre Lösung meine gesicherten Daten? (Verschlüsselung, RBAC, Multi-Faktor-Authentifizierung, Unveränderbarkeit, Erkennung von Ransomware-Attacken usw.)
- Kann ich meine gesicherten Daten verwenden, um Sicherheits- und Compliance-Vorschriften zu erfüllen, wie z. B. das Auffinden von personenbezogenen Daten?
- Welche Fähigkeiten neben Datensicherung und -wiederherstellung bietet Ihre Lösung?
- Erlaubt Ihre Lösung es mir, virtuelle Maschinen direkt innerhalb der Sicherungs-Infrastruktur auszuführen, um sicherzustellen, dass bei einer Wiederherstellung keine Schwachstellen in die Produktionsumgebung eingeführt werden?

## Wie eine moderne Datensicherung und -wiederherstellung aussieht

Auf Ihrem Weg zur Implementierung einer modernen Lösung für Datensicherung und -wiederherstellung werden Sie schnell erkennen, dass sich das Lösungsumfeld in den letzten Jahren drastisch verändert hat.

Sie müssen Ihre Datensicherungs-Umgebung nicht mehr als Reihe von Silos behandeln. Nun können Sie eine umfassende Plattform nutzen und einfach über eine einzelne Konsole verwalten. Sie müssen vor Ransomware-Attacken keine Angst mehr haben. Sie haben Mittel und Wege zur Verteidigung. Sie müssen sich keine Sorgen mehr machen, dass Sie eines Tages die Kapazitäten Ihrer Lösung überschreiten und mit einem Forklift-Upgrade das gesamte System disruptiv austauschen müssen. Moderne Lösungen sind skalierbar und vereinfachen so Erweiterungen, Upgrades und das Austauschen von Nodes erheblich.

Aber das ist nur der Anfang. Ein modernes Produkt für Datensicherung und -wiederherstellung bietet Funktionen, die bei Legacy-Ansätzen entweder unmöglich oder zu kostspielig wären. Native Cloud-Funktionen, unmittelbare Massen-Wiederherstellung von VMs und ein umfassendes API für erweiterte Workflows sollten Teil Ihrer nächsten Lösung sein.

Weitere Informationen über das führende Unternehmen im Bereich moderne Datensicherung und -wiederherstellung finden Sie bei Cohesity unter [www.cohesity.com/solution/backup-and-recovery/](http://www.cohesity.com/solution/backup-and-recovery/)